Topics in the theory of p-adic heights on elliptic curves



Francesca Bianchi

Balliol College

University of Oxford

A thesis submitted for the degree of

Doctor of Philosophy

Trinity 2019

Acknowledgements

I am thankful to my supervisors Jennifer Balakrishnan and Alan Lauder for their guidance. I am extremely grateful to Jennifer for introducing me to this area of mathematics, for suggesting many of the questions that are addressed in this thesis and for being so supportive throughout, even from the far away Boston. I thank Alan for his supervision mostly in the early stages of my DPhil, for providing insights into some of his work, but also for kindly reading through the whole of this thesis at the end.

I have benefitted greatly from group meetings with Minhyong Kim and my fellow students Jamie Beacom, Noam Kantor and Alex Saad. My deepest thanks to Minhyong also for insightful conversations and generous suggestions. I am indebted to Andrew Wiles for his time and invaluable ideas on a project in my second year and to Thanasis Bouganis for long fruitful conversations about p-adic L-functions and for constant encouragement since I was an undergraduate student. I also thank Jan Vonk for useful discussions.

Thank you to the people I collaborated with: Jennifer Balakrishnan, Amnon Besser, Victoria Cantoral-Farfán, Mirela Çiperiani, Anastassia Etropolski and Steffen Müller.

I would like to thank my examiners Victor Flynn and Chris Wuthrich for numerous suggestions and helpful comments. For reading parts of this thesis and providing useful feedback and suggestions (directly or via Jennifer Balakrishnan) I am also grateful to: Jamie Beacom, Josha Box, Kiran Kedlaya, Barry Mazur and Chris Wuthrich. I would like to thank Noam Elkies and William Stein for forwarding to Jennifer on my behalf an email correspondence about the family of elliptic curves which is studied in Appendix 3.A.

My thanks are also due to my college advisers Frances Kirwan and Vicky Neale for their support, encouragement and advice.

Finally, thanks to Jamie Beacom, Sofia Lindqvist and Ollie McGrath for making the work time in the office very enjoyable.

During my DPhil I have been funded by the Engineering and Physical Sciences Research Council (EPSRC) and by Balliol College through a Balliol Dervorguilla scholarship.

Abstract

This thesis deals with several theoretical and computational problems in the theory of p-adic heights on elliptic curves.

In Chapter 3 we provide a new algorithm for the computation of the Mazur–Tate p-adic height in a family of elliptic curves over the rationals. As an application, we study the conjectural non-degeneracy properties of the pairing induced by the height, as well as orders of vanishing and arithmetic interpretations of some of the coefficients of the regulator series.

In Chapter 4 we use the decomposition of the p-adic height as a sum of local contributions to explore a number of problems related to the quadratic Chabauty method for determining integral points on hyperbolic curves. For instance, we remove the assumption of semistability in the description of the quadratic Chabauty sets $\mathcal{X}(\mathbb{Z}_p)_2$ containing the integral points $\mathcal{X}(\mathbb{Z})$ of an elliptic curve of rank at most 1. Motivated by a conjecture of Kim, we then investigate theoretically and computationally the set-theoretic difference $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$.

In Chapter 5 we describe an implementation of the Chabauty–Coleman method for genus 3 hyperelliptic curves over $\mathbb{Q}$ whose Jacobians have rank 1. This is used to compute the rational points on approximately $17,000$ curves and to provide evidence for a conjecture of Stoll.

In Chapter 6 we extend the explicit quadratic Chabauty techniques to compute integral points on elliptic curves and rational points on genus 2 bielliptic curves to general number fields.

Finally, in Chapter 7 we prove that the first two coefficients in the series expansion around $s = 1$ of the p-adic L-function of an elliptic curve over the rationals are related by a formula involving the conductor of the curve.

The introductory Chapter 1 outlines the common themes of the thesis; Chapter 2 introduces some preliminary notions.

Contents

1 Introduction **1**

2 Preliminaries on *p*-adic heights on elliptic curves **11**

2.1 Introduction: from real to p-adic heights 11

2.2 The cyclotomic p-adic height 13

2.2.1 The local Néron functions away from p 14

2.2.2 The local Néron functions above p 16

2.2.2.1 The Mazur–Tate local heights above p 18

2.2.3 The global p-adic height 20

2.3 The p-adic height in this thesis 21

2.3.1 Conjectural non-degeneracy 21

2.3.2 Connections with the Chabauty–Kim method 22

3 Computation of *p*-adic heights in families of elliptic curves **24**

3.1 Introduction 24

3.1.1 Generic ranks and specialisations 28

3.2 The algorithm 29

3.2.1 The denominator 29

3.2.2 The p-adic sigma-function 32

3.2.3 The weight 2 Eisenstein series 33

3.2.3.1 Kedlaya's algorithm and the computation of $\mathbf{E}_2$ in [96] 33

3.2.3.2 A modified version of Lauder's deformation method . 40

3.2.4 The p-adic height 52

3.3 Examples and applications 57

3.3.1 Height computations 57

3.3.2 Applications to non-degeneracy 59

3.3.3 An example of a family of families 62

Appendices 68

3.A One family from §3.3.3 . . . 68
3.B Heights on points defined over extensions of degree 4 . . . 70

4 Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture 72
4.1 Introduction . . . 72
4.2 Description of $\mathcal{X}(\mathbb{Z}_p)_2$ . . . 76
4.2.1 Auxiliary results on local heights . . . 76
4.2.2 Proof of Theorems 4.1.2 and 4.1.3 . . . 79
4.3 Obstructions to $\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}_p)_2$ in rank 0 . . . 84
4.3.1 Automorphisms . . . 85
4.3.2 Non-cyclotomic p-adic heights . . . 89
4.3.3 Proof of Theorem 4.1.4 . . . 96
4.4 Algorithm and computations in rank 0 . . . 97
4.4.1 The algorithm . . . 97
4.4.2 Examples for Section 4.3 . . . 98
4.4.3 Large-scale data . . . 101
4.4.4 Variation of the prime . . . 103
4.4.5 Further observations and analogies with the Strong Chabauty Conjecture . . . 106
4.5 The rank 1 case . . . 107
4.5.1 Algebraic non-rational points in $\mathcal{X}(\mathbb{Z}_p)_2'$ in rank 1 . . . 107
4.5.2 Computations in rank 1 . . . 110
4.6 Rational points on bielliptic curves . . . 112
4.6.1 Explicit formulae for the sets W^i . . . 117
Appendices . . . 120
4.A Using a sieve to compute $\mathcal{X}(\mathbb{Z})$ in rank 1 . . . 120

5 Chabauty–Coleman experiments for genus 3 hyperelliptic curves 125
5.1 Introduction . . . 125
5.2 The Chabauty–Coleman method and Coleman integration . . . 127
5.2.1 Chabauty–Coleman method . . . 127
5.2.2 Computing Coleman integrals . . . 129
5.2.2.1 Coleman integral within a residue disk . . . 130
5.2.2.2 Coleman integral between different residue disks . . . 131
5.3 The algorithm . . . 131
5.3.1 Upper bounds in residue disks . . . 132
5.3.2 Roots of p-adic power series . . . 134

5.3.3 Outline of the algorithm . . . 137
5.3.4 Generalisations of the algorithm . . . 141
5.3.4.1 What if we do not know $P_0 \in C(\mathbb{Q})$ such that $[P_0 - \infty] \notin J(\mathbb{Q})_{\text{tors}}$? . . . 141
5.3.4.2 Even degree model . . . 141
5.3.4.3 Other ranks and genera . . . 142
5.4 Curve analysis . . . 142
5.4.1 Examples . . . 143
5.4.2 Variation of the prime and the Strong Chabauty Conjecture . 147

6 Quadratic Chabauty for (bi)elliptic curves over number fields 149
6.1 Introduction . . . 149
6.1.1 Notation . . . 153
6.2 Idele class characters and p-adic heights . . . 153
6.3 Chabauty over number fields . . . 157
6.4 Quadratic Chabauty for integral points on elliptic curves over number fields . . . 160
6.5 Quadratic Chabauty for rational points on bielliptic curves over number fields . . . 164
6.6 Algorithms and examples for integral points . . . 168
6.6.1 Elliptic curves over real quadratic fields . . . 169
6.6.2 Elliptic curves over imaginary quadratic fields . . . 172
6.7 Examples for rational points . . . 173
6.7.1 Rank 4 over imaginary quadratic fields . . . 173
6.7.2 Rank 3 over real quadratic fields . . . 175
Appendices . . . 180
6.A Roots of multivariate systems of p-adic equations . . . 180

7 Consequences of the functional equation of the p-adic L-function of an elliptic curve 185
7.1 Introduction . . . 185
7.2 Notation and statement of the functional equation . . . 186
7.3 Relation between the leading and sub-leading coefficients of the p-adic L-function of an elliptic curve . . . 189
7.4 Results for $\mathcal{L}_p(E, \alpha, \psi, T)$ . . . 192
7.5 Generalisations to the base change of an elliptic curve . . . 193

Appendices 195
7.A The interpolation property 195
7.B The functional equation 200
7.C Statement of p-adic BSD 201

Bibliography **203**

Chapter 1

Introduction

The underlying theme of this thesis is the central role of p-adic methods in modern number theory and arithmetic geometry. This is to be interpreted broadly. Firstly, we are concerned with methods that give rise to algorithms to compute solutions to Diophantine equations and, in particular, with explicit versions of the Chabauty–Coleman–Kim programme. Secondly, we are interested in the p-adic reformulation of classical results and conjectures in the arithmetic of elliptic curves. The unifying ingredient is to be found in the theory of p-adic heights.

We give here a short introduction to the field, with the aim of tying together the various chapters that compose this thesis and to give a rough outline. For precise formulations of the results the reader is invited to consult the introductions at the beginning of each chapter.

p-adic methods to compute integral or rational points

A Diophantine equation is a polynomial equation that we want to solve in integers or rationals. It owes its name to Diophantus of Alexandria, who is commonly believed to have lived in the third century AD [115]. Although the question of solving a Diophantine equation is arithmetic, the nature of the solution is determined by the geometry of the curve that the polynomial defines in either an affine or a projective space.

In particular, suppose that C is a smooth, projective, absolutely irreducible curve over the field of rational numbers $\mathbb{Q}$. When viewed as a curve over the complex numbers, the points of C are endowed with a natural topology coming from the complex topology on projective space. This makes C into a compact, connected Riemann surface of genus g for some $g \geq 0$.

The structure of the set $C(\mathbb{Q})$ of rational points on C is determined by the invariant g. If $g = 0$, then either $C(\mathbb{Q})$ is empty or is infinite and parametrised by a line. For example, as was already known to Diophantus (cf. [115]), we can generate infinitely many $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ on the unit circle

$$x^2 + y^2 = 1 \tag{1.1}$$

by substituting $t \in \mathbb{Q} \cup \{\infty\}$ in the formula $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$; conversely, every rational solution to (1.1) arises in this way.

When $g = 1$ and if there exists at least one point $O \in C(\mathbb{Q})$, then one can define on $C(\mathbb{Q})$ a binary operation which gives $C(\mathbb{Q})$ the structure of an abelian group with identity element O. In this case, we say that $C/\mathbb{Q}$ is an elliptic curve. On the one hand, we have a lot of information about the rational points on an elliptic curve, as Mordell [103] showed that $C(\mathbb{Q})$ is finitely generated as an abelian group, i.e. there exists a finite group T and a non-negative integer r, called the rank of $C(\mathbb{Q})$, such that

$$C(\mathbb{Q}) \cong T \times \mathbb{Z}^r.$$

On the other hand, the rank is in many respects still a mysterious arithmetic property of C. In fact, there is at present no algorithm that is guaranteed to succeed in the computation of r (although in practice r can often be bounded sharply from below and above simultaneously [54, Ch. 3]), nor is it known which integer values r can attain. We certainly do know that it can be positive, in which case $C(\mathbb{Q})$ is an infinite group. Nevertheless, if we fix an affine equation for $X = C \setminus \{O\}$ with integral coefficients, then Siegel proved in 1929 [121] that the set of integral points $X(\mathbb{Z})$ is finite.

Finally, all curves C of genus $g \geq 2$ have a remarkable property: the set $C(\mathbb{Q})$ is finite, as proved by Faltings in 1983 [58, 59] and previously conjectured by Mordell in [103]. Perhaps counterintuitively, though, finiteness does not in any way imply that determining $C(\mathbb{Q})$ is in practice an easy problem, as the set $C(\mathbb{Q})$ lacks structure. In fact, Faltings's proof is not constructive and there is no known algorithm which is guaranteed to succeed in computing $C(\mathbb{Q})$.

It is natural to try to approach the problem of determining $C(\mathbb{Q})$ for a curve of genus $g \geq 0$ using p-adic techniques. For instance, if we can show that $C(\mathbb{R})$ or $C(\mathbb{Q}_p)$, for some prime p, is empty then we will deduce that $C(\mathbb{Q})$ is also empty. This works extremely well in genus 0, where the converse also holds: if $C(\mathbb{Q}) = \emptyset$, then either $C(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$ for at least one p. However, there are examples of curves with $g \geq 1$ which have points everywhere locally, i.e. $C(\mathbb{R}) \neq \emptyset$ and $C(\mathbb{Q}_p) \neq \emptyset$

for all p, but satisfy $C(\mathbb{Q}) = \emptyset$. This is known as the failure of the Hasse principle. In fact, there is no known algorithm which is guaranteed to decide if $C(\mathbb{Q}) \neq \emptyset$ if $g \geq 1$.

We do not explore here the techniques that are generally used to decide on the existence of rational points (see for instance [38]) and we assume from now on that $C(\mathbb{Q})$ contains at least one point.

Suppose for the moment that $g \geq 2$ and fix an odd prime p of good reduction for C. The basic philosophy of the methods of Chabauty–Coleman–Kim is somewhat to turn the quantitative nature of the Hasse principle into something more qualitative: is it possible to realise $C(\mathbb{Q})$ as a subset of the zero set of at least one explicitly computable locally analytic function $f\colon C(\mathbb{Q}_p) \to \mathbb{Q}_p$? When $g = 1$, the same question applies if we replace $C(\mathbb{Q})$ (resp. $C(\mathbb{Q}_p)$) by $X(\mathbb{Z})$ (resp. $X(\mathbb{Z}_p)$).

In Chapter 5, we explain in detail how one constructs such f using the structure of the Jacobian of C in the classical Chabauty–Coleman method and what assumptions are needed. It is not in the scope of this thesis to present the theory of Kim's non-abelian programme in its full generality. However, we explore explicit descriptions in some cases (cf. Chapter 4). In particular, the functions that we consider and that do not factor through the Jacobian can all be understood in terms of the theory of local p-adic heights on elliptic curves. See also Chapter 2 for the definition and properties of local p-adic heights and their connection with Kim's unipotent Albanese maps.

The next question that naturally arises is the extent to which these methods are effective. Generically, the zero set of a function f as above will contain some points in $C(\mathbb{Q}_p) \setminus C(\mathbb{Q})$ (resp. $X(\mathbb{Z}_p) \setminus X(\mathbb{Z})$). If that is the case, it may not be possible to determine $C(\mathbb{Q})$ (resp. $X(\mathbb{Z})$) without auxiliary information. In this thesis we often consider settings where we have two functions f_1, f_2 at our disposal. One might then expect that the points in the intersection $\mathcal{K}$ of the zero loci of f_1 and f_2 should have some sort of structure. For instance, if all the points in $\mathcal{K}$ are p-adic localisations of algebraic points that appear for geometric reasons, it should be possible to recognise $C(\mathbb{Q})$ (resp. $X(\mathbb{Z})$) inside $\mathcal{K}$. More specifically, in the case of classical Chabauty, the structure of $\mathcal{K}$ is predicted by a conjecture of Stoll [133]; in the case of non-abelian Chabauty, Kim conjectured that by picking sufficiently many functions f one should always be able to exactly define $C(\mathbb{Q})$ inside $C(\mathbb{Q}_p)$ (resp. $X(\mathbb{Z})$ inside $X(\mathbb{Z}_p)$).

The modest contribution of the results in this thesis to this story can be summarised as follows. In [15], the description of the first non-abelian level of the Chabauty–Kim method (a.k.a. quadratic Chabauty) was made explicit for integral points on semistable elliptic curves of rank 0. Concretely, this produces a finite set

$X(\mathbb{Z}_p)_2 \subset X(\mathbb{Z}_p)$, containing $X(\mathbb{Z})$, of the form

$$X(\mathbb{Z}_p)_2 = \bigcup_{w \in W} \{z \in X(\mathbb{Z}_p) : f_1(z) = 0, f_2(z) + w = 0\} \tag{1.2}$$

for some computable finite $W \subset \mathbb{Q}_p$ and some locally analytic functions f_1 and f_2 defined in terms of single and double Coleman integrals. Then $X(\mathbb{Z}_p)_2$ was computed for 256 curves: for each X, this recovered exactly the set $X(\mathbb{Z})$, hence providing evidence for Kim's conjecture. We extend in Chapter 4 the description of $X(\mathbb{Z}_p)_2$ to elliptic curves with arbitrary reduction and use this to further investigate the conjecture. For example, we can prove that there exist infinitely many elliptic curves of rank 0 for which $X(\mathbb{Z}_p)_2 \supsetneq X(\mathbb{Z})$ for infinitely many primes p and that there exists at least one curve for which $X(\mathbb{Z}_p)_2 \supsetneq X(\mathbb{Z})$ for all primes p of good reduction, underlining the necessity to produce more functions with Kim's machinery in order to hope to precisely characterise $X(\mathbb{Z})$ inside $X(\mathbb{Z}_p)$. We attempt to give partial answers then to questions such as: what kind of points can arise in $X(\mathbb{Z}_p)_2 \setminus X(\mathbb{Z})$? This is supported by large-scale computations. Similar questions are addressed in rank 1, building upon [80, 15], and some algorithmic remarks on Balakrishnan–Dogra's explicit quadratic Chabauty for the rational points of certain genus 2 bielliptic curves [16] also follow from our study of elliptic curves. As an example of this, we provide a new solution to a problem from the *Arithmetica* of Diophantus which was first solved by Wetherell in his thesis [145].

The interest in our investigation on points in $X(\mathbb{Z}_p)_2 \setminus X(\mathbb{Z})$ for elliptic curves of rank 0 (and 1) lies in the connections with the effectiveness of Kim's programme, rather than in its producing algorithms to compute integral points. Indeed, determining the integral points of an elliptic curve of rank 0 is trivial; in rank 1, efficient techniques using linear forms in elliptic logarithms (see e.g. [130, 112, 136]) are generally applicable, as the computation of a generator for the free part of $C(\mathbb{Q})$ is usually feasible. On the other hand, in Chapter 5 we also make algorithmic the Chabauty–Coleman method for rational points on genus 3 hyperelliptic curves whose Jacobians have rank 1: this can be used both to address the now non-trivial task of computing the rational points on these curves and to provide evidence for Stoll's conjecture (as well as Kim's). In particular, thanks to the extra structure imposed by the vanishing of two functions simultaneously, we succeed in computing $C(\mathbb{Q})$ for approximately $17,000$ genus 3 hyperelliptic curves. This is joint work with Jennifer Balakrishnan, Victoria Cantoral-Farfán, Mirela Çiperiani and Anastassia Etropolski and is essentially the article [11].

The problem of finding rational or integral points on curves naturally generalises to number fields K. The Chabauty–Coleman method, when applicable, then produces a finite subset of $C(K_\mathfrak{p})$ containing $\psi_\mathfrak{p}(C(K))$, for every good enough prime $\mathfrak{p}$ of K and for $\psi_\mathfrak{p}\colon C(K) \hookrightarrow C(K_\mathfrak{p})$ being the embedding induced by the completion map $K \hookrightarrow K_\mathfrak{p}$. Inspired by a talk by Wetherell, Siksek [122] proposed to weaken the assumptions that the Chabauty–Coleman method requires, by considering instead functions $\prod_{\mathfrak{p}|p} C(K_\mathfrak{p}) \to \mathbb{Q}_p$ vanishing on $\prod_{\mathfrak{p}|p} \psi_\mathfrak{p}(C(K))$ for a fixed rational prime p. In Chapter 6, we use a similar idea to extend the explicit quadratic Chabauty techniques for elliptic and bielliptic curves discussed above to number fields. As an example, we consider again the curve arising from the work of Diophantus and determine its set of $\mathbb{Q}(\sqrt{34})$-rational points. This is joint work with Jennifer Balakrishnan, Amnon Besser and Steffen Müller and is a less general version of [8].

p-adic reformulation of classical results

Let us go back to the case of $C/\mathbb{Q}$ being an elliptic curve, so that $C(\mathbb{Q})$ is a finitely generated abelian group of rank r, for some non-negative integer r. Understanding r is tightly linked with the celebrated conjecture of Birch and Swinnerton-Dyer (BSD). In particular, in its weak form this predicts that the L-series that we can attach to $C/\mathbb{Q}$, denoted $L(C, s)$, (or more precisely its analytic continuation to the whole complex plane) should have a zero at $s = 1$ of order equal to r.

As was observed by Manin [91, Theorem 11.1], this conjecture would lead to an algorithm which is guaranteed to compute r, since approximations of the expansion of $L(C, s)$ around $s = 1$ would give upper bounds for r, whereas lower bounds could be obtained by searching for independent points in $C(\mathbb{Q})$. Eventually, the upper and lower bound would have to converge to the same value, that is, to r. Unfortunately, very few cases of BSD are known. By work of Kolyvagin [82], Gross–Zagier [65] and others, if the order of vanishing of $L(C, s)$ at $s = 1$ is $r_{\mathrm{an}} \leq 1$, then $r = r_{\mathrm{an}}$ and the Tate–Shafarevich group $Ш_{C/\mathbb{Q}}$ of $C/\mathbb{Q}$ is finite; conversely, under some technical assumptions, Skinner–Urban [129], Skinner [128] and Zhang [149] proved that $r_{\mathrm{an}} = r$, if $r \leq 1$ and $Ш_{C/\mathbb{Q}}$ is finite. For larger rank we can at present only rely on computational evidence (see [53]).

Let now p be an odd rational prime. A p-adic L-function is a p-adic analogue of a complex L-function, which we can express as a power series with p-adic coefficients. In general, one can construct such an object in two very different ways. On the one hand, by analytic interpolation of special values of the complex L-function twisted by the characters of some Galois group Γ (say $\Gamma \cong \mathbb{Z}_p$) and normalised by a period;

on the other hand, by considering a suitable algebraic object (e.g. the dual of a p-Selmer group of an elliptic curve with ordinary reduction at p), which can be given the structure of a finitely-generated torsion $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$-module and thus comes with a characteristic series.

The analytic and algebraic constructions are related by a "Main Conjecture" of Iwasawa theory, which predicts equality of the two functions up to multiplication by a unit p-adic series. In particular, an analytic and an algebraic p-adic L-function ($L_p^{\mathrm{an}}(T)$ resp. $L_p^{\mathrm{alg}}(T)$) can be defined for $C/\mathbb{Q}$, for a prime p of good ordinary reduction. We consider $L_p^{\mathrm{an}}(T)$ in Chapter 7, whereas $L_p^{\mathrm{alg}}(T)$ was mentioned here only for completeness of exposition, but we never concretely work with it; see [64] for a definition. Mazur–Tate–Teitelbaum [100] conjectured a p-adic analogue of BSD: the series $L_p^{\mathrm{an}}(T)$ should vanish at $T = 0$ to order equal to r.

This perfectly illustrates how it is often easier to prove results in the p-adic world than it is in the complex one: for example, thanks to work of Kato on the Main Conjecture [72] and of Schneider [117] and Perrin-Riou [110] on properties of $L_p^{\mathrm{alg}}(T)$, we know unconditionally that $r \leq \mathrm{ord}_{T=0} L_p^{\mathrm{an}}(T)$. See [132] for how this can often be used to compute r in practice.

There is at least one instance, however, where a problem that is trivial in the real or complex setting becomes extremely hard p-adically, as we now explain. Recall that the complex BSD conjecture also predicts an exact formula for the leading coefficient of $L(C, s)$. This involves arithmetic invariants of $C/\mathbb{Q}$, such as the product of its Tamagawa numbers, the size of its Tate–Shafarevich group and of its torsion subgroup, the Néron period and the real regulator. The normalisation by a period happens a priori in the definition of $L_p^{\mathrm{an}}(T)$; of the remaining quantities appearing in the BSD formula, the only one which is not necessarily a rational number is the regulator Reg, which is defined as the discriminant of the real canonical height on the free part of $C(\mathbb{Q})$. It is elementary to show that Reg is positive, since the real height extends to a positive-definite quadratic form on $C(\mathbb{Q}) \otimes \mathbb{R}$ (see for example [127, VIII, Proposition 9.6]).

In order for a p-adic analogue of this strong version of BSD to be formulated, a $\mathbb{Q}_p$-valued height function h_p on $C(\mathbb{Q})$ was constructed in several equivalent ways [116, 98, 46]. Mazur–Tate–Teitelbaum then conjectured that the leading coefficient of $L_p^{\mathrm{an}}(T)$ should be

$$\epsilon_p \cdot \frac{\prod_q c_q \cdot \#Ш_{C/\mathbb{Q}}}{\#C(\mathbb{Q})_{\mathrm{tors}}^2} \cdot \mathrm{Reg}_p \tag{1.3}$$

(see also Conjecture 7.C.1). Here, ignoring the p-adic multiplier ϵ_p, the integer c_q is the Tamagawa number at the prime q, $Ш_{C/\mathbb{Q}}$ is, as above, the Tate–Shafarevich group and Reg_p is the p-adic regulator, i.e. it is the discriminant of the pairing induced by h_p on the free part of $C(\mathbb{Q})$. If $\mathrm{Reg}_p = 0$, then this conjecture of Mazur–Tate–Teitelbaum fails trivially. Non-vanishing of Reg_p for any curve $C/\mathbb{Q}$ was conjectured by Schneider in 1982 [116] and is at present very much an open problem. One says that h_p is non-degenerate if Schneider's conjecture holds, or, more generally, if independence of any set of points of $C(\mathbb{Q})$ translates into non-vanishing of the discriminant of the pairing restricted to the subgroup generated by this set.

This is the motivation for Chapter 3: we develop an algorithm for the computation of the p-adic height in one-parameter families of elliptic curves. By doing so, we are able to consider non-degeneracy questions for infinitely many curves at once and to provide some evidence for Schneider's conjecture. We also investigate properties of coefficients and orders of vanishing of the resulting height/regulator series, and analyse in detail many examples. The algorithm relies on an adaptation of Lauder's deformation method [87, 88].

In Chapter 7 we see that the p-adic L-function $L_p^{\mathrm{an}}(T)$ satisfies a functional equation which relates its values at T with its values at $(1+T)^{-1} - 1$. Following an idea of Wuthrich [148] for the complex L-function, this allows us to derive a relation between its leading and sub-leading coefficient, which involves the conductor of $C/\mathbb{Q}$. Assuming the p-adic BSD formula (1.3), we can then deduce an exact formula also for the sub-leading coefficient.

To close the circle, we emphasise that the functions arising from the instance of the Chabauty–Kim method that we consider have an interpretation given by the properties of the p-adic height h_p. The function h_p is a function on $C(\mathbb{Q})$ and does not extend to a function on $C(\mathbb{Q}_p)$; nevertheless, it secretly comes from a function on adelic points $\prod_q C(\mathbb{Q}_q)$, where the product runs over all the non-archimedean primes of $\mathbb{Q}$. Explicitly, the global p-adic height h_p admits a decomposition as a sum of local heights $\lambda_q \colon C(\mathbb{Q}_q) \to \mathbb{Q}_p$:

$$h_p = \sum_q \lambda_q;$$

furthermore, there is a clear dichotomy between the local height at p and those away from p. At a prime $q \neq p$ the function λ_q is, on a subgroup of finite index, the composition of a p-adic functional with a naive height. One can deduce that there

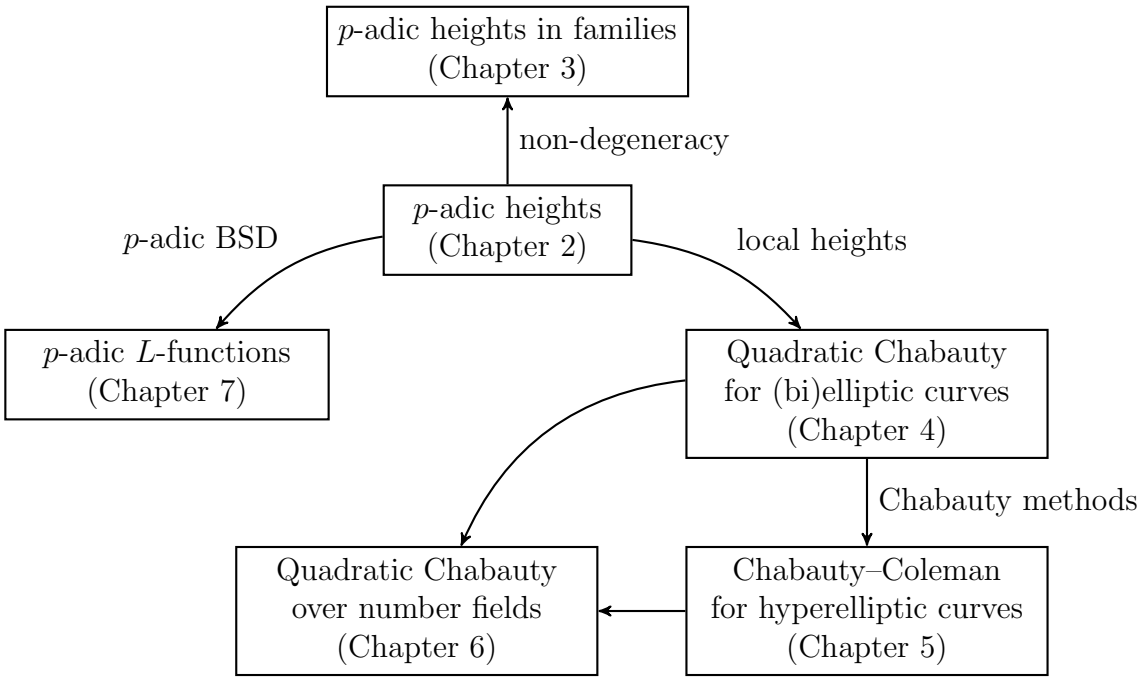
exists an explicitly computable finite subset W of $\mathbb{Q}_p$ such that

$$\left(\sum_{q \neq p} \lambda_q\right)(X(\mathbb{Z})) \subset W.$$

The local height at p restricts to a locally analytic function $f_2 \colon X(\mathbb{Z}_p) \to \mathbb{Q}_p$ and can be defined either in terms of a double Coleman integral or in terms of a p-adic analogue of the Weierstrass sigma function. This is exactly how one obtains the second equation defining $X(\mathbb{Z}_p)_2$ in (1.2), since h_p vanishes on $C(\mathbb{Q})$ (and hence on $X(\mathbb{Z})$) if the rank is zero.

Outline

The following diagram summarises the connections between the various topics in this thesis. Chapter 2 collects some preliminary results that are used throughout. Each of the other chapters could be read independently.



Notation

We list here some recurrent notation in the thesis.

We denote by $\mathbb{N}$ the set of natural numbers *not* including 0 and by $\mathbb{Z}$ the ring of rational integers. We use the standard notation $\mathbb{Q}$ and $\mathbb{R}$ for the field of rational and real numbers. Given a prime p, we denote by $\mathbb{Q}_p$ the field of p-adic numbers, by $\mathbb{Z}_p$ the ring of p-adic integers and by $\mathbb{F}_p$ the residue field of $\mathbb{Z}_p$. The field $\mathbb{C}_p$ is the field of p-adic complex numbers, that is, the completion of the algebraic closure of $\mathbb{Q}_p$. We also write ord_p for the p-adic valuation on $\mathbb{Q}_p$ and $|\cdot|_p$ for the p-adic absolute value, extended to $\mathbb{C}_p$.

We write $\log_{\mathbb{R}}$ for the real logarithm, log for the p-adic logarithm (as defined in Section 2.2) and exp for the p-adic exponential map, defined for $z \in \mathbb{C}_p$ with $|z|_p < p^{-1/(p-1)}$ by $\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$.

Given a field F, we write $\overline{F}$ for a fixed algebraic closure of F and $F(t)$ for the field of rational functions in the variable t over F. For a ring R, we write $R[t_1, \ldots, t_n]$ and $R[[t_1, \ldots, t_n]]$ for the ring of polynomials and formal power series in the variables $t_1, \ldots, t_n$ with coefficients in R; we write $R((t))$ for the ring of formal Laurent series in t. Furthermore, we denote by $R^\times$ the group of units in R. If F is a number field, we denote by $\mathcal{O}_F$ its ring of integers. If v is a place of F, we write F_v for the completion of F at v and, if v is non-archimedean, we also denote by $\mathcal{O}_v$ the ring of integers of F_v and by $\mathbb{F}_v$ the residue field. If $R = \mathcal{O}_F$ for a number field F or $R = \mathbb{Z}_p \subset F := \mathbb{Q}_p$, the symbol $\overline{R}$ is used to indicate the integral closure of R in $\overline{F}$.

For a finite field extension L/F, we denote by $N_{L/F} \colon L \to F$ and $\mathrm{tr}_{L/F} \colon L \to F$ the field norm and trace, respectively.

If v is a non-archimedean place of a number field F and C is a curve over F_v of genus ≥ 1 with good reduction at v, we let $\overline{C}$ be the special fibre of a minimal proper regular model for C over $\mathcal{O}_v$. Then there exists a natural reduction map $C(F_v) \to \overline{C}(\mathbb{F}_v)$ and we define a *residue disk* to be a fibre of this map.

For a set S, we denote by $\#S$ its cardinality.

Given an elliptic curve E over any field F, we let $j(E)$ be its j-invariant and we let $\mathrm{Aut}(E/F)$ be the group of automorphisms of E/F *which fix the identity* of $E(F)$; moreover, the notation f_m is often used for the m-th division polynomial of E (see Definition 2.2.1). If C is a curve of genus ≥ 2, we denote by $\mathrm{Aut}(C)$ its automorphism group (here no ambiguity exists).

Chapter 2

Preliminaries on p-adic heights on elliptic curves

2.1 Introduction: from real to p-adic heights

Let L be a field. By a *height* on a curve (or a variety) X over a number field F we mean a function $h\colon X(F) \to L$ that, roughly, turns geometric relations of points into arithmetic relations. For example, if X is an abelian variety, then h should have some compatibility with the group law. Let E be an elliptic curve over the number field F, with distinguished point O, and fix a Weierstrass equation

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

for $E \setminus \{O\}$, with coefficients $a_1, \ldots, a_4, a_6$ in the ring of integers of F. Given P in the set $E(F)$ of F-rational points of E and $P \neq O$, write $x(P)$ for the x-coordinate of P with respect to this model.

For a place v of F, let F_v be the completion of F at v, let n_v be the degree of the extension $F_v/\mathbb{Q}_v$ and let $|\cdot|_v$ be the absolute value on F_v, normalised as follows. If v is an archimedean place and $x \in \mathbb{Q}$, we have $|x|_v = \max\{x, -x\}$. If v is a finite prime of norm q_v and $x \in F_v^\times$, then

$$|x|_v = q_v^{-\mathrm{ord}_v(x)/n_v},$$

where the valuation ord_v is such that $\mathrm{ord}_v(F_v^\times) = \mathbb{Z}$. The *naive height* of $P \in E(F)$ is defined as

$$h_{\mathrm{naive}}(P) = \begin{cases} 0 & \text{if } P = O, \\ \frac{1}{[F\colon \mathbb{Q}]} \sum_v n_v \log_{\mathbb{R}}(\max\{|x(P)|_v, 1\}) & \text{otherwise,} \end{cases}$$

where $\log_{\mathbb{R}}$ is the real logarithm and the sum is over all (finite and infinite) places v of F. The *canonical real height* on E is the unique function $\hat{h}\colon E(F) \to \mathbb{R}$ satisfying:

(i) $\hat{h}(mP) = m^2\hat{h}(P)$ for all $m \in \mathbb{Z}$ and $P \in E(F)$ (quadraticity);

(ii) $\hat{h}(P+Q)+\hat{h}(P-Q) = 2\hat{h}(P)+2\hat{h}(Q)$ for all $P, Q \in E(F)$ (parallelogram law);

(iii) $\{|\hat{h}(P) - h_{\text{naive}}(P)| : P \in E(F)\}$ is a bounded set

(see for example [127, VIII, Theorem 9.3]). The existence of $\hat{h}$ was proved by Néron and Tate. While Tate showed that $\hat{h}$ can be constructed as a limit of naive heights, Néron [106] proved that the restriction of $\hat{h}$ to $E(F) \setminus \{O\}$ admits a decomposition as a sum of the form

$$\frac{1}{[F\colon \mathbb{Q}]} \sum_v n_v \widehat{\lambda}_v$$

for quasi-quadratic local functions $\widehat{\lambda}_v \colon E(F_v) \setminus \{O\} \to \mathbb{R}$, one for each place v of F (see [125, VI]). This is a description that turned out to be suited for the definition of $\mathbb{Q}_p$-valued functions on $E(F)$ satisfying (i) and (ii), starting from the end of the 1970s.

An alternative approach to the definition of $\mathbb{Q}_p$-valued height functions was followed by Perrin-Riou [110] and Schneider [116], in light of Bloch's description of the canonical real height given in [33]. These definitions were shown to be equivalent to the ones coming from Néron's local heights [98] and we will thus not explore them here.

If v is a finite place, on a subgroup of finite index of $E(F_v)$, the local function $\widehat{\lambda}_v$ coincides with the v-adic term in the naive height. For $v \nmid p$ the p-adic analogue of $\widehat{\lambda}_v$ is obtained by replacing the real-valued $\log_{\mathbb{R}} \colon \mathbb{Q}_{>0} \to \mathbb{R}$ with a p-adic functional.

On the other hand, local heights at infinite places are defined as the logarithm of potentially transcendental quantities. In particular, let Λ be a lattice such that $\phi\colon \mathbb{C}/\Lambda \to E$ parametrises the points of $E(\mathbb{C})$ with respect to the embedding v of F into $\mathbb{C}$ and the discriminant[1] of Λ equals the discriminant of (2.1). Let σ and ζ be the Weierstrass sigma and zeta function with respect to Λ (see [85, Ch. 18, §1] for definitions and properties). The function ζ is quasi-periodic; one defines its quasi-period by $\eta(\omega) = \zeta(z+\omega)-\zeta(\omega)$ for all $\omega \in \Lambda$ and $z \in \mathbb{C}$ and extends it to a function $\mathbb{C} \to \mathbb{C}$ by insisting that it should be $\mathbb{R}$-linear. Then, if $\phi(z) = P$, one has

$$\widehat{\lambda}_v(P) = -2\log_{\mathbb{R}} |\sigma(z)e^{-\frac{1}{2}z\eta(z)}|,$$

where $|\cdot|$ is the complex absolute value.

[1] in the sense of [127, VI, Proposition 3.6 (a)]

The task of defining p-adic analogues of the Weierstrass sigma function was taken up by Bernardi [22], Néron [107] and Mazur–Tate [99]. The article [111] gives an overview of the three constructions, the first two of which are equivalent. The reason why several definitions appear in the literature is the following. Suppose that $v \mid p$ and that E has good reduction at v. Let $E_{1,v}$ denote the formal group of E at v. Let σ_v be an odd function on some subset V of $E_{1,v}(\overline{F}_v)$, such that in terms of the parameter $t = -x/y$ for $E_{1,v}$ we have $\sigma_v \in t(1 + F_v[[t]])$, and such that

$$\frac{\sigma_v(P+Q)\sigma_v(P-Q)}{\sigma_v(P)^2\sigma_v(Q)^2} = x(Q) - x(P) \quad \text{for all } P, Q \in V \setminus \{O\}.$$

Then σ_v is determined only up to multiplication by $\exp(\beta L_v(t)^2)$, where $L_v(t) \in F_v[[t]]$ is the formal logarithm and $\beta \in F_v$ (see [111, Lemme, p. 5] and §2.2.2).

The function σ_v constructed by Bernardi using the Taylor expansion of the complex sigma function and by Néron as a v-adic limit of rational functions on E, is convergent only for $\mathrm{ord}_v(t) > \mathrm{ord}_v(p)/(p-1)$. On the other hand, Mazur–Tate's construction requires the reduction to be ordinary at v, but produces a function which converges on all points of $E_{1,v}(\overline{F_v})$.

Thanks to work of Coleman–Gross [46] and Balakrishnan–Besser [7], the local height defined with a v-adic sigma function can be interpreted as a double Coleman integral. In particular, Coleman–Gross gave a construction of a p-adic height on divisors with disjoint support on a curve of genus greater than zero. Balakrishnan–Besser extended the definition of the Coleman–Gross height to divisors with non-disjoint support and showed that, in the elliptic curve case, the already-known equality with the global height of Mazur–Tate ([44, 26]) is local in nature.

2.2 The cyclotomic p-adic height

Let p be an odd prime and extend the usual p-adic logarithm $\log\colon 1 + p\mathbb{Z}_p \to \mathbb{Q}_p$ to $\mathbb{Q}_p^\times$ via $\log(p) = 0$. Let E be an elliptic curve over the number field F, as in (2.1), and assume that p is unramified in F, that E has good reduction at all the primes v of F above p and that (2.1) is minimal at all such v. In this section we explain in more detail the construction of the *cyclotomic*[2] *p-adic height*

$$h_p\colon E(F) \to \mathbb{Q}_p$$

[2]If the space of continuous idele class characters $\mathbb{A}_F^\times/F^\times \to \mathbb{Q}_p$ has dimension larger than 1, we will see in §4.3.2 and Section 6.2 that one can define other types of p-adic heights.

as a sum of local heights that was sketched in Section 2.1. We define $h_p(O) = 0$ and for $P \in E(F) \setminus \{O\}$ we let[3]

$$h_p(P) = \frac{1}{[F\colon \mathbb{Q}]} \sum_v n_v \lambda_v(P), \tag{2.2}$$

where the sum is over all finite primes v of F and

$$\lambda_v\colon E(F_v) \setminus \{O\} \to \mathbb{Q}_p$$

is a *p-adic local Néron function at v*.

By summing over primes of a finite extension L of F, the height h_p can be evaluated also on points of $E(L)$. If K/L is a further finite extension, w is a prime of K above the prime v of L and $P \in E(L_v)$, then

$$\lambda_v(P) = \lambda_w(P).$$

In order to define the properties of λ_v, it is convenient to recall the definition of division polynomials (cf. [127, III, Exercise 3.7]).

Definition 2.2.1. Let m be a positive integer and let E be an elliptic curve over a field K. The *m-th division polynomial* f_m for E is a function on the points of E, which can be written as a polynomial over $\mathbb{Z}[a_1, \ldots, a_6]$ in the variable x only, if m is odd, and in x, y if m is even, such that:

- The divisor of f_m is $\sum_{R \in E[m]} (R) - m^2(O)$;
- As a polynomial in x, $f_m^2(x) = m^2 x^{m^2-1} + O(x^{m^2-2})$;
- For $m, n \in \mathbb{N}$ and $P \in E(\overline{K})$, $f_{nm}(P) = f_n^{m^2}(P) f_m(nP)$.

2.2.1 The local Néron functions away from p

As already mentioned in Section 2.1, the p-adic local Néron function at a non-archimedean prime $v \nmid p$ is equal to the real local Néron function at v with the p-adic logarithm in place of the real one. Thus, any reference that we provide for $\widehat{\lambda}_v$ can be applied also to our setting. For instance, analogously to the real case, for $v \nmid p$, the following properties determine a unique function $\lambda_v\colon E(F_v) \setminus \{O\} \to \mathbb{Q}_p$:

[3]Here we choose to normalise the p-adic height in such a way that it becomes independent of the choice of the field F containing the coordinates of P; note that this is not the case in many other references, such as [96].

(i) λ_v is continuous on $E(F_v) \setminus \{O\}$ and bounded on the complement of any neighbourhood of O with respect to the v-adic topology.

(ii) $\lim_{P \to O}(\lambda_v(P) - \log |x(P)|_v)$ exists.

(iii) λ_v satisfies the *quasi-parallelogram law*: for all $P, Q \in E(F_v)$ such that $P, Q, P \pm Q \neq O$, we have

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) - 2\log|x(P) - x(Q)|_v. \qquad (2.3)$$

Indeed, for uniqueness: the difference of two such functions extends to a continuous map $\rho\colon E(F_v) \to \mathbb{Q}_p$, which induces a continuous homomorphism

$$E(F_v) \to \mathbb{Q}_p, \qquad P \mapsto \rho(P+Q) - \rho(P) - \rho(Q),$$

for every fixed $Q \in E(F_v)$. This must be trivial for topological reasons and then the same argument implies that ρ is trivial too. For existence, it suffices to show that the p-adic analogue of $\widehat{\lambda}_v$ obtained as described above satisfies (i)-(iii) (see [125, VI, Exercise 6.3]).

We also have

(iv) For all $P \in E(F_v)$ and all $m \geq 1$ with $mP \neq O$,

$$\lambda_v(mP) = m^2\lambda_v(P) - 2\log|f_m(P)|_v.$$

We say that λ_v is *quasi-quadratic*.

Moreover, uniqueness implies the following key fact:

(v) If ψ is an automorphism of E defined over F_v, then, for all $P \in E(F_v)$, $\lambda_v(\psi(P)) = \lambda_v(P)$.

See also [22] for a more general transformation property under isogeny.

We may assume that (2.1) is minimal at v, since, if this is not the case, we can switch to a minimal equation at v and use [55, Lemma 4]:

$$\lambda_v = \lambda_v^{\min} + \frac{1}{6}\log|\Delta/\Delta^{\min}|_v, \qquad (2.4)$$

where Δ denotes the discriminant and the superscript min has the obvious meaning.

Denote by $\overline{E}_{ns}(\mathbb{F}_v)$ the group of non-singular points of the reduction of E modulo v and let

$$E_0(F_v) = \{P \in E(F_v) : \overline{P} \in \overline{E}_{ns}(\mathbb{F}_v)\}.$$

If E has good reduction at v, we may also write $\overline{E}(\mathbb{F}_v)$ for $\overline{E}_{ns}(\mathbb{F}_v)$.

Lemma 2.2.2. *Suppose $v \nmid p$. Then*

(i) If $P \in E_0(F_v) \setminus \{O\}$, $\lambda_v(P) = \log(\max\{1, |x(P)|_v\})$.

(ii) If $P \notin E_0(F_v)$, $\lambda_v(P)$ depends exclusively on the image of P in $E(F_v)/E_0(F_v)$.

Proof. See [124] or [55, Proposition 5]. □

In Chapter 4, we will see explicitly what values λ_v attains on $E(F_v) \setminus E_0(F_v)$.

2.2.2 The local Néron functions above p

Let now v be a prime of F above p. Consider the Laurent expansions of x, y and

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

in terms of the parameter $t = -\frac{x}{y}$ for the formal group:

$$\begin{aligned} x(t) &= t^{-2} - a_1t^{-1} - a_2 + \cdots \\ y(t) &= -t^{-3} + a_1t^{-2} + a_2t^{-1} + \cdots \\ \omega(t) &= (1 + a_1t + (a_1^2 + a_2)t^2 + \cdots)dt =: s(t)dt \end{aligned} \tag{2.5}$$

(see for instance [127, IV]).

Proposition 2.2.3. *Let $\beta \in F_v$. Then there exists a unique odd*[4] *function $\sigma_v^{(\beta)}(t) = t + \cdots \in F_v[[t]]$ such that*

$$x(t) + \beta = -\frac{d}{\omega}\left(\frac{1}{\sigma_v^{(\beta)}}\frac{d\sigma_v^{(\beta)}}{\omega}\right). \tag{2.6}$$

Proof. Expanding (2.6) in terms of the parameter t, denoting by $'$ the derivative d/dt and writing $\sigma_v := \sigma_v^{(\beta)}$, we obtain

$$x(t) + \beta = -\frac{1}{s(t)}\left(\frac{\sigma_v(t)'}{\sigma_v(t)s(t)}\right)'.$$

Since $s(t)(x(t) + \beta) - t^{-2} \in F_v[[t]]$ by (2.5), the formal integral

$$\int s(t)(x(t) + \beta)dt = -t^{-1} + O(t)$$

is an element of $F_v((t))$ and we have

$$\frac{\sigma_v(t)'}{\sigma_v(t)} = -s(t)\left(\int s(t)(x(t) + \beta)dt + C_1\right),$$

[4] Odd as a function on a subset of the formal group and not as a function of t.

for some constant of integration C_1. As in [67], let $\theta = t^{-1}\sigma_v$. Then

$$\frac{\theta'}{\theta} = -s(t)\left(\int s(t)(x(t)+\beta)dt + C_1\right) - \frac{1}{t} \in F_v[[t]],$$

so

$$\theta = \exp(C_2)\cdot\exp\left(\int\left(-s(t)\left(\int s(t)(x(t)+\beta)dt + C_1\right) - \frac{1}{t}\right)dt\right) \in F_v[[t]] \quad (2.7)$$

for some constant of integration C_2. We now show that the conditions that σ_v is odd and $\sigma_v = t + \dots$ determine C_1 and C_2 uniquely. The parameter $i(t)$ for $-(x,y)$ is

$$i(t) = -t - a_1t^2 + \cdots,$$

so, if $\sigma_v = t + c_2t^2 + O(t^3)$, then $\sigma_v(t) = -\sigma_v(i(t))$ yields $c_2 = a_1/2$ and hence $\frac{\theta'}{\theta}\big|_{t=0} = \frac{a_1}{2}$. On the other hand,

$$\left.\frac{\theta'}{\theta}\right|_{t=0} = a_1 - C_1,$$

giving $C_1 = \frac{a_1}{2}$. Since the coefficient of t in σ_v is 1, then $C_2 = 0$. This shows uniqueness. For existence, we only need to show that the function that we have constructed is indeed odd. By (2.7) and the just established independence of C_1 and C_2 from β, we have

$$\frac{\sigma_v^{(\beta)}(t)}{\sigma_v^{(0)}(t)} = \exp\left(-\frac{\beta}{2}\left(\int s(t)dt\right)^2\right) = \exp\left(-\frac{\beta}{2}L_v(t)^2\right), \quad (2.8)$$

where L_v is the (odd) formal group logarithm. It follows that it suffices to show that $\sigma_v^{(\beta)}$ is odd for one choice of β. It is convenient to do so for

$$\beta = \frac{a_1^2 + 4a_2}{12},$$

which gives the v-adic sigma function of Bernardi [22]. In fact, in this case, the differential equation satisfied by $\sigma_v^{(\beta)}(t)$ is the same, after changing variables to the parameter $z = L_v(t)$ for the additive group, as the one satisfied by the complex Weierstrass sigma function $\sigma(z)$:

$$\wp(z) = -\frac{d}{dz}\left(\frac{1}{\sigma(z)}\frac{d\sigma(z)}{dz}\right),$$

where $\wp(z)$ is the Weierstrass $\wp$-function and, since $\sigma(z)$ is odd, then so is $\sigma_v^{(\beta)}$. □

Lemma 2.2.4. *Let $\sigma_v^{(\beta)}$ be the function of Proposition 2.2.3 and let V be a neighbourhood of O on which $\sigma_v^{(\beta)}$ converges. Then*

(i) For all $P, Q \in V \setminus \{O\}$,

$$\frac{\sigma_v^{(\beta)}(P+Q)\sigma_v^{(\beta)}(P-Q)}{\sigma_v^{(\beta)}(P)^2\sigma_v^{(\beta)}(Q)^2} = x(Q) - x(P).$$

(ii) For all integers $m \geq 1$ and for all points $Q \in V$,

$$\sigma_v^{(\beta)}(mQ) = \sigma_v^{(\beta)}(Q)^{m^2} f_m(Q).$$

Proof. As in the proof of Proposition 2.2.3, equation (2.8) implies that it suffices to show the lemma for the v-adic sigma function of Bernardi. The theory of complex elliptic functions shows that the Weierstrass sigma function has the required transformation properties (see for example [85, Ch. 18, §1, Theorem 2]) and, therefore, so does $\sigma_v^{(\beta)}$ in its domain of convergence. □

Fix a $\beta \in F_v$ such that $\sigma_v^{(\beta)}(t)$ has non-zero radius of convergence and let V be a neighbourhood of O on which $\sigma_v^{(\beta)}$ converges. Then the local height at v with respect to this choice of β is defined on $V \setminus \{O\}$ by

$$\lambda_v(P) = -\frac{2}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(\sigma_v^{(\beta)}(P))),$$

where $\log_v \colon F_v^\times \to F_v$ extends log (note that λ_v is well-defined since the only zero of $\sigma_v^{(\beta)}$ in V is O by (2.7)). Using Lemma 2.2.4 (ii), we may extend the definition of λ_v to points outside of V. This gives a function $\lambda_v \colon E(F_v) \setminus \{O\} \to \mathbb{Q}_p$ satisfying

(i) λ_v is locally analytic on $E(F_v) \setminus \{O\}$.

(ii) For all $P \in E(F_v)$ and all $m \geq 1$ with $mP \neq O$,

$$\lambda_v(mP) = m^2\lambda_v(P) - \frac{2}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(f_m(P))).$$

(iii) For all $P, Q \in E(F_v)$ such that $P, Q, P \pm Q \neq O$,

$$\lambda_v(P+Q) + \lambda_v(P-Q) = 2\lambda_v(P) + 2\lambda_v(Q) - \frac{2}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(x(P) - x(Q))).$$

2.2.2.1 The Mazur–Tate local heights above p

As before, let v be a prime of F above p. Consider the reduction $\overline{E}$ of E over the residue field $\mathbb{F}_v$ of $\mathcal{O}_v$ of q_v elements. Then $\overline{E}$ is equipped with the Frobenius morphisms $\phi \colon (x, y) \mapsto (x^{q_v}, y^{q_v})$. The trace of the induced endomorphism ϕ_ℓ of the ℓ-adic Tate module of $\overline{E}$ ($\ell \neq p$) satisfies $a_v := \operatorname{tr}(\phi_\ell) = 1 + q_v - \#\overline{E}(\mathbb{F}_v)$ [127, V,

Theorem 2.3.1]. We we say that E has *supersingular reduction* at v if $a_v \equiv 0 \bmod p$ and E has *ordinary reduction* otherwise.

In spite of the lack of uniqueness, if the reduction of E at v is ordinary, there is a choice of β which is "canonical". We assume here that $p \geq 5$.

A *Katz p-adic modular form* f over $\mathbb{Z}_p$ of level 1, weight k and growth condition 1 is a rule which assigns to a pair $(E/R, \omega)$, where R is a $\mathbb{Z}_p$-algebra in which p is nilpotent or a p-adically complete $\mathbb{Z}_p$-algebra, E/R is an ordinary elliptic curve and ω is a non-vanishing differential on E, an element $f(E/R, \omega) \in R$ which

- depends only on the isomorphism class of $(E/R, \omega)$;
- commutes with base change;
- satisfies $f(E/R, \lambda\omega) = \lambda^{-k} f(E/R, \omega)$ for all $\lambda \in R^\times$.

By evaluating f on the Tate curve, one obtains the q-expansion for f (cf. [73, §2.2]).

Definition 2.2.5. ([73], [74]) The *weight* 2 *Katz p-adic Eisenstein series* is a p-adic modular form of weight 2 and level 1 with q-expansion

$$\mathbf{E}_2(q) = 1 - 24 \sum_{n=1}^{\infty} (\sum_{d|n} d) q^n.$$

Let K be a finite unramified extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_{p^n}$ and ring of integers $\mathcal{O}_K$. Let E/K be an elliptic curve with good ordinary reduction and choose an equation for E over $\mathcal{O}_K$ of the form $E\colon y^2 = 4x^3 - g_2 x - g_3$. The space $H^1_{\mathrm{dR}}(E/K)$ is spanned by $\omega = \frac{dx}{y}$ and $\eta = \frac{x dx}{y}$ and is equipped with a canonical action of Frobenius, which lifts the p^n-th power map in characteristic p. By ordinarity, there is exactly one eigenspace of $H^1_{\mathrm{dR}}(E/K)$ for Frobenius whose eigenvalue is in $\mathcal{O}_K^\times$. Let $u = \gamma\omega + \delta\eta$ be any vector in this eigenspace. Then

$$\mathbf{E}_2(E, \omega) = -12 \frac{\gamma}{\delta}.$$

Recall that, by Proposition 2.2.3, the v-adic sigma function attached to $\beta \in F_v$ is a power series with coefficients in F_v. Mazur and Tate showed the following

Theorem 2.2.6 (Mazur–Tate [99]). *If E has ordinary reduction at v, there is a unique choice of $\beta \in F_v$ for which $\sigma_v^{(\beta)}(t) \in \mathcal{O}_v[[t]]$. Furthermore,*

$$\beta = \frac{a_1^2 + 4a_2}{12} - \frac{1}{12}\mathbf{E}_2(E, \omega).$$

2.2.3 The global p-adic height

Let $h := h_F$ be the class number of F. For each $v \mid p$ choose $\beta_v \in F_v$ such that the domain of convergence V_v of $\sigma_v^{(\beta)}$ is larger than $\{O\}$. Let $P \in E(F)$ be a point of infinite order and let $m \in \mathbb{N}$ such that $mP \in V_v$ for all $v \mid p$ and mP reduces to a non-singular point at all primes of bad reduction for E, with respect to our chosen Weierstrass equation.

Then, by §§2.2.1, 2.2.2, (2.2) and [146, §3], we have

$$h_p(P) = -\frac{2}{(mh)^2[F\colon \mathbb{Q}]} \log\left(\prod_{v|p} N_{F_v/\mathbb{Q}_p}\left(\frac{\sigma_v^{(\beta_v)}(mhP)}{d(mhP)}\right)\right), \tag{2.9}$$

where $mhP = \left(\frac{a(mhP)}{d(mhP)^2}, \frac{b(mhP)}{d(mhP)^3}\right)$ with $a(mhP), b(mhP), d(mhP) \in \mathcal{O}_F$ such that the ideal generated by $d(mhP)$ is coprime to both the ideal generated by $a(mhP)$ and the one generated by $b(mhP)$. If P is torsion, then $h_p(P) = 0$. From the quasi-parallelogram and quasi-quadratic laws satisfied by the local heights, we deduce:

Properties 2.2.7. The p-adic height $h_p\colon E(F) \to \mathbb{Q}_p$ satisfies the following properties.

(i) For every integer m and every point $P \in E(F)$, $h_p(mP) = m^2 h_p(P)$. We say h_p is a *quadratic* function.

(ii) For every $P, Q \in E(F)$,

$$h_p(P+Q) + h_p(P-Q) = 2h_p(P) + 2h_p(Q),$$

i.e. h_p satisfies the *parallelogram law*.

Suppose that E has good ordinary reduction at all primes above p. We may then choose, at each such prime, the local height defined with the v-adic sigma function of Mazur–Tate (§2.2.2.1). We call the resulting height the *(cyclotomic) p-adic height of Mazur–Tate*.

Remark 2.2.8. The normalisation that we choose for h_p differs from the ones of [146, 96, 67]. When $F = \mathbb{Q}$, ours agrees with the one of `SageMath` [131] and differs in sign from the one of `Magma` [36].

2.3 The p-adic height in this thesis

2.3.1 Conjectural non-degeneracy

Properties 2.2.7 imply that the p-adic height on an elliptic curve E/F induces a symmetric bilinear pairing

$$\begin{aligned}\langle\cdot,\cdot\rangle\colon E(F)\times E(F)&\to\mathbb{Q}_p,\\ \langle P,Q\rangle&=\frac{1}{2}(h_p(P+Q)-h_p(P)-h_p(Q)).\end{aligned}$$

The *p-adic regulator* is the discriminant of this pairing on the free part of the Mordell–Weil group $E(F)$, i.e. given generators $P_1,\dots,P_r$ of $E(F)/E(F)_{\mathrm{tors}}$, we define the regulator

$$\mathrm{Reg}_p=\begin{cases}\det(\langle P_i,P_j\rangle)_{1\le i,j\le r} & \text{if } r\ge 1,\\ 1 & \text{otherwise}\end{cases}\tag{2.10}$$

and we say that the pairing is *non-degenerate* if Reg_p is non-zero.

Assume now that E has good ordinary reduction at all primes of F above p and that $\langle\cdot,\cdot\rangle$ is the p-adic height pairing of Mazur–Tate.

Conjecture 2.3.1 (Schneider [116]). *The Mazur–Tate p-adic height pairing is non-degenerate on $E(F)/E(F)_{\mathrm{tors}}$.*

The p-adic Birch and Swinnerton-Dyer conjecture, due to Mazur–Tate–Teitelbaum [100], only makes sense conditionally on Conjecture 2.3.1. See Appendix 7.C for a precise formulation.

More generally, given points $Q_1,\dots,Q_n\in E(F)$, define the regulator with respect to $Q_1,\dots,Q_n$ as

$$\mathrm{Reg}_p(Q_1,\dots,Q_n)=\det(\langle Q_i,Q_j\rangle)_{1\le i,j\le n}.\tag{2.11}$$

In analogy with the real height, the following stronger version of Conjecture 2.3.1 is expected to hold.

Conjecture 2.3.2. *If $Q_1,\dots,Q_n$ are linearly independent non-torsion points, then*

$$\mathrm{Reg}_p(Q_1,\dots,Q_n)\neq 0.$$

Theorem 2.3.3 (Bertrand [24]). *Conjecture 2.3.2 holds if E is an elliptic curve over $\mathbb{Q}$ with complex multiplication and $n=1$.*

Remark 2.3.4. With the assumptions of Theorem 2.3.3, the value at (E,ω) of the weight 2 Katz p-adic Eisenstein series is independent of the good ordinary prime p and belongs to the field of complex multiplication of E by [74, Lemma 8.0.13].

In Chapter 3, we describe an algorithm to compute p-adic heights in one-parameter families of elliptic curves over $\mathbb{Q}$ and discuss applications to the study of non-degeneracy.

2.3.2 Connections with the Chabauty–Kim method

Let X be a hyperbolic curve over $\mathbb{Q}$: e.g. a compact curve of genus greater than one, or a punctured elliptic curve. The set of integral points $X(\mathbb{Z})$ (which in the case of a compact curve coincides with the set of rational points) is finite by Faltings's [58, 59] or Siegel's [121] theorem. When applicable, the methods of Chabauty–Coleman–Kim produce locally analytic functions on subsets of $X(\mathbb{Z}_p)$, for a prime p of good reduction, which annihilate $X(\mathbb{Z})$.

The functions in question are defined in terms of abelian Coleman integrals in the case of the Chabauty–Coleman method (cf. Chapter 5) and in terms of iterated Coleman integrals when we consider non-abelian quotients of the étale fundamental group of $X_{\overline{\mathbb{Q}}}$ at an integral base point b in the Chabauty–Kim programme.

In this subsection, we relate the local heights of §2.2.2 to the Chabauty–Kim method for an elliptic curve punctured at the origin, by expressing them in terms of certain double Coleman integrals. This is equivalent to showing that the local p-adic heights that we defined in terms of v-adic sigma functions coincide with the local heights of the Coleman–Gross p-adic height (see [46] and [7]). In Chapter 4 the relation with the Chabauty–Kim method will be made explicit.

The p-adic local height λ_v^{CG} of Coleman–Gross at a prime $v \mid p$ depends on a choice of subspace $N_v \subset H^1_{\mathrm{dR}}(E/F_v)$ complementary to the space of holomorphic differentials (see [46]). Let

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

and let $\eta = x\omega$.

Let ξ_v be the one-form of the second kind with a double pole at O and no others, representative of the class in N_v dual to ω with respect to the cup product (i.e. such that $[\omega] \cup [\xi_v] = 1$). By [7, Theorem 4.1], for all $P \in E(F_v) \setminus \{O\}$ one has

$$\lambda_v^{CG}(P) = \frac{1}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p} \left(2 \int_b^P \omega \xi_v \right),$$

where b is a tangential base point at O and the integral is a double Coleman integral (see [45, 25]). In particular,

$$\xi_v = \eta + \beta\omega \quad \text{for some } \beta \in F_v$$

and hence

$$\lambda_v^{CG}(P) = \frac{1}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p}(2D_2(P) + \beta \operatorname{Log}(P)^2),$$

where

$$\operatorname{Log}(P) = \int_b^P \omega \quad \text{and} \quad D_2(P) = \int_b^P \omega\eta.$$

Note that, on the formal group at v, $\operatorname{Log}(P)$ coincides with the formal group logarithm $L_v(t)$ of §2.2.2. In [7, Corollary 3.2], it is shown that if E has good ordinary reduction at v and N_v is the unit root eigenspace of Frobenius, then λ_v is related to the logarithm of the v-adic sigma function of Mazur–Tate.

In fact, it is easy to see that their proof (combined with the proof of Proposition 2.2.3) shows the following stronger result.

Proposition 2.3.5. *Let $\beta \in F_v$, let V be a neighbourhood of O on which $\sigma_v^{(\beta)}$ converges and let λ_v^{CG} be the v-adic height of Coleman–Gross with respect to this choice of β. Then, for all $P \in V \setminus \{O\}$, we have*

$$\lambda_v^{CG}(P) = -\frac{2}{n_v} \operatorname{tr}_{F_v/\mathbb{Q}_p}(\log_v(\sigma_v^{(\beta)}(P))).$$

In view of Proposition 2.3.5, we may henceforth use the Coleman–Gross local height λ_v^{CG} and the local height of §2.2.2 interchangeably and the superscript CG will be dropped.

Chapter 3

Computation of p-adic heights in families of elliptic curves

3.1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and let $p \geq 5$ be a prime of good ordinary reduction for E. As we saw in Chapter 2, the Mazur–Tate p-adic height is a quadratic $\mathbb{Q}_p$-valued function on $E(\mathbb{Q})$, which satisfies the parallelogram law and hence induces a symmetric bilinear pairing on $E(\mathbb{Q})$. The p-adic regulator Reg_p is the discriminant of this pairing, restricted to the free part of $E(\mathbb{Q})$. Mazur–Tate–Teitelbaum [100] conjectured an exact formula for the leading term of the p-adic L-function of $E/\mathbb{Q}$, which involves some arithmetic invariants of E, including Reg_p. This p-adic analogue of the Birch and Swinnerton-Dyer conjecture relies on the non-vanishing of Reg_p, which is also at present only conjectural.

In practice, we can verify if $\mathrm{Reg}_p \neq 0$ for an explicit curve E thanks to work of Wuthrich [146], Mazur–Stein–Tate [96] and Harvey [67]. The algorithm of [96] (and its improvement in [67]) uses the fact that the differential equation satisfied by the p-adic sigma function is elementary to solve if we have prior knowledge of the value at (E, ω) of the Katz p-adic Eisenstein series $\mathbf{E}_2$ of weight 2, where ω is the invariant differential for the chosen Weierstrass equation for E (cf. Proposition 2.2.3 and Theorem 2.2.6). Since the quantity $\mathbf{E}_2(E, \omega)$ encodes the direction of the unit root eigenspace of Frobenius acting on the de Rham cohomology of some model for E over $\mathbb{Z}_p$, Mazur–Stein–Tate suggest using Kedlaya's algorithm [75] to find a p-adic approximation of $\mathbf{E}_2(E, \omega)$.

Although computationally less efficient, Wuthrich's work additionally considers the problem of computing p-adic heights in one-parameter families of curves. That

is, given

$$\mathcal{E}\colon y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \qquad a_i(t) \in \mathbb{Z}[t], \tag{3.1}$$

say with $j(\mathcal{E}) \notin \mathbb{Q}$, one might wonder under which conditions on $P \in \mathcal{E}(\mathbb{Q}(t))$ and $a_i(t)$ it is possible to define a function $h_p(P)$ of t such that $h_p(P)(t_0) = h_p(P_{t_0})$ for almost all $t_0 \in \mathbb{Z}$. Here P_{t_0} is the point of intersection between P and the fibre of $\mathcal{E}$ at t_0.

In this chapter, we propose a new algorithm to compute p-adic heights and regulators in families of elliptic curves. The main theoretical input which allows us to adapt [96] and [67] to families is a modified version of Lauder's deformation method, which plays the role of Kedlaya's algorithm. The question of whether this might be possible was posed in [96, §7.2], where it was however suggested that issues of overconvergence may arise.

Lauder's algorithm [87, 88] computes the action of Frobenius on the Monsky–Washnitzer cohomology of some fibres of an elliptic surface over $\mathbb{Q}_p$. The deformation the name refers to is the deformation of the curve over $\overline{\mathbb{F}_p}$. More precisely, since Lauder defines the action of Frobenius on t by $t \mapsto t^p$, the resulting matrix specialises to the Frobenius matrix only at those $t \in \overline{\mathbb{Z}_p}$ which satisfy $t^{p^n} = t$ for some integer n. Although useful for computations of zeta functions over finite fields, this is not amenable to specialisations at integers. Thus, we instead let t be invariant under Frobenius, at the expense of restricting to families which are constant modulo p.

This is not as strong an assumption as it may seem. Indeed, given $t_0 \in \mathbb{Z}$, let $a \in \{0, \dots, p-1\}$ be such that $t_0 \equiv a \bmod p$ and let $\mathcal{E}^{(a)}$ be the family obtained from $\mathcal{E}$ by replacing t with $pt+a$, so the reduction of $\mathcal{E}^{(a)}$ modulo p is independent of t. The fibre $\mathcal{E}_{t_0}$ of $\mathcal{E}$ at t_0 is also a fibre of $\mathcal{E}^{(a)}$. Therefore, we can think of calculating p-adic heights in families as calculating p power series, each convergent in the open unit disk centred at a residue modulo p. For simplicity, we state here what this discussion leads to when the point is particularly "nice".

Theorem 3.1.1. *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}(t)$, with a Weierstrass equation of the form (3.1). Let $a \in \mathbb{Z}$ and let $p \geq 5$ be a prime of good ordinary reduction for the fibre $\mathcal{E}_a$. Let $P \in \mathcal{E}(\mathbb{Q}(t))$ be a non-torsion point with coordinates defined over $\mathbb{Z}[t]$ such that*

(a) P has non-singular reduction at all primes of $\mathbb{Z}[t]$ of height 1.

(b) For all $t_0 \in \mathbb{Z}$ and for every rational prime q, the point $P_{pt_0+a} \in \mathcal{E}_{pt_0+a}(\mathbb{Q})$ has good reduction at q.

Then there exists an algorithm which, given a fixed choice of $N \in \mathbb{N}$, outputs a truncated power series

$$f_a(t) = \sum_{i=0}^{N-1} c_i t^i + O(t^N), \qquad c_i \in \mathbb{Q}_p + O(p^N),$$

satisfying the following properties:

(i) $\mathrm{ord}_p(c_0) \geq 1 - \delta$ *and, for* $i \geq 1$, $\mathrm{ord}_p(c_i) \geq i - \mathrm{ord}_p(i) - \delta$, *where* $\delta = \begin{cases} 2 & \text{if } p \mid \#\overline{\mathcal{E}_a}(\mathbb{F}_p), \\ 0 & \text{otherwise.} \end{cases}$

(ii) For all $t_0 \in \mathbb{Z}$,

$$f_a(t_0) \equiv h_p(P_{pt_0+a}) \bmod p^{\tilde{N}}, \quad \text{where } \tilde{N} = \min_{i \geq N}\{i - \mathrm{ord}_p(i)\} - \delta.$$

Here $h_p(P_{pt_0+a})$ *is the Mazur–Tate p-adic height of* $P_{pt_0+a} \in \mathcal{E}_{pt_0+a}(\mathbb{Q})$.

By combining values of f_a for different $a \in \mathbb{Z}$, we can also recover the p-adic height of a point on a fibre defined only over a non-trivial extension of $\mathbb{Q}$ (cf. Theorem 3.2.27).

As an application of Theorem 3.1.1, we study the non-degeneracy properties of the pairing $\langle \cdot, \cdot \rangle$ induced by the p-adic height on the $\mathbb{Q}$-rational points of the fibres. Recall from §2.3.1 that, generally, one says that the p-adic height is non-degenerate for $E/\mathbb{Q}$ if $\mathrm{Reg}_p \neq 0$, but that, in analogy with the real height, we expect a stronger statement of non-degeneracy to hold: that is, $\det(\langle P_i, P_j \rangle)_{1 \leq i,j \leq n}$ should be non-zero for any linearly independent non-torsion points $P_1, \ldots, P_n \in E(\mathbb{Q})$. Hardly anything is known about these conjectures, except for Bertrand's result on the non-vanishing of the p-adic height of a point of infinite order on a curve with complex multiplication (Theorem 2.3.3).

The set of $\mathbb{Q}(t)$-rational points of $\mathcal{E}$ has the structure of a finitely generated abelian group and Silverman showed in [123] that the specialisation map $\mathcal{E}(\mathbb{Q}(t)) \to \mathcal{E}_{t_0}(\mathbb{Q})$ is injective for all but finitely many $t_0 \in \mathbb{Q}$. Therefore, we expect the regulator of a set of linearly independent points in $\mathcal{E}(\mathbb{Q}(t))$ to vanish at $t_0 \in \mathbb{Z}$ only if t_0 is in the exceptional set of Silverman's Specialisation Theorem. The theory of Newton polygons implies that the regulator of a set of (good enough) points on a family either vanishes identically or has finitely many zeros in $\mathbb{Z}$, as was already observed by Wuthrich (see [146, Theorem 3]). Throughout the chapter, we find the zeros in $\mathbb{Z}_p$ of the regulator series in some examples. Theorem 3.2.28 shows that f_a maintains some quadratic properties also when evaluated at integers in imaginary quadratic

fields, which can be used to prove algebraicity of some of the zeros. When a zero is not recognised as algebraic, observe that, since our series can only be specialised at $t \in \mathbb{Z}$ (rather than $t \in \mathbb{Q}$), by computing p-adic approximations of the roots, one could provably deduce lower bounds for the values of $t \in \mathbb{Z}$ at which degeneracy could potentially occur.

We show that:

(ND) Let $\mathcal{E}\colon y^2 = x^3 - (37t+1)^2x + 1$ and let $P = (0,1), Q = (-1,(37t+1))$ and $R = (-(37t+1),1)$, which are linearly independent and generate a subgroup of $\mathcal{E}(\mathbb{Q}(t))$ of finite index. Then for $t \equiv 1,3 \bmod 6$ the 37-adic regulator of P, Q, R can be expressed as a power series in t with no roots in $\mathbb{Z}_{37}$. See Example 3.3.4.

Consider now

$$\mathcal{E}\colon y^2 + y = (x+A)(x+B)(x+C+pt) \quad \text{for some } A, B, C \in \mathbb{Z}, \tag{3.2}$$

with the points $P = (-A, 0)$ and $Q = (-B, 0)$. We show that, for $A \neq B$ (resp. $A = B$), P and Q (resp. P) generate(s) the rank two (resp. rank one) Mordell-Weil lattice $\mathcal{E}(\mathbb{Q}(t))$. We study the zeros and leading coefficients of the regulator series of P and Q and compare the regulator series of the non-isomorphic families of the form (3.2) specialising to the same curve at $t = 0$.

The organisation of the chapter is as follows. We end this section with a summary of definitions and results on elliptic surfaces. This can be skipped and referred to if necessary. In Section 3.2, we describe in detail the steps of the algorithm and prove results from which Theorem 3.1.1 will follow. Furthermore, we derive some properties of the p-adic height series. In §3.3.1, we implement the algorithm in `Magma` [36] to compute some examples of heights, amongst which we successfully replicate the ones in [146]. In §3.3.2, we study the non-degeneracy of the p-adic height and prove (ND). In §3.3.3, we turn our attention to the families of the form (3.2). Finally, in Appendix 3.A we explicitly compute the regulator series for one of the families of §3.3.3: some of the roots found are algebraic; in Appendix 3.B we use Theorem 3.2.27 to compute the p-adic height of a point defined over an extension of $\mathbb{Q}$ of degree 4. The precision to which we present the computations in this chapter is chosen for readability; in practice, all computations could be carried out, if needed, at much larger p-adic precision.

3.1.1 Generic ranks and specialisations

We now recall a few facts about elliptic curves over function fields. An elliptic curve over $K(t)$, for some field K, is the generic fibre of an elliptic surface over K. By an *elliptic surface S over K* we mean a surface (i.e. a two-dimensional projective variety) with a morphism (*elliptic fibration*) $\pi\colon S \to \mathbb{P}^1$ such that, for all but finitely many points $t_0 \in \mathbb{P}^1(\overline{K})$, the fibre $S_{t_0} = \pi^{-1}(t_0)$ is a non-singular curve of genus 1, and there is a morphism $\sigma_0\colon \mathbb{P}^1 \to S$ such that $\pi \circ \sigma_0$ is the identity map. By abuse of notation, we also write $\mathcal{E}_{t_0}$ for S_{t_0} if $\mathcal{E}/K(t)$ is the generic fibre of S. We also refer to $\mathcal{E}/K(t)$ (or S/K) as a *family of elliptic curves*.

An elliptic surface is said to be *rational* if it is birational to $\mathbb{P}^2$. An elliptic curve over $K(t)$ is *isotrivial* if its j-invariant is constant, that is, it is independent of the parameter t.

The following theorem is a special case of [125, III, Theorem 6.1].

Theorem 3.1.2 (Mordell–Weil Theorem over function fields). *Let $\mathcal{E}$ be a non-isotrivial elliptic curve over $\overline{\mathbb{Q}}(t)$. Then $\mathcal{E}(\overline{\mathbb{Q}}(t))$ is a finitely generated abelian group.*

The Mordell–Weil group $\mathcal{E}(\overline{\mathbb{Q}}(t))$ is equipped with a height pairing which endows $\mathcal{E}(\overline{\mathbb{Q}}(t))/\mathcal{E}(\overline{\mathbb{Q}}(t))_{\mathrm{tors}}$ with the structure of a lattice (see [120]).

Theorem 3.1.3 ([108]). *Let $\mathcal{E}$ be a non-isotrivial elliptic curve over $\overline{\mathbb{Q}}(t)$ such that the corresponding elliptic surface is rational. Then the Mordell–Weil group $\mathcal{E}(\overline{\mathbb{Q}}(t))$ is one of 26 groups and its structure as an abstract group, as well as as a lattice with respect to the height pairing, is completely determined by the reducible fibres of the elliptic fibration.*

For the following theorem see also [125, III, Theorem 11.4].

Theorem 3.1.4 (Silverman Specialisation Theorem [123]). *Let K be a number field and let $\mathcal{E}$ be a non-isotrivial elliptic curve over $K(t)$. Then the specialisation map*

$$\mathcal{E}(K(t)) \to \mathcal{E}_{t_0}(K)$$

is injective for all but finitely many $t_0 \in K$.

Conjecture 3.1.5 (Nagao [105]). *Let $\mathcal{E}$ be a non-isotrivial elliptic curve over $\mathbb{Q}(t)$. Then the rank of the finitely generated abelian group $\mathcal{E}(\mathbb{Q}(t))$ is equal to*

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \left(\frac{-\log_{\mathbb{R}} p}{p} \sum_{t_0=0}^{p-1} a_p(\mathcal{E}_{t_0}) \right),$$

where the sum runs over all primes less than or equal to X and $a_p(\mathcal{E}_{t_0})$ is the trace of Frobenius at p of the fibre $\mathcal{E}_{t_0}$ if the reduction at p is good (cf. §2.2.2.1) and is zero otherwise.

Theorem 3.1.6 (Rosen–Silverman [113]). *Nagao's conjecture is true if the elliptic surface corresponding to $\mathcal{E}$ is rational.*

Suppose we are given an elliptic surface over $\mathbb{Q}$ and we pick a Weierstrass equation of the form

$$\mathcal{E}\colon y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

with $a_i(t) \in \mathbb{Z}[t]$ for the generic fibre. Then, if the fibre $\mathcal{E}_{t_0}$ has good reduction at p, we have

$$-a_p(\mathcal{E}_{t_0}) = \#\overline{\mathcal{E}_{t_0}}(\mathbb{F}_p) - p - 1 = \sum_{x=0}^{p-1} \left(\frac{x^3 + a_2(t_0)x^2 + a_4(t_0)x + a_6(t_0)}{p} \right), \qquad (3.3)$$

where the brackets indicate the Legendre symbol. In particular, if the degree of $a_i(t)$, for $i = 2, 4, 6$, is at most 2, following methods of [3] and [28], we can evaluate Nagao's formula by standard Legendre identities.

Given a family $\mathcal{E}/\mathbb{Q}(t)$, define the average root number

$$\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{E}}) = \lim_{T\to\infty} \frac{1}{2T} \sum_{|t_0|\leq T} \varepsilon(\mathcal{E}_{t_0}),$$

where $\varepsilon(\mathcal{E}_{t_0})$ is the root number of $\mathcal{E}_{t_0}$ if $\mathcal{E}_{t_0}$ is an elliptic curve and is zero otherwise.

Theorem 3.1.7 (Helfgott [69, Theorem 1.7.1]). *Conditionally on the square-free sieve conjecture and Chowla's conjecture, if there exists a place of multiplicative reduction of $\mathcal{E}$ over $\mathbb{Q}(t)$, besides the one at infinity, then $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{E}}) = 0$.*

3.2 The algorithm

3.2.1 The denominator

Let p be an odd prime different from 3 and let

$$\mathcal{E}\colon y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \qquad (3.4)$$

be a Weierstrass equation with coefficients $a_i(t) \in \mathbb{Z}[t]$, $i \in \{1, 2, 3, 4, 6\}$, and non-identically zero discriminant; let O be the point at infinity of $\mathcal{E}$. For each $t_0 \in \overline{\mathbb{Z}}_p$, we write $\mathcal{E}_{t_0}$ for the fibre of $\mathcal{E}$ at t_0.

Following [146], we write $\mathcal{E}^\circ(\mathbb{Q}(t))$ for the subgroup of $\mathcal{E}(\mathbb{Q}(t))$ consisting of those points which have non-singular reduction at all primes of $\mathbb{Z}[t]$ of height 1. Since $\mathbb{Z}[t]$ is a unique factorisation domain, a point $P \in \mathcal{E}(\mathbb{Q}(t)) \setminus \{O\}$ can be written in the form

$$P = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3} \right),$$

for some polynomials $a(P)$, $b(P)$ and $d(P) \in \mathbb{Z}[t]$ such that $d(P)$ is coprime with $a(P)$ and with $b(P)$. (So in Wuthrich's notation, $\mathcal{E}^\circ(\mathbb{Q}(t)) = \mathcal{E}^\bullet(\mathbb{Q}(t))$).

Ideally, we would like to evaluate $d(P)$ at any $t_0 \in \mathbb{Z}$ and obtain the denominator of the point P_{t_0} at which P meets the fibre $\mathcal{E}_{t_0}$, provided that $P_{t_0} \neq O_{t_0}$. This may fail, however, if some cancellation between $a(P)(t_0)$ and $d(P)(t_0)^2$ occurs. More generally, suppose that t_0 is an algebraic integer such that $\mathcal{O}_{\mathbb{Q}(t_0)}$ is a unique factorisation domain. If $P_{t_0} \neq O_{t_0}$, write

$$P_{t_0} = \left(\frac{a(P_{t_0})}{d(P_{t_0})^2}, \frac{b(P_{t_0})}{d(P_{t_0})^3} \right),$$

for some $a(P_{t_0}), b(P_{t_0}), d(P_{t_0}) \in \mathcal{O}_{\mathbb{Q}(t_0)}$, well-defined up to elements in $\mathcal{O}^\times_{\mathbb{Q}(t_0)}$, with $d(P_{t_0})$ coprime with $a(P_{t_0})$ and $b(P_{t_0})$. We want to have some control on $\gamma(P, t_0) \in \mathcal{O}_{\mathbb{Q}(t_0)}$, defined as in [146, (4.2)] by

$$d(P_{t_0}) \cdot \gamma(P, t_0) = d(P)(t_0);$$

note that, since $\gamma(P, t_0)$ is well-defined only up to multiplication by $\mathcal{O}^\times_{\mathbb{Q}(t_0)}$, an equality between $\gamma(\cdot, t_0)$ is to be interpreted as an equality up to units.

We say that P has *everywhere good reduction* if P_{t_0} has non-singular reduction at all primes of $\mathbb{Z}$, for each $t_0 \in \mathbb{Z}$. Proposition 5 in [146] asserts that if $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$ has everywhere good reduction, then, for each $t_0 \in \mathbb{Z}$,

$$\gamma(mP, t_0) = \gamma(P, t_0)^{m^2} \tag{3.5}$$

for all non-zero integers m such that $(mP)_{t_0} \neq O_{t_0}$. Thus, for any non-zero integer m and any point $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$ of everywhere good reduction satisfying $d(P) = 1$, we have $d((mP)_{t_0}) = \pm d(mP)(t_0)$ (by interpreting this as $0 = 0$, we can also include the case $mP_{t_0} = O_{t_0}$). More generally, writing $\mathcal{E}(\mathbb{Z}[t])$ for the points with denominator equal to 1, we can say the following.

Proposition 3.2.1. *Let $P \in \mathcal{E}^\circ(\mathbb{Z}[t])$. Let m be a non-zero integer such that $Q = mP$ has everywhere good reduction. Then $\gamma(nQ, t_0) = \gamma(Q, t_0)^{n^2} \in \mathbb{Z}$ is a product of powers of primes at which P_{t_0} has singular reduction.*

Proof. Let q be a prime at which P_{t_0} has non-singular reduction. Since $\mathbb{Z}_q$ is a Noetherian Krull domain with a unique non-trivial prime, namely (q), at which P has non-singular reduction, we may repeat the argument of [146, Proposition 5] with $\mathbb{Q}_q$ in place of the number field. This yields $\gamma(Q, t_0) \in \mathbb{Z}_q^\times$ for all primes q of good reduction. For completeness, we include some details. Since $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$, by [146, Corollary 2] we have

$$d(Q) = d(P)^{m^2} \cdot f_m(P),$$

where f_m is the m-th division polynomial of $\mathcal{E}/\mathbb{Q}(t)$ (cf. Definition 2.2.1); similarly, for each prime q of good reduction,

$$d(Q_{t_0}) =_{\mathbb{Z}_q^\times} d(P_{t_0})^{m^2} \cdot f_m(P_{t_0}) = d(P_{t_0})^{m^2} \cdot f_m(P)(t_0),$$

where the subscript on the equal sign indicates equality up to units in $\mathbb{Z}_q$ and f_m in the middle term is the m-th division polynomial of $\mathcal{E}_{t_0}/\mathbb{Q}$. Let $t_0 \in \mathbb{Z}$ such that Q_{t_0} is not the point at infinity. Then

$$\begin{aligned}\gamma(Q, t_0) = \frac{d(Q)(t_0)}{d(Q_{t_0})} &= \frac{d(P)(t_0)^{m^2} \cdot f_m(P)(t_0)}{d(Q_{t_0})} \\ &=_{\mathbb{Z}_q^\times} \frac{d(P)(t_0)^{m^2} \cdot f_m(P)(t_0)}{d(P_{t_0})^{m^2} \cdot f_m(P)(t_0)} = \gamma(P, t_0)^{m^2} = 1,\end{aligned}$$

as desired. □

Remark 3.2.2. Suppose $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$ is such that $Q = mP \in \mathcal{E}^\circ(\mathbb{Q}(t))$ has everywhere good reduction, but $P \notin \mathcal{E}^\circ(\mathbb{Z}[t])$ (so Proposition 3.2.1 does not apply). As in the proof of [146, Proposition 3] we note that, if a prime q divides $\gamma(Q, t_0)$ then $q \mid a(Q)(t_0)$ and $q \mid d(Q)(t_0)$, thus q divides the resultant of $a(Q)$ and $d(Q)$.

Remark 3.2.3. It may happen that even if P is a point of everywhere good reduction, we have $P \notin \mathcal{E}^\circ(\mathbb{Q}(t))$, as the following example shows. Consider the family

$$\mathcal{E}\colon y^2 = x^3 - (t+1)^2 x + 1$$

and the point $P = (-(t+1), 1)$ lying on it. The point P_{t_0} is singular at the prime 2 and non-singular at all other primes, for all $t_0 \in \mathbb{Z}$. For each $t_0 \in \mathbb{Z}$, $3P_{t_0}$ has good reduction at 2 (using Tate's algorithm [125, IV, §9], we see that at 2 each fibre has Kodaira symbol IV and Tamagawa number 3 and that the given model for $\mathcal{E}$ specialises to a minimal model at 2). Therefore, $Q = 3P$ is a point of everywhere

good reduction. However, we claim that $Q \notin \mathcal{E}^\circ(\mathbb{Q}(t))$. Indeed, first of all note that P itself is not in $\mathcal{E}^\circ(\mathbb{Q}(t))$ as

$$3x^2 - (t+1)^2|_{-(t+1)} \equiv 0 \in \mathbb{F}_2[t].$$

Then, over the fraction field of $\mathbb{F}_2[t]$, we can check that

$$Q \equiv \left(\frac{t^9 + t^8 + t^3 + t^2}{t^8 + t^2}, \frac{t^{12} + t^9 + t^6 + t^3}{t^{12} + t^9 + t^6 + t^3} \right) = (t+1, 1) \equiv P, \tag{3.6}$$

whence $Q \notin \mathcal{E}^\circ(\mathbb{Q}(t))$. The right multiple of P to consider turns out to be $2Q = 6P$, which over the fraction field of $\mathbb{F}_2[t]$ equals $(t^4 + 1, t^6 + t^4 + t^3 + t + 1)$, at which $3x^2 - (t+1)^2$ does not vanish identically.

3.2.2 The *p*-adic sigma-function

In §2.2.2.1, we defined the p-adic sigma function of Mazur–Tate for a good ordinary elliptic curve over $\mathbb{Q}_p$. The definition generalises to more general base rings (see [99, Appendix II]): we can consider curves over $\mathbb{Z}_p$-algebras in which p is nilpotent and, by passing to limits, p-adically complete $\mathbb{Z}_p$-algebras.

In particular, we may view equation (3.4) as a Weierstrass equation over the standard affinoid algebra

$$\mathbb{Z}_p\langle t \rangle = \left\{ \sum_{i=0}^{\infty} b_i t^i \in \mathbb{Z}_p[[t]] : \lim_{i \to \infty} \mathrm{ord}_p(b_i) = \infty \right\}.$$

Let $x(T) \in \mathbb{Z}_p\langle t \rangle((T))$ be the formal series expansion of x around infinity, where $T = -\frac{x}{y}$. Assume that $\mathcal{E}_{t_0}$ has good ordinary reduction at p for each t_0 in $\overline{\mathbb{Z}_p}$. Then the construction of the p-adic sigma function of [99] makes sense also on the formal group of $\mathcal{E}$ over $\mathbb{Z}_p\langle t \rangle$ (see also [146, Theorem 1]). That is, there exists a unique odd function $\sigma_p(T) = T + \cdots \in \mathbb{Z}_p\langle t \rangle[[T]]$ on the formal group of $\mathcal{E}$ over $\mathbb{Z}_p\langle t \rangle$ such that

$$x(T) + \beta = -\frac{d}{\omega} \left(\frac{1}{\sigma_p} \frac{d\sigma_p}{\omega} \right),$$

where

$$\omega = \frac{dx}{2y + a_1(t)x + a_3(t)} \quad \text{and} \quad \beta = \frac{a_1(t)^2 + 4a_2(t)}{12} - \frac{1}{12}\mathbf{E}_2(\mathcal{E}, \omega).$$

Here $\mathbf{E}_2(\mathcal{E}, \omega)$ is the value of the weight 2 Katz p-adic Eisenstein series of Definition 2.2.5 at the pair $(\mathcal{E}, \omega)$.

If we know β, the series σ_p can be computed precisely in the same way as in [67, §4], i.e.

$$\sigma_p(T) = T \cdot \exp\left(\int h(T)dT\right),$$

where

$$h(T) = -s(T)\left(\int s(T)(x(T)+\beta)dT + \frac{a_1(t)}{2}\right) - \frac{1}{T},$$
$$s(T) = \frac{x'(T)}{2y(T) + a_1(t)x(T) + a_3(t)}$$

(see also the proof of Proposition 2.2.3).

Remark 3.2.4. We will eventually restrict to families of elliptic curves defined by Weierstrass equations with coefficients in $\mathbb{Z}[pt]$. Since $\mathbb{Z}_p[[pt]] \cong \varprojlim_n \mathbb{Z}_p[pt]/(p,pt)^n$, both $\mathbf{E}_2(\mathcal{E},\omega)$ and the coefficients of the p-adic sigma function then belong to $\mathbb{Z}_p[[pt]]$.

3.2.3 The weight 2 Eisenstein series

3.2.3.1 Kedlaya's algorithm and the computation of $\mathbf{E_2}$ in [96]

We now summarise Kedlaya's algorithm [75] for the computation of the matrix of Frobenius acting on the Monsky–Washnitzer cohomology of a hyperelliptic curve over a finite field of characteristic p and explain how this is used in the algorithm of Mazur–Stein–Tate [96]. Furthermore, we recall the proof of some results of Harrison [66] on the integrality properties of the entries of this matrix. The main references are [75] and [66]. For the formalism of Monsky–Washnitzer cohomology, the reader is also invited to consult [140].

As far as the theory behind Kedlaya's algorithm is concerned, there is no advantage in restricting to elliptic curves or in working over $\mathbb{Q}_p$, so we fix here a hyperelliptic curve defined affinely by $y^2 = Q(x)$ for some monic polynomial $Q(x) \in R[x]$ of degree $2g+1 \geq 3$, where R is the ring of integers of an unramified extension K of $\mathbb{Q}_p$. Let k be the residue field of K and assume that $\overline{Q}(x) \in k[x]$ has no repeated roots. Since $K/\mathbb{Q}_p$ is unramified, there is a unique automorphism ϕ_p of K which lifts the map $a \mapsto a^p$ on k. We also assume that p is odd and that $p \neq 2g+1$.

The p-power map on $\overline{A} = k[x,y,y^{-1}]/(y^2 - \overline{Q}(x))$ is a k-semilinear endomorphism called the p-power Frobenius, which we want to lift to some coordinate ring in characteristic zero. The p-adic completion $\hat{A}_R$ of $A_R = R[x,y,y^{-1}]/(y^2 - Q(x))$ admits a lift of Frobenius; however, the de Rham cohomology of $\hat{A}_R \otimes K$ is larger than the one

of $A_R \otimes K$, since a power series can converge in the closed unit disk slowly enough that its term-wise integral does not converge.

The Monsky–Washnitzer weak completion of A_R is a subalgebra of $\hat{A}_R$ which admits a lift of Frobenius and whose de Rham cohomology groups are finite-dimensional as K-vector spaces.

Definition 3.2.5. Let $B = R[x_1, \dots, x_n]/(g_1, \dots, g_m)$ for some $n \geq 1$ and $m \geq 1$, $g_i \in R[x]$. The *Monsky–Washnitzer weak completion* of B is

$$B^\dagger = R\langle x_1, \dots, x_n \rangle^\dagger / (g_1, \dots, g_m),$$

where

$$R\langle x_1, \dots, x_n \rangle^\dagger = \left\{ \sum_\alpha c_\alpha x^\alpha \in R[[x_1, \dots, x_n]] \mid \exists \gamma \in \mathbb{R}, \rho > 0 : \forall \alpha,\ \mathrm{ord}_p(c_\alpha) \geq \gamma + |\alpha|\rho \right\}$$

with $\alpha = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $|\alpha| = \sum_{i=1}^n \alpha_i$ and ord_p is the extension of the valuation on $\mathbb{Z}_p$ to R. The Monsky–Washnitzer cohomology of $\overline{B} = k[x_1, \dots, x_n]/(\overline{g_1}, \dots, \overline{g_m})$, denoted $H^i(\overline{B}, K)$, is the de Rham cohomology of $B^\dagger \otimes_R K$.

Remark 3.2.6. By [140, (2.4.5) Corollary], the cohomology groups $H^i(\overline{B}, K)$ are well-defined, i.e. they are independent of the lift B in characteristic zero. However, the computation of $\mathbf{E}_2$ requires an explicit choice of basis and so depends crucially on the lift.

Explicitly, we have

$$A_R^\dagger = \left\{ \sum_{n=-\infty}^{\infty} S_n(x) y^n : S_n(x) \in R[x], \deg S_n(x) \leq 2g, \liminf_{n\to\infty} \frac{\mathrm{ord}_p(S_n(x))}{n} > 0, \right.$$
$$\left. \liminf_{n\to\infty} \frac{\mathrm{ord}_p(S_{-n}(x))}{n} > 0 \right\} / (y^2 - Q(x)),$$

where by the valuation of a polynomial we mean the minimal valuation of its coefficients. Furthermore, $H^i(\overline{A}, K) = 0$ for all $i \geq 2$; $H^1(\overline{A}, K)$ is the quotient of the universal module of differentials by the exact forms and the set

$$\left\{ \frac{x^i dx}{y} : 0 \leq i \leq 2g-1 \right\} \cup \left\{ \frac{x^i dx}{y^2} : 0 \leq i \leq 2g \right\} \tag{3.7}$$

forms a K-basis[1] for $H^1(\overline{A}, K)$. In particular, Kedlaya describes an explicit reduction procedure to write an element in $H^1(\overline{A}, K)$ in terms of (3.7), which we now outline.

[1]Note that the given set of differentials also forms a K-basis for $H^1_{\mathrm{dR}}(\mathrm{Spec}(A_R \otimes K)/K)$ (see [77, 76]).

It follows from the description of $A_R^\dagger$ and the relation $y^2 = Q(x)$ that any differential can be written, uniquely, in the form $\sum_{m=-\infty}^{\infty} \frac{S_m(x)}{y^m} dx$ with $\deg(S_m) \leq 2g$. We call this representation the *standard expansion.*

Let $Q' = \frac{d}{dx}Q(x)$. Since $\overline{Q}(x)$ has no repeated roots, there exist $U, V \in R[x]$ such that $UQ + VQ' = 1$. Let $m > 2$ and assume without loss of generality that $S_m(x) \in R[x]$ (we make this assumption only to keep track more easily of potential appearance of denominators in the reduction). Then there exist $P_m, R_m \in R[x]$ with $S_m = P_m Q + R_m Q'$ and hence

$$S_m \frac{dx}{y^m} = P_m \frac{dx}{y^{m-2}} + \frac{2}{m-2} R_m' \frac{dx}{y^{m-2}} - \frac{1}{m-2} d\left(\frac{2R_m}{y^{m-2}}\right);$$

in $H^1(\overline{A}, K)$, this yields

$$S_m \frac{dx}{y^m} \equiv \left(P_m + \frac{2}{m-2} R_m'\right) \frac{dx}{y^{m-2}}. \tag{RednA}$$

Note that, since $\deg S_m < \deg Q + \deg Q'$, we may pick P_m, R_m such that $\deg P_m < 2g$ and $\deg R_m < 2g+1$, so $P_m + 2(m-2)^{-1} R_m'$ has degree at most $2g-1$. Indeed, since Q is monic and the leading coefficient of Q' is a unit in R (as we are assuming $p \neq 2g+1$), there exist $q(S_m U, Q'), q(S_m V, Q), r(S_m U, Q'), r(S_m V, Q) \in R[x]$, with $\deg r(S_m U, Q') < \deg Q'$, $\deg r(S_m V, Q) < \deg Q$ such that

$$S_m U = q(S_m U, Q')Q' + r(S_m U, Q'), \quad S_m V = q(S_m V, Q)Q + r(S_m V, Q).$$

By definition of U and V, we have $S_m UQ + S_m VQ' = S_m$. Therefore,

$$S_m - r(S_m U, Q')Q - r(S_m V, Q)Q' = (q(S_m U, Q') + q(S_m V, Q))QQ'.$$

By comparing degrees, we conclude that $q(S_m U, Q') + q(S_m V, Q) = 0$.

Applying (RednA) sufficiently many times expresses $S_m \frac{dx}{y^m}$ in terms of the subset $\left\{\frac{x^i dx}{y^{m \bmod 2}} : 0 \leq i \leq 2g-1\right\}$ of the basis (3.7).

If $m \leq 0$, we use the relation $y^2 = Q(x)$ to get

$$S_m \frac{dx}{y^m} = \tilde{S}_m \frac{dx}{y^{m \bmod 2}};$$

this increases the degree in x. We then add scalar multiples of

$$\begin{aligned} d(x^r) &= r x^{r-1} dx = r x^{r-1} Q(x) dx / y^2 \\ d(2x^r y) &= (2r x^{r-1} Q(x) + x^r Q'(x)) dx / y, \end{aligned} \tag{RednB}$$

for $r \geq 0$, to kill the leading terms and reduce the degree in x. Finally, if $m = 1$ and S_m has degree $2g$, we also apply (RednB).

The following lemma, due to Kedlaya (but with some corrections in [66]), explains what powers of p can appear in the denominator under (RednA) and (RednB). Here $\log_p$ is the logarithm in base p.

Lemma 3.2.7 (Kedlaya). *(i) Let $m > 2$, $S \in R[x]$ such that $\deg S \leq 2g$. Under (RednA), $Sdx/y^m \equiv Tdx/y^{m \bmod 2}$, for some $T \in K[x]$ with[2] $\deg T \leq 2g-1$ and $p^{\lfloor \log_p(m-2) \rfloor} T \in R[x]$.*

(ii) Let $S \in R[x]$ of degree $m \geq 2g$. Under (RednB), $Sdx/y \equiv Tdx/y$ for some $T \in K[x]$ with $\deg T < 2g$. Then $p^{\lfloor \log_p(2m-2g+1) \rfloor} T \in R[x]$.

Furthermore, in either case, the differential $d(\sum S_r(x) y^r)$ of the reduction can be chosen so that $p^u S_r(x) \in R[x]$, with the same u as the reduction remainder.

We now define an operator Frob_p on $A_R^\dagger \otimes K$ which lifts the p-power Frobenius on $\overline{A}$. First, we let Frob_p act on K as ϕ_p; then we define $\mathrm{Frob}_p(x) = x^p$, which forces

$$\mathrm{Frob}_p(y)^2 = Q^{\phi_p}(x^p),$$

where $Q^{\phi_p}(x)$ is obtained from Q by replacing each coefficient with its image under ϕ_p. Thus,

$$\mathrm{Frob}_p(y) = Q^{\phi_p}(x^p)^{1/2} = y^p \left(1 + \left(\frac{Q^{\phi_p}(x^p) - Q(x)^p}{y^{2p}}\right)\right)^{1/2}; \ \mathrm{Frob}_p(1/y) = \mathrm{Frob}_p(y)^{-1}.$$

Since $Q^{\phi_p}(x^p) - Q(x)^p$ is divisible by p in $R[x]$, these converge to elements of $A_R^\dagger \otimes K$. The operator Frob_p induces a ϕ_p-semilinear automorphism of $H^1(\overline{A}, K)$, which preserves the eigenspaces of the hyperelliptic involution. In particular, let $H^1(\overline{A}, K)^-$ be the subspace of $H^1(\overline{A}, K)$ spanned by

$$\mathcal{B} = \left\{ \frac{x^i dx}{y} : 0 \leq i \leq 2g-1 \right\}.$$

Then Frob_p induces a ϕ_p-semilinear automorphism of $H^1(\overline{A}, K)^-$, which we also denote Frob_p. The following lemma first finds the standard expansion of $\mathrm{Frob}_p(b)$ for $b \in \mathcal{B}$ and then uses Kedlaya's lemma to deduce integrality properties of the coefficients of the image of $\mathrm{Frob}_p(b)$ in $H^1(\overline{A}, K)^-$ in terms of the basis $\mathcal{B}$. We reproduce Harrison's proof, as we show that it gives a slightly stronger result than the one stated in [66] (which is used in the algorithm of [96]).

[2] Lemma 3.3 in [66] says $\deg T \leq 2g$, but the above discussion implies our stronger statement.

Lemma 3.2.8 (Harrison). *(i) (RednA) on the $\sum_{n\geq 3} S_n(x)\frac{dx}{y^n}$ part of the standard expansion of $\mathrm{Frob}_p(x^i dx/y)$ gives a form which is a linear combination of the elements of $\mathcal{B}$ with coefficients that are p-integral and divisible by p.*

(ii) Consider the coefficients of the $\mathcal{B}$-expansion resulting from (RednB) on the $\sum_{n\geq -1} S_n(x)y^n dx$ part of the standard expansion of $\mathrm{Frob}_p(x^{i-1}dx/y)$. Then the coefficients are p-integral and divisible by p for $i \leq g$ and have denominator bounded by $p^{-\lfloor \log_p(2r-1)\rfloor}$ for $i = g + r$.

Proof. By definition, for $1 \leq i \leq 2g$, we have

$$\begin{aligned}\mathrm{Frob}_p(x^{i-1}dx/y) &= x^{p(i-1)}y^{-p}\left(1 + py^{-2p}\left(\frac{Q^{\phi_p}(x^p) - Q(x)^p}{p}\right)\right)^{-1/2} dx^p \\ &= px^{pi-1}y^{-p}\left(1 + \sum_{n=1}^{\infty}\binom{-1/2}{n}p^n y^{-2pn}\left(\frac{Q^{\phi_p}(x^p) - Q(x)^p}{p}\right)^n\right)dx.\end{aligned}$$

Since

$$\binom{-1/2}{n} = \left(-\frac{1}{2}\right)^n \frac{1\cdot 3\cdot 5\cdots(2n-1)}{n!}$$

is p-integral (note that p is odd) and

$$y^{-2pn}\left(\frac{Q^{\phi_p}(x^p) - Q(x)^p}{p}\right)^n = A_1^{(n)}y^{-2} + \cdots + A_{pn}^{(n)}(x)y^{-2pn},$$

for some $A_i^{(n)}(x) \in R[x]$ of degree at most $2g$ (note that $(Q^{\phi_p}(x^p) - Q(x)^p)^n$ has degree at most $np\deg Q - 1$), we get

$$\mathrm{Frob}_p(x^{i-1}dx/y) = px^{pi-1}\left(\sum_{m\,\mathrm{odd}\geq p} p^{\lceil \frac{m-p}{2p}\rceil} b_m(x)y^{-m}\right)dx,$$

for $b_m(x) \in R[x]$ of degree at most $2g$, $b_p(x) = 1$. We multiply each term of the sum by px^{pi-1} and use the relation $y^2 = Q(x)$ to obtain

$$\mathrm{Frob}_p(x^{i-1}dx/y) = \left(\sum_{m\,\mathrm{odd}\geq m_0} c_m(x)y^{-m}\right)dx$$

where $m_0 \geq p - 2\left\lfloor \frac{pi-1}{2g+1}\right\rfloor$ and $c_m(x)$ of degree at most $2g$. For the lower bound on m_0, we are using the fact that $b_p(x) = 1$ and $p + 2k - 2\left\lfloor \frac{2g+pi-1}{2g+1}\right\rfloor \geq p - 2\left\lfloor \frac{pi-1}{2g+1}\right\rfloor$ for $k \geq 1$.

Note that

$$c_m(x) \in pR[x] \quad \text{for all } m \quad \text{and} \quad c_m(x) \in p^{\lceil \frac{m-p}{2p}\rceil + 1}R[x] \quad \text{for all } m \geq p.$$

By Lemma 3.2.7 (i), (i) follows if we can show that

$$g(m) := \begin{cases} \left\lceil \frac{m-p}{2p} \right\rceil + 1 - \lfloor \log_p(m-2) \rfloor & \text{if } m \geq p, \\ 1 - \lfloor \log_p(m-2) \rfloor & \text{if } 3 \leq m < p \end{cases}$$

satisfies $g(m) > 0$. For $m > 2$, let

$$f(m) = \left(\frac{m-p}{2p} \right) + 1 - \log_p(m-2).$$

Then

$$f'(m) = \frac{1}{2p} - \frac{1}{\log_{\mathbb{R}}(p)(m-2)} > \frac{m-2-2p}{2p(m-2)} \geq 0 \text{ for } m \geq 2p+2$$

and

$$f(2p+2) = \frac{1}{2} + \frac{1}{p} - \log_p(2) > 0 \tag{3.8}$$

since $p^{1/2+1/p} > 2$ for all odd p; thus $f(m) > 0$ for all $m \geq 2p+2$ and so $g(m) \geq f(m) > 0$. For $3 \leq m < p+2$, we have $\lfloor \log_p(m-2) \rfloor = 0$ and for $p+2 \leq m < 2p+2 < p^2$, we have $g(m) = 2-1 = 1$.

We now show (ii). Consider $c_n(x)y^{-n}$ for $m_0 \leq n \leq 1$. These come from $p^{\lceil \frac{m-p}{2p} \rceil} p x^{pi-1} b_m(x) y^{-m}$ for some $m \geq p$. For $x^{pi-1}b_m(x) = u_r(x)y^{2r} + \cdots + u_0(x)$ (with $\deg u_i(x) \leq 2g$) to give some contribution to $c_n(x)y^{-n}$, $m_0 \leq n \leq 1$, we need $2r - m \geq -1$ and so $p \leq m \leq \left\lfloor \frac{2((pi-1)+\deg b_m(x))}{2g+1} \right\rfloor + 1 =: C$. Using $y^2 = Q(x)$, we get

$$\sum_{n=m_0}^{1} c_n(x) y^{-n} dx = \sum_{m=p}^{C} S_m(x) dx/y$$

where $\deg S_m(x) = pi - 1 + \deg b_m(x) - (2g+1)\left(\frac{m-1}{2}\right)$. This has not introduced any denominator. However, if $\deg S_m(x) \geq 2g$, we need to apply (RednB). By Lemma 3.2.7 (ii), we then get that $p^{\alpha(m)} S_m(x) \in R[x]$, where

$$\alpha(m) = \lfloor \log_p(2pi - m(2g+1) + 2\deg b_m(x)) \rfloor - 1 - \left\lceil \frac{m-p}{2p} \right\rceil.$$

Since $b_p(x) = 1$, we have

$$\alpha(p) = \lfloor \log_p(2pi - p(2g+1)) \rfloor - 1;$$

furthermore, $\alpha(m) \leq \alpha(p)$ for all m in the range above, given that $\deg b_m(x) \leq 2g$.

For $i \leq g$ note that $2pi - p(2g+1) < 0$, which means that we have not applied any (RednB). Thus for $i \leq g$, the coefficients are divisible by p. For $i = g + r$, $1 \leq r \leq g$, $\alpha(p) = \lfloor \log_p(p(2r-1)) \rfloor - 1$. □

We now specialise to our case of interest: $R = \mathbb{Z}_p$, $K = \mathbb{Q}_p$ and

$$Q(x) = x^3 + ax + b \in \mathbb{Z}_p[x],$$

where p is a prime larger than 3 and ϕ_p is the identity on $\mathbb{Q}_p$. The polynomial Q defines an elliptic curve E over $\mathbb{Q}_p$ with invariant differential $\omega = \frac{dx}{2y}$ and we assume that E has good ordinary reduction at p. The set $\mathcal{B} = \{\frac{dx}{y}, \frac{xdx}{y}\}$ is a $\mathbb{Q}_p$-basis for the cohomology space $H^1(\overline{A}, K)^-$. Note that in Definition 2.2.5 we identified this group with the first de Rham cohomology of E: by [77, Example 1.5.1], $H^1_{\mathrm{dR}}(E)$ is in bijection with $H^1_{\mathrm{dR}}(E \setminus O)$ and by [77, Example 1.2.1] $\mathcal{B}$ generates $H^1_{\mathrm{dR}}(E \setminus O)$ over $\mathbb{Q}_p$.

Let $F = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ be the matrix of Frob_p acting on the left on $H^1(\overline{A}, K)^-$ with respect to $\mathcal{B}$. By Lemma 3.2.8, $A, B, C, D \in \mathbb{Z}_p$ and $A, C \in p\mathbb{Z}_p$. Furthermore, since p is ordinary and $A \in p\mathbb{Z}_p$, we also have $D \in \mathbb{Z}_p^\times$, as one deduces from the fixed-point theorem for Monsky–Washnitzer cohomology that the trace of F equals $1 + p - \#\overline{E}(\mathbb{F}_p)$ (see for example the proof of [66, Lemma 3.1]).

We now show how F is used in [96] to compute the value of $\mathbf{E}_2$ at (E, ω).

Lemma 3.2.9. *Let n be a positive integer and write $F^n = \left(\begin{smallmatrix} A_n & B_n \\ C_n & D_n \end{smallmatrix}\right)$ for some A_n, B_n, C_n, $D_n \in \mathbb{Z}_p$. Then $\mathbf{E}_2(E, \omega) \equiv -12\frac{B_n}{D_n} \mod p^n$.*

Proof. We fixed an equation for E of the form $y^2 = Q(x)$ with Q monic. Applying the change of variables $36\tilde{x} = x$, $108\tilde{y} = y$ we obtain an equation of the form $\tilde{E}\colon \tilde{y}^2 = 4\tilde{x}^3 - g_2\tilde{x} - g_3$, for some $g_2, g_3 \in \mathbb{Z}_p$ (note $p \geq 5$). We have

$$\frac{d\tilde{x}}{\tilde{y}} = 3\frac{dx}{y}, \qquad \frac{\tilde{x}d\tilde{x}}{\tilde{y}} = \frac{1}{12}\frac{xdx}{y}.$$

Let

$$u = \tilde{\gamma}\frac{d\tilde{x}}{\tilde{y}} + \tilde{\delta}\frac{\tilde{x}d\tilde{x}}{\tilde{y}} = 3\tilde{\gamma}\frac{dx}{y} + \frac{\tilde{\delta}}{12}\frac{xdx}{y} = \gamma\frac{dx}{y} + \delta\frac{xdx}{y} \tag{3.9}$$

be an eigenvector for Frobenius with unit eigenvalue. By Definition 2.2.5,

$$\mathbf{E}_2\left(E, \frac{dx}{2y}\right) = 36\mathbf{E}_2\left(E, 3\frac{dx}{y}\right) = 36\mathbf{E}_2\left(\tilde{E}, \frac{d\tilde{x}}{\tilde{y}}\right) = 36(-12)\frac{\tilde{\gamma}}{\tilde{\delta}} = -12\frac{\gamma}{\delta}.$$

Let α be the eigenvalue of u. Since $A \in p\mathbb{Z}_p$, we have $\alpha \equiv D \bmod p$. We prove the lemma by induction on n. If $n = 1$, then $F(F(\frac{xdx}{y})) = F(B\frac{dx}{y} + D\frac{xdx}{y}) = BF(\frac{dx}{y}) + DF(\frac{xdx}{y}) \equiv DF(\frac{xdx}{y}) \bmod p$. Suppose that $F^{n-1}(\frac{xdx}{y}) = u + p^{n-1}(r\frac{dx}{y} + s\frac{xdx}{y})$ for some

$r, s \in \mathbb{Z}_p$. Then $F^n(\frac{xdx}{y}) \equiv F(u) + sp^{n-1}(B\frac{dx}{y} + D\frac{xdx}{y}) \bmod p^n$ as $F(\frac{dx}{y}) \equiv 0 \bmod p$. Thus

$$\begin{aligned} F\left(F^n\left(\frac{xdx}{y}\right)\right) &\equiv F^2(u) + Dsp^{n-1}F\left(\frac{xdx}{y}\right) \bmod p^n \\ &\equiv \alpha F(u) + Dsp^{n-1}\left(B\frac{dx}{y} + D\frac{xdx}{y}\right) \bmod p^n \\ &\equiv \alpha\left(F(u) + sp^{n-1}\left(B\frac{dx}{y} + D\frac{xdx}{y}\right)\right) \bmod p^n \equiv \alpha F^n\left(\frac{xdx}{y}\right). \end{aligned}$$

The lemma then follows, since no precision is lost upon division by $D_n \in \mathbb{Z}_p^\times$. □

3.2.3.2 A modified version of Lauder's deformation method

Our goal here is to set up a theory for one-parameter families of elliptic curves which specialises to Kedlaya's construction on the fibres and which can be used to compute a power series interpolating the values of the Katz p-adic Eisenstein series. We use Lauder's deformation method [87, 88] applied to Monsky–Washnitzer cohomology as in Hubrechts's work [71] as a guideline. For our intended applications, we are forced to modify all the definitions: the base ring, the dagger ring and the action of Frobenius (see also [71, Note 4]). However, the results that we need are analogues of those in [71], so we will mostly adapt the proofs there to our situation.

Let $\mathcal{E}$ be as in (3.4) and consider a short Weierstrass model

$$\mathcal{E}_{\text{short}} \colon y^2 = Q(x,t) := x^3 + a(t)x + b(t) \tag{3.10}$$

with $a(t), b(t) \in \mathbb{Z}_p[t]$. We may assume that $\mathcal{E} = \mathcal{E}_{\text{short}}$, since

$$\mathbf{E}_2\left(\mathcal{E}_{\text{short}}, \frac{dx}{2y}\right) = u^2\mathbf{E}_2(\mathcal{E}, \omega),$$

where $u^{12} = \Delta_{\mathcal{E}_{\text{short}}}/\Delta_{\mathcal{E}}$ (here Δ denotes the discriminant).

We would like to define a base ring S and an S-algebra T, such that

$$S \subseteq \mathbb{Q}_p[[t]], \qquad T \subseteq \mathbb{Q}_p[[t, x, y, y^{-1}]]/(y^2 - Q(x,t))$$

and with the following properties:

(1) Specialising S and T at $t_0 \in \mathbb{Z}_p$ is meaningful and returns Kedlaya's setting. That is, $S \mapsto \mathbb{Q}_p$, $T \mapsto A^\dagger_{\mathbb{Z}_p} \otimes \mathbb{Q}_p$, where $A^\dagger_{\mathbb{Z}_p}$ is the Monsky–Washnitzer weak completion of $A_{\mathbb{Z}_p} = \mathbb{Z}_p[x, y, y^{-1}]/(y^2 - Q(x, t_0))$.

(2) Cohomology requirement: the quotient Tdx by $\mathrm{d}\,T$ (where d is $\frac{\partial}{\partial x}dx$) is free of finite rank over S, with basis $\left\{\frac{x^i dx}{y}, \frac{x^j dx}{y^2} : i = 0, 1,\ j = 0, 1, 2\right\}$.

(3) There is a well-defined action of Frobenius on S and T which lifts the absolute Frobenius in characteristic p and specialises to Kedlaya's Frobenius.

We make the following assumption

Assumption 3.2.10. The polynomials $a(t), b(t) \in \mathbb{Z}_p[t]$ reduce to constant polynomials over $\mathbb{F}_p$.

Let $r(t)$ be the resultant with respect to x of $Q(x,t)$ and $\frac{\partial Q}{\partial x}(x,t)$. Assumption 3.2.10 implies that $r(t)$ is constant modulo p and we assume that $\overline{r(t)} \in \mathbb{F}_p^\times$, so the fibres above $\mathbb{Z}_p$ have good reduction at p.

Even though the curve in characteristic p is constant, by (1) the algebra T should depend on the parameter t and, consequently, S should contain $\mathbb{Z}_p[t]$ in view of (2). Recall that to perform (RednA) in Kedlaya's algorithm we used the fact that $r(t_0) \in \mathbb{Z}_p^\times$. Similarly, we must insist here that $\frac{1}{r(t)} \in S$.

Furthermore, the reduction process will require handling infinite sums of certain elements of S and integrating power series in x with coefficients in S. For these reasons, we define $S = \mathbb{Z}_p\langle t\rangle^\dagger \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Writing $r(t) = \alpha(1 - pq(t))$ for some $\alpha \in \mathbb{Z}_p^\times$ and $q(t) \in \mathbb{Z}_p[t]$, we have $r(t)^{-1} = \alpha^{-1}\sum_{\ell=0}^\infty p^\ell q^\ell = \sum_{k=0}^\infty b_k t^k$ with $\mathrm{ord}_p(b_k) \geq k/\deg_t q$, so $r(t)^{-1} \in S$.

An infinite sum of elements in S might not be well-defined. In analogy with [71, Definition 7, Lemmas 8, 9], for the definition of T (and in particular, for (2)), we need to consider infinite sequences of elements in S whose sum of terms is itself an element in S.

Definition 3.2.11. Let $(s_k(t) = \sum_{\ell\geq 0} b_{k\ell}t^\ell)_{k\in\mathbb{Z}}$ be a sequence of elements in S. Then $(s_k)_k \in \mathcal{S}$ if and only if there exists $c \in \mathbb{Q}_p$ and $\delta > 0$ such that

$$\mathrm{ord}_p(cb_{k\ell}) \geq \delta(|k| + \ell).$$

Lemma 3.2.12. *Let $(s_k)_k \in \mathcal{S}$. Then $\sum_k s_k$ converges to an element of S. Furthermore, $\mathcal{S}$ is closed under addition and if $\tilde{s}(t) \in S$, then $(\tilde{s}s_k)_k \in \mathcal{S}$.*

Proof. Let $s_k(t) = \sum_{\ell\geq 0} b_{k\ell}t^\ell$. Since $b_{k\ell} \to 0$ as $\max(|k|, \ell) \to \infty$, by [62, Proposition 4.1.3], we have

$$\sum_k s_k(t) = \sum_k \left(\sum_{\ell=0}^\infty b_{k\ell}t^\ell\right) = \sum_{\ell=0}^\infty \left(\sum_{k\in\mathbb{Z}} b_{k\ell}\right)t^\ell \in \mathbb{Q}_p[[t]].$$

We need to show that there exist $\gamma \in \mathbb{R}$, $\rho > 0$, such that $\mathrm{ord}_p(\sum_{k\in\mathbb{Z}} b_{k\ell}) \geq \gamma + \ell\rho$ for all $\ell \in \mathbb{Z}_{\geq 0}$. This follows from the non-archimedean triangle inequality and

$$\inf_{k\in\mathbb{Z}} \mathrm{ord}_p(b_{k\ell}) \geq \inf_{k\in\mathbb{Z}} (\delta(|k|+\ell) - \mathrm{ord}_p(c)) \geq \gamma + \rho\ell$$

for $\gamma = -\mathrm{ord}_p(c)$ and $\rho = \delta$.

We now show that $\mathcal{S}$ is closed under addition and multiplication by S. Let $(s_k^{(1)})_k, (s_k^{(2)})_k \in \mathcal{S}$; $s_k^{(1)} + s_k^{(2)} = \sum_{\ell=0}^{\infty}(b_{k\ell}^{(1)} + b_{k\ell}^{(2)})t^\ell$ and let $c^{(i)}$, $\delta^{(i)}$ be the constants of Definition 3.2.11 for $s_k^{(i)}$. Then

$$\begin{aligned}\max_i \mathrm{ord}_p(c_i) + \mathrm{ord}_p(b_{k\ell}^{(1)} + b_{k\ell}^{(2)}) &\geq \max_i \mathrm{ord}_p(c_i) + \min_i \mathrm{ord}_p(b_{k\ell}^{(i)}) \\ &\geq \min_i(\delta^{(i)}(|k|+\ell)),\end{aligned}$$

proving that $(s_k^{(1)} + s_k^{(2)})_k \in \mathcal{S}$.

Let now $(s_k(t)) \in \mathcal{S}$ as above and $\tilde{s}(t) = \sum_j c_j t^j \in S$. Then, by [50, Corollary 2.10],

$$\tilde{s}(t)s_k(t) = \sum_{j,\ell} b_{k\ell}c_j t^{\ell+j} = \sum_r \Big(\sum_{j+\ell=r} b_{k\ell}c_j\Big)t^r$$

and

$$\begin{aligned}\mathrm{ord}_p\Big(\sum_{j+\ell=r} b_{k\ell}c_j\Big) &\geq \min_{j+\ell=r}(\mathrm{ord}_p(b_{k\ell}) + \mathrm{ord}_p(c_j)) \\ &\geq \min_{j+\ell=r}(\delta(|k|+\ell) + j\rho + \gamma) \\ &\geq \min_{j+\ell=r}(\delta'(|k|+\ell+j) + \gamma) \\ &= \delta'(|k|+r) + \gamma,\end{aligned}$$

for some $\delta, \rho, \gamma, \delta' \in \mathbb{R}$ with $\delta, \delta', \rho > 0$. □

Lemma 3.2.13. *For $m \in \mathbb{Z}_{\geq 0}$, let $s_m = \sum_{k\geq 0,\ell\geq 0} p_{k\ell}^{(m)} r^{-k} t^\ell$, where $p_{k\ell}^{(m)} \in \mathbb{Q}_p[t]$, $\deg p_{k\ell}^{(m)} \leq A(k+m)$ and $\mathrm{ord}_p(p_{k\ell}^{(m)}) \geq \delta(k+m+\ell)$ for some constants $A, \delta > 0$. Then $(s_m)_m \in \mathcal{S}$.*

Proof. Let N be a fixed positive integer and assume without loss of generality that $A \geq 1$. By assumption, $p_{k\ell}^{(m)} \equiv 0 \bmod p^N$, provided that $k+m+\ell \geq N/\delta$. Since the expansion of $1/r$ as a power series in t is, modulo p^N, a polynomial of degree at most $(N-1)\deg r$, then $s_m \bmod p^N$ is a polynomial in t. For $k+m+\ell < N/\delta$, we have

$$\begin{aligned}\deg_t(p_{k\ell}^{(m)} r^{-k} t^\ell \bmod p^N) &\leq A(k+m) + (N-1)\deg r + \ell \\ &\leq A(k+m+\ell) + (N-1)\deg r \\ &\leq AN/\delta + (N-1)\deg r.\end{aligned}$$

Thus $s_m \bmod p^N$ is a polynomial of degree at most cN for some constant c (independent of N). It follows that, writing $s_m = \sum_j b_{mj} t^j$, the coefficient of t^j is zero modulo p^N for all N such that $cN < j$, i.e. $\mathrm{ord}_p(b_{mj}) \geq \frac{j}{c}$. Furthermore, $\mathrm{ord}_p(b_{mj}) \geq \delta m$ from $\mathrm{ord}_p(p_{k\ell}^{(m)}) \geq \delta(k+m+\ell)$. Thus $\mathrm{ord}_p(b_{mj}) \geq \max\{j/c, \delta m\} \geq \frac{1}{2c} j + \frac{\delta}{2} m$. □

We then define the coordinate ring as

$$T = \left\{ \sum_{k \in \mathbb{Z}} y^k \left(\sum_{i=0}^{2} s_{ik} x^i \right) : (s_{ik})_k \in \mathcal{S} \right\} / (y^2 - Q(x,t)).$$

By Lemma 3.2.12, T is an S-module. A similar computation shows that T is an S-algebra. Let $\mathbb{Z}_p^{ur}$ be the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$.

Lemma 3.2.14. *Let $t_0 \in \mathbb{Z}_p$ or $t_0 \in \mathbb{Z}_p^{ur}$ such that t_0 generates the residue field extension corresponding to $\mathbb{Q}_p(t_0)/\mathbb{Q}_p$. Then $S \otimes \mathbb{Q}_p(t_0)/(t - t_0) \simeq \mathbb{Q}_p(t_0)$ as rings and $T \otimes \mathbb{Q}_p(t_0)/(t - t_0) = A^\dagger \otimes \mathbb{Q}_p(t_0)$, where $A^\dagger \otimes \mathbb{Q}_p(t_0)$ is the $\mathbb{Q}_p(t_0)$-algebra used by Kedlaya for $\mathcal{E}_{t_0}$.*

Proof. Let $e_{S,t_0} \colon S \otimes \mathbb{Q}_p(t_0) \to \mathbb{Q}_p(t_0)$ be the evaluation map at $t_0 \in \mathbb{Z}_p^{ur}$. This is well-defined, since elements in S converge on the closed unit disk and $\mathbb{Q}_p(t_0)$ is complete; furthermore, it is surjective and a ring homomorphism. Since $\mathbb{Z}_p\langle t \rangle^\dagger \otimes \mathbb{Q}_p(t_0)$ satisfies the Weierstrass Preparation and Division Theorems ([140, (2.2) Proposition]), $s(t) \in \ker e_{S,t_0}$ iff it is divisible by $t - t_0$.

Assume now that t_0 is either in $\mathbb{Z}_p$ or generates the residue field extension corresponding to $\mathbb{Q}_p(t_0)/\mathbb{Q}_p$. In particular, the ring of integers of $\mathbb{Q}_p(t_0)$ is $\mathbb{Z}_p[t_0]$ (see [86, Proposition 23]). Let

$$A^\dagger \otimes \mathbb{Q}_p(t_0) = \Bigg\{ \sum_{k \in \mathbb{Z}} y^k \left(\sum_{i=0}^{2} a_{ik} x^i \right) \mid a_{ik} \in \mathbb{Q}_p(t_0) \text{ and } \exists\, \gamma \in \mathbb{R}, \rho > 0 : \forall\, k, \min_i \mathrm{ord}_p(a_{ik}) \geq \gamma + |k|\rho \Bigg\} / (y^2 - Q(x, t_0))$$

and let $e_{T,t_0} : T \otimes \mathbb{Q}_p(t_0) \to A^\dagger \otimes \mathbb{Q}_p(t_0)$ be the evaluation map on T. First we need to show this is well-defined, i.e. that evaluating makes sense and results in an element of $A^\dagger \otimes \mathbb{Q}_p(t_0)$.

That evaluation makes sense again is because we are considering overconvergent power series. Let $F = \sum_{k \in \mathbb{Z}} y^k (\sum_{i=0}^{2} s_{ik} x^i) \in T$ and $t_0 \in \mathbb{Z}_p^{ur}$. Write $s_{ik}(t) = \sum_\ell b_{k\ell i} t^\ell$ and let c_i, δ_i be the constants for s_{ik} from Definition 3.2.11. Then, for all i, k, we have

$$\mathrm{ord}_p(c_i s_{ik}(t_0)) \geq \mathrm{ord}_p(c_i) + \min_\ell \mathrm{ord}_p(b_{k\ell i} t_0^\ell) \geq \delta_i |k|,$$

so, for all k,

$$\max_i \operatorname{ord}_p(c_i) + \min_i \operatorname{ord}_p(s_{ik}(t_0)) \geq \min_i \delta_i |k|$$

which yields $e_{T,t_0}(F) \in A^\dagger \otimes \mathbb{Q}_p(t_0)$. Conversely, consider $\sum_{k\in\mathbb{Z}} y^k \big(\sum_{i=0}^2 a_{ik}x^i\big) \in A^\dagger \otimes \mathbb{Q}_p(t_0)$, with $\liminf_{k\to\infty} \frac{\operatorname{ord}_p(a_{ik})}{|k|} > 0$ for each i. Write $a_{ik} = p^{\alpha_{ik}} b_{ik}$ where $b_{ik} \in \mathbb{Z}_p[t_0]^\times$ and $\operatorname{ord}_p(a_{ik}) = \alpha_{ik}$. Then there exists a polynomial $s_{ik}(t) \in \mathbb{Z}_p[t]$ of degree less than $[\mathbb{Q}_p(t_0)\colon \mathbb{Q}_p]$ such that $s_{ik}(t_0) = b_{ik}$ and $p^{\alpha_{ik}} s_{ik}(t)$ has valuation equal to α_{ik}. □

Let d be the differential operator $\frac{\partial}{\partial x}dx$ on T. We want to show that the quotient $H_{MW} := T dx / \operatorname{d} T$ is a free S-module with basis $\big\{\frac{x^i dx}{y}, \frac{x^j dx}{y^2} : 0 \leq i \leq 1, 0 \leq j \leq 2\big\}$. We say that a differential is *exact* if it belongs to $\operatorname{d} T$. We first prove the analogue of [70, Lemma 3.23] for our T.

Lemma 3.2.15. *Let T_+^{even} be the subset of T consisting of all elements of the form $\sum_{k\geq 0} y^{2k} \big(\sum_{i=0}^2 s_{ik}(t)x^i\big)$, with $(s_{ik}(t))_k \in \mathcal{S}$. Then*

$$T_+^{\mathrm{even}} = \left\{ \sum_{k\geq 0} s_k(t)x^k : (s_k)_k \in \mathcal{S} \right\}.$$

In particular, any differential in $T_+^{\mathrm{even}} dx$ is exact.

Proof. Denote by $\tilde{T}$ the set we want to prove equal to T_+^{even}. We first show that $T_+^{\mathrm{even}} \subset \tilde{T}$. Let $B_k(x,t) = \sum_{i=0}^2 s_{ik}(t)x^i$ and $Q(x,t)^k = \sum_{i=0}^{3k} a_i^{(k)}(t)x^i$. Then

$$\sum_{k\geq 0} y^{2k} B_k(x,t) = \sum_{k\geq 0} \Bigg(\sum_{\substack{0\leq i\leq 2 \\ 0\leq j\leq 3k}} s_{ik}(t) a_j^{(k)}(t) x^{i+j} \Bigg) = \sum_{\ell\geq 0} \Bigg(\sum_{\substack{i+j=\ell \\ k\geq \lceil \frac{\ell-2}{3} \rceil}} s_{ik}(t) a_j^{(k)}(t) \Bigg) x^\ell.$$

Now, write $s_{ik}(t) = \sum_{r\geq 0} b_{ikr} t^r$, $a_j^{(k)}(t) = \sum_{s\geq 0} c_{js}^{(k)} t^s$. Then

$$\sum_{\substack{i+j=\ell \\ k\geq \lceil \frac{\ell-2}{3} \rceil}} s_{ik}(t) a_j^{(k)}(t) = \sum_{n\geq 0} \Bigg(\sum_{\substack{i+j=\ell,\ r\leq n \\ k\geq \lceil \frac{\ell-2}{3} \rceil}} b_{ikr} c_{j(n-r)}^{(k)} \Bigg) t^n.$$

Since (without loss of generality) $\operatorname{ord}_p(b_{ikr}) \geq \delta^{(i)}(k+r)$ for some $\delta^{(i)} > 0$ and $a_j^{(k)}$ is a polynomial with coefficients in $\mathbb{Z}_p$, then $\sum_{i+j=\ell,\ r\leq n} b_{ikr} c_{j(n-r)}^{(k)} \to 0$ as $k \to \infty$.

Furthermore, Assumption 3.2.10 implies that $\operatorname{ord}_p(c_{js}^{(k)}) \geq s/\deg_t Q$ and so

$$\begin{aligned}\operatorname{ord}_p\Bigg(\sum_{\substack{i+j=\ell,\ r\leq n\\ k\geq\lceil\frac{\ell-2}{3}\rceil}} b_{ikr}c_{j(n-r)}^{(k)}\Bigg) &\geq \min_{\substack{i+j=\ell,\ r\leq n\\ k\geq\lceil\frac{\ell-2}{3}\rceil}} (\operatorname{ord}_p(b_{ikr}) + \operatorname{ord}_p(c_{j(n-r)}^{(k)}))\\ &\geq \min_{\substack{i+j=\ell,\ r\leq n\\ k\geq\lceil\frac{\ell-2}{3}\rceil}} (\delta^{(i)}(k+r) + (n-r)/\deg_t Q)\\ &\geq \min_{0\leq i\leq 2} (\min(1/\deg_t Q, \delta^{(i)})(3^{-1}(\ell-2)+n)).\end{aligned}$$

This shows that $T_+^{\text{even}} \subset \tilde{T}$. Conversely, let $\sum_{k\geq 0} s_k(t)x^k \in \tilde{T}$, with $(s_k(t) = \sum_{\ell\geq 0} b_{\ell k}t^\ell)_k \in \mathcal{S}$. Since $Q(x,t)$ is monic in x, there exist $c_{kr}(x,t) \in \mathbb{Z}_p[x,t]$ of degree at most 2 in x and at most $k\deg_t Q$ in t, such that

$$x^k = \sum_{r=0}^{\lfloor k/3\rfloor} c_{kr}(x,t)y^{2r}.$$

Thus,

$$\sum_{k\geq 0} s_k(t)x^k = \sum_{k\geq 0}\sum_{\ell\geq 0} b_{\ell k}t^\ell \sum_{r=0}^{\lfloor k/3\rfloor} c_{kr}(x,t)y^{2r} = \sum_{r=0}^{\infty} y^{2r}\Bigg(\sum_{\substack{\lfloor k/3\rfloor\geq r\\ \ell\geq 0}} b_{\ell k}c_{kr}t^\ell\Bigg).$$

We may assume without loss of generality that $c_{kr} \in \mathbb{Z}_p[t]$, say $c_{kr} = \sum_s a_{krs}t^s$ with $\operatorname{ord}_p(a_{krs}) \geq s/\deg_t Q$. We then need to show that

$$\tilde{s}_r = \sum_{m\geq 0}\Bigg(\sum_{\substack{\lfloor k/3\rfloor\geq r\\ \ell\leq m}} b_{\ell k}a_{kr(m-\ell)}\Bigg)t^m$$

satisfies $(\tilde{s}_r)_r \in \mathcal{S}$. We have

$$\operatorname{ord}_p\Bigg(\sum_{\substack{\lfloor k/3\rfloor\geq r\\ \ell\leq m}} b_{\ell k}a_{kr(m-\ell)}\Bigg) \geq \min_{\substack{\lfloor k/3\rfloor\geq r\\ \ell\leq m}} (\operatorname{ord}_p(b_{\ell k}) + \operatorname{ord}_p(a_{kr(m-\ell)}))$$

and the claim then follows similarly to above.

We next show that $\sum_{k\geq 0}\frac{s_k(t)}{k+1}x^{k+1} \in \tilde{T}$. For each k, ℓ, we have

$$\operatorname{ord}_p((k+1)^{-1}b_{\ell k}) \geq \delta(k+\ell)+\gamma-\operatorname{ord}_p(k+1) \geq \delta(k+\ell)+\gamma-\log_p(k+1),$$

for some $\delta,\gamma \in \mathbb{R}$, $\delta > 0$. Let M such that $\log_p(k+1) < \frac{\delta}{2}k$ for $k \geq M$. Then for $k \geq M$,

$$\operatorname{ord}_p((k+1)^{-1}b_{\ell k}) \geq \frac{\delta}{2}(k+\ell)+\gamma$$

and, for $k < M$,

$$\operatorname{ord}_p((k+1)^{-1}b_{\ell k}) \geq \delta(k+\ell)+\gamma-\max_{1\leq i\leq M}\operatorname{ord}_p(i). \qquad \square$$

We now adapt the proof of [71, Lemma 13] to our setting.

Lemma 3.2.16. *The set $\mathcal{B}$ generates H_{MW} over S.*

Proof. Let $\sum_{k\in\mathbb{Z}} y^k B_k(x,t)dx \in Tdx$, where $B_k(x,t) = \sum_{i=0}^{2} s_{ik}(t)x^i$. With the notation of Lemma 3.2.15, we have

$$\sum_{\substack{k\geq 0\\ k\,\text{even}}} y^k B_k(x,t)dx \in T_+^{\text{even}}dx$$

and the lemma shows that every element in $T_+^{\text{even}}dx$ is exact.

We may thus assume that $B_k(x,t) = 0$ unless k is negative, or positive and odd. As in Kedlaya's algorithm, we first want to get rid of y^k, for $k \neq -1, -2$.

If $k \geq 0$ and $k = 2\ell + 1$ for some $\ell \in \mathbb{Z}_{\geq 0}$ then $y^k = (y^2)^{\ell+1}/y$. Therefore,

$$y^k B_k(x,t)dx = y^{-1}H_k(x,t)dx$$

for some polynomial $H_k(x,t)$ in x.

Suppose now that $k < -2$. Since there exist $U(x,t), V(x,t) \in \mathbb{Z}[x,t]$, with $\deg_x U < 2$, $\deg_x V < 3$, such that

$$r(t) = U(x,t)Q(x,t) + V(x,t)\frac{\partial}{\partial x}Q(x,t),$$

and $\deg_x B_k(x,t) \leq 2$, as in (RednA) we can write

$$B_k(x,t) = \frac{1}{r}\left(P_k Q + R_k\frac{\partial Q}{\partial x}\right) = \frac{1}{r}\left(P_k y^2 + R_k\frac{\partial Q}{\partial x}\right) \tag{3.11}$$

where $\deg_x P_k < 2$, $\deg_x R_k < 3$ (recall that $r(t)^{-1} \in S$). Thus,

$$y^k B_k(x,t)dx = \left(\frac{1}{r}P_k - \frac{2}{(k+2)r}\frac{\partial R_k}{\partial x}\right)y^{k+2}dx + \mathrm{d}\left(\frac{2}{(k+2)r}y^{k+2}R_k\right) \quad \text{(RednA(t))}$$

Repeating this if necessary, we eventually find that $y^k B_k(x,t)dx$ can be written as an exact form plus a linear polynomial in x divided by y or y^2.

If $k \geq 0$ and k is odd, we have reduced our differential form to an exact form plus a polynomial in x of possibly large degree divided by y and for $k = -1$ we have a polynomial of degree at most 2 divided by y. In both cases, we may need to decrease the degree in x to turn it into a linear polynomial. For $m \geq 2$, we have

$$\mathrm{d}\left(\frac{x^{m-2}y}{m-1/2}\right) - \left(\left(\frac{m-2}{m-1/2}\right)x^{m-3}y + \frac{1}{2m-1}\frac{x^{m-2}}{y}\frac{\partial Q}{\partial x}\right)dx = 0;$$

thus, adding $y^{-1}x^m dx$, we get

$$\frac{x^m dx}{y} = \left(\frac{2m-4}{2m-1}\right)\left(\frac{x^m - x^{m-3}Q}{y}\right)dx + \frac{1}{2m-1}\left(\frac{3x^m - x^{m-2}\frac{\partial Q}{\partial x}}{y}\right)dx \tag{RednB(t))}$$
$$+ \mathrm{d}\left(\frac{x^{m-2}y}{m-1/2}\right),$$

where $3x^m - x^{m-2}\frac{\partial Q}{\partial x}$ has degree strictly less than m, $(2m-4)(x^m - x^{m-3}Q)$ has degree less than m if $m \geq 3$ and is zero if $m = 2$.

Thus far, we have shown that we can write $y^k B_k dx$ as an exact form plus $\sum_{b\in\mathcal{B}} \alpha_b^{(k)} b$, for some $\alpha_b^{(k)} \in S$. We still need to prove that, for each b, $\sum_k \alpha_b^{(k)}$ converges to an element in S and that the sum of the exact forms converges to an element in T. Since we will eventually consider only the odd part of H_{MW}, we limit ourselves to showing this for k odd.

We slightly change notation and start with $\sum_{k=1}^{\infty} y^{-(2k+1)} s_k(t) x^u dx$, $0 \leq u \leq 2$, $s_k(t) = \sum_{\ell=0}^{\infty} s_{k\ell} t^\ell$. We may assume that $s_{k\ell} \in \mathbb{Z}_p$ and hence that there exists $\delta > 0$ such that $\mathrm{ord}_p(s_{k\ell}) \geq \delta(k+\ell) + \lfloor \log_p(2k-1) \rfloor$.

Let now $s_{k\ell}^{(k)} = s_{k\ell} x^u$ and for $i = k, \ldots, 1$, define $s_{k\ell}^{(i)}, f_{k\ell}^{(i)} \in S[x]$ by the formula

$$y^{-(2i+1)} s_{k\ell}^{(i)} dx = y^{-(2i-1)} s_{kl}^{(i-1)} dx + \mathrm{d}(y^{-(2i-1)} f_{k\ell}^{(i-1)}),$$

obtained using (RednA(t)). Then

$$y^{-(2k+1)} s_{k\ell} x^u dx = y^{-1} s_{k\ell}^{(0)} dx + \mathrm{d}\left(\sum_{i=0}^{k-1} y^{-(2i+1)} f_{k\ell}^{(i)}\right) =: y^{-1} s_{k\ell}^{(0)} dx + \mathrm{d}\,\varphi_{k\ell}.$$

and we first need to show that $\sum_k \sum_\ell \varphi_{k\ell} t^\ell \in T$. Note that $f_{k\ell}^{(i)}$ is a polynomial in x of degree at most 2. The coefficient of $y^{-(2m+1)}$ in $\sum_{k,\ell} \varphi_{k\ell} t^\ell$ is $\tilde{s}_m(x) := \sum_{k,\ell} f_{k\ell}^{(m)} t^\ell$. We need to show that $(\tilde{s}_m[i])_m \in \mathcal{S}$ for each $i = 0, 1, 2$ and where $\tilde{s}_m[i]$ is the i-th coefficient as a polynomial in x. We have $f_{k\ell}^{(m)} = r^{-k} p_{k\ell}^{(m)}$ where $p_{k\ell}^{(m)}$ is a polynomial both in x and t. By Lemma 3.2.7 (i) and Lemma 3.2.14,

$$\mathrm{ord}_p(p_{k\ell}^{(m)}(t_0)[i]) \geq \mathrm{ord}_p(s_{k\ell}) - \lfloor \log_p(2k-1) \rfloor \geq \delta(k+\ell) \geq \frac{\delta}{2}(k+\ell+m)$$

for all $t_0 \in \mathbb{Z}_p^{ur}$ such that the ring of integers of $\mathbb{Q}_p(t_0)$ is $\mathbb{Z}_p[t_0]$ and thus[3]

$$\mathrm{ord}_p(p_{k\ell}^{(m)}[i]) \geq \frac{\delta}{2}(k+\ell+m).$$

[3]Suppose that $q(t) \in \mathbb{Q}_p[t]$ satisfies $\mathrm{ord}_p(q(t_0)) \geq \alpha \in \mathbb{R}$ for all such t_0. Then $\mathrm{ord}_p(q(t)) \geq \alpha$. Indeed, we may assume that $\alpha = 0$ (if not, multiply by $p^{-\lfloor \alpha \rfloor}$). Suppose that there exists $T \in \mathbb{N}$ such that $\mathrm{ord}_p(p^T q(t)) = 0$. Then $\overline{p^T q(t)}$ is a non-zero polynomial over $\mathbb{F}_p$ with infinitely many zeros in $\overline{\mathbb{F}_p}$.

Furthermore,

$$\begin{aligned}\deg_t(p_{k\ell}^{(m)}[i]) &= m\deg_t r(t) + \deg_t(r^{k-m}f_{k\ell}^{(m)}) \\ &\leq m\deg_t r(t) + (k-m)(\deg_t Q + \max\{\deg_t V, \deg_t U\}) \leq A(k+m),\end{aligned}$$

for some $A > 0$. For the first inequality, note that $r^{k-m}f_{k\ell}^{(m)}$ equals, up to multiplication by elements in $\mathbb{Q}_p$, the remainder of $r^{k-(m+1)}s_{k\ell}^{(m+1)}V$ by division (in x) by Q. Since $\deg_x(s_{k\ell}^{(m+1)}V) \leq 4$ and the coefficient of x^2 in $Q(x,t)$ is zero, it suffices to match the leading terms, so $\deg_t(r^{k-m}f_{k\ell}^{(m)}) \leq \deg_t Q + \deg_t V + \deg_t(r^{k-(m+1)}s_{k\ell}^{(m+1)})$. Similarly, since $\deg_x(s_{k\ell}^{(m+1)}U) \leq 3$ and the coefficient of x in Q' is zero,

$$\deg_t(r^{k-(m+1)}s_{k\ell}^{(m+1)}) \leq \deg_t Q + \max\{\deg_t U, \deg_t V\} + \deg_t(r^{k-(m+2)}s_{k\ell}^{(m+2)}).$$

The claim then follows inductively.

By Lemma 3.2.13, $\sum_{k\ell}\varphi_{k\ell}t^\ell \in T$. We also need to show that $y^{-1}\sum_{k,\ell}s_{k\ell}^{(0)}t^\ell \in T$. As above, we can use Kedlaya's lemma to show that the polynomial (in x and t) $r^k s_{k\ell}^{(0)}$ satisfies

$$\operatorname{ord}_p(r^k s_{k\ell}^{(0)}) \geq \delta(k+\ell).$$

Furthermore, its degree in t is bounded by a linear function in k. Thus, the proof of Lemma 3.2.13 implies the result.

For $\sum_{k=-1}^{\infty} y^{2k+1}s_k(t)x^u dx$, the operation of (RednB(t)) increases the degree in t by at most $\deg_t Q$ and by Lemmas 3.2.7 (ii) and 3.2.14, we can again find lower bounds for the valuation. Then a much simpler version of Lemma 3.2.13 completes the proof. □

Proposition 3.2.17. *The set $\mathcal{B}$ is a basis for H_{MW} over S.*

Proof. In view of Lemma 3.2.16, it suffices to show that $\mathcal{B}$ is free over S. Suppose by contradiction that for each $b \in \mathcal{B}$ there exists $s_b \in S$ such that $\sum_b s_b b = 0$ and at least one of the s_b is non-zero, say $s_{\tilde{b}}$. Since $s_{\tilde{b}}(t)$ is a non-identically zero overconvergent power series, there exists $t_0 \in \mathbb{Z}_p$ such that $s_{\tilde{b}}(t_0) \neq 0$. Then $\sum_b s_b(t_0)b(t_0) = 0$ is a non-trivial relation, contradicting the fact that $\{b(t_0) : b \in \mathcal{B}\}$ is a basis for the Monsky–Washnitzer cohomology of the fibre at t_0 (see §3.2.3.1). □

We now define an S-linear operator Frob_p on T and show that it commutes with d, hence inducing an action on H_{MW}. Furthermore, both Frob_p and d commute with partial differentiation with respect to t and this can be used to define a differential equation.

First note that over $\mathbb{F}_p$ our curve does not depend on the parameter t. Since we are working over $\mathbb{Q}_p$ and are interested in specialising at $t_0 \in \mathbb{Z}_p \subset \mathbb{Q}_p$, we define the action of Frobenius on the base ring S as the identity.

Then we want to lift the Frobenius morphism on the curve over $\mathbb{F}_p$, which is defined by $(x, y) \mapsto (x^p, y^p)$. Following Kedlaya (§3.2.3.1), we define $\mathrm{Frob}_p(x) = x^p$ and then let $\mathrm{Frob}_p(y)$ be the solution of $\mathrm{Frob}_p(y)^2 = Q(\mathrm{Frob}_p(x), t)$ (note that both Q and t are invariant under Frob_p). Thus

$$\mathrm{Frob}_p(y) = Q(x^p, t)^{1/2} = y^p \left(1 - \frac{Q(x,t)^p - Q(x^p,t)}{Q(x,t)^p}\right)^{1/2}, \quad \mathrm{Frob}_p(1/y) = 1/\mathrm{Frob}_p(y)$$

and we need to show that $\mathrm{Frob}_p(y) \in T$, or, equivalently, that $\mathrm{Frob}_p(1/y) \in T$.

In view of Assumption 3.2.10,

$$Q(x,t)^p - Q(x^p,t) = (a(t)^p - a(t))x^p + (b(t)^p - b(t)) + ph(x,t) = pP(x,t)$$

for some $h(x,t), P(x,t) \in \mathbb{Z}[x,t]$. We have $\deg_x P \leq 3p-1$ and $\deg_t P(x,t) \leq p \deg_t Q$. Therefore,

$$\mathrm{Frob}_p\left(\frac{1}{y}\right) = y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(-pP)^i}{y^{2pi}} = y^{-p} \sum_{i=0}^{\infty} \frac{p^i c_i}{y^{2pi}},$$

where c_i is an integral polynomial of degree at most $i(3p-1)$ in x and at most $ip \deg_t Q$ in t.

By repeatedly using the relation $y^2 = Q(x,t)$ to remove the term with largest degree in x, for each $i \geq 1$ we may write

$$c_i = c_1^{(i)} y^{2pi-2} + c_2^{(i)} y^{2pi-4} \cdots + c_{pi}^{(i)}, \qquad \deg_x c_j^{(i)} \leq 2$$

and hence

$$\mathrm{Frob}_p\left(\frac{1}{y}\right) = y^{-p} + \sum_{j=1}^{\infty} y^{-p-2j} \sum_{i \geq j/p} p^i c_j^{(i)}. \tag{3.12}$$

We now show inductively that

$$\deg_t c_j^{(i)} \leq \deg_t c_i + (3j-2) \deg_t Q. \tag{3.13}$$

First note that

$$Q^n = (x^3 + (a(t)x + b(t)))^n = \sum_{k=0}^{n} \binom{n}{k} x^{3(n-k)} (a(t)x + b(t))^k. \tag{3.14}$$

Thus, when $n = pi - 1$, either $c_1^{(i)} = 0$, or its leading term $a_{1,d}^{(i)} x^d$, with $d \leq 2$, has degree in t at most $\deg_t c_i$. If the leading term of $c_i - a_{1,d}^{(i)} x^d Q^{pi-1}$ is of degree greater

than or equal to $\deg_x Q^{pi-1}$, then it either comes from c_i only, in which case its degree in t is at most $\deg_t c_i$, or has a contribution from $a_{1,d}^{(i)} x^d Q^{pi-1}$. In view of (3.14), this contribution has degree in t bounded above by $\deg_t a_{1,d}^{(i)} + k \deg_t Q$, where k is maximal such that $d+3(pi-1-k)+k \geq 3(pi-1)$, that is $2k \leq d$. This shows (3.13) for $j=1$. Assume now that (3.13) holds for all $j < m$. Then, if $c_m^{(i)}$ is non-zero, the degree of its leading term is bounded above by

$$\max_{j<m}\{\deg_t c_j^{(i)} + \deg_t Q \cdot \max\{k : d+3(pi-j-k)+k \geq 3(pi-m) \text{ for some } d \leq 2\}\};$$

by the induction assumption, this is at most

$$\deg_t c_i + 3(m-1)\deg_t Q.$$

Finally, similarly to the case $j=1$, any non-zero term of $c_m^{(i)}$ has degree bounded by $\deg_t c_i + (1+3(m-1))\deg_t Q$, completing the proof by induction.

Consider the coefficient of y^{-p-2j} in (3.12). As a polynomial in x, it has degree at most 2 and we denote by $\sum_\ell d_{j\ell} t^\ell$ one of its coefficients. On the one hand, we have $\mathrm{ord}_p(d_{j\ell}) \geq j/p$. On the other hand, if $p^i c_j^{(i)}$ contributes non-trivially to $d_{j\ell}$, then using (3.13) and the inequality $\deg_t c_i \leq ip \deg_t Q$, we get

$$i \geq \frac{\ell}{p\deg_t Q} + \frac{2}{p} - \frac{3}{p}j.$$

Therefore,

$$\begin{aligned}\mathrm{ord}_p(d_{j\ell}) \geq \max\left\{\frac{j}{p}, \frac{\ell}{p\deg_t Q} + \frac{2}{p} - \frac{3}{p}j\right\} &\geq \frac{j}{2p} + \frac{1}{12}\left(\frac{\ell}{p\deg_t Q} + \frac{2}{p} - \frac{3}{p}j\right) \\ &= \frac{j}{4p} + \frac{\ell}{12p\deg_t Q} + \frac{1}{6p}\end{aligned}$$

and hence $\mathrm{Frob}_p(1/y) \in T$.

Let $\nabla = \frac{\partial}{\partial t} dt$ on T. Extend the definition of Frob_p to dx and dt by $\mathrm{Frob}_p(dx) = p dx^{p-1}$ and $\mathrm{Frob}_p(dt) = dt$. Then

Lemma 3.2.18. *We have the following commutative diagrams*

$$\begin{array}{ccc} T & \xrightarrow{\mathrm{d}} & Tdx \\ {\scriptstyle \mathrm{Frob}_p}\downarrow & & \downarrow{\scriptstyle \mathrm{Frob}_p} \\ T & \xrightarrow{\mathrm{d}} & Tdx \end{array} \qquad \begin{array}{ccc} T & \xrightarrow{\mathrm{d}} & Tdx \\ {\scriptstyle \nabla}\downarrow & & \downarrow{\scriptstyle \nabla} \\ T & \xrightarrow{\mathrm{d}} & Tdx \end{array} \qquad \begin{array}{ccc} T & \xrightarrow{\nabla} & Tdt \\ {\scriptstyle \mathrm{Frob}_p}\downarrow & & \downarrow{\scriptstyle \mathrm{Frob}_p} \\ T & \xrightarrow{\nabla} & Tdt. \end{array}$$

Proof. Each operator is $\mathbb{Q}_p$-linear. The differential operators d and ∇ are independent an hence commute. For the two remaining diagrams, since Frob_p respects the ring structure and ∇ and d satisfy the chain rule, it is enough to show commutativity on t and x, which follows from our definition of Frob_p on dx and dt. □

From this and the fact that the hyperelliptic involution commutes with the action of Frobenius, we obtain the commutative diagram

$$\begin{array}{ccc} H^-_{MW} & \xrightarrow{\nabla} & H^-_{MW}dt \\ {\scriptstyle \mathrm{Frob}_p}\downarrow & & \downarrow{\scriptstyle \mathrm{Frob}_p} \\ H^-_{MW} & \xrightarrow{\nabla} & H^-_{MW}dt, \end{array} \tag{3.15}$$

where H^-_{MW} is the S-submodule of H_{MW} spanned by $\{\frac{dx}{y}, \frac{xdx}{y}\}$.

Let $F(t)$ (resp. $G(t)$) be the matrix of the action of Frobenius (resp. of the connection ∇) on H^-_{MW} with respect to the basis $\{\frac{dx}{y}, \frac{xdx}{y}\}$. We view F and G as acting from the left.

A matrix $M(t)$ in the ring of 2×2 matrices over $\mathbb{Q}_p[[t]]$ is a solution to the differential equation

$$\frac{d}{dt}M(t) + G(t)M(t) = 0 \tag{3.16}$$

if and only if its columns are zeros of ∇ (where we have possibly base-extended from S to $\mathbb{Q}_p[[t]]$). It is easy to check that there is a unique solution $J(t)$ to (3.16) with $J(0) = I$ and that any other solution $M(t)$ to (3.16) satisfies $M(t) = J(t)H$ for some constant matrix H (see also [88], [87] and [71]). Since Frobenius acts trivially on t and $\mathbb{Q}_p$ and commutes with ∇ by (3.15), the columns of $F(t)J(t)$ are solutions to $\nabla = 0$; thus,

$$F(t) = J(t)F(0)J(t)^{-1}, \tag{3.17}$$

where $F(0)$ and $J(t)$ can be computed using Kedlaya's and Lauder's algorithm, respectively.

Let $F(t) = \left(\begin{smallmatrix} A(t) & B(t) \\ C(t) & D(t) \end{smallmatrix}\right)$. We have already shown that the entries of $F(t)$ belong to S and it is also clear that at $t_0 \in \mathbb{Z}_p$ the matrix $F(t_0)$ equals the matrix of Frobenius computed by Kedlaya's algorithm on $\mathcal{E}_{t_0}$.

Remark 3.2.19. The formula of (3.17) is consistent with Remark 3.2.6: for each $t_0 \in \mathbb{Z}_p$, there is a basis for the Monsky–Washnitzer cohomology of $\mathcal{E}_{t_0}$ with respect to which the matrix of Frobenius is $F(0)$. The computation of the matrix $J(t)$ is an intermediate step also in Lauder's algorithm and is carried out identically here; in particular, Assumption 3.2.10 does not lead to any simplification. The only difference is that while in our case the entries of the matrix $J(t)F(0)J(t)^{-1}$ are power series convergent on a disk slightly larger than the closed unit disk, the analogue in Lauder's algorithm returns the Frobenius matrix as a matrix over $\mathbb{Q}_p[[t]]$ and further work is needed to recover its representation as a matrix over the base ring S of that setting.

Lemma 3.2.20. $A(t), C(t) \in p\mathbb{Z}_p\langle t\rangle^\dagger$, $C(t), D(t) \in \mathbb{Z}_p\langle t\rangle^\dagger$.

Proof. By Lemma 3.2.8, $A(t_0), C(t_0) \in p\mathbb{Z}_p$ and $B(t_0), D(t_0) \in \mathbb{Z}_p$ for all $t_0 \in \mathbb{Z}_p$. For $t_0 \in \mathbb{Z}_p^{ur\times} \setminus \mathbb{Z}_p$, the matrix $F(t)$ does not specialise to the matrix of Frobenius on $\mathcal{E}_{t_0}$, as Frobenius does not act trivially on t_0. However, the proof of Lemma 3.2.8 goes through also for this different operator, as $Q(x^p, t_0) - Q(x, t_0)^p$ is divisible by p and has degree at most $3p-1$. We show the claim of the lemma for $A(t) = p\sum_{k=0}^{\infty} b_k t^k \in \mathbb{Z}_p\langle t\rangle^\dagger \otimes \mathbb{Q}_p$. Let $K \in \mathbb{Z}_{\geq 0}$ minimal such that $\mathrm{ord}_p(b_k) \geq 1$ for all $k \geq K$ and let $T = \min_{0\leq k<K}\{\mathrm{ord}_p(b_k)\}$. If $T \leq -1$, then $p^{-T}\sum_{k=0}^{K-1} b_k t^k$ reduces modulo p to a non-zero polynomial over $\mathbb{F}_p$ with infinitely many roots in $\overline{\mathbb{F}_p}$. □

In practice, we always work with a stronger assumption than Assumption 3.2.10, that is:

Assumption 3.2.21. The coefficients of the Weierstrass equation for $\mathcal{E}$ are polynomials in $\mathbb{Z}[pt]$.

Suppose now, in addition, that p is ordinary for $\mathcal{E}_0$ and for a positive integer N write

$$F(t)^N = \begin{pmatrix} A_N(t) & B_N(t) \\ C_N(t) & D_N(t) \end{pmatrix}.$$

If $B_N(t) = \sum_{n=0}^{\infty} h_n t^n$ and $D_N(t) = \sum_{n=0}^{\infty} e_n t^n$ $(h_n, e_n \in \mathbb{Z}_p)$, then $B_N(t)/D_N(t) = \sum_{n=0}^{\infty} d_n t^n$ where

$$d_n = \frac{1}{e_0}\left(h_n - \sum_{k=1}^{n} e_k d_{n-k}\right).$$

By Lemma 3.2.9, $\mathbf{E}_2(\mathcal{E}_{t_0}, \omega_{t_0}) \equiv -12B_N(t_0)/D_N(t_0) \bmod p^N$ for all $t_0 \in \mathbb{Z}_p$ and by Remark 3.2.4, the n-th coefficient of $\mathbf{E}_2(\mathcal{E}, \omega) \in \mathbb{Z}_p[[t]]$ has valuation greater than or equal to n. Furthermore, e_0 is a p-adic unit by the discussion preceding Lemma 3.2.9. Therefore,

Lemma 3.2.22.

$$-12\frac{B_N(t) \bmod (p^N, t^N)}{D_N(t) \bmod (p^N, t^N)} \equiv \mathbf{E}_2(\mathcal{E}, \omega) \bmod p^N\mathbb{Z}_p[[t]] \equiv \mathbf{E}_2(\mathcal{E}, \omega) \bmod (p, pt)^N\mathbb{Z}_p[[pt]].$$

3.2.4 The p-adic height

As in the end of the previous subsection, we suppose here that p is a prime of good ordinary reduction for the fibre of $\mathcal{E}$ above 0 and work under Assumption 3.2.21, until stated otherwise.

Let $Q \in \mathcal{E}^\circ(\mathbb{Q}(t))$; assume that Q has everywhere good reduction and that the specialisation Q_{t_0} belongs to the formal group of $\mathcal{E}_{t_0}$ at p, for each t_0 in $\mathbb{Z}$. Then

$$h_p(Q) := \begin{cases} 0 & \text{if } Q \text{ is torsion,} \\ -2\log\left(\frac{\gamma(Q,t)\sigma_p(Q)}{d(Q)}\right) & \text{otherwise} \end{cases} \tag{3.18}$$

satisfies $h_p(Q)(t_0) = h_p(Q_{t_0})$ for all $t_0 \in \mathbb{Z}$, where $h_p(Q_{t_0})$ is the Mazur–Tate p-adic height of Q_{t_0} (see §2.2.3). By (3.5) and the properties of the p-adic sigma function and the denominator, h_p is a quadratic function on its domain of definition.

By Tate's algorithm, the index of $\mathcal{E}^\circ(\mathbb{Q}(t))$ in $\mathcal{E}(\mathbb{Q}(t))$ is finite; furthermore the subgroup of points lying in the formal group at p on the fibres is also of finite index.

In order to extend h_p to a quadratic function on $\mathcal{E}(\mathbb{Q}(t))$ via the relation

$$h_p(mP) = m^2 \cdot h_p(P) \quad \text{for all } m \in \mathbb{Z}, \tag{3.19}$$

we also need to be able to find, for each $P \in \mathcal{E}(\mathbb{Q}(t))$, a multiple which has everywhere good reduction. By [146, Proposition 6], this is always possible if no fibre $\mathcal{E}_{t_0}$ for $t_0 \in \mathbb{Z}$ is of multiplicative type.

Let $\mathcal{E}'$ be the Weierstrass equation obtained from our fixed equation for $\mathcal{E}$ by the linear change of variable $t \mapsto t/p$. By Assumption 3.2.21, the Weierstrass coefficients of $\mathcal{E}'$ belong to $\mathbb{Z}[t]$. Consider the point $Q' \in \mathcal{E}'(\mathbb{Q}(t))$ corresponding to the point $Q \in \mathcal{E}(\mathbb{Q}(t))$ considered above. We have

$$\frac{a(Q)(t)}{d(Q)^2(t)} = \frac{a(Q')(pt)}{d(Q')(pt)^2}.$$

Suppose that $q(t) \in \mathbb{Z}[t]$ divides $a(Q')(pt)$ and $d(Q')(pt)$. Then $\tilde{q}(pt) := p^{\deg q} q(t)$ divides $a(Q')(pt)$ and $d(Q')(pt)$ in $\mathbb{Q}[t]$. By Gauss's lemma and since $a(Q')$, $d(Q')$ are coprime in $\mathbb{Z}[t]$, $\tilde{q}(t)$ must be constant and then, if not a unit, a power of p. So if $\gamma(Q', 0)$ is not divisible by p, then

$$a(Q)(t) = a(Q')(pt),\ b(Q)(t) = b(Q')(pt),\ d(Q)(t) = d(Q')(pt) \in \mathbb{Z}[pt].$$

Proposition 3.2.23. *With the notation as above, suppose that $\gamma(Q,t)$ is constant for $t \in \mathbb{Z}$ and that $\gamma(Q', 0) \in \mathbb{Z}_p^\times$. Then $h_p(Q)$ is a power series in $\mathbb{Z}_p[[t]]$. Furthermore, if $h_p(Q) = \sum_{n=0}^\infty c_n t^n$, then*

$$\mathrm{ord}_p(c_n) \geq n - \mathrm{ord}_p(n) \quad \text{for all } n \geq 0 \quad \text{and} \quad \mathrm{ord}_p(c_0) \geq 1. \tag{3.20}$$

Proof. By Remark 3.2.4, $\sigma_p(T) = T + \cdots \in \mathbb{Z}_p[[pt]][[T]]$. By the discussion preceding the proposition, we have $a(Q), b(Q), d(Q) \in \mathbb{Z}[pt]$ with $a(Q)(0)$ and $b(Q)(0)$ both not divisible by p.

Thus, as a power series, $\frac{a(Q)}{b(Q)} \in \mathbb{Z}_p[[pt]]^\times$ and we have

$$\sigma_p(Q) = \sigma_p\left(-\frac{x(Q)}{y(Q)}\right) = \sigma_p\left(-\frac{a(Q)d(Q)}{b(Q)}\right) = -\frac{a(Q)}{b(Q)}d(Q) + f(pt)d(Q)^2,$$

for some $f(pt) \in \mathbb{Z}_p[[pt]]$. Since the specialisations of Q all belong to the formal group at p, then $\frac{\gamma\sigma_p(Q)}{d(Q)} = c(1 + b_1(pt) + b_2(pt)^2 + \cdots) \in \mathbb{Z}_p[[pt]]^\times$ and

$$h_p(Q) = -2\bigg(\log(c) + \sum_{m=1}^{\infty}(-1)^{m+1}\frac{(\sum_{n=1}^{\infty} b_n(pt)^n)^m}{m}\bigg).$$

This shows the claim on the constant term, as the image of the p-adic logarithm on $\mathbb{Z}_p^\times$ is $p\mathbb{Z}_p$. Fix $k \geq 1$ and let b'_m be the coefficient of $(pt)^k$ in $\left(\sum_{n=1}^{k} b_n(pt)^n\right)^m$. Then the coefficient of $(pt)^k$ in $h_p(Q)$ equals

$$-2\sum_{m=1}^{k}\frac{(-1)^{m+1}b'_m}{m}.$$

Now, b'_m is a sum of terms of the form

$$\binom{m}{r_1, \ldots, r_k}\prod_{n=1}^{k} b_n^{r_n}, \quad \text{where } r_1, \ldots, r_k \geq 0, \quad \sum_{n=1}^{k} r_n = m \quad \text{and} \quad \sum_{n=1}^{k} n r_n = k;$$

here $\binom{m}{r_1,\ldots,r_k}$ is the multinomial coefficient $\frac{m!}{r_1!\cdots r_k!}$. Let $s \in \{1, \ldots, k\}$ such that $\min_n(\mathrm{ord}_p(r_n)) = \mathrm{ord}_p(r_s)$. Then $\mathrm{ord}_p(k) \geq \mathrm{ord}_p(r_s)$. By Kummer's Theorem on the p-adic valuation of binomial coefficients [84] we have

$$\mathrm{ord}_p\binom{m}{r_s} \geq \mathrm{ord}_p(m) - \mathrm{ord}_p(r_s);$$

since $\binom{m}{r_s}$ divides $\binom{m}{r_1,\ldots,r_k}$ we conclude that $\mathrm{ord}_p(b'_m/m) \geq -\mathrm{ord}_p(k)$, which completes the proof. □

Remark 3.2.24. For a general $Q \in \mathcal{E}(\mathbb{Q}(t))$, we must subtract from the lower bounds of Proposition 3.2.23 the valuation of m^2, where m is minimal such that $mQ \in \mathcal{E}^\circ(\mathbb{Q}(t))$ has everywhere good reduction and Q_{t_0} belongs to the formal group of $\mathcal{E}_{t_0}$ at p, for each t_0 in $\mathbb{Z}$. For example, if p is an anomalous prime (i.e. $p \mid \#\overline{\mathcal{E}}(\mathbb{F}_p)$) then we could have $p \mid m$. Theorem 3.1.1 follows.

Corollary 3.2.25. *With the notation as in Proposition 3.2.23, suppose $h_p(Q)$ is not identically zero and $n = \mathrm{ord}_p(c_0) < \infty$. Then there are at most N values of $t_0 \in \mathbb{Z}$ for which $h_p(Q_{t_0}) = 0$, where N is the smallest integer for which $\mathrm{ord}_p(m) < m - n$ for all $m > N$.*

Proof. This is straightforward from Newton polygon considerations. □

Proposition 3.2.26. *Suppose that $a_1 = 0$ and let $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$ be a point of everywhere good reduction and which specialises to a torsion point P_0 at $t = 0$. Assume that $\gamma(P', t) = 1$, where $P' \in \mathcal{E}'(\mathbb{Q}(t))$ corresponds to P. Then the p-adic height of P is a power series in t with vanishing constant term and coefficient of t equal to*

$$c_1 = -\frac{2}{m^2}\left(\frac{\alpha_1\beta_0 - \alpha_0\beta_1}{\alpha_0\beta_0}\right) \in \mathbb{Q},$$

where m is the additive order of P_0 and $mP = \left(\frac{a(mP)}{d(mP)^2}, \frac{b(mP)}{d(mP)^3}\right)$ with $a(mP) = \sum_{i\geq 0}\alpha_i t^i$ and $b(mP) = \sum_{i\geq 0}\beta_i t^i$. In particular, c_1/p is independent of p and belongs to $N^{-1}\mathbb{Z}$, where N is an integer whose prime factors are $2, 3$, the anomalous primes and the primes which are not of good ordinary reduction for the fibre at $t = 0$.

Proof. Since $(mP)_0$ is the point at infinity, the point $(mP)_{t_0}$ belongs to the formal group at p for each $t_0 \in \mathbb{Z}$ and the parameter $T(mP) = -\frac{x(mP)}{y(mP)}$ for the formal group at mP is a power series in t with rational coefficients and vanishing constant term. Its coefficients as a series in the variable $s = pt$ are independent of p. Since by assumption $\mathcal{E}$ is given by a Weierstrass equation with vanishing a_1-invariant, the p-adic sigma function $\sigma_p(T)$ has coefficient of T^2 equal to zero (cf. proof of Proposition 2.2.3). Thus, evaluating σ_p at $T(mP)$ gives a power series in t whose coefficient of t and t^2 agree with the respective coefficients in $T(mP)$. It follows that $\frac{\sigma_p(T(mP))}{d(mP)} = -\frac{x(mP)}{y(mP)d(mP)} + O(t^2) = -\frac{a(mP)}{b(mP)} + O(t^2)$. Since $(mP)_0 = O$, the constant term of this series is ± 1 and its logarithm is hence 0. Indeed, $t \mid d(mP)$, so if $q \mid a(mP)(0)$ then $q \mid \gamma(P, q)$. Normalising by the constant term, taking the p-adic logarithm and finally multiplying by $-2m^{-2}$ yields the statement of the proposition. □

For the next two theorems, we go back to the general $\mathcal{E}$ of (3.4) (i.e. Assumption 3.2.21 is not needed). Let K be a number field of class number 1 with ring of integers $\mathcal{O}_K$. Let $P \in \mathcal{E}^\circ(\mathbb{Z}[t])$ such that P_{t_0} has everywhere good reduction for all $t_0 \in \mathcal{O}_K$.

Given $\alpha \in \mathbb{Z}$ and $R \in \mathcal{E}(\mathbb{Q}(t))$, we denote by $\mathcal{E}^{(\alpha)}$ the family $\mathcal{E}_{pt+\alpha}$ (as in Section 3.1) and by $R^{(\alpha)}$ the point $(x(R)(pt + \alpha), y(R)(pt + \alpha)) \in \mathcal{E}^{(\alpha)}(\mathbb{Q}(t))$.

Theorem 3.2.27. *Let $p \geq 5$ be a prime which splits completely in K and denote by $\psi_1, \ldots, \psi_n$ the embeddings of K into $\mathbb{Q}_p$. Suppose $t_0 \in \mathcal{O}_K$ is such that $\mathcal{E}_{\psi_i(t_0)}$ has good ordinary reduction at p for all $1 \leq i \leq n$. Then*

$$[K\colon \mathbb{Q}]h_p(P_{t_0}) = \sum_{i=1}^{n} h_p(P^{(\alpha_i)}) \left(\psi_i\left(\frac{t_0 - \alpha_i}{p}\right)\right),$$

where $\alpha_i \in \mathbb{Z}$ is such that $\psi_i(t_0) \equiv \alpha_i \bmod p$. Here $h_p(P^{(\alpha_i)})$ is the power series computed by Theorem 3.1.1 with a replaced by α_i.

Proof. Let $m \in \mathbb{N}$ such that mP_{t_0} belongs to the formal group at all primes π_i, $i = 1, \ldots, n$, of K above p. Note that the assumptions that K is of class number 1 and that P_{t_0} has good reduction at all primes of $\mathcal{O}_K$ imply, by (2.9), that

$$[K\colon \mathbb{Q}]h_p(P_{t_0}) = -\frac{2}{m^2} \log\left(\prod_{i=1}^{n} N_{K_{\pi_i}/\mathbb{Q}_p}\left(\frac{\sigma_{\pi_i}(mP_{t_0})}{d(mP_{t_0})}\right)\right).$$

In principle, $d(mP_{t_0})$ is well-defined only up to multiplication by elements of $\mathcal{O}_K^\times$, but taking norms guarantees that $h_p(P_{t_0})$ is independent of the choice. In particular, we can take $d(mP_{t_0}) = d(mP)(t_0)$, which equals $f_m(P_{t_0}) = f_m(P)(t_0)$ up to multiplication by ± 1, where f_m denotes the m-th division polynomial. Then we have $[K\colon \mathbb{Q}]h_p(P_{t_0}) = \sum_{i=1}^{n} h_{\pi_i}(P_{t_0})$, where

$$h_{\pi_i}(P_{t_0}) = -\frac{2}{m^2} \log\left(\frac{\psi_i(\sigma_{\pi_i}(mP_{t_0}))}{d(mP)(\psi_i(t_0))}\right).$$

For each i, let $m_i \in \mathbb{N}$ such that $m_i \mid m$ and $m_i P_{t_0}$ lies in the formal group at π_i, or equivalently, such that $m_i P^{(\alpha_i)}$ reduces to O in $\overline{\mathcal{E}_{\alpha_i}}(\mathbb{F}_p)$. Then

$$\begin{aligned} d(mP)(t) = \pm d(mP^{(\alpha_i)})\left(\frac{t-\alpha_i}{p}\right) &= \pm f_m(P^{(\alpha_i)})\left(\frac{t-\alpha_i}{p}\right) \\ &= \pm (f_{m_i}(P^{(\alpha_i)})^{(m/m_i)^2} f_{m/m_i}(m_i P^{(\alpha_i)}))\left(\frac{t-\alpha_i}{p}\right) \end{aligned}$$

by Definition 2.2.1 and

$$\begin{aligned} \psi_i(\sigma_{\pi_i}(mP_{t_0})) = \sigma_p(mP^{(\alpha_i)})\left(\frac{t-\alpha_i}{p}\right)\Bigg|_{t=\psi_i(t_0)} \\ = (\sigma_p(m_i P^{(\alpha_i)})^{(m/m_i)^2} f_{m/m_i}(m_i P^{(\alpha_i)}))\left(\frac{t-\alpha_i}{p}\right)\Bigg|_{t=\psi_i(t_0)} \end{aligned}$$

by Lemma 2.2.4 (ii). Therefore,

$$h_{\pi_i}(P_{t_0}) = \left(-\frac{2}{m_i^2} \log\left(\frac{\sigma_p(m_i P^{(\alpha_i)})}{d(m_i P^{(\alpha_i)})}\right)\right)\left(\psi_i\left(\frac{t_0 - \alpha_i}{p}\right)\right),$$

as desired. □

Theorem 3.2.28. *Let $t_0 \in \mathcal{O}_K$ and suppose that there exists an embedding $\psi\colon K \hookrightarrow \mathbb{Q}_p$ such that $\mathcal{E}_{\psi(t_0)}$ has good ordinary reduction at p. Let $\alpha \in \mathbb{Z}$ such that $\psi(t_0) \equiv \alpha \bmod p$. Then $h_p(P^{(\alpha)})\left(\frac{\psi(t_0)-\alpha}{p}\right)$ is quadratic up to multiples of logarithms of elements in $\mathcal{O}_K^\times$, in the sense that, if $Q \in \mathcal{E}^\circ(\mathbb{Z}[t])$ satisfies the same assumptions as P and there exists $m, n \in \mathbb{Z}$ such that $mQ_{t_0} = nP_{t_0}$, then*

$$n^2 h_p(P^{(\alpha)})\left(\frac{\psi(t_0)-\alpha}{p}\right) = 2c^2\log(\psi(u)) + m^2 h_p(Q^{(\alpha)})\left(\frac{\psi(t_0)-\alpha}{p}\right)$$

for some $c \in \mathbb{Q}$ and $u \in \mathcal{O}_K^\times$. In particular, if K is imaginary quadratic, then

$$n^2 h_p(P^{(\alpha)})\left(\frac{\psi(t_0)-\alpha}{p}\right) = m^2 h_p(Q^{(\alpha)})\left(\frac{\psi(t_0)-\alpha}{p}\right).$$

Proof. The theorem follows from the properties of the p-adic sigma function and of the denominator of a point, which is a well-defined element of $\mathcal{O}_K$ only up to multiplication by units. □

3.3 Examples and applications

3.3.1 Height computations

The first two p-adic heights that we compute implementing the algorithm of §3.2 in `Magma` [36] are also calculated in [146, p. 35] (at a lower precision and with a different normalisation: see Remark 2.2.8).

Example 3.3.1. Consider

$$\mathcal{E}\colon y^2 + y = x^3 + (13t-1)x, \qquad P = (0,0) \in \mathcal{E}^\circ(\mathbb{Q}(t))$$

and let $p = 13$, which is of good ordinary reduction for $\mathcal{E}_{t_0}$ for all $t_0 \in \mathbb{Z}_p$. We have $\mathbf{E}_2(\mathcal{E},\omega) = \frac{1}{2^2}\mathbf{E}_2(\mathcal{E}',\omega')$, where

$$\mathcal{E}'\colon y'^2 = x'^3 + 16(13t-1)x' + 16, \qquad \omega' = \frac{dx'}{y'}.$$

Using the algorithm of §3.2.3.2, we find

$$\begin{aligned}\mathbf{E}_2(\mathcal{E},\omega) = {} & -374760905 + O(13^8) - (11820768\cdot 13 + O(13^9))\cdot t \\ & + (406858327\cdot 13^2 + O(13^{10}))\cdot t^2 + (262589076\cdot 13^3 + O(13^{11}))\cdot t^3 \\ & + (99777012\cdot 13^4 + O(13^{12}))\cdot t^4 - (185530083\cdot 13^5 + O(13^{13}))\cdot t^5 \\ & - (314221733\cdot 13^6 + O(13^{14}))\cdot t^6 - (91501177\cdot 13^7 + O(13^{15}))\cdot t^7 \\ & + (271042270\cdot 13^8 + O(13^{16}))\cdot t^8 - (46702117\cdot 13^9 + O(13^{17}))\cdot t^9 \\ & + O(13^{10}).\end{aligned}$$

Since the point P has everywhere good reduction, by Proposition 3.2.1 any multiple of P has γ-factor equal to ± 1. Furthermore $Q_{t_0} = (16 \cdot P)_{t_0}$ belongs to the formal group at p for all $t_0 \in \mathbb{Z}$. Therefore

$$h_p(P) = \frac{1}{16^2} h_p(Q),$$

where $h_p(Q)$ may be computed as in §3.2.4. We find

$$\begin{aligned} h_p(P) = {} & 300142556 \cdot 13^2 + O(13^{10}) + (5013199330 \cdot 13 + O(13^{10})) \cdot t \\ & - (342928063 \cdot 13^2 + O(13^{10})) \cdot t^2 + (18197876 \cdot 13^3 + O(13^{10})) \cdot t^3 \\ & + (323932 \cdot 13^4 + O(13^{10})) \cdot t^4 - (123559 \cdot 13^5 + O(13^{10})) \cdot t^5 \\ & + (480 \cdot 13^7 + O(13^{10})) \cdot t^6 + (523 \cdot 13^7 + O(13^{10})) \cdot t^7 \\ & - (59 \cdot 13^8 + O(13^{10})) \cdot t^8 - (4 \cdot 13^9 + O(13^{10})) \cdot t^9 + O(13^{10}). \end{aligned}$$

Example 3.3.2. Consider

$$\mathcal{E} \colon y^2 = x^3 - (10t+1)^2 x + (10t+1)^2, \qquad P = (10t+1, 10t+1) \in \mathcal{E}(\mathbb{Q}(t))$$

and let $p = 5$. The point P has bad reduction at 2, but $3P$ is in $\mathcal{E}^\circ(\mathbb{Q}(t))$ and has everywhere good reduction. Explicitly, we have

$$3P = \left(\frac{250t^3 + 25t^2 - 10t}{25t^2 - 10t + 1}, \frac{3750t^4 - 375t^3 - 75t^2 + 1}{125t^3 - 75t^2 + 15t - 1} \right).$$

We cannot use Proposition 3.2.1 to compute $\gamma(3P, t)$, as $P \notin \mathcal{E}^\circ(\mathbb{Q}(t))$. Nevertheless, we notice that $a(3P) - (50t^2 + 15t + 1) d(3P) = 1$, where we have chosen $d(3P) = 5t - 1$. Thus $\gamma(3P, t) = \pm 1$ and, by (3.5), $\gamma(3mP, t) = \pm 1$ for all non-zero integers m. The specialisations of $Q = 8(3P)$ belong to the formal group at p on all the fibres. We obtain

$$\begin{aligned} h_p(P) = {} & -3960818 \cdot 5 + O(5^{11}) + (2145011 \cdot 5 + O(5^{11})) \cdot t - (884578 \cdot 5^2 + O(5^{11})) \cdot t^2 \\ & - (13204 \cdot 5^3 + O(5^{11})) \cdot t^3 + (5267 \cdot 5^5 + O(5^{11})) \cdot t^4 + (35441 \cdot 5^4 + O(5^{11})) \cdot t^5 \\ & - (432 \cdot 5^6 + O(5^{11})) \cdot t^6 + (34 \cdot 5^7 + O(5^{11})) \cdot t^7 - (56 \cdot 5^8 + O(5^{11})) \cdot t^8 \\ & + (5^{10} + O(5^{11})) \cdot t^9 - (3 \cdot 5^9 + O(5^{11})) \cdot t^{10} + O(5^{11}). \end{aligned}$$

In Examples 3.3.1 and 3.3.2, the γ-factor is constant (and in fact trivial). This is not always the case, as the following example shows.

Example 3.3.3. Consider the family

$$\mathcal{E} \colon y^2 = x^3 - (37t+1)^2 x + 1,$$

with discriminant $\Delta(t) = 16(4(37t+1)^6 - 27)$. Let $P = (0,1) \in \mathcal{E}(\mathbb{Q}(t))$ and $p = 37$. The point P_{t_0} has non-singular reduction at every prime if t_0 is even and has singular reduction at 2 if t_0 is odd. Note that $P \in \mathcal{E}^\circ(\mathbb{Q}(t))$ as P is non-singular modulo 2. By Proposition 3.2.1, then $\gamma(mP, 2t_0) = 1$ for all t_0 in $\mathbb{Z}$ and $\gamma(mP, 2t_0+1)$ is a power of 2. The point $3P$ is of everywhere good reduction. Letting $t = 2r+1$, we see that $a(3P)(r) = 2^6 \cdot q(r)$, $d(3P)(r)^2 = 2^8 \cdot s(r)$, where $2 \nmid q(r)$ for all $r \in \mathbb{Z}$. Thus $\gamma(3P, 2t_0+1) = 2^3$. The point $Q = 12P$ belongs to the formal group at p and we find

$$\begin{aligned} h_p(P) = \alpha &- (458517 \cdot 37 + O(37^5)) \cdot t - (18110 \cdot 37^2 + O(37^5)) \cdot t^2 \\ &- (355 \cdot 37^3 + O(37^5)) \cdot t^3 - (9 \cdot 37^4 + O(37^5)) \cdot t^4 + O(37^5), \end{aligned}$$

where $\alpha = \begin{cases} 931191 \cdot 37 + O(37^5) & \text{if } t \text{ is even,} \\ 255288 \cdot 37 + O(37^5) & \text{if } t \text{ is odd.} \end{cases}$

3.3.2 Applications to non-degeneracy

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{Q}(t)$, let p be a prime of good ordinary reduction for the fibre $\mathcal{E}_0$ and work under Assumption 3.2.21.

Suppose that $P_{(1)}, \ldots, P_{(n)} \in \mathcal{E}^\circ(\mathbb{Q}(t))$ are linearly independent points with everywhere good reduction. Using the algorithm of Section 3.2, we can compute a power series $\mathrm{Reg}_p(P_{(1)}, \cdots, P_{(n)})$ interpolating the values $\mathrm{Reg}_p(P_{(1)t_0}, \ldots, P_{(n)t_0})$ defined by (2.11) as t_0 ranges through the integers. Furthermore, Proposition 3.2.23 and Remark 3.2.24 give lower bounds for the valuation of the coefficients of $\mathrm{Reg}_p(P_{(1)}, \ldots, P_{(n)})$ and we can thus apply the theory of Newton polygons to study its zeros.

Assume now that $P_{(1)}, \ldots, P_{(n)}$ generate a subgroup of finite index in $\mathcal{E}(\mathbb{Q}(t))$. If $\mathcal{E}$ is $\mathbb{Q}$-rational (resp. $\mathbb{Q}$-unirational) and non-isotrivial, it was shown by Billard [32] (resp. Salgado [114]) that there are infinitely many $t_0 \in \mathbb{Q}$ for which the fibre $\mathcal{E}_{t_0}$ is an elliptic curve whose Mordell–Weil rank is strictly larger than n.

Thus, if we can prove that $\mathrm{Reg}_p(P_{(1)}, \cdots, P_{(n)})$ has no zeros in $\mathbb{Z}$ outside of the exceptional set of Theorem 3.1.4, we will provide evidence for Conjecture 2.3.1 for all those fibres whose Mordell–Weil rank over $\mathbb{Q}$ does not exceed the rank of $\mathcal{E}(\mathbb{Q}(t))$, but we expect that for infinitely many fibres we will gather evidence only for Conjecture 2.3.2 for the subgroup generated by the points at which the fibre meets $P_{(1)}, \ldots, P_{(n)}$.

We now prove the result (ND) stated in the introduction to this chapter.

Example 3.3.4. Consider the curve from Example 3.3.3. There are other obvious global points besides P, namely $Q = (-1, (37t+1))$ and $R = (-(37t+1), 1)$.

We show by means of Nagao's formula[4] (see Conjecture 3.1.5, Theorem 3.1.6 and (3.3)) that the generic rank over $\mathbb{Q}(t)$ is 3. We have

$$\operatorname{rank}(\mathcal{E}(\mathbb{Q}(t))) = \lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{\log_{\mathbb{R}} p}{p} \sum_{x=0}^{p-1} \sum_{t_0=0}^{p-1} \left(\frac{(-37^2x)t_0^2 - (74x)t_0 + x^3 - x + 1}{p} \right),$$

where the brackets on the right indicate the Legendre symbol. The t_0-sum is equal to p if $x = 0$; the discriminant of the quadratic polynomial $(-37^2x)t_0^2-(74x)t_0+x^3-x+1$ is $4\cdot 37^2x(x+1)(x^2-x+1)$. Denote by δ_p one of the roots, if there are any, of x^2-x+1 over $\mathbb{F}_p$. Note that δ_p is a square in $\mathbb{F}_p$ if and only if its conjugate is also a square, as their product is 1. Using a standard Legendre identity[5], we find that

$$\begin{aligned}\operatorname{rank}(\mathcal{E}(\mathbb{Q}(t))) &= \lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{\log_{\mathbb{R}} p}{p} \left(2p + p \sum_{x^2-x+1\equiv 0} \left(\frac{-x}{p}\right) - \sum_{x=1}^{p-1} \left(\frac{-x}{p}\right) \right) \\ &= 2 + 2 \lim_{X\to\infty} \frac{1}{X} \sum_{\substack{p\le X \\ \left(\frac{-3}{p}\right)=1}} \log_{\mathbb{R}} p \left(\frac{-\delta_p}{p}\right) = 3\end{aligned}$$

by the Prime Number Theorem, as, if $-\delta_p \in \mathbb{F}_p$, then $-\delta_p = (\delta_p - 1)^2 \in \mathbb{F}_p^{\times 2}$ and the proportion of primes counted in the last sum is $1/2$. See also [105, Lemmas 2.2, 2.3]. An explicit computation of the canonical height pairing matrix on $\{P, Q, R\}$ gives $\begin{pmatrix} 1 & 0 & -1/2 \\ 0 & 1 & -1/2 \\ -1/2 & -1/2 & 1 \end{pmatrix}$, which has determinant $1/2 \neq 0$. Therefore P, Q, R are linearly independent non-torsion global points[6] in $\mathcal{E}(\mathbb{Q}(t))$ and hence they span a subgroup of $\mathcal{E}(\mathbb{Q}(t))$ of maximal rank.

We first compute the heights of Q and $P + Q$, from which we would be able to deduce the discriminant of the p-adic height pairing restricted to the free subgroup of $\mathcal{E}(\mathbb{Q}(t))$ generated by the points P, Q. Suppose q is a prime at which the point Q_{t_0} has singular reduction, for some $t_0 \in \mathbb{Z}$. Then either $q = 2$ or $37t_0 + 1 \equiv 0 \bmod q$. If $q = 2$ it is clear that the reduction of Q_{t_0} is singular if and only if t_0 is even. If $37t_0 + 1 \equiv 0 \bmod q$, then the discriminant of $\mathcal{E}_{t_0}$ satisfies $\Delta(t_0) \equiv -2^4 \cdot 3^3 \bmod q$ and hence if q is an odd prime of bad reduction, then q must be equal to 3. It is easy to

[4]Only after doing this computation did the author become aware of the fact that also Eikenberg's thesis [57, Theorem 5.1.1] and Tadić's article [137, Proposition 2.1] prove that the points $(0, 1), (-m, 1), (-1, m)$ generate the Modell–Weil group over $\mathbb{Q}(m)$ of $y^2 = x^3 - m^2x + 1$. Neither of these proofs, however, uses Nagao's formula.

[5]If p is odd and $A \not\equiv 0 \bmod p$ or $B \not\equiv 0 \bmod p$, then $\sum_{t_0=0}^{p-1} \left(\frac{At_0^2+Bt_0+C}{p}\right)$ is equal to $(p-1)\left(\frac{A}{p}\right)$ if $p \mid (B^2 - 4AC)$ and to $-\left(\frac{A}{p}\right)$ otherwise (see for instance [3, Lemma A.2]).

[6]Alternatively, we could check that P, Q, R are linearly independent by checking that they specialise to linearly independent points on at least one fibre.

verify that if $37t_0 + 1 \equiv 0 \bmod 3$, then we indeed have that Q_{t_0} reduces to a singular point over $\mathbb{F}_3$. So for t_0 odd and $t_0 \not\equiv 2 \bmod 3$, the point $Q_{t_0} \in \mathcal{E}_{t_0}(\mathbb{Q})$ has good reduction at all primes of $\mathbb{Z}$.

To avoid having to deal with non-trivial γ-factors for Q, we thus *assume now that* $t \equiv 1$ *or* $3 \bmod 6$. Then we find that

$$\begin{aligned} h_p(Q) = {} & 27333616607580 \cdot 37 + O(37^{10}) - (6165048856723 \cdot 37 + O(37^{10})) \cdot t \\ & + (1451491704474 \cdot 37^2 + O(37^{10})) \cdot t^2 - (33315662136 \cdot 37^3 + O(37^{10})) \cdot t^3 \\ & + (683158069 \cdot 37^4 + O(37^{10})) \cdot t^4 - (12821342 \cdot 37^5 + O(37^{10})) \cdot t^5 \\ & + (163696 \cdot 37^6 + O(37^{10})) \cdot t^6 + (9561 \cdot 37^7 + O(37^{10})) \cdot t^7 \\ & - (543 \cdot 37^8 + O(37^{10})) \cdot t^8 + (15 \cdot 37^9 + O(37^{10})) \cdot t^9 + O(37^{10}) \end{aligned}$$

$$\begin{aligned} h_p(P+Q) = {} & 15008325121889 \cdot 37 + O(37^{10}) + (30949172734588 \cdot 37 + O(37^{10})) \cdot t \\ & - (1632168174147 \cdot 37^2 + O(37^{10})) \cdot t^2 + (35661491430 \cdot 37^3 + O(37^{10})) \cdot t^3 \\ & - (806642831 \cdot 37^4 + O(37^{10})) \cdot t^4 - (11191971 \cdot 37^5 + O(37^{10})) \cdot t^5 \\ & - (322802 \cdot 37^6 + O(37^{10})) \cdot t^6 + (22490 \cdot 37^7 + O(37^{10})) \cdot t^7 \\ & + (326 \cdot 37^8 + O(37^{10})) \cdot t^8 + (13 \cdot 37^9 + O(37^{10})) \cdot t^9 + O(37^{10}). \end{aligned}$$

Now, the point R has singular reduction at 2. However, $3R$ has everywhere good reduction. By Remark 3.2.3, we need to compute $6R$ in order to deduce the gamma factor. Then, proceeding in a similar manner as above, we eventually find that, for $t \equiv 1, 3 \bmod 6$,

$$\begin{aligned} \mathrm{Reg}_p(P,Q,R) = {} & 26453729251735 \cdot 37^3 + O(37^{12}) + (55142202863317 \cdot 37^3 + O(37^{12})) \cdot t \\ & + (43241250505824 \cdot 37^3 + O(37^{12})) \cdot t^2 - (50988058335916 \cdot 37^3 + O(37^{12})) \cdot t^3 \\ & - (368889027678 \cdot 37^4 + O(37^{12})) \cdot t^4 + (5813041976 \cdot 37^5 + O(37^{12})) \cdot t^5 \\ & + (75553590 \cdot 37^6 + O(37^{12})) \cdot t^6 + (33606862 \cdot 37^7 + O(37^{12})) \cdot t^7 \\ & + (286018 \cdot 37^8 + O(37^{12})) \cdot t^8 - (1724 \cdot 37^9 + O(37^{12})) \cdot t^9 \\ & - (643 \cdot 37^{10} + O(37^{12})) \cdot t^{10} + O(37^{11}). \end{aligned}$$

The polynomial obtained by reducing the coefficients of $37^{-3}\mathrm{Reg}_p(P,Q,R)$ modulo 37 has no roots in $\mathbb{Z}/37\mathbb{Z}$. Thus $\mathrm{Reg}_p(P,Q,R)$ has no roots in $\mathbb{Z}_{37}$.

Remark 3.3.5. With the notation of Example 3.3.3, we may wonder what the set

$$A = \{t_0 \in \mathbb{Z} : [\mathcal{E}_{t_0}(\mathbb{Q}) : \langle P_{t_0}, Q_{t_0}, R_{t_0} \rangle_{\mathbb{Z}}] < \infty\}$$

looks like. Given a family $\mathcal{F}/\mathbb{Q}(t)$ of generic rank $r_{\mathcal{F}}$, define the average rank

$$\mathrm{Av}_{\mathbb{Z}}(r_{\mathcal{F}}) = \lim_{T \to \infty} \frac{1}{2T} \sum_{|t_0| \leq T} r(\mathcal{F}_{t_0});$$

here $r(\mathcal{F}_{t_0})$ is the rank of $\mathcal{F}_{t_0}(\mathbb{Q})$ if $\mathcal{F}_{t_0}$ is an elliptic curve and zero otherwise.

According to [28], it is conjectured[7] that

$$\mathrm{Av}_{\mathbb{Z}}(r_{\mathcal{F}}) = r_{\mathcal{F}} + \frac{1-(-1)^{r_{\mathcal{F}}}\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{F}})}{2}. \tag{3.21}$$

Assuming the square-free sieve conjecture and Chowla's conjecture, by Theorem 3.1.7 the curve $\mathcal{E}/\mathbb{Q}(t)$ satisfies $\mathrm{Av}_{\mathbb{Z}}(\varepsilon_{\mathcal{E}}) = 0$, which, under (3.21), would imply that A is an infinite set.

3.3.3 An example of a family of families

In this subsection we derive some properties of the coefficients and orders of vanishing of p-adic height (and regulator) series for a one-parameter family which lives in a prescribed two-parameter family. In Appendix 3.A, we provide explicit formulae and study the zeros for one of these families.

Let $B \in \mathbb{Z}$ and consider the family

$$^{B}\mathcal{E}\colon y^2 + y = x(x+B)(x+t). \tag{3.22}$$

Note that, for any $A \in \mathbb{Z}$, an equation of the form $y^2 + y = (x+A)(x+B)(x+t)$ transforms, under the change of variables $x \mapsto x - A$, to

$$y^2 + y = x(x+B-A)(x-A+t)$$

and, by readjusting the parameter if necessary, the curve is in the form (3.22).

Proposition 3.3.6. *If $B \neq 0$, the Mordell–Weil group of $^{B}\mathcal{E}$ over $\mathbb{Q}(t)$ has rank 2 and is generated by $P = (0,0)$ and $Q = (-B,0)$. If $B = 0$, the group $^{B}\mathcal{E}(\mathbb{Q}(t))$ is of rank 1 and is generated by the point $(0,0)$.*

Proof. Denote by a_i, for $i = 1,\dots,4,6$ the usual coefficients for the Weierstrass equation for $^{B}\mathcal{E}$. For each i, a_i is a polynomial in t of degree strictly less than i and hence $^{B}\mathcal{E}$ is rational over $\overline{\mathbb{Q}}$ (see [118, §8.4]). In order to find $^{B}\mathcal{E}(\overline{\mathbb{Q}}(t))$, we study the set of reducible fibres of the elliptic fibration associated to $^{B}\mathcal{E}$. The discriminant of $^{B}\mathcal{E}$, as a polynomial in t, has discriminant

$$(-268435456)(B^6 + 27/16)^3,$$

[7] The author could not find other sources where this precise conjecture is formulated. However, see also [126, §5] for a discussion.

which is non-zero at $B \in \mathbb{Z}$. Thus, the singular fibres of ${}^B\mathcal{E}$ not lying above infinity are irreducible.

For the fibre at infinity, we apply Tate's algorithm to the model

$$y^2 + s^3 y = x(x + Bs^2)(x + s). \tag{3.23}$$

obtained by setting $s = 1/t$ and applying the change of variables $x \mapsto s^{-2}x$, $y \mapsto s^{-3}y$: if $B \neq 0$ (resp. $B = 0$) we have Kodaira symbol I_2^* (resp. I_3^*).

Therefore, by [120, Lemma 7.2] the irreducible components not containing the identity of the reducible fibre at infinity generate a sublattice of the Néron-Severi group of ${}^B\mathcal{E}$ whose opposite is D_6 (resp. D_7). Finally, by the Main Theorem of [108] (cf. Theorem 3.1.3), we have

1. if $B \neq 0$, then ${}^B\mathcal{E}(\overline{\mathbb{Q}}(t))$ is of rank 2, it has trivial torsion and it has two orthogonal generators each of canonical height $1/2$.

2. if $B = 0$, then ${}^B\mathcal{E}(\overline{\mathbb{Q}}(t))$ is of rank 1, it has trivial torsion and its generator has canonical height $1/4$.

The case $B = 0$ is then already nearly exhausted. Indeed, since ${}^B\mathcal{E}(\overline{\mathbb{Q}}(t))$ has no torsion, neither does ${}^B\mathcal{E}(\mathbb{Q}(t))$. Thus $P = (0, 0)$ is a point of infinite order over $\mathbb{Q}(t)$ and $\mathrm{rank}({}^B\mathcal{E}(\mathbb{Q}(t))) = 1$. If we want to show that P generates ${}^B\mathcal{E}(\mathbb{Q}(t))$, it suffices to show that the height of P is $1/4$ (or that P meets at least one fibre in the generator of its Mordell–Weil group over $\mathbb{Q}$). See below.

When B does not vanish, a similar argument shows that $P = (0, 0)$ and $Q = (-B, 0)$ are infinite order points over $\mathbb{Q}(t)$, so the $\mathbb{Q}(t)$-rank of ${}^B\mathcal{E}$ is greater than or equal to 1, and bounded above by the $\overline{\mathbb{Q}}(t)$-rank 2. In order to show that the rank is precisely 2 also over $\mathbb{Q}$, we explicitly find the height pairing of P with Q. Since we are working over $\mathbb{Q}$ (and thus over $\mathbb{C}$), the height pairing of Shioda [120] coincides with the one of Cox–Zucker [52] (see [120, Theorem 8.6]). In particular, for any $R, T \in {}^B\mathcal{E}(\mathbb{Q}(t))$, we have

$$\begin{aligned} \langle R, R\rangle &= 2 + 2(RO) - \mathrm{contr}_\infty(R) \\ \langle R, T\rangle &= \frac{1}{2}(\langle R + T, R + T\rangle - \langle R, R\rangle - \langle T, T\rangle), \end{aligned}$$

where (RO) is the intersection number of the sections corresponding to R and O and $\mathrm{contr}_\infty(R)$ is a correction term coming from the reducible fibre at infinity. The sections $P, Q, P + Q = (-t, -1)$ are disjoint from the zero section O away from the

fibre at infinity. In the model (3.23), $P = (0, 0)$, $Q = (-s^2B, 0)$, $P + Q = (-s, -s^3)$ and O is again the point at infinity. Thus,

$$(PO) = (QO) = ((P + Q)O) = 0.$$

The terms $\mathrm{contr}_\infty(P)$, $\mathrm{contr}_\infty(Q)$, $\mathrm{contr}_\infty(P + Q)$ depend on the component of the fibre at infinity on which the sections $P, Q, P+Q$ lie and may be computed using [52, Proposition (2.25), Table (1.19)][8].

First of all, note that the points P, Q and $P+Q$ have singular reduction at infinity. A suitable change of variables transforms (3.23) into

$$\tilde{y}^2 = 4\tilde{x}^3 - g_2\tilde{x} - g_3,$$

where

$$g_2 = -\left(-\frac{4}{3}s^2B^2 + \frac{4}{3}sB - \frac{4}{3}\right)s^2,\ g_3 = -\left(\frac{8}{27}s^3B^3 - \frac{4}{9}s^2B^2 + s^3 - \frac{4}{9}sB + \frac{8}{27}\right)s^3;$$

in particular,

$$\begin{aligned} \tilde{x}(P) &= \frac{1}{3}(s + s^2B), & 12\tilde{x}(P)^2 - g_2 &= 4s^3B \\ \tilde{x}(Q) &= \frac{1}{3}(s - 2s^2B), & 12\tilde{x}(Q)^2 - g_2 &= -4s^3B + 4s^4B^2 \\ \tilde{x}(P + Q) &= -\frac{2}{3}s + \frac{1}{3}Bs^2. \end{aligned}$$

In the notation of [52, Proposition (2.25)], we have $a = \frac{1}{3}$ and q is a square root of $16B^2$. Thus, one of P and Q hits C_5 and the other one hits C_6; $P + Q$ hits C_1. By [52, Table (1.19)], then $\mathrm{contr}_\infty(P) = \mathrm{contr}_\infty(Q) = 3/2$ and $\mathrm{contr}_\infty(P + Q) = 1$. This shows that for $B \neq 0$, ${}^B\mathcal{E}(\mathbb{Q}(t)) = \langle P, Q\rangle_{\mathbb{Z}}$. Similarly, when $B = 0$, $\mathrm{contr}_\infty(P) = 7/4$, giving $\langle P, P\rangle = 1/4$. □

By Theorem 3.1.4, if $B \neq 0$, then the points P_{t_0} and Q_{t_0} in ${}^B\mathcal{E}_{t_0}(\mathbb{Q})$ are linearly independent for all but finitely many $t_0 \in \mathbb{Q}$. Similarly, for $B = 0$, P_{t_0} is a point of infinite order on ${}^B\mathcal{E}_{t_0}$ for all but finitely many rational values of t_0. There are some obvious values of t_0 for which injectivity fails. Indeed, the group law on ${}^B\mathcal{E}/\mathbb{Q}(t)$ gives that

$$-(P + Q) = (-t, 0),$$

for all $B \in \mathbb{Z}$. Therefore, we have

[8]These contributions are the analogue of the local heights (for example of the p-adic height) of an integral point on an elliptic curve over $\mathbb{Q}$ at the primes of bad reduction (in particular, compare [52, Table (1.19)] with the values in Table 4.1).

– If $B = 0$, then $3P_0 = O$. The curve $y^2+y = x^3$ is 27.a4 [90], whose Mordell–Weil group is isomorphic to $\mathbb{Z}/3$;

– If $B \neq 0$, then if $t_0 = 0$, $Q_{t_0} = -2P_{t_0}$; if $t_0 = B$, $P_{t_0} = -2Q_{t_0}$.

  – Consider first the case $t_0 = 0$. We have $3P_0 = \left(\frac{1}{B^2}, -\frac{B^3+1}{B^3}\right)$, which by [127, VII, Application 3.5] can be torsion only if $B^2 \in \{1, 4\}$. Either using Mazur's classification of the torsion subgroup of an elliptic curve [94] or reduction modulo some primes, we conclude that the only value of B for which P_0 is torsion is -1. In fact, the curve $y^2 + y = x^2(x - 1)$ is 11.a3 [90], which has rank 0 and torsion group isomorphic to $\mathbb{Z}/5$. Hence for $B \neq 0, -1$, the curve ${}^B\mathcal{E}_0$ has an infinite order point P_0 and $Q_0 = -2P_0$. (Note that, combined with the above, this also shows that the exceptional set of Silverman's Specialisation Theorem when $B = 0$ is $\{-1, 0\}$.)

  – If $t_0 = B$, the change of variables $x \mapsto x - B$ gives the equation $y^2 + y = x^2(x - B)$. This is the same as the $t_0 = 0$ case, with B replaced by $-B$. Hence, for $B \neq 0, 1$, the points P_B and Q_B are of infinite order and satisfy $P_B = -2Q_B$ and for $B = 1$ we get the rank 0 curve $y^2 + y = x(x + 1)^2$, which is isomorphic to 11.a3.

Another case in which the linear independence of P and Q is not preserved in the specialisation is when $B = 1$ or -1 and $t_0 = -1$ and $t_0 = 1$, respectively. Indeed, the group of rational points on the curve $y^2 + y = x^3 - x$ ([90, Elliptic Curve 37.a1]) is generated by $(0, 0)$ and, in particular, $2(0, 0) = (1, 0)$.

Now consider

$$ {}^{ABC}\mathcal{F}\colon y^2 + y = (x + A)(x + B)(x + C + pt), \tag{3.24}$$

where A, B, C are integers (not necessarily distinct) and p is a prime such that ${}^{ABC}\mathcal{F}_0$ is an elliptic curve with good ordinary reduction at p. There are at most three families[9] of the form (3.24) specialising to the curve $y^2 + y = (x + A)(x + B)(x + C)$ at $t = 0$, namely ${}^{ABC}\mathcal{F}$, ${}^{BCA}\mathcal{F}$ and ${}^{CAB}\mathcal{F}$. Consider the points of everywhere good reduction

$$ {}^{ABC}P = (-A, 0),\ {}^{ABC}Q = (-B, 0) \in {}^{ABC}\mathcal{F}^\circ(\mathbb{Q}(t))$$

[9]Even if A, B, C are pairwise distinct, it could happen that the three families are related by a linear change of variable of the parameter t. For example, if $2A = B + C$, then the change of variables $x \mapsto x + C - A$ maps ${}^{ABC}\mathcal{F}$ to $y^2 + y = (x + A)(x + 2C - A + pt)(x + C)$. To rule out this possibility it suffices to find $t_0 \in \mathbb{Z}$ such that $j({}^{CAB}\mathcal{F})(t) - j({}^{ABC}\mathcal{F})(t_0) = 0$ has no solutions over $\mathbb{Q}$. Note that the families being related by a linear change of variables in t is different from the families being isomorphic (over $\overline{\mathbb{Q}(t)}$), which can be checked by comparing j-invariants.

We can ask how the coefficients of the regulator of ${}^{\star}P$ and ${}^{\star}Q$ vary as $\star$ runs through $I = \{ABC, BCA, CAB\}$. Note that, since ${}^{ABC}P + {}^{ABC}Q = -(-C - pt, 0)$, the constant term is just the regulator of $(-A, 0)$, $(-B, 0)$ on the common fibre at $t = 0$; thus, the first interesting term is the one of degree one and we have the following.

Proposition 3.3.7. *The coefficient of t in $\sum_{\star \in I} \mathrm{Reg}_p({}^{\star}P, {}^{\star}Q)$ is zero.*

Proof. Denote by a_{11}, a_{12}, a_{13} the coefficients of t for the regulator series for $\star = BCA, CAB, ABC$ respectively and by a_0 the common constant term. Consider the three-parameter family

$$\mathfrak{F}\colon y^2 + y = (x + A + pt_1)(x + B + pt_2)(x + C + pt_3)$$

together with the points $\mathscr{P} = (-(A + pt_1), 0)$ and $\mathscr{Q} = (-(B + pt_2), 0)$ (note $-(\mathscr{P} + \mathscr{Q}) = (-(C + pt_3), 0)$). The expansion for the regulator series of $\mathscr{P}, \mathscr{Q}$ around $(t_1, t_2, t_3) = (0, 0, 0)$ is

$$\mathrm{Reg}(\mathscr{P}, \mathscr{Q}) = a_0 + a_{11}t_1 + a_{12}t_2 + a_{13}t_3 + O(t_1^2, t_1t_2, t_2^2).$$

Suppose that we set $t = t_1 = t_2 = t_3$ in the equation defining $\mathfrak{F}$ and denote the resulting one-parameter family by $\mathfrak{F}_t$ and by $\mathscr{P}_t, \mathscr{Q}_t$ the obvious points. For each fixed rational number t_0, the specialisation of $\mathfrak{F}_t$ at t_0 is $\mathbb{Q}$-isomorphic to $y^2 + y = (x + A)(x + B)(x + C)$. Therefore,

$$\mathrm{Reg}(\mathscr{P}_t, \mathscr{Q}_t) = \mathrm{Reg}(\mathscr{P}, \mathscr{Q})_{t_1=t_2=t_3=t} = a_0 + (a_{11} + a_{12} + a_{13})t + O(t^2)$$

is independent of $t \in \mathbb{Z}$ and hence must be constant: thus, $a_{11} + a_{12} + a_{13} = 0$. □

As an immediate consequence, we get:

Corollary 3.3.8. $\mathrm{Reg}_p({}^{ABA}P, {}^{ABA}Q)$ *has a zero of order greater than or equal to* 2 *at* $t = 0$.

Remark 3.3.9. Corollary 3.3.8 implies that the order of vanishing at $t = 0$ of the regulator of two linearly independent points P, Q of a family $\mathcal{E}$ could be larger than $2 - \mathrm{rank}(\langle P_0, Q_0 \rangle)$ (which could have been a natural guess). Indeed, for example when $A = -1$ and $B = 0$, the Mordell–Weil group of the curve ${}^{ABA}\mathcal{F}_0/\mathbb{Q}$ is generated by the infinite order point $(1, 0)$ (see also Appendix 3.A).

If A, B, C are pairwise distinct, we expect in general the t-coefficients of $\mathrm{Reg}_p({}^{\star}P, {}^{\star}Q)$ to be non-zero for each $\star$. Nevertheless, according to Proposition 3.3.7, their sum vanishes. The next proposition gives an example of this phenomenon.

Proposition 3.3.10. *Suppose that, as sets,* $\{A, B, C\} = \{-1, 0, 1\}$ *and that* ${}^{ABC}\mathcal{F}_0$ *has good ordinary reduction at* p*. Let* $T = (0, 0) \in {}^{ABC}\mathcal{F}_0(\mathbb{Q})$*. Then the coefficient of* t *in* $\mathrm{Reg}_p({}^{ABC}P, {}^{ABC}Q)$ *is* $2\alpha \cdot p \cdot h_p(T)$ *where* $\alpha = \begin{cases} -4 & \text{if } C = -1, \\ 3 & \text{if } C = 0, \\ 1 & \text{if } C = 1. \end{cases}$

Proof. We may drop ^{ABC} from the notation. Let $R = (-(C + pt), 0)$. Write $h_p(P) = \sum_{i=0}^{\infty} c_i t^i$, $h_p(Q) = \sum_{i=0}^{\infty} d_i t^i$ and $h_p(R) = \sum_{i=0}^{\infty} f_i t^i$. Then the coefficient of t in $\mathrm{Reg}_p(P, Q)$ is

$$\frac{1}{2}(c_1(d_0 + f_0 - c_0) + d_1(c_0 + f_0 - d_0) + f_1(c_0 + d_0 - f_0)). \tag{3.25}$$

Since $\{c_0, d_0, f_0\} = \{h_p(T), 4h_p(T), 9h_p(T)\}$ as sets, (3.25) becomes

$$h_p(T) \cdot \begin{cases} 3h_p(1 - pt, 0)_1 + 6h_p(0, 0)_1 - 2h_p(-1, 0)_1 & \text{if } C = -1, \\ 3h_p(1, 0)_1 + 6h_p(-pt, 0)_1 - 2h_p(-1, 0)_1 & \text{if } C = 0, \\ 3h_p(1, 0)_1 + 6h_p(0, 0)_1 - 2h_p(-1 - pt, 0)_1 & \text{if } C = 1, \end{cases}$$

where the subscript 1 indicates the coefficient of t. Consider the point $D = 2(-pt_1, 0) - (1 - pt_2, 0)$ on the three-parameter family $\mathfrak{E}\colon y^2 + y = (x + pt_1)(x - 1 + pt_2)(x + 1 + pt_3)$. Using the parallelogram law twice and quadraticity (see Properties 2.2.7), we obtain

$$\begin{aligned} h_p(D) &= 8h_p(-pt_1, 0) + 2h_p(1 - pt_2, 0) - h_p(2(-pt_1, 0) + (1 - pt_2, 0)) \\ &= 8h_p(-pt_1, 0) + 2h_p(1 - pt_2, 0) - h_p((-pt_1, 0) - (-1 - pt_3, 0)) \\ &= 6h_p(-pt_1, 0) + 2h_p(1 - pt_2, 0) - 2h_p(-1 - pt_3, 0) + \\ &\quad + h_p((-pt_1, 0) + (-1 - pt_3, 0)) \\ &= 6h_p(-pt_1, 0) + 3h_p(1 - pt_2, 0) - 2h_p(-1 - pt_3, 0). \end{aligned}$$

Furthermore, the point D specialises to the point at infinity at $t_1 = t_2 = t_3 = 0$. The result then follows by applying Proposition 3.2.26 to the point $D_{t_1=t_3=0}$, $D_{t_2=t_3=0}$ and $D_{t_1=t_2=0}$, respectively. □

Proposition 3.3.11. *Let* $\mathcal{E}\colon y^2 + y = x(x - 1)(x + pt)$ *have good ordinary reduction at* p*. Then the regulator series for* $P = (0, 0)$ *and* $Q = (1, 0)$ *has leading term* $-\frac{p^2}{25}t^2$*.*

Proof. The proof follows directly from Proposition 3.2.26. More explicitly, the $\mathbb{Q}$-rational torsion subgroup of the fibre $\mathcal{E}_0$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ and hence each of $P_0 = (0, 0)$, $Q_0 = (1, 0)$ and $P_0 + Q_0 = (0, -1)$ have order $m = 5$. Furthermore, $a(5P) = 1 - 6pt + O(t^2)$, $b(5P) = 1 - 9pt + O(t^2)$; $a(5Q) = 1 - 4pt + O(t^2)$, $b(5Q) = 1 - 6pt + O(t^2)$ and finally, $a(5(P + Q)) = 1 + 4pt + O(t^2)$ and $b(5(P + Q)) = -1 - 6pt + O(t^2)$. □

In Appendix 3.A, we provide explicitly the regulator series for the family given by $y(y+1) = x(x-1)(x+t)$ and the prime $p = 5$, together with their zeros.

Appendix

3.A One family from §3.3.3

Consider the family

$$\mathcal{E}\colon y^2 + y = x(x-1)(x+t).$$

By Proposition 3.3.6, the Mordell–Weil group of its generic fibre over $\mathbb{Q}(t)$ is generated by the two linearly independent points $P = (0,0)$ and $Q = (1,0)$. The prime $p = 5$ is of good ordinary reduction at all $t \in \mathbb{Z}$ and for $a \in \{0, 1, 2, -2, -1\}$ we define the subfamily

$$\mathcal{E}^{(a)}\colon y^2 + y = x(x-1)(x+pt+a)$$

and its points $P^{(a)} = (0,0), Q^{(a)} = (1,0) \in \mathcal{E}^{(a)}(\mathbb{Q}(t))$. Note that p is anomalous for $\mathcal{E}^{(a)}$ when $a = 0$ or $a = -1$. Using the algorithm of §3.2.4 and Proposition 3.3.11, we find

$$\begin{aligned}\mathrm{Reg}_5(P^{(0)}, Q^{(0)}) = {} & -t^2 - (50727361 \cdot 5 + O(5^{13})) \cdot t^3 + (24332108 \cdot 5^2 + O(5^{13})) \cdot t^4 \\ & - (301708 \cdot 5^4 + O(5^{13})) \cdot t^5 + (2153663 \cdot 5^3 + O(5^{13})) \cdot t^6 \\ & + (47619 \cdot 5^4 + O(5^{13})) \cdot t^7 + (51178 \cdot 5^5 + O(5^{13})) \cdot t^8 \\ & - (16742 \cdot 5^6 + O(5^{13})) \cdot t^9 + (33209 \cdot 5^6 + O(5^{13})) \cdot t^{10} \\ & + (574 \cdot 5^8 + O(5^{13})) \cdot t^{11} - (12 \cdot 5^{11} + O(5^{13})) \cdot t^{12} \\ & - (23 \cdot 5^{10} + O(5^{13})) \cdot t^{13} + (5^{11} + O(5^{13})) \cdot t^{14} \\ & + (9 \cdot 5^{11} + O(5^{13})) \cdot t^{15} + O(5^{13}).\end{aligned}$$

The series $\mathrm{Reg}_5(P^{(0)}, Q^{(0)})$ has a double root at $t = 0$ since $\mathcal{E}_0^{(0)} = \mathcal{E}_0$ has rank 0 over $\mathbb{Q}$ and no other root in $\mathbb{Z}_p$. In particular, for all $t_0 \in \mathbb{Z} \setminus \{0\}$, $\mathrm{Reg}_5(P_{t_0}^{(0)}, Q_{t_0}^{(0)}) \neq 0$.

The series

$$\begin{aligned}\mathrm{Reg}_5(P^{(1)}, Q^{(1)}) = {} & -(376028063 \cdot 5^2 + O(5^{15})) \cdot t + (138961179 \cdot 5^2 + O(5^{15})) \cdot t^2 \\ & + (107958183 \cdot 5^3 + O(5^{15})) \cdot t^3 + (16277206 \cdot 5^4 + O(5^{15})) \cdot t^4 \\ & - (3024774 \cdot 5^5 + O(5^{15})) \cdot t^5 - (827972 \cdot 5^5 + O(5^{15})) \cdot t^6 \\ & + (866513 \cdot 5^6 + O(5^{15})) \cdot t^7 - (46316 \cdot 5^7 + O(5^{15})) \cdot t^8 \\ & - (24487 \cdot 5^8 + O(5^{15})) \cdot t^9 - (38141 \cdot 5^8 + O(5^{15})) \cdot t^{10} \\ & - (1182 \cdot 5^{10} + O(5^{15})) \cdot t^{11} + (126 \cdot 5^{11} + O(5^{15})) \cdot t^{12} \\ & + (52 \cdot 5^{12} + O(5^{15})) \cdot t^{13} + O(5^{13})\end{aligned}$$

has a simple root at $t = 0$ ($\mathcal{E}_0^{(1)} = \mathcal{E}_1$ has rank 1 over $\mathbb{Q}$) and a simple root at

$$\alpha = 2 + 5 + 4 \cdot 5^2 + 2 \cdot 5^4 + 2 \cdot 5^5 + 4 \cdot 5^6 + 5^9 + 3 \cdot 5^{10} + O(5^{11}).$$

By Proposition 3.3.10, $10h_p(P_0^{(1)})$ equals the coefficient of t of $\mathrm{Reg}_5(P^{(1)}, Q^{(1)})$.

The roots of

$$\begin{aligned}\mathrm{Reg}_5(P^{(2)}, Q^{(2)}) = {} & 459124311 \cdot 5^2 + O(5^{15}) - (62255423 \cdot 5^3 + O(5^{15})) \cdot t \\ & + (457047919 \cdot 5^2 + O(5^{15})) \cdot t^2 + (117486341 \cdot 5^3 + O(5^{15})) \cdot t^3 \\ & + (7454518 \cdot 5^4 + O(5^{15})) \cdot t^4 - (3756667 \cdot 5^5 + O(5^{15})) \cdot t^5 \\ & - (1954737 \cdot 5^5 + O(5^{15})) \cdot t^6 + (509616 \cdot 5^6 + O(5^{15})) \cdot t^7 \\ & + (36674 \cdot 5^7 + O(5^{15})) \cdot t^8 + (19482 \cdot 5^8 + O(5^{15})) \cdot t^9 \\ & + (33464 \cdot 5^8 + O(5^{15})) \cdot t^{10} + (739 \cdot 5^{10} + O(5^{15})) \cdot t^{11} \\ & + (113 \cdot 5^{11} + O(5^{15})) \cdot t^{12} - (54 \cdot 5^{12} + O(5^{15})) \cdot t^{13} + O(5^{13})\end{aligned}$$

are

$$\alpha_1 \in \mathbb{Z}_p \quad \text{such that } 5\alpha_1^2 + 4\alpha_1 + 1 = 0$$

$$\alpha_2 = 4 + 4 \cdot 5^5 + 2 \cdot 5^7 + 5^8 + 2 \cdot 5^9 + 2 \cdot 5^{10} + O(5^{11}).$$

Let ψ be the embedding of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$ such that $\frac{-2+\psi(i)}{5} \in \mathbb{Z}_p$. The elliptic curve $\mathcal{E}^{(2)}_{\psi^{-1}(\alpha_1)} = \mathcal{E}_i$ over $\mathbb{Q}(i)$ is the curve with LMFDB label 233.1-a1 [90]. Its Mordell–Weil group over $\mathbb{Q}(i)$ is generated by $P_i = (0, 0)$ and we have the relation $Q_i = -3P_i$. The vanishing of $\mathrm{Reg}_5(P^{(2)}, Q^{(2)})$ at α_1 is explained by Theorem 3.2.28.

The power series

$$\begin{aligned}\mathrm{Reg}_5(P^{(-2)}, Q^{(-2)}) = {} & (283409127 \cdot 5^2 + O(5^{15})) \cdot t - (149466108 \cdot 5^2 + O(5^{15})) \cdot t^2 \\ & - (13546588 \cdot 5^3 + O(5^{15})) \cdot t^3 + (7574141 \cdot 5^4 + O(5^{15})) \cdot t^4 \\ & + (1992089 \cdot 5^5 + O(5^{15})) \cdot t^5 + (2574544 \cdot 5^5 + O(5^{15})) \cdot t^6 \\ & + (168542 \cdot 5^6 + O(5^{15})) \cdot t^7 + (120832 \cdot 5^7 + O(5^{15})) \cdot t^8 \\ & + (33892 \cdot 5^8 + O(5^{15})) \cdot t^9 + (5512 \cdot 5^8 + O(5^{15})) \cdot t^{10} \\ & - (803 \cdot 5^{10} + O(5^{15})) \cdot t^{11} + (211 \cdot 5^{11} + O(5^{15})) \cdot t^{12} \\ & + (3 \cdot 5^{12} + O(5^{15})) \cdot t^{13} + O(5^{13})\end{aligned}$$

has a simple root as $t = 0$, which is consistent with the fact that $\mathcal{E}_0^{(-2)} = \mathcal{E}_{-2} \cong \mathcal{E}_1$ has rank one over $\mathbb{Q}$. The change of variables $x \mapsto x + 1$ transforms $\mathcal{E}^{(-2)}$ into ${}^{01-1}\mathcal{F}$. Thus, by Proposition 3.3.10, the leading term is $-40h_p(P_1)t$. $\mathrm{Reg}_5(P^{(-2)}, Q^{(-2)})$ also has a simple root at

$$\alpha \in \mathbb{Z}_p \quad \text{such that } 5\alpha^2 - 4\alpha + 1 = 0.$$

With the notation as above, let ψ' be the second embedding of $\mathbb{Q}(i)$ into $\mathbb{Q}_p$. Then we have $\alpha = \psi'(\frac{2+i}{5})$ and the curve $\mathcal{E}^{(-2)}_{\psi'^{-1}(\alpha)}$ is the same curve as $\mathcal{E}^{(2)}_{\psi^{-1}(\alpha_1)}$. Thus the

vanishing of $\mathrm{Reg}_5(P^{(-2)}, Q^{(-2)})$ at $t = \alpha$ is again a consequence of Theorem 3.2.28. By Theorem 3.2.27, we can compute the cyclotomic 5-adic height of $P_i = (0, 0)$ on the curve $\mathcal{E}_i \colon y^2 + y = x(x-1)(x+i)$ from the series $h_p(P^{(2)})$ and $h_p(P^{(-2)})$:

$$h_p(P_i) = 4 \cdot 5 + 5^2 + 2 \cdot 5^3 + 5^4 + 2 \cdot 5^5 + 5^6 + 3 \cdot 5^7 + 5^8 + 3 \cdot 5^9 + 2 \cdot 5^{10} + 3 \cdot 5^{11} + 2 \cdot 5^{12} + O(5^{14}).$$

Finally,

$$\begin{aligned}\mathrm{Reg}_5(P^{(-1)}, Q^{(-1)}) = &-(507634134 + O(5^{13})) \cdot t^2 - (13589728 \cdot 5^2 + O(5^{13})) \cdot t^3 \\ &+ (1186173 \cdot 5^3 + O(5^{13})) \cdot t^4 + (4167561 \cdot 5^3 + O(5^{13})) \cdot t^5 \\ &- (4586773 \cdot 5^3 + O(5^{13})) \cdot t^6 - (104292 \cdot 5^5 + O(5^{13})) \cdot t^7 \\ &- (6671 \cdot 5^5 + O(5^{13})) \cdot t^8 - (5167 \cdot 5^6 + O(5^{13})) \cdot t^9 \\ &+ (18851 \cdot 5^6 + O(5^{13})) \cdot t^{10} + (29 \cdot 5^{10} + O(5^{13})) \cdot t^{11} \\ &- (49 \cdot 5^9 + O(5^{13})) \cdot t^{12} - (2 \cdot 5^{10} + O(5^{13})) \cdot t^{13} \\ &- (5^{11} + O(5^{13})) \cdot t^{14} - (5^{12} + O(5^{13})) \cdot t^{15} + O(5^{13}),\end{aligned}$$

which has a zero of order 2 at $t = 0$ and no other. In particular, for all $t_0 \in \mathbb{Z} \setminus \{0\}$, the 5-adic regulator of $P_{t_0}, Q_{t_0} \in \mathcal{E}_{t_0}^{(-1)}(\mathbb{Q})$ is non-zero. The fibre $\mathcal{E}_0^{(-1)}$ has rank one over $\mathbb{Q}$ and the vanishing of the coefficient of t in $\mathrm{Reg}_5(P^{(-1)}, Q^{(-1)})$ was proved in Corollary 3.3.8 (see also Remark 3.3.9).

3.B Heights on points defined over extensions of degree 4

Consider the family

$$\mathcal{E} \colon y(y+1) = x(x-1)(x+t),$$

with $P = (0, 0)$ and $Q = (1, 0)$ in $\mathcal{E}^\circ(\mathbb{Z}[t])$. Let t_0 be a root of $p(x) = x^4 - 3x^3 + 3x^2 - 3x + 1$. Then $Q_{t_0} = 4P_{t_0}$. The prime $p = 71$ splits completely in $\mathbb{Q}(t_0)$ and, for each root $\alpha \in \mathbb{Q}_p$ of $p(x)$, the elliptic curve $\mathcal{E}_\alpha/\mathbb{Z}_p$ has good ordinary reduction. The roots of $p(x)$ in $\mathbb{F}_p$ are $22, 38, 42, 43$. Denote by α_1, α_2, α_3 and α_4 the corresponding roots over $\mathbb{Z}_p$ and by a_1, a_2, a_3, a_4 the integers $22, 38, 42, 43$. For $1 \leq i \leq 4$, let

$$\mathcal{E}^{(a_i)} \colon y(y+1) = x(x-1)(x+pt+a_i).$$

Using Theorem 3.2.27, we compute

$$\begin{aligned}h_p(P_{t_0}) &= \frac{1}{4} \sum_{i=1}^{4} h_p(P^{(a_i)}) \left(\frac{\alpha_i - a_i}{p} \right) \\ &= 66 \cdot 71^{-1} + 35 + 42 \cdot 71 + 33 \cdot 71^2 + 61 \cdot 71^3 + 66 \cdot 71^4 + 38 \cdot 71^5 + 49 \cdot 71^6 + 54 \cdot 71^7 + O(71^8)\end{aligned}$$

and

$$\begin{aligned} h_p(Q_{t_0}) &= \frac{1}{4}\sum_{i=1}^{4} h_p(Q^{(a_i)})\left(\frac{\alpha_i - a_i}{p}\right) \\ &= 62\cdot 71^{-1} + 6 + 41\cdot 71 + 40\cdot 71^2 + 60\cdot 71^3 + 4\cdot 71^4 + 55\cdot 71^5 + 11\cdot 71^6 + 23\cdot 71^7 + O(71^8) \\ &\equiv 16\cdot h_p(P_{t_0}) \bmod 71^8. \end{aligned}$$

Chapter 4

Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture

This chapter is essentially the article [31].

4.1 Introduction

Let (E, O) be an elliptic curve over $\mathbb{Q}$ and fix an odd prime p of good reduction. Denote by $\mathcal{E}$ the regular minimal model of E and by $\mathcal{X}$ the complement of the origin in $\mathcal{E}$.

When E has Mordell–Weil rank 1 and the Tamagawa number of $E/\mathbb{Q}$ is trivial at all primes, Kim [80] and Balakrishnan–Kedlaya–Kim [19] described an explicit locally analytic function on $\mathcal{X}(\mathbb{Z}_p)$ which vanishes on the set $\mathcal{X}(\mathbb{Z})$ of global integral points.

Subsequently, Balakrishnan–Dan-Cohen–Kim–Wewers [15] generalised the result to arbitrary semistable elliptic curves of rank 1 and gave a similar p-adic characterisation of $\mathcal{X}(\mathbb{Z})$ when E is semistable and has rank 0.

The discussion fits into Kim's non-abelian Chabauty programme as introduced in [78] and [79]. In particular, Kim constructed a sequence of subsets of p-adic points

$$\mathcal{X}(\mathbb{Z}_p) \supset \mathcal{X}(\mathbb{Z}_p)_1 \supset \mathcal{X}(\mathbb{Z}_p)_2 \supset \cdots \supset \mathcal{X}(\mathbb{Z})$$

(see §4.2.2). The p-adic locally analytic functions from [15] are essentially those that define $\mathcal{X}(\mathbb{Z}_p)_2$, the set of *cohomologically global points of level* 2, in the larger $\mathcal{X}(\mathbb{Z}_p)$.

Having given an explicit description of $\mathcal{X}(\mathbb{Z}_p)_2$ in the rank 0 semistable case, the authors of [15] were able to provide computational evidence for the following conjecture (see [15, §3.1]).

Conjecture 4.1.1 (Kim, 2012). *For sufficiently large n, we have*

$$\mathcal{X}(\mathbb{Z}_p)_n = \mathcal{X}(\mathbb{Z}).$$

Indeed, they verified the equality

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$$

for the prime $p = 5$ and for all the 256 semistable elliptic curves of rank 0 for which they computed $\mathcal{X}(\mathbb{Z}_p)_2$.

The first goal of this chapter is to extend the description of $\mathcal{X}(\mathbb{Z}_p)_2$ to an arbitrary elliptic curve of rank 0 and at the same time correct a slight imprecision in the analogous statement in the semistable case [15, Theorem 1.12] (see Remark 4.2.4).

Before stating the theorem, we introduce some additional notation, which is convenient to maintain similar to [15]. Let $\mathcal{E}$ be described by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1}$$

and let S be the set of primes at which E has bad reduction.

For each $q \in S$, define the set $W_q \subset \mathbb{Q}_p$ as follows. If the Tamagawa number at q is 1, let

$$W_q = \{0\};$$

in all other cases,

$$W_q = \begin{cases} W_q^{\mathrm{bad}} & \text{if } q = 2 \text{ and } E \text{ is split multiplicative at } q, \\ W_q^{\mathrm{bad}} \cup \{0\} & \text{otherwise,} \end{cases}$$

where W_q^{bad} is the finite subset of $\mathbb{Q}_p$ described in Table 4.1 (with $F = \mathbb{Q}$ and $v = (q_v) = (q)$); in particular, W_q^{bad} only depends on the reduction type of E at q. Let

$$W = \prod_{q \in S} W_q$$

and, if $w \in W$, write $||w|| = \sum_{q \in S} w_q$. Let b be the integral tangent vector at the origin which is dual to $\omega(O)$, where

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

and let $\eta = x\omega$. Furthermore, for $z \in \mathcal{X}(\mathbb{Z}_p)$ write

$$\mathrm{Log}(z) = \int_b^z \omega \quad \text{and} \quad D_2(z) = \int_b^z \omega\eta,$$

where the integrals are Coleman integrals.

Theorem 4.1.2. *Suppose that E has rank 0 and that the p-primary part of its Tate–Shafarevich group is finite.*

1. *If, for at least one of* $q \in \{2,3\}$*, the reduction of* E *at* q *is good and* $\overline{E}(\mathbb{F}_q) = \{O\}$*, or if* E *has split multiplicative reduction of Kodaira type* I_1 *at* 2*, then*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \emptyset.$$

2. *Otherwise,*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \bigcup_{w \in W} \phi(w),$$

where

$$\phi(w) = \{z \in \mathcal{X}(\mathbb{Z}_p) : \mathrm{Log}(z) = 0, 2D_2(z) + ||w|| = 0\}.$$

We also remove the assumption of semistable reduction in the rank 1 case [15, Proposition 5.12]. Assume E has good ordinary[1] reduction at p. Let $\mathbf{E}_2$ be the Katz p-adic weight 2 Eisenstein series of Definition 2.2.5 and let

$$C = \frac{a_1^2 + 4a_2 - \mathbf{E}_2(E,\omega)}{12}. \tag{4.2}$$

Let $h_p \colon E(\mathbb{Q}) \to \mathbb{Q}_p$ be the p-adic height of Mazur–Tate with the normalisation of Section 2.2 and define

$$c = \frac{h_p(z_0)}{\mathrm{Log}(z_0)^2},$$

for a non-torsion point $z_0 \in E(\mathbb{Q})$.

Theorem 4.1.3. *Suppose that* E *has rank* 1 *and that* p *is a prime of good ordinary reduction.*

1. *If, for at least one of* $q \in \{2,3\}$*, the reduction of* E *at* q *is good and* $\overline{E}(\mathbb{F}_q) = \{O\}$*, or if* E *has split multiplicative reduction of Kodaira type* I_1 *at* 2*, then*

$$\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \emptyset.$$

2. *Otherwise,*

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)'_2 := \bigcup_{w \in W} \psi(w),$$

where

$$\psi(w) = \{z \in \mathcal{X}(\mathbb{Z}_p) : 2D_2(z) + C(\mathrm{Log}(z))^2 + ||w|| = c(\mathrm{Log}(z))^2\}.$$

[1] Although not explicitly stated in [15], their statement also holds only when p is ordinary. However, a similar result holds in the supersingular case: see Remark 4.2.6.

According to [15], the set $\cup_{w\in W}\psi(w)$ should equal $\mathcal{X}(\mathbb{Z}_p)_2$: hence the notation $\mathcal{X}(\mathbb{Z}_p)_2'$. Section 4.2 is devoted to the proofs of Theorems 4.1.2 and 4.1.3.

The equations defining the sets of p-adic points of the two theorems can be given an elementary interpretation as linear relations amongst $\mathbb{Q}_p$-valued quadratic functions on $E(\mathbb{Q})$, dictated by the assumptions on the rank. This point of view is crucial in our investigation, in Section 4.3, of what points could arise in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ in rank 0. In §4.3.3, we prove the following

Theorem 4.1.4. *There exist infinitely many rank* 0 *elliptic curves for which*

$$\mathcal{X}(\mathbb{Z}) \subsetneq \mathcal{X}(\mathbb{Z}_p)_2$$

for infinitely many good primes p*.*

We then present in Section 4.4 the computations of the sets $\mathcal{X}(\mathbb{Z}_p)_2$ for all the elliptic curves over $\mathbb{Q}$ of rank 0 and conductor less than or equal to $30,000$ and for some choices of p. We propose a slightly different but equivalent way of computing the set $\mathcal{X}(\mathbb{Z}_p)_2$, compared to the one used in [15]. In particular, our method does not require explicit computations of double Coleman integrals.

Our computations (run in `SageMath` [131]), together with the theoretical results derived in Section 4.3, show the following (see also Theorem 4.4.10).

Theorem 4.1.5. *There exists exactly one rank* 0 *elliptic curve of conductor at most* $30,000$ *for which*

$$\mathcal{X}(\mathbb{Z}) \subsetneq \mathcal{X}(\mathbb{Z}_p)_2$$

for all primes p *of good (ordinary and supersingular) reduction. This is the curve 8712.u5 [90].*

In future work, it would be interesting to verify whether Conjecture 4.1.1 holds at level 3 for the curves and primes for which we found $\#\mathcal{X}(\mathbb{Z}_p)_2 > \#\mathcal{X}(\mathbb{Z})$.

So far we have been concerned with sufficient conditions for $\mathcal{X}(\mathbb{Z}_p)_2$ to be larger than $\mathcal{X}(\mathbb{Z})$. We conjecture in §4.4.5 a necessary condition for a point to belong to $\mathcal{X}(\mathbb{Z}_p)_2$ and explain why this could be regarded as a non-abelian version of Stoll's Strong Chabauty Conjecture [133, Conjecture 9.5].

When E has rank 1, the set described in Theorem 4.1.3 (2) is generally larger than $\mathcal{X}(\mathbb{Z})$ (however, in Appendix 4.A we follow an idea of [10] to determine $\mathcal{X}(\mathbb{Z})$ from $\mathcal{X}(\mathbb{Z}_{p_i})_2'$ for some sequence of primes $(p_i)_{i\in I}$ in some examples). In §4.5.1, we ask what algebraic points can belong to $\mathcal{X}(\mathbb{Z}_p)_2' \setminus \mathcal{X}(\mathbb{Z})$. In §4.5.2 we compute $\mathcal{X}(\mathbb{Z}_p)_2'$ for

all the 14,783 rank 1 elliptic curves of conductor at most 5,000; for each curve, we let p be the smallest prime greater than or equal to 5 at which the curve has good ordinary reduction.

Finally, in Section 4.6 we explain how one can replace computations of double Coleman integrals with computations involving the p-adic sigma function and division polynomials also for determining the quadratic Chabauty sets containing the rational points of bielliptic curves as in [16]. We make the computation explicit for a curve arising from a problem from the *Arithmetica* of Diophantus and use it to give an alternative proof to the one given by Wetherell in his thesis [145] of the fact that the curve has exactly 8 rational points (see also Chapter 6 for a computation of the K-rational points on this curve for a real quadratic field K). Furthermore, by combining results of [16] with properties of local p-adic heights on elliptic curves, in §4.6.1 we give an algorithm that takes as input a bielliptic curve C whose associated elliptic curves have Mordell–Weil rank one together with a good prime p and outputs a finite set of p-adic points containing $C(\mathbb{Q})$.

The code used for the computations in this chapter is available at [29].

4.2 Description of $\mathcal{X}(\mathbb{Z}_p)_2$

4.2.1 Auxiliary results on local heights

Retain the notation of Section 2.2. In particular, E is an elliptic curve over a number field F, p is an odd prime such that E has good reduction at all primes above p. Here we want to develop further the description of the local heights $\lambda_v\colon E(F_v) \to \mathbb{Q}_p$, for a finite prime v, of a global cyclotomic height $h_p\colon E(F) \to \mathbb{Q}_p$. We may actually assume that E is the elliptic curve over $\mathbb{Q}$ of Section 4.1 and that we consider its F-rational points for an arbitrary number field F.

Recall that for $v \nmid p$ there is a unique choice of local height λ_v. Our first task is to determine which values λ_v can attain on $\mathcal{X}(\mathcal{O}_v)$, where $\mathcal{O}_v$ is the ring of integers of F_v. As in §2.2.1, we may assume, in view of (2.4), that $\mathcal{E}$ is minimal at v.

Proposition 4.2.1. *If $v \nmid p$ and $[E(F_v)\colon E_0(F_v)] = 1$, then*

$$\lambda_v(\mathcal{X}(\mathcal{O}_v)) = \begin{cases} \{0\} & \text{if } \#\overline{E}_{ns}(\mathbb{F}_v) > 1, \\ \emptyset & \text{otherwise.} \end{cases}$$

Proof. By Lemma 2.2.2 (i), $\lambda_v(\mathcal{X}(\mathcal{O}_v)) \subseteq \{0\}$, with equality if and only if $\mathcal{X}(\mathcal{O}_v) \neq \emptyset$. Let

$$E_1(F_v) = \{P \in E(F_v) : \overline{P} = \overline{O}\};$$

in particular, $\mathcal{X}(\mathcal{O}_v) \cap E_1(F_v)$ is empty and every point in $E_0(F_v) \setminus E_1(F_v)$ comes from a point in $\mathcal{X}(\mathcal{O}_v)$. According to [127, VII, Proposition 2.1], the sequence

$$0 \to E_1(F_v) \to E_0(F_v) \to \overline{E}_{ns}(\mathbb{F}_v) \to 0$$

is exact, which proves the proposition. □

We now give an elementary necessary condition for $\#\overline{E}_{ns}(\mathbb{F}_v) = 1$. We show it is also a sufficient condition in all cases except when v is of good reduction.

Lemma 4.2.2. *The group $\overline{E}_{ns}(\mathbb{F}_v)$ has cardinality at least 2 in all of the following cases:*

1. *E has additive or non-split multiplicative reduction at v;*
2. *E has good reduction at v and $q_v > 4$;*
3. *E has split multiplicative reduction at v and $q_v > 2$.*

Conversely, if E has split multiplicative reduction at v and $q_v = 2$, then

$$\#\overline{E}_{ns}(\mathbb{F}_v) = 1.$$

Proof. If E has additive reduction at v, then $\overline{E}_{ns}(\mathbb{F}_v) \cong \mathbb{F}_v^+$ always contains at least two elements. If the reduction is non-split multiplicative, then

$$\overline{E}_{ns}(\mathbb{F}_v) \cong \{a \in k^\times : N_{k/\mathbb{F}_v}(a) = 1\},$$

where $[k\colon \mathbb{F}_v] = 2$. Thus, if $q_v > 2$, then the statement is clear; if $q_v = 2$, then k is the splitting field of $x^4 - x$ over $\mathbb{F}_2$ and each element in $k^\times$ has norm 1 over $\mathbb{F}_2$.

When E has good reduction at v and $q_v > 4$, the Hasse bound yields $\#\overline{E}(\mathbb{F}_v) > 1$. Finally, if the reduction is split multiplicative, then $\overline{E}_{ns}(\mathbb{F}_v) \cong \mathbb{F}_v^\times$. □

Proposition 4.2.3. *If $v \nmid p$ and $[E(F_v)\colon E_0(F_v)] \neq 1$, then*

$$n_v \lambda_v(\mathcal{X}(\mathcal{O}_v)) = \begin{cases} W_v^{\mathrm{bad}} & \text{if } q_v = 2 \text{ and } E \text{ is split multiplicative at } v, \\ W_v^{\mathrm{bad}} \cup \{0\} & \text{otherwise,} \end{cases}$$

where W_v^{bad} is defined in Table 4.1.

Kodaira symbol	$[E(F_v)\colon E_0(F_v)]$	W_v^{bad}
$\mathrm{I}_n (n \geq 2)$	2 (non-split)	$\{-\frac{n}{4}\log q_v\}$
	n (split)	$\{-\frac{i(n-i)}{n}\log q_v : 1 \leq i \leq \lfloor \frac{n}{2} \rfloor\}$
III	2	$\{-\frac{1}{2}\log q_v\}$
IV	3	$\{-\frac{2}{3}\log q_v\}$
I_0^*	2 or 4	$\{-\log q_v\}$
$\mathrm{I}_n^* (n \geq 1)$	2	$\{-\log q_v\}$
	4	$\{-\log q_v, -\frac{n+4}{4}\log q_v\}$
IV^*	3	$\{-\frac{4}{3}\log q_v\}$
III^*	2	$\{-\frac{3}{2}\log q_v\}$

Table 4.1: The sets W_v^{bad}.

Proof. By a similar argument to the proof of Proposition 4.2.1, each non trivial coset of $E(F_v)/E_0(F_v)$ is represented by an element in $\mathcal{X}(\mathcal{O}_v)$ and there exists at least one point in $\mathcal{X}(\mathcal{O}_v)$ which reduces to a non-singular point in $\overline{E}_{ns}(\mathbb{F}_v)$ if and only if $\#\overline{E}_{ns}(\mathbb{F}_v) > 1$.

By Lemma 2.2.2 (i), if $P \in \mathcal{X}(\mathcal{O}_v)$ reduces to a non-singular point, then $\lambda_v(P) = 0$; by Lemma 4.2.2, such P exists unless $q_v = 2$ and E is split multiplicative at 2.

Therefore, by Lemma 2.2.2 (ii), it suffices to show that W_v^{bad} coincides exactly with the values of $n_v\lambda_v$ on $E(F_v)/E_0(F_v) \setminus \{0\}$. For this, we use the work of Cremona–Prickett–Siksek [55] for the local heights of the real canonical height. The proof of Proposition 6 in *loc. cit.* can be used verbatim here with the p-adic logarithm in place of the real one and Table 4.1 is nothing but the translation of [55, Table 2] to the p-adic setting. □

Recall from §2.2.2 and §2.3.2 that at the primes $v \mid p$ the p-adic local Néron functions are not unique. For our applications, we may assume that there is an isomorphism $F_v \simeq \mathbb{Q}_p$, which is now fixed. We will use the following convention. If the reduction is good *ordinary* at v, we choose N_v to be the unit root eigenspace of Frobenius (cf. §2.3.2), i.e. with the notation of §2.2.2

$$\beta = C,$$

where C is defined in (4.2). If P belongs to the formal group at v, then

$$\lambda_v(P) = -2\log(\sigma_p(P)),$$

where σ_p is Mazur–Tate's p-adic sigma function of Theorem 2.2.6 (see also Proposition 2.3.5).

If E is good *supersingular* at v, we let

$$\beta = \frac{a_1^2 + 4a_2}{12},$$

so that $\sigma_p^{(\beta)}$ is the p-adic sigma function of Bernardi [22]. Unlike the p-adic sigma function of Mazur and Tate, the one of Bernardi does not converge on the whole formal group over $\overline{F_v}$, as it may not have p-adically integral coefficients, as a power series in t. However, since we are assuming that $F_v \simeq \mathbb{Q}_p$, the function $\sigma_p^{(\beta)}$ converges on all the points P of the formal group whose coordinates are defined over F_v, since these satisfy $\mathrm{ord}_v(t(P)) > \frac{1}{p-1}$.

In both the ordinary and supersingular cases, λ_v satisfies, besides the properties (i)-(iii) of §2.2.2:

(iv) If ψ is an automorphism of E defined over F_v, then, for all $P \in E(F_v)$, $\lambda_v(\psi(P)) = \lambda_v(P)$. Note that, in view of the assumption that $F_v \simeq \mathbb{Q}_p$ and by Deuring's criterion, at supersingular primes this is simply saying that λ_v is an even function. At ordinary primes, let ζ be the root of unity such that $\psi^*(\omega) = \zeta\omega$. Then $f_m(\psi(P)) = \zeta^{1-m^2} f_m(P)$ by [99, Appendix I, Proposition 2], and the Mazur–Tate p-adic sigma function satisfies $\sigma_p(\psi(P)) = \zeta\sigma_p(P)$ if P is in the formal group [99, §3]. The claim then follows since $\log(\zeta) = 0$.

4.2.2 Proof of Theorems 4.1.2 and 4.1.3

It would be pointless to reproduce here the whole proofs, as they are straightforward from §2.2 and the proofs in [15]. Thus we content ourselves with giving a sketch and correcting a few imprecisions in Theorem 1.12 of *loc. cit.*

We start with some notation and we refer the reader to [78], [79], [15] for more details. Let $T = S \cup \{p\}$ and denote by G_T the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside T. For a prime q, write G_q for the absolute Galois group of $\mathbb{Q}_q$. For $q \in T$, G_q may be identified with a subgroup of G_T. For $q \notin T$, this is not possible; however, we may still define maps $G_q \to G_T$ which are trivial on the inertia subgroup $I_q \leq G_q$.

As in Section 4.1, let b be the integral tangent vector to $\mathcal{E}$ at O dual to ω. Let U be the unipotent p-adic étale fundamental group of $\mathcal{X}_{\overline{\mathbb{Q}}}$ at b and U_n the quotient of U by the n-th level of its central series.

For each prime q and $n \geq 1$, we have commutative diagrams

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}) & \longrightarrow & \mathcal{X}(\mathbb{Z}_q) \\ \downarrow & & \downarrow{\scriptstyle j_q^n} \\ H^1_f(G_T, U_n) & \xrightarrow{\mathrm{loc}_q^n} & H^1(G_q, U_n); \end{array}$$

here the H^1 are cohomology sets and $H^1_f(G_T, U_n) = (\mathrm{loc}_p^n)^{-1}(H^1_f(G_p, U_n))$, where $H^1_f(G_p, U_n)$ is the subset of $H^1(G_p, U_n)$ of crystalline U_n-torsors. We are interested in determining

$$\mathcal{X}(\mathbb{Z}_p)_n = (j_p^n)^{-1}(\mathrm{loc}_p^n(\mathrm{Sel}^n(\mathcal{X}))),$$

where the Selmer scheme $\mathrm{Sel}^n(\mathcal{X})$ is defined as

$$\mathrm{Sel}^n(\mathcal{X}) = \bigcap_{q \neq p} (\mathrm{loc}_q^n)^{-1}(\mathrm{Im} j_q^n).$$

From now on, we will focus on $n = 2$ and will drop the superscript n from the maps j_q and loc_q. In this case, U_2 fits into the exact sequence

$$0 \to \mathbb{Q}_p(1) \to U_2 \to V_p(E) \to 0, \tag{4.3}$$

where $\mathbb{Q}_p(1)$ is the p-adic cyclotomic character and $V_p(E)$ is the $\mathbb{Q}_p$-Tate module of E.

Proof of Theorem 4.1.2. If $\mathcal{X}(\mathbb{Z}_q)$ is empty for some q, then $\mathcal{X}(\mathbb{Z}_p)_2$ is trivially empty. Lemma 4.2.2 shows that this occurs precisely when E has good reduction at q, where $q = 2$ or 3, and $\overline{E}(\mathbb{F}_q) = \{O\}$, or when E has split multiplicative reduction of type I_1 at $q = 2$. This shows (1).

We may now suppose that $\mathcal{X}(\mathbb{Z}_q) \neq \emptyset$ for all q (including $q = p$). Since $E(\mathbb{Q})$ has rank 0 and the p-primary part of the Tate–Shafarevich group is finite, by Lemma 5.2 in [15],

$$\mathrm{Sel}^2(\mathcal{X}) \subset H^1_f(G_T, \mathbb{Q}_p(1)),$$

where $H^1_f(G_T, \mathbb{Q}_p(1)) \subset H^1_f(G_T, U_2)$ via (4.3).

For $q \neq p$, we have

$$j_q \colon \mathcal{X}(\mathbb{Z}_q) \to H^1(G_q, U_2) \simeq H^1(G_q, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

the last map being $c \mapsto \log\chi \cup c \in H^2(G_q, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$, where χ is the p-adic cyclotomic character and $\cup$ is the cup product (note $\log\chi \in H^1(G_q, \mathbb{Q}_p)$). The middle bijection is proved in [15, §4.1.5]. Thus, finding the image of j_q is equivalent to finding

$$\{\phi_q(z) := \log\chi \cup j_q(z) : z \in \mathcal{X}(\mathbb{Z}_q)\}.$$

Theorem 4.1.6 in [15] shows that

$$2\phi_q \colon \mathcal{X}(\mathbb{Z}_q) \to \mathbb{Q}_q, \qquad z \mapsto 2(\log\chi \cup j_q(z))$$

is the restriction to $\mathcal{X}(\mathbb{Z}_q)$ of a p-adic local Néron function in the sense of §2.2.1 and must thus be equal to the function λ_q.

In particular, for each $q \neq p$, the set $2\phi_q(\mathcal{X}(\mathbb{Z}_q))$ is the finite set described by Proposition 4.2.1 and Proposition 4.2.3.

The cup product $\log\chi \cup c$, for $c \in H^1_f(G_p, \mathbb{Q}_p(1))$, and local reciprocity also yield an isomorphism

$$\psi_p \colon H^1_f(G_p, \mathbb{Q}_p(1)) \xrightarrow{\sim} H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

and we get a commutative diagram

$$\begin{array}{ccc} H^1_f(G_T, \mathbb{Q}_p(1)) & \xrightarrow{\oplus_{q\in T}\mathrm{loc}_q} & H^1_f(G_p, \mathbb{Q}_p(1)) \oplus \bigoplus_{q\in S} H^1(G_q, \mathbb{Q}_p(1)) \\ \Big\downarrow{\scriptstyle g=\log\chi\cup\,\cdot} & & \Big\downarrow{\scriptstyle \wr} \\ H^2(G_T, \mathbb{Q}_p(1)) & \xrightarrow{\oplus_{q\in T}\mathrm{loc}_q} & \bigoplus_{q\in T} H^2(G_q, \mathbb{Q}_p(1)) \simeq \bigoplus_{q\in T} \mathbb{Q}_p. \end{array}$$

On the other hand, by global class field theory and Hilbert's Theorem 90, the image of $H^2(G_T, \mathbb{Q}_p(1))$ in the bottom row is the kernel of the map

$$\bigoplus_{q\in T} \mathbb{Q}_p \to \mathbb{Q}_p, \qquad (a_q) \mapsto \sum_q a_q$$

and by dimension considerations, one concludes that the map g is in fact also an isomorphism.

From above we know that the image of $\bigoplus_{q\in S} j_q(\mathcal{X}(\mathbb{Z}_q))$ in $\bigoplus_{q\in S} \mathbb{Q}_p$ is precisely $(1/2)\bigoplus_{q\in S} W_q$, where

- if $[E(\mathbb{Q}_q) \colon E_0(\mathbb{Q}_q)] = 1$, then $W_q = \{0\}$
- if $[E(\mathbb{Q}_q) \colon E_0(\mathbb{Q}_q)] \neq 1$, then

$$W_q = \begin{cases} W_q^{\mathrm{bad}} & \text{if } q = 2 \text{ and } E \text{ is split multiplicative at } q, \\ W_q^{\mathrm{bad}} \cup \{0\} & \text{otherwise} \end{cases}$$

  and W_q^{bad} is defined in Proposition 4.2.3.

Let $W = \prod_{q \in S} W_q$. It follows from the above that for every $w = (w_q)_{q \in S} \in W$ there exists a unique $c \in H^1_f(G_T, \mathbb{Q}_p(1))$ with $2(\log \chi \cup \mathrm{loc}_q(c)) = w_q$ for every $q \in S$. Furthermore, this satisfies $2\psi_p(\mathrm{loc}_p(c)) = -||w||$.

On the other hand, if $q \notin T$ and $c \in H^1_f(G_T, \mathbb{Q}_p(1))$ then $\mathrm{loc}_q(c) = 0$ and $\mathrm{Im}(j_q) = \{0\}$ by Proposition 4.2.1. Therefore,

$$\mathrm{Sel}^2(\mathcal{X}) = \bigcap_{q \in S} \mathrm{loc}_q^{-1}(\mathrm{Im} j_q)$$

and

$$\mathrm{loc}_p(\mathrm{Sel}^2(\mathcal{X})) = \bigcup_{w \in W} \{c \in H^1_f(G_p, \mathbb{Q}_p(1)) : 2\psi_p(c) + ||w|| = 0\}.$$

It remains to compute the preimage of this set under j_p. As is shown in [15, §5.7], we find

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{z \in \mathcal{X}(\mathbb{Z}_p) : \mathrm{Log}(z) = 0, 2D_2(z) + ||w|| = 0\};$$

indeed, the condition $\mathrm{Log}(z) = 0$ is equivalent to requiring that

$$j_p(z) \in H^1_f(G_p, \mathbb{Q}_p(1)) \subset H^1_f(G_p, U_2)$$

and the other condition comes from the explicit formula

$$\psi_p(j_p(z)) = D_2(z) \quad \text{for } j_p(z) \in H^1_f(G_p, \mathbb{Q}_p(1)). \qquad \square$$

Remark 4.2.4. The corrections to the proof in [15] made here are the following. First of all, if $\mathcal{X}(\mathbb{Z}_q)$ is empty for some q, the proof does not hold. Of course this is a trivial case (treated in (1)), but it is not clear that the union given in Theorem 1.12 of *loc. cit.* should be empty. In fact, in Example 4.4.2 we find a curve satisfying the hypotheses of Theorem 4.1.2 (1), but for which $\bigcup_{w \in W} \phi(w) \neq \emptyset$.

Secondly, if the reduction type at q is non-split multiplicative of type I_m, with $m > 2$, not all the values in their sets W_q will be attained by a point in $E(\mathbb{Q}_q) \backslash E_0(\mathbb{Q}_q)$. Therefore, if a prime in S is non-split multiplicative, their statement should just be an inclusion of $\mathcal{X}(\mathbb{Z}_p)_2$ into the union of the $\Psi(w)$. One should note, however, that it seems like this was taken care of in the computations when the Tamagawa number at q is 1, but not when it is 2 (and hence m is even).

For the same reasons, if $q = 2$ is a prime of split multiplicative reduction of type I_m, with $m > 0$, the element 0 should not be included in W_q.

We remark that in all the examples they provided the set they computed turned out to be equal to $\mathcal{X}(\mathbb{Z})$ and hence to $\mathcal{X}(\mathbb{Z}_p)_2$.

Remark 4.2.5. The proof of [15, Theorem 1.12] is rather technical. However, for an elliptic curve of any rank, denoting by $\mathcal{X}(\mathbb{Z})_{\mathrm{tors}}$ the set of points of $\mathcal{X}(\mathbb{Z})$ of finite order, the easier statement

$$\mathcal{X}(\mathbb{Z})_{\mathrm{tors}} \subseteq \bigcup_{w \in W} \{z \in \mathcal{X}(\mathbb{Z}_p) : \mathrm{Log}(z) = 0, 2D_2(z) + ||w|| = 0\} \tag{4.4}$$

is elementary to prove. Indeed, the condition $\mathrm{Log}(z) = 0$ cuts out the torsion points in $\mathcal{X}(\mathbb{Z}_p)$. On the other hand, let

$$\beta = \begin{cases} C & \text{if } E \text{ is ordinary at } p, \\ \frac{a_1^2+4a_2}{12} & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{cases} \mathrm{Log}(z) = 0 \\ 2D_2(z) + ||w|| = 0 \end{cases} \iff \begin{cases} \mathrm{Log}(z) = 0 \\ 2D_2(z) + \beta\,\mathrm{Log}(z)^2 + ||w|| = 0 \end{cases}$$

$$\iff \begin{cases} \mathrm{Log}(z) = 0 \\ \lambda_p(z) + ||w|| = 0 \end{cases}$$

and, for $z \in \mathcal{X}(\mathbb{Z})$, $h_p(z) = \lambda_p(z) + ||w||$ for some $w \in W$, where h_p and λ_p are the global and local p-adic heights of §4.2.1. In particular, if $z \in \mathcal{X}(\mathbb{Z})_{\mathrm{tors}}$, we have $h_p(z) = 0$. In fact, we could have also obtained a height function by setting the local height at p to be the dilogarithm $2D_2(z)$.

Proof of Theorem 4.1.3. The proof of part (1) is identical to the proof of Theorem 4.1.2 (1). The proof of part (2) is straightforward from §4.2.2 and the proof of [15, Proposition 5.12]: the idea is that any two quadratic functions on the rank-one $E(\mathbb{Q})$ must be linearly dependent. See also Theorem 6.4.2 for a generalisation to number fields. Note that in the semistable case our statement is slightly different, as our set W is smaller if there are primes of non-split multiplicative reduction of type I_m, with $m > 2$ and also if $q = 2$ is a prime of split multiplicative reduction (cf. Remark 4.2.4). □

Remark 4.2.6. Theorem 4.1.3 is a consequence of the quadraticity of the p-adic height and of the square of the elliptic curve logarithm. Of course, that the latter function is quadratic follows from the linearity of the logarithm. We remark that Log^2 is in fact the p-adic height attached to the basis element ω of the Dieudonné module of E, in the language of generalised p-adic heights (see for instance [132, §4]), whereas the p-adic height h_p of Mazur–Tate is the one attached to an eigenvector with unit eigenvalue under the action of Frobenius. We could remove the assumption that p is ordinary in the statement of Theorem 4.1.3 if we replaced C with $\frac{a_1^2+4a_2}{12}$ and let h_p be the global p-adic height that we defined in §4.2.1 when p is supersingular.

4.3 Obstructions to $\mathcal{X}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}_p)_2$ in rank 0

We now derive some criteria for $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. In Section 4.4, we will compute $\mathcal{X}(\mathbb{Z}_p)_2$ for several curves and provide explicit examples for the results of this section. Since a necessary condition for $z \in \mathcal{X}(\mathbb{Z}_p)_2$ is that $\mathrm{Log}(z) = 0$, which can only occur if $z \in \mathcal{X}(\mathbb{Z}_p)_{\mathrm{tors}}$, after having fixed all appropriate embeddings, we must have

$$\mathcal{X}(\mathbb{Z}_p)_2 \subset \mathcal{E}(\overline{\mathbb{Z}})_{\mathrm{tors}} = E(\overline{\mathbb{Q}})_{\mathrm{tors}}.$$

We consider two reasons why extra points could arise in $\mathcal{X}(\mathbb{Z}_p)_2$: invariance of local heights under automorphism (§4.3.1) and existence of non-cyclotomic local heights over certain number fields (§4.3.2). Sometimes, a combination of the two is needed, as is the case in Proposition 4.3.14, which provides us with infinitely many curves over $\mathbb{Q}$ with points over a quartic field appearing in $\mathcal{X}(\mathbb{Z}_p)_2$ for suitable choices of p. In §4.3.3, we use this to deduce Theorem 4.1.4.

We start by proving an elementary fact: any obstruction to $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$ must come from points defined over number fields larger than $\mathbb{Q}$.

Proposition 4.3.1. *Suppose that E satisfies the assumptions of Theorem 4.1.2 (2) and that p is an odd prime of good reduction. Then*

$$\mathcal{X}(\mathbb{Z}_p)_2 \cap \mathcal{E}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z}).$$

Proof. Suppose $P \in \mathcal{X}(\mathbb{Z}_p)_2 \cap \mathcal{E}(\mathbb{Z})$. In particular, $\mathrm{Log}(P) = 0$, so P is torsion and hence $h_p(P) = 0$. On the other hand, since $P \in \mathcal{X}(\mathbb{Z}_p)_2$,

$$\lambda_p(P) + ||w|| = 0$$

for some $w \in W$. Therefore,

$$\sum_{q \neq p} \lambda_q(P) = ||w||.$$

By definition, we have

$$\sum_{q \neq p} \lambda_q(z) = \sum_{q \neq p} \alpha_q \log q, \qquad ||w|| = \sum_{q \neq p} \beta_q \log q$$

for some $\alpha_q, \beta_q \in \mathbb{Q}$, $\alpha_q = 0$ for all but finitely many q, $\beta_q = 0$ for all $q \notin S$ and $\beta_q \leq 0$ for all q. Thus

$$\log\left(\prod_{q \neq p} q^{d(\alpha_q - \beta_q)}\right) = 0,$$

for some non-zero integer d such that $d(\alpha_q - \beta_q) \in \mathbb{Z}$ for all q. This implies that $\alpha_q = \beta_q$ for all q, since the kernel of the p-adic logarithm is the subgroup of $\mathbb{Q}_p^\times$ generated by p and by the roots of unity. Suppose that z is not integral at q. Then by Lemma 2.2.2 (i), $\alpha_q > 0$, but $\beta_q \leq 0$, a contradiction. □

Remark 4.3.2. According to [127, VII, Application 3.5], if $P \in \mathcal{E}(\mathbb{Z})_{\text{tors}}$ then P is integral at all primes except possibly at 2 if P is 2-torsion. Thus the only q for which the proof of Proposition 4.3.1 is non-empty is $q = 2$. However, note that, with minor changes, the same proof shows the perhaps less trivial fact that $\mathcal{X}(\mathbb{Z}_p)_2' \cap \mathcal{E}(\mathbb{Z}) = \mathcal{X}(\mathbb{Z})$ in rank 1.

Remark 4.3.3. Unlike in §4.2.1, given a prime v of a number field, henceforth the notation λ_v will be used for the local height at v computed with respect to the model $\mathcal{E}$, which may not be minimal at v. The translation with the values computed with respect to a minimal model (Lemma 2.2.2 and Proposition 4.2.3) is given by (2.4).

4.3.1 Automorphisms

Recall that local heights are even functions. Therefore, if K is a quadratic field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and $z \in \mathcal{X}(\mathcal{O}_K)$ satisfies $\tau(z) = -z$, then

$$h_p(z) = \sum_q \lambda_{\mathfrak{q}}(z) = \lambda_{\mathfrak{p}}(z) + \sum_{q \in S} \lambda_{\mathfrak{q}}(z),$$

where $\mathfrak{q}$ (resp. $\mathfrak{p}$) is any prime of K above q (resp. p). Intuitively, in terms of local p-adic heights, the point z behaves as if it were defined over $\mathbb{Q}$; if furthermore z is a torsion point and p is split in K, then z will give rise to a point in $\mathcal{X}(\mathbb{Z}_p)_2$, provided that $\lambda_{\mathfrak{q}}(z) \in W_q$ at every $q \in S$. If the j-invariant of E is different from 0 and 1728, the automorphism group of $E/\overline{\mathbb{Q}}$ is generated by $z \mapsto -z$. On the other hand, if $j(E) \in \{0, 1728\}$, we can use the invariance of our local heights under any automorphism (cf. property (v) in §2.2.1 and property (iv) in §4.2.1) to generalise the above example as follows.

Proposition 4.3.4. *Suppose that E satisfies the assumptions of Theorem 4.1.2 and that p is an odd prime of good reduction. Let K be a Galois extension of $\mathbb{Q}$, such that there is an embedding $\rho\colon K \hookrightarrow \mathbb{Q}_p$. Extend ρ to a map $\mathcal{E}(\mathcal{O}_K) \hookrightarrow \mathcal{E}(\mathbb{Z}_p)$. Let $z \in \mathcal{X}(\mathcal{O}_K)_{\text{tors}}$ and suppose that for every $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ there exists $\psi_\tau \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ such that $\tau(z) = \psi_\tau(z)$.*

1. *For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and let $\lambda_{\mathfrak{q}}$ be the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. If*

$$\sum_{q \in S} \lambda_{\mathfrak{q}}(z) = ||w||$$

for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.

2. *In particular, if $z = \psi'(P)$ for some $\psi' \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ and some $P \in \mathcal{X}(\mathbb{Z})$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.*

Proof. The assumption that z is a torsion point implies that $h_p(z) = 0$ and $\mathrm{Log}(z) = 0$. Since for $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ there is an automorphism ψ_τ of E which acts on z in the same way as τ and local heights are invariant under automorphisms, for each prime $\mathfrak{q}$ of K we have

$$\lambda_{\mathfrak{q}}(z) = \lambda_{\mathfrak{q}}(\psi_\tau(z)) = \lambda_{\mathfrak{q}}(\tau(z)) = \lambda_{\tau^{-1}(\mathfrak{q})}(z).$$

Therefore,

$$0 = [K\colon \mathbb{Q}]h_p(z) = [K\colon \mathbb{Q}]\left(\lambda_p(\rho(z)) + \sum_{q \in S} \lambda_{\mathfrak{q}}(z)\right)$$

and (1) follows. For (2), since $z = \psi'(P)$, we have, similarly to above,

$$\lambda_{\mathfrak{q}}(z) = \lambda_{\mathfrak{q}}(\psi'(P)) = \lambda_q(P).$$

In particular, the hypothesis of (1) is satisfied. □

We now list a few consequences of Proposition 4.3.4. See Section 4.4 for explicit examples.

Corollary 4.3.5. *Suppose that E satisfies the assumptions of Theorem 4.1.2 and that p is an odd prime of good ordinary reduction. Suppose that*

$$\mathcal{E}\colon y^2 + a_3 y = x^3 + a_6, \quad \text{for some } a_6 \in \mathbb{Z} \text{ and } a_3 \in \{0, 1\},$$

and that there exists $y_0 \in \mathbb{Z}$ such that $a_6 - y_0^2 - a_3 y_0$ is a cube in $\mathbb{Z}$ and the points over $\overline{\mathbb{Q}}$ with y-coordinate equal to y_0 have finite order. Then $s(x) = x^3 + a_6 - y_0^2 - a_3 y_0$ splits completely in $\mathbb{Q}_p$ and for each root $\alpha \in \mathbb{Z}_p$ of $s(x)$, $\pm(\alpha, y_0) \in \mathcal{X}(\mathbb{Z}_p)_2$.

Remark 4.3.6. If in the corollary we have $a_3 = 1$, then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/3\mathbb{Z}$, since $E(\mathbb{Q})[2] = \{O\}$ and E has good reduction at 2 with $\#\overline{E}(\mathbb{F}_2) = 3$. By looking at the 3-rd division polynomial for E, it is then straightforward to check that Corollary 4.3.5 applies non-trivially only if $4a_6 = -(27n^6 + 1)$,

for some $n \in \mathbb{Z}$, $n \equiv 1 \bmod 2$. All such curves are isomorphic over $\mathbb{Q}$ to the elliptic curve 27.a3 [90]. When $a_3 = 0$, there are infinitely many curves non-isomorphic over $\mathbb{Q}$ for which the corollary applies with $y_0 = 0$: see for example §4.3.3. There is also at least one curve for which the Corollary applies to points of order 6, namely 36.a4 (see Table 4.2).

Proof. Since E has vanishing j-invariant, its automorphism group $\mathrm{Aut}(E/\overline{\mathbb{Q}})$ is a cyclic group of order 6 generated by $\psi\colon E \to E$, $\psi(x, y) = (\zeta x, -y - a_3)$, for a primitive third root of unity ζ.

Let $x_0 \in \mathbb{Z}$ such that $x_0^3 = y_0^2 + a_3 y_0 - a_6$. We may assume that $y_0^2 + a_3 y_0 - a_6$ is non-zero, as otherwise the statement of the corollary is trivial. Thus $s(x)$ has three distinct roots x_0, ζx_0 and $\zeta^2 x_0$ in $\overline{\mathbb{Z}}$.

Note also that, by Deuring's criterion [85, Ch. 13, Theorem 12], the primes of good ordinary reduction for E split completely in $\mathbb{Q}(\zeta)$, so $s(x)$ splits completely over $\mathbb{Q}_p$. Successively applying ψ to $(x_0, y_0) \in \mathcal{X}(\mathbb{Z})$ and localising at p we obtain all points of the form $\pm(\alpha, y_0)$. The corollary then follows from Proposition 4.3.4 (2). □

The following corollary to Proposition 4.3.4 is a special case of the motivating example of the beginning of this subsection.

Corollary 4.3.7. *Suppose that E satisfies the assumptions of Theorem 4.1.2 and that p is an odd prime of good reduction. Let K be a quadratic field, in which p splits. Fix an embedding $\rho\colon K \hookrightarrow \mathbb{Q}_p$ and let τ be the non-trivial element in* $\mathrm{Gal}(K/\mathbb{Q})$. *Assume that no prime in S ramifies in K and that, if $q \in S$ is inert, then either E has Kodaira symbol I_0^* at q with Tamagawa number at least 2 or E has maximal Tamagawa number for its Kodaira symbol. Then*

$$\mathcal{X}(\mathbb{Z}_p)_2 \supset \mathcal{X}(\mathbb{Z}) \cup \{\rho(z) \in \mathcal{X}(\mathbb{Z}_p) : z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}, \tau(z) = -z\}.$$

Proof. Since no prime in S ramifies in $K/\mathbb{Q}$, Tate's algorithm [125, IV, §9] shows that the equation for $\mathcal{E}$ defines a global minimal model for the base change E/K and that the Kodaira symbol at $\mathfrak{q} \mid q$ is the same as the Kodaira symbol at q. The Tamagawa number does not change if q is split in K; if q is inert, by assumption the Tamagawa number is unvaried, except possibly if the Kodaira symbol is I_0^*.

If q splits in K, fix a prime $\mathfrak{q}$ above it and an isomorphism $\rho_q\colon K_{\mathfrak{q}} \simeq \mathbb{Q}_q$. Let $z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}$ such that $\tau(z) = -z$. With the notation as in Proposition 4.3.4 and by Proposition 4.2.3, we have

$$\sum_{q \in S} \lambda_{\mathfrak{q}}(z) = \sum_{\substack{q \in S \\ q \text{ split}}} \lambda_q(\rho_q(z)) + \sum_{\substack{q \in S \\ q \text{ inert}}} \lambda_{\mathfrak{q}}(z) = ||w||$$

for some $w \in W$. For the last step note that Proposition 4.2.3 gives the values of $2\lambda_{\mathfrak{q}}(z)$ for $\mathfrak{q}$ inert. However, the norm of $\mathfrak{q}$ is q^2. The corollary then follows from Proposition 4.3.4 (1) with $\psi = -\mathrm{id} \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$. □

Remark 4.3.8. Another source of quadratic points in $\mathcal{X}(\mathbb{Z}_p)_2$ comes from elliptic curves with j-invariant equal to 1728. Suppose that E satisfies the assumptions of Theorem 4.1.2, that p is an odd prime of good reduction and that

$$\mathcal{E}\colon y^2 = x^3 + a_4 x \quad \text{for some } a_4 \in \mathbb{Z}, -a_4 \notin \mathbb{Z}^2.$$

Let $z \in \{(\pm\sqrt{-a_4}, 0)\}$ and $K = \mathbb{Q}(\sqrt{-a_4})$ be its field of definition. Let $\psi \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$ be defined by $\psi(x, y) = (-x, iy)$. Then $\psi(z) = \tau(z)$, where $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$. Therefore, under suitable conditions on how the reduction types change in $K/\mathbb{Q}$ and on the splitting of p in K, the localisations of the points z appear in $\mathcal{X}(\mathbb{Z}_p)_2$.

The following corollary explains how points over biquadratic extensions can show up in $\mathcal{X}(\mathbb{Z}_p)_2$ when the j-invariant is zero. For ease of notation, we assume that the a_3-coefficient in the equation defining $\mathcal{E}$ is zero, but this assumption could be removed.

Corollary 4.3.9. *Suppose that E satisfies the assumptions of Theorem 4.1.2 and that p is an odd prime of good ordinary reduction. Suppose that*

$$\mathcal{E}\colon y^2 = x^3 + a_6 \quad \textit{for some } a_6 \in \mathbb{Z}$$

and that there exists $x_0 \in \mathbb{Z}$ such that the points over $\overline{\mathbb{Q}}$ with x-coordinate equal to x_0 have finite order. Assume that p splits in $\mathbb{Q}(\sqrt{x_0^3 + a_6})$. Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{x_0^3 + a_6})$. For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and $\lambda_{\mathfrak{q}}$ the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. Let $\beta \in \mathbb{Z}_p$ be a root of $t(y) = y^2 - x_0^3 - a_6$. If

$$\sum_{q \in S} \lambda_{\mathfrak{q}}(x_0, \beta) = ||w||$$

for some $w \in W$, then for each root $\alpha \in \mathbb{Z}_p$ of $s(x) = x^3 - x_0^3$ and for each root $\beta \in \mathbb{Z}_p$ of $t(y) = y^2 - x_0^3 - a_6$, we have $(\alpha, \beta) \in \mathcal{X}(\mathbb{Z}_p)_2$.

Proof. If $x_0^3 + a_6$ is a square in $\mathbb{Z}$, the statement is precisely Corollary 4.3.5. Thus, we may assume that either

(i) K has degree 4 over $\mathbb{Q}$, or

(ii) $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{x_0^3 + a_6})$.

Let $\zeta \in K$ be a primitive third root of unity. The automorphism group $\mathrm{Aut}(E/K)$ is generated by $\psi\colon E \to E$, $\psi(x,y) = (\zeta x, -y)$. In case (i), the Galois group of K over $\mathbb{Q}$ is generated by two elements: σ, whose fixed field is $\mathbb{Q}(\sqrt{x_0^3 + a_6})$ and τ, whose fixed field is $\mathbb{Q}(\sqrt{-3})$. In case (ii), the Galois group is generated by $\sigma\colon \sqrt{-3} \mapsto -\sqrt{-3}$. Let $P = (a,b)$ where $a \in K$ is a root of $s(x)$ and $b \in K$ is a root of $t(y)$. Then in (i)

$$\sigma(P) \in \{P, -\psi(P), \psi^2(P)\}, \qquad \tau(P) = -P.$$

Similarly, in case (ii), we have

$$\sigma(P) \in \{-P, \psi(P), -\psi^2(P)\}.$$

Therefore, we may apply Proposition 4.3.4 (1). □

4.3.2 Non-cyclotomic *p*-adic heights

The set $\mathcal{X}(\mathbb{Z}_p)_2$ is a finite set of p-adic points containing $\mathcal{X}(\mathbb{Z})$. After having fixed a choice of a subspace of $H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$ complementary to the space of holomorphic forms, there is only one Coleman–Gross global height pairing on $E(\mathbb{Q})$, up to multiplication by a constant. The definition of $\mathcal{X}(\mathbb{Z}_p)_2$ depends on this height function. Nevertheless, when analysing what points could arise in the set $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$, we should bear in mind that other global height functions may exist on $E(F)$, where F is a number field, and that these also vanish on $E(F)_{\mathrm{tors}}$. In particular, suppose that there exists at least one embedding $\rho\colon F \hookrightarrow \mathbb{Q}_p$. It may happen that, for some $w \in W$ and some $Q \in \mathcal{X}(\mathcal{O}_F)$,

$$2D_2(\rho(Q)) + \beta \,\mathrm{Log}(\rho(Q))^2 + ||w|| = h_p^\star(Q)$$

for some non-cyclotomic global height $h_p^\star$. Then, if Q is in addition a torsion point, we have $\rho(Q) \in \mathcal{X}(\mathbb{Z}_p)_2$.

In order to define these more general types of heights, we need to introduce idele class characters. The definitions and properties that we list here summarise the results of Section 6.2, to which we refer the reader for more details.

Definition 4.3.10. Let $\mathbb{A}_F^\times$ be the group of ideles of F. An *idele class character* is a continuous homomorphism

$$\chi = \sum_{\mathfrak{q}} \chi_{\mathfrak{q}}\colon \mathbb{A}_F^\times / F^\times \to \mathbb{Q}_p;$$

here the sum is over all places of F.

The idele class character χ satisfies the following properties.

(PI) The local character $\chi_{\mathfrak{q}}$ is trivial at an archimedean place $\mathfrak{q}$. Thus, henceforth, $\mathfrak{q}$ will always denote a finite prime.

(PII) At a prime $\mathfrak{q}$ not above p, the local character $\chi_{\mathfrak{q}}$ vanishes on the units $\mathcal{O}_{\mathfrak{q}}^{\times}$. Thus, the value of $\chi_{\mathfrak{q}}$ at a uniformiser determines $\chi_{\mathfrak{q}}$ completely.

(PIII) At a prime $\mathfrak{p}$ above p, the restriction of the character $\chi_{\mathfrak{p}}$ to $\mathcal{O}_{\mathfrak{p}}^{\times}$ equals the composition

$$\mathcal{O}_{\mathfrak{p}}^{\times} \xrightarrow{\log_{\mathfrak{p}}} F_{\mathfrak{p}} \xrightarrow{t_{\mathfrak{p}}} \mathbb{Q}_p$$

for some $\mathbb{Q}_p$-linear map $t_{\mathfrak{p}}$. Here $\log_{\mathfrak{p}}$ is the restriction to $\mathcal{O}_{\mathfrak{p}}^{\times}$ of the extension of log to $F_{\mathfrak{p}}^{\times}$.

(PIV) The character χ is completely determined by the additive characters $(t_{\mathfrak{p}})_{\mathfrak{p}|p}$ and, conversely, a tuple of $\mathbb{Q}_p$-linear maps $(t_{\mathfrak{p}}\colon F_{\mathfrak{p}} \to \mathbb{Q}_p)_{\mathfrak{p}|p}$ gives an idele class character χ if and only if

$$\sum_{\mathfrak{p}|p} t_{\mathfrak{p}}(\log_{\mathfrak{p}}(\rho_{\mathfrak{p}}(\epsilon))) = 0 \quad \text{for all } \epsilon \in \mathcal{O}_F^{\times}, \tag{4.5}$$

where $\rho_{\mathfrak{p}}\colon F \hookrightarrow F_{\mathfrak{p}}$ is the completion (see Lemmas 6.2.2 and 6.2.3, and their proofs).

In particular, it suffices to check that (4.5) is satisfied for a set of fundamental units and (PIV) gives a concrete method for classifying all idele class characters for a given number field F.

For instance, for any number field F, the *cyclotomic* idele class character is the idele class character corresponding to the tuple of additive characters $(\mathrm{tr}_{F_{\mathfrak{p}}/\mathbb{Q}_p})_{\mathfrak{p}|p}$ (see also Example 6.2.7). When $F = \mathbb{Q}$, this is the only non-trivial idele class character, up to multiplication by a scalar. The p-adic height we have considered so far is implicitly associated to this character.

More generally though, we can define a p-adic height as a composition of two maps: firstly, we associate to a point $P \in E(F)$ an idele $i(P)$ and, secondly, we apply to $i(P)$ an idele class character χ. The theory of local heights that we outlined in the cyclotomic case in Section 2.2 goes through unvaried at the primes $\mathfrak{q} \nmid p$, after replacing the p-adic logarithm with $-\frac{\chi_{\mathfrak{q}}}{n_{\mathfrak{q}}}$. At the primes $\mathfrak{p} \mid p$, we may assume here that we always work with points not in the residue disk of the point at infinity[2]. So

[2]There is a subtlety in the disk at infinity which has to do with the choice of branch of the $\mathfrak{p}$-adic logarithm. See also Remark 6.2.1.

let $z \in \mathcal{X}(\mathcal{O}_\mathfrak{p})$ and $m \in \mathbb{N}$ such that mz is in the domain of convergence of $\sigma_\mathfrak{p}^{(\beta)}$. Then

$$\lambda_\mathfrak{p}^\chi(z) = -\frac{2}{m^2}\frac{\chi_\mathfrak{p}}{n_\mathfrak{p}}\left(\frac{\sigma_\mathfrak{p}^{(\beta)}(mz)}{f_m(z)}\right) = -\frac{2}{m^2 n_\mathfrak{p}} t_\mathfrak{p}\left(\log_\mathfrak{p}\left(\frac{\sigma_\mathfrak{p}^{(\beta)}(mz)}{f_m(z)}\right)\right), \tag{4.6}$$

since

$$\mathrm{ord}_\mathfrak{p}(\sigma_\mathfrak{p}^{(\beta)}(mz)) = \mathrm{ord}_\mathfrak{p}(x(mz)y(mz)^{-1}) = \mathrm{ord}_\mathfrak{p}(f_m(z))$$

(see §4.4.1 for how to interpret (4.6) when $mz = O$). We will omit χ from our notation when using the cyclotomic character.

Example 4.3.11. Let F be an imaginary quadratic field in which p splits. Then by (PIV), any pair of $\mathbb{Q}_p$-linear maps $\mathbb{Q}_p \to \mathbb{Q}_p$ gives rise to an idele class character.

We now give an instance of how the existence of non-cyclotomic heights for imaginary quadratic fields can give rise to points in $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$.

Proposition 4.3.12. *Suppose that E satisfies the assumptions of Theorem 4.1.2 and that p is an odd prime of good reduction. Let K be an imaginary quadratic field in which p splits. Fix an embedding $\rho\colon K \hookrightarrow \mathbb{Q}_p$. Suppose that $z \in \mathcal{X}(\mathcal{O}_K)_{\mathrm{tors}}$ has good reduction at all primes that split in K. Then*

$$2D_2(\rho(z)) + \sum_{q\in S}\lambda_\mathfrak{q}(z) = 0,$$

where $\mathfrak{q}$ is a prime of K above q. In particular, if $\sum_{q\in S}\lambda_\mathfrak{q}(z) = ||w||$, for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2$.

Proof. It suffices to show that $2D_2(\rho(z)) + \sum_{q\in S}\lambda_\mathfrak{q}(z)$ is the value at z of a height function on $E(K)$, since then the assumption that z is a torsion point will imply the vanishing. The height function that we are after is the one corresponding to an idele class character $\mathbb{A}_K^\times/K^\times \to \mathbb{Q}_p$ which vanishes on $\mathcal{O}_{\bar{\mathfrak{p}}}^\times$, if $\mathfrak{p}$ is the prime corresponding to the embedding ρ. Indeed, with the notation of (PIV), consider the idele class character corresponding to $(\mathrm{id}\colon K_\mathfrak{p} \simeq \mathbb{Q}_p \to \mathbb{Q}_p, 0\colon K_{\bar{\mathfrak{p}}} \simeq \mathbb{Q}_p \to \mathbb{Q}_p)$. Then

$$\lambda_\mathfrak{p}(z) = \lambda_\mathfrak{p}^\chi(z) \quad \text{and} \quad \lambda_{\bar{\mathfrak{p}}}^\chi(z) = 0.$$

Furthermore, since χ factors through $\mathbb{A}_K^\times/K^\times$ and in view of (PII), if there is a unique prime $\mathfrak{q}$ above q, we have

$$\chi_\mathfrak{q}(q) = -\chi_\mathfrak{p}(q) - \chi_{\bar{\mathfrak{p}}}(q) = -\log(q),$$

so that $2\lambda_\mathfrak{q}^\chi = \lambda_\mathfrak{q}$ for all primes which are either inert or ramified. Thus $2h_p^\chi(z) = 2D_2(\rho(z)) + \sum_{q\in S}\lambda_\mathfrak{q}(z)$. □

In some cases, extra points in $\mathcal{X}(\mathbb{Z}_p)_2$ are explained by a combination of automorphisms and non-cyclotomic idele class characters, as in Proposition 4.3.14. Before we state it and prove it, we need an auxiliary lemma.

Lemma 4.3.13. *Let F be a number field and let L be a finite extension of F. Suppose that $\chi\colon \mathbb{A}_F^\times/F^\times \to \mathbb{Q}_p$ is an idele class character determined by the tuple of $\mathbb{Q}_p$-linear maps $(t_\mathfrak{p}\colon F_\mathfrak{p} \to \mathbb{Q}_p)_{\mathfrak{p}|p}$. Then the tuple $(t_\mathfrak{q}^L\colon L_\mathfrak{q} \to \mathbb{Q}_p)_{\mathfrak{q}|p}$, defined by $t_\mathfrak{q}^L = t_\mathfrak{p} \circ \mathrm{tr}_{L_\mathfrak{q}/F_\mathfrak{p}}$ for $\mathfrak{q} \mid \mathfrak{p}$, determines an idele class character $\chi^L\colon \mathbb{A}_L^\times/L^\times \to \mathbb{Q}_p$ such that $\chi^L|_{\mathbb{A}_F^\times/F^\times} = [L\colon F]\chi$.*

Proof. Each $t_\mathfrak{q}^L$ is $\mathbb{Q}_p$-linear as a composition of $\mathbb{Q}_p$-linear maps. We need to check that (PIV) is satisfied. If $\epsilon \in \mathcal{O}_L^\times$, then

$$\begin{aligned}\sum_{\mathfrak{q}|p} t_\mathfrak{q}^L(\log_\mathfrak{q}(\rho_\mathfrak{q}(\epsilon))) &= \sum_{\mathfrak{p}|p} t_\mathfrak{p} \circ \left(\sum_{\mathfrak{q}|\mathfrak{p}} \mathrm{tr}_{L_\mathfrak{q}/F_\mathfrak{p}} \circ \log_\mathfrak{q}(\rho_\mathfrak{q}(\epsilon))\right)\\ &= \sum_{\mathfrak{p}|p} t_\mathfrak{p} \circ \log_\mathfrak{p}\left(\prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/F_\mathfrak{p}}(\rho_\mathfrak{q}(\epsilon))\right)\\ &= \sum_{\mathfrak{p}|p} t_\mathfrak{p} \circ \log_\mathfrak{p}\left(\rho_\mathfrak{p}(N_{L/F}(\epsilon))\right) = 0,\end{aligned}$$

since by [138, Corollary 10.2.3] we have $N_{L/F}(\alpha) = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/F_\mathfrak{p}}(\rho_\mathfrak{q}(\alpha))$ for any $\alpha \in L$, and since $N_{L/F}(\epsilon) \in \mathcal{O}_F^\times$. By construction, the resulting idele class character χ^L restricts to $[L\colon F]\chi$ on $\mathbb{A}_F^\times/F^\times$. □

Proposition 4.3.14. *Let d be a non-zero square-free integer and let E^d be the quadratic twist of $X_0(49)$ by d; assume that E^d satisfies the assumptions of Theorem 4.1.2 and let $\mathcal{X}^d$ be the complement of the origin in the regular minimal model of E^d. Let $p \nmid 7d$ be an odd prime with at least 3 primes lying above it in $L = \mathbb{Q}[x]/(x^4+7d^2)$. Then*

$$\mathcal{X}^d(\mathbb{Z}_p)_2 \supseteq \mathcal{X}^d(\mathbb{Z}) \cup \{\pm\rho(Q)\}$$

for some $Q \in \mathcal{X}^d(\mathcal{O}_L)$ of order 4 and for every embedding $\rho\colon L \hookrightarrow \mathbb{Q}_p$.

Remark 4.3.15. The proposition also holds in rank 1 if we replace $\mathcal{X}^d(\mathbb{Z}_p)_2$ with $\mathcal{X}^d(\mathbb{Z}_p)_2'$.

Proof. The elliptic curve $E = X_0(49)$ has reduced minimal model

$$\mathcal{E}\colon y^2 + xy = x^3 - x^2 - 2x - 1; \tag{4.7}$$

however, since we are considering quadratic twists of E, it is more convenient to work (at least until we introduce heights) with the following model

$$\mathcal{E}_{\text{short}}\colon y^2 = x^3 - 2835x - 71442,$$

as then the twist E^d of E by the non-zero square-free integer d admits the Weierstrass equation

$$\mathcal{E}^d_{\text{short}}\colon y^2 = x^3 - 2835d^2x - 71442d^3.$$

Recall that E^d has complex multiplication by $K = \mathbb{Q}(a)$, where a is a root of $x^2 + 7$. Over $K[x, y]$, the fourth division polynomial f_4^d of $\mathcal{E}^d_{\text{short}}$ has the following factorisation

$$f_4^d(x, y) = 4y(x - 9ad)(x + 9ad)(x + (-18a + 63)d)(x + (18a + 63)d)\\ (x^2 - 126xd - 5103d^2).$$

In particular, since

$$x^3 - 2835d^2x - 71442d^3 = (x - 63d)(x + (-9/2a + 63/2)d)(x + (9/2a + 63/2)d),$$

all the points of order 2 are defined over K. As for the points of order 4, we see that, as a polynomial in x, $f_4^d(x, y)/y$ has two roots in $\mathbb{Q}(\sqrt{7})$ and four roots in K. Substituting the latter roots into the equation for $\mathcal{E}^d_{\text{short}}$, we find that the y-coordinates of the points with $x = 9ad$ and $x = -(18a+63)d$ are defined over $\mathbb{Q}(\sqrt{-ad})$, whereas those with $x = -9ad$ and $x = -(-18a + 63)d$ are over $\mathbb{Q}(\sqrt{ad})$.

Therefore, over the quartic field $L = K[x]/(x^2 - ad) = K(b) \cong \mathbb{Q}[x]/(x^4 + 7d^2)$, $E^d(L)[4] \cong \mathbb{Z}/2 \times \mathbb{Z}/4$. Let $\mathrm{Gal}(L/K) = \langle\overline{\tau}\rangle$ and let

$$Q_{\text{short}} = (18b^2 - 63d, \pm(54b^3 - 378bd)) \in \mathcal{E}^d_{\text{short}}(L)[4], \qquad P_{\text{short}} = (63d, 0).$$

Then Q_{short} satisfies

$$\overline{\tau}(Q_{\text{short}}) = -Q_{\text{short}}. \tag{4.8}$$

Let Q be the image of Q_{short} in a minimal model $\mathcal{E}^d$ for E^d over $\mathbb{Z}$ and let P be the image of P_{short}. Note that

- if $d \equiv 1 \bmod 4$, we may apply to $\mathcal{E}^d_{\text{short}}$ the change of variables

  $$x \mapsto 36x - 9d, \qquad y \mapsto 216y + 108x$$

  to obtain the integral model

  $$\mathcal{E}^d_1\colon y^2 + xy = x^3 - \frac{3d + 1}{4}x^2 - 2d^2x - d^3.$$

The discriminant of $\mathcal{E}_1^d$ is $\Delta = -7^3 d^6$, so by [127, VII, Remark 1.1] $\mathcal{E}_1^d$ is a minimal model for $E^d/\mathbb{Q}$ and we may set $\mathcal{E}^d = \mathcal{E}_1^d$. Then $x(P) = 2d \in \mathbb{Z}$ and $x(Q) \in \mathcal{O}_K$.

- if $d \equiv 2, 3 \bmod 4$, then we may take

$$\mathcal{E}^d \colon y^2 = x^3 - 3dx^2 - 32d^2x - 64d^3,$$

which has discriminant $\Delta = -2^{12} \cdot 7^3 \cdot d^6$. Minimality of $\mathcal{E}^d$ at the primes different from 2 follows as in the case $d \equiv 1 \bmod 4$. At the prime 2, it can be deduced following Tate's algorithm. We have $x(P) = 8d \in \mathbb{Z}$ and $x(Q) \in \mathcal{O}_K$.

Now, let p be an odd prime of good reduction for E^d which splits in K. By Deuring's criterion, this is equivalent to requiring that p is a prime of good ordinary reduction. Let $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. The prime p is unramified also in L, since we are assuming that it is of good reduction. We suppose furthermore that $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1\overline{\mathfrak{q}_1}$, $\overline{\mathfrak{p}}\mathcal{O}_L = \mathfrak{q}_2$ or $\overline{\mathfrak{p}}\mathcal{O}_L = \mathfrak{q}_2\overline{\mathfrak{q}_2}$, for some primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ of L. These conditions, together, are equivalent to those of the statement of the proposition.

By Lemma 4.3.13, the idele class character on $\mathbb{A}_K^\times/K^\times$ which is trivial on $\mathcal{O}_{\overline{\mathfrak{p}}}^\times$ (and which we used also in the proof of Proposition 4.3.12) extends to an idele class character on $\mathbb{A}_L^\times/L^\times$. In particular, the tuple of linear maps

$$(\mathrm{id}_{L_{\mathfrak{q}_1} \simeq \mathbb{Q}_p}, \mathrm{id}_{L_{\overline{\mathfrak{q}_1}} \simeq \mathbb{Q}_p}, 0 \colon \prod_{\mathfrak{q} \mid \overline{\mathfrak{p}}} L_{\mathfrak{q}} \to \mathbb{Q}_p)$$

determines an idele class character χ. Consider the associated global height h_p^χ on $E^d(L)$ with local heights λ_v^χ with respect to the model $\mathcal{E}^d$. Since Q is a torsion point, we must have

$$h_p^\chi(Q) = 0.$$

It follows from (4.8) and the definition of χ that

$$\lambda_{\mathfrak{q}_1}^\chi(Q) = \lambda_{\overline{\mathfrak{q}_1}}^\chi(Q) = \lambda_{\mathfrak{q}_1}(Q) \quad \text{and} \quad \lambda_{\mathfrak{q}}^\chi(Q) = 0 \text{ for } \mathfrak{q} \mid \overline{\mathfrak{p}}.$$

Furthermore, using (PII) and the fact that χ is trivial on $L^\times$, we find that, for a fixed rational prime ℓ,

$$\sum_{v \mid \ell} \chi_v(\ell) = -2 \log \ell. \tag{4.9}$$

Since $P \in \mathcal{X}^d(\mathbb{Z})$, where $\mathcal{X}^d$ is the complement of the origin in $\mathcal{E}^d$, in order to prove the proposition it then suffices to show that

$$\frac{1}{2} \sum_{v \nmid p} n_v \lambda_v^\chi(Q) = \sum_{\ell \nmid p} \lambda_\ell(P),$$

where the left sum runs over primes of L and the right sum over rational primes.

In view of Lemma 4.3.13 and (2.4), we are allowed to perform isomorphisms over extensions of L to calculate local heights. In particular, the change of variables $(x, y) \mapsto (36dx - 9d, 216d\sqrt{d}y + 108d\sqrt{d}x)$, defined over $\mathbb{Q}(\sqrt{d})$, maps $\mathcal{E}^d_{\text{short}}$ to (4.7), which has discriminant -7^3. Under this isomorphism,

$$x(P_{\text{short}}) \mapsto 2 \in \mathbb{Z} \quad \text{and} \quad x(Q_{\text{short}}) \mapsto \frac{a-3}{2} \in \mathcal{O}_K.$$

Therefore, the local heights of P and Q away from $7p$ are trivial when computed with respect to (4.7). Using (4.9) and letting $d' = 7^{-\operatorname{ord}_7(d)}d$, we then have

$$\frac{1}{2}\sum_{v\nmid 7p} n_v \lambda_v^{\chi}(Q) = -\frac{1}{12[F\colon L]}\sum_{w\nmid 7p} \chi_w^F(\Delta^{-1}) = \begin{cases} -\log d' & \text{if } d \equiv 1 \bmod 4, \\ -\log 4d' & \text{otherwise,} \end{cases}$$

where $F = L(\sqrt{d})$, the second sum runs over the primes w of F and the character χ^F is the idele class character of F obtained from χ as in Lemma 4.3.13. Similarly, to calculate heights of P away from $7p$ we may base change to $\mathbb{Q}(\sqrt{d})$ and get:

$$\sum_{\ell\nmid 7p} \lambda_\ell(P) = \frac{1}{2}\sum_{u\nmid 7p} n_u \lambda_u(P) = \frac{1}{2}\sum_{u\nmid 7p} \frac{n_u}{6}\log(|\Delta|_u) = \begin{cases} -\log d' & \text{if } d \equiv 1 \bmod 4, \\ -\log 4d' & \text{otherwise,} \end{cases}$$

where u runs over primes of $\mathbb{Q}(\sqrt{d})$.

It remains to calculate the local contributions at primes above 7. For this, it is convenient to work with $\mathcal{E}^d_{\text{short}}$ which is minimal over $\mathbb{Z}_7$. Let v be the unique prime above 7 in L. Then $\operatorname{ord}_v(\Delta) = 12 + 24\operatorname{ord}_7(d)$. On the other hand, by [127, VII, Exercise 7.2], a minimal equation at v has discriminant of valuation at most 11. Therefore, E^d has good reduction at v and, since we are not in characteristic 2 or 3, a minimal equation at v is obtained from $\mathcal{E}^d_{\text{short}}$ via $(x, y) \mapsto (\pi_7^{\operatorname{ord}_v(\Delta)/6}x, \pi_7^{\operatorname{ord}_v(\Delta)/4}y)$, where π_7 is a uniformiser at v. Under such a change of variables, P_{short} and Q_{short} are mapped to v-adically integral points. Comparing discriminants as above, we then conclude that

$$\frac{1}{2}\sum_{v\nmid p} n_v \lambda_v^{\chi}(Q) = \sum_{\ell\nmid p} \lambda_\ell(P) = \begin{cases} -\frac{1}{2}\log 7 - \log d & \text{if } d \equiv 1 \bmod 4, \\ -\frac{1}{2}\log 7 - \log 4d & \text{otherwise.} \end{cases}$$

□

Remark 4.3.16. In the course of the proof of Proposition 4.3.14 it is actually also shown that if $v \nmid 7p$ is a prime of L, then $\lambda_v(Q) = \frac{1}{6}\log|\Delta|_v$, where Δ is the discriminant of a minimal model for E^d. Since 7 is totally ramified in L, we conclude that if

$v \nmid p$ then $\lambda_v(Q)$ only depends on the rational prime v lies above. Furthermore, in the notation of the proof, it is shown that if $\mathfrak{q} \mid p$ then $\lambda_{\mathfrak{q}}(Q)$ only depends on whether $\mathfrak{q}$ divides $\mathfrak{p}$ or $\overline{\mathfrak{p}}$ and that

$$\lambda_{\mathfrak{q}_1}(Q) + \frac{1}{4}\sum_{v \nmid p} n_v \lambda_v(Q) = 0.$$

Therefore, for each rational prime q, the set $\{\lambda_v(Q) : v \mid q\}$ is of size one.

4.3.3 Proof of Theorem 4.1.4

In this subsection we explain how Theorem 4.1.4 can be deduced either from Corollary 4.3.5 or from Proposition 4.3.14. For an elliptic curve E over $\mathbb{Q}$, denote by $L(E, s)$ its complex L-function.

Theorem 4.3.17 ([144], [141], [104, Ch. 6, Theorem 1.1]). *Let E be an elliptic curve over $\mathbb{Q}$. There exists infinitely many non-zero square-free integers d such that the quadratic twist E^d of E by d satisfies $L(E^d, 1) \neq 0$.*

Theorem 4.3.18 (Kolyvagin [82]). *Let E be an elliptic curve over $\mathbb{Q}$ such that $L(E, 1) \neq 0$. Then the rank of $E(\mathbb{Q})$ is zero and the Tate–Shafarevich group of $E/\mathbb{Q}$ is finite.*

It follows from Theorems 4.3.17 and 4.3.18 that there are infinitely many twists of $X_0(49)$ satisfying the hypotheses of Proposition 4.3.14. For each such curve, by Chebotarev's density theorem, there are infinitely many primes for which the proposition holds.

We now see how Corollary 4.3.5 also provides us with an alternative proof of Theorem 4.1.4. Consider the elliptic curve E with LMFDB label 36.a3 (see [90, 36.a3]), which has reduced minimal equation

$$\mathcal{E} \colon y^2 = x^3 - 27.$$

We have $\mathcal{E}(\mathbb{Z}) = \mathcal{E}(\mathbb{Z})[2] = \{O, (3, 0)\}$. It follows that every quadratic twist E^d of E by a non-zero square-free integer d satisfies $E^d(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$. The equation

$$\mathcal{E}^d \colon y^2 = x^3 - 27d^3$$

has discriminant equal to $-2^4 \cdot 3^9 \cdot d^6$ and is hence globally minimal, except if $3 \mid d$, in which case we apply $(x, y) \mapsto (9x, 27y)$ to obtain a minimal model. Thus, the point of exact order 2 of E^d defined over $\mathbb{Q}$ is integral. Therefore, by Theorems 4.3.17 and 4.3.18, there exists infinitely many d for which Corollary 4.3.5 holds with $y_0 = 0$.

4.4 Algorithm and computations in rank 0

4.4.1 The algorithm

We wish to explicitly compute the sets $\phi(w)$ and $\psi(w)$ from Theorems 4.1.2 and 4.1.3. Each of $D_2(z)$ and $\mathrm{Log}(z)$ are locally analytic functions on $\mathcal{X}(\mathbb{Z}_p)$. In other words, given a point $\overline{P} \in \overline{E}(\mathbb{F}_p) \setminus \{O\}$ and a fixed point $P \in \mathcal{X}(\mathbb{Z}_p)$ reducing to $\overline{P}$ modulo p, one can pick a uniformiser $t \in \mathbb{Q}_p(E)$ at P, which reduces to a uniformiser at $\overline{P}$. Then, for each $Q \in \mathcal{X}(\mathbb{Z}_p)$ in the residue disk of P, we have

$$\mathrm{Log}(Q) = f_P(t(Q)) \quad \text{and} \quad D_2(Q) = g_P(t(Q))$$

for some $f_P(x), g_P(x) \in \mathbb{Q}_p[[x]]$ convergent at all $x \in \mathbb{Z}_p$ with $|x|_p < 1$.

On the other hand, let $\beta = C$ if p is of good ordinary reduction and $\beta = \frac{a_1^2+4a_2}{12}$ if p is of good supersingular reduction. By Proposition 2.3.5 and §2.2.2 (ii), provided that $mQ \neq O$, where $m = \#\overline{E}(\mathbb{F}_p)$, then

$$2D_2(Q) + \beta\,\mathrm{Log}(Q)^2 = -\frac{2}{m^2}\log\left(\frac{\sigma_p^{(\beta)}(mQ)}{f_m(Q)}\right). \tag{4.10}$$

Since there are finitely many[3] points in each residue disk satisfying $mQ = O$, the local expansion of the right hand side of (4.10) in terms of the local parameter t holds in the whole residue disk. In fact, the local expansion of $\sigma_p^{(\beta)}(mQ)$ and $f_m(Q)$ have precisely the same zeros with the same multiplicity 1 and two p-adic power series which agree at infinitely many points in $\mathbb{Z}_p$ of absolute value less than 1 are equal by the p-adic Weierstrass Preparation Theorem [81, Ch. IV, §4, Theorem 14].

By the same observation as in Remark 4.2.5, we obtain a way of computing the intersections of $\phi(w)$ and $\psi(w)$ with each residue disk using local expansions of the p-adic sigma function (of Mazur–Tate or Bernardi) and the m-th division polynomial[4], in place of the double Coleman integral $D_2(z)$.

The function $\mathrm{Log}\colon \mathcal{X}(\mathbb{Z}_p) \to \mathbb{Q}_p$ is odd; the function $\lambda_p\colon \mathcal{X}(\mathbb{Z}_p) \to \mathbb{Q}_p$ is even (cf. property (iv) in §4.2.1). Therefore,

$$z \in \phi(w) \iff -z \in \phi(w)$$

and it will thus suffice to consider residue disks up to $\overline{P} \mapsto -\overline{P}$. The same holds for $\psi(w)$.

[3] In fact, at most one (cf. Remark 6.6.1).

[4] Computationally, it is more convenient to take m to be the order of $\overline{P}$ in $\overline{E}(\mathbb{F}_p)$, i.e. to choose potentially different values of m for different residue disks.

We also notice that different models can be used for computing the p-adic heights and the single Coleman integrals. In fact, we defined local p-adic heights using an integral minimal model and, for instance, there is an implementation for the Mazur–Tate p-adic sigma function in `SageMath` due to Harvey (see [67] and also [96]). On the other hand, for Coleman computations in `SageMath` (see [13]), one requires the elliptic curve to be described by a Weierstrass model whose a_1 and a_3 coefficients are zero and there is no requirement on minimality; the only requirement on integrality is $\mathbb{Z}_p$-integrality.

4.4.2 Examples for Section 4.3

In the examples that follow, as well as in the ones of the next sections, we avoid making distinctions between the curve $E/\mathbb{Q}$ and the model $\mathcal{E}/\mathbb{Z}$. The Weierstrass equations that we work with are always minimal and reduced, unless stated otherwise.

Example 4.4.1 (Corollary 4.3.7, Proposition 4.3.12). Consider the rank 0 elliptic curve 17.a1 [90]

$$E\colon y^2 + xy + y = x^3 - x^2 - 91x - 310 \tag{4.11}$$

and the prime $p = 5$ of good ordinary reduction.

Since none of the conditions of Theorem 4.1.2 (1) are satisfied, we need to explicitly compute $\mathcal{X}(\mathbb{Z}_p)_2$ as a union of $\phi(w)$. The curve has split multiplicative reduction at 17 with Kodaira symbol I_1 and good reduction everywhere else: thus, $W = \{0\}$. We find

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{(-5, 2 \pm \rho(i))\},$$

where $\rho\colon \mathbb{Z}[i] \hookrightarrow \mathbb{Z}_p$ is a fixed embedding. If a priori our computations only return approximations of p-adic points, by Corollary 4.3.7 the p-adic points found are the localisations of the points over $\mathbb{Z}[i]$ listed above. Let us nevertheless explain it in detail for this example.

The Weierstrass equation (4.11) defines a global minimal model also for the base change $E/\mathbb{Q}(i)$ and the prime p splits in $K = \mathbb{Q}(i)$. We extend ρ to a map $E(K) \hookrightarrow E(\mathbb{Q}_p)$. The point

$$Q = (-5, 2 + i) \in E(K)$$

is integral with respect to the global minimal model above and satisfies

$$4Q = O.$$

Thus, since the reduction types at the bad primes of $E/\mathbb{Q}(i)$ are the same as over $\mathbb{Q}$, we have

$$0 = h_p(Q) = \frac{1}{2}(\lambda_{\mathfrak{p}_1}(Q) + \lambda_{\mathfrak{p}_2}(Q)),$$

where $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$ and explicitly (without loss of generality)

$$\lambda_{\mathfrak{p}_1}(Q) = \lambda_p(\rho(Q)), \qquad \lambda_{\mathfrak{p}_2}(Q) = \lambda_p(\rho(\tau(Q))),$$

where $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$, so $\tau(Q) = (-5, 2-i)$. On the other hand, $\tau(Q) = -Q$ and λ_p is an even function. Therefore

$$0 = \lambda_p(\rho(Q)) = \lambda_p(\rho(\tau(Q))).$$

Note that Proposition 4.3.12 would also explain why the p-adic localisation of the point Q belongs to $\mathcal{X}(\mathbb{Z}_p)_2$.

Example 4.4.2 (Proposition 4.3.12, Proposition 4.3.4 (1)). Consider the elliptic curve 121.d3 [90]

$$E\colon y^2 + y = x^3 - x^2 - 40x - 221 \tag{4.12}$$

and the prime $p = 5$, at which E has good ordinary reduction. We have

$$\#\overline{E}(\mathbb{F}_2) = 1$$

and thus

$$\mathcal{X}(\mathbb{Z}_p)_2 = \emptyset$$

by Theorem 4.1.2 (1). On the other hand, we can still compute $\bigcup_{w\in W}\phi(w)$ of Theorem 4.1.3 (2). The curve has additive reduction of type I_1^* at 11 with Tamagawa number 2 and has good reduction everywhere else. Therefore,

$$W = \{0, -\log 11\}.$$

We find that $\phi(0) = \emptyset$, but

$$\phi(-\log 11) = \left\{\left(-7, \rho\Big(\frac{-1\pm 11\sqrt{-11}}{2}\Big)\right), \left(4, \rho\Big(\frac{-1\pm 11\sqrt{-11}}{2}\Big)\right)\right\},$$

where $\rho\colon \mathbb{Z}[(1+\sqrt{-11})/2] \hookrightarrow \mathbb{Z}_p$ is a fixed embedding.

Let $K = \mathbb{Q}(\sqrt{-11})$. The prime 11 ramifies in $K/\mathbb{Q}$ and E/K has split multiplicative reduction of type I_2 at $\mathfrak{q}$, where $\mathfrak{q}^2 = 11$. Let

$$Q \in \left\{\left(-7, \frac{-1\pm 11\sqrt{-11}}{2}\right), \left(4, \frac{-1\pm 11\sqrt{-11}}{2}\right)\right\} \subset E(K).$$

The point Q has order 5. Unlike in Example 4.4.1, the Weierstrass equation (4.12) is minimal at all primes except at $\mathfrak{q}$ and hence we cannot use straightforwardly the explicit formulae for the local height at $\mathfrak{q}$ given in §2.2.1. The curve E/K admits the global minimal model

$$E^{\min} : y^2 + y = x^3 - x^2$$

and the image of Q in $E^{\min}(K)$ has good reduction at $\mathfrak{q}$, so that $\lambda_{\mathfrak{q}}^{\min}(Q) = 0$. Equation (2.4) then yields $\lambda_{\mathfrak{q}}(Q) = -\log 11$. Therefore, by Proposition 4.3.12, we have

$$0 = \lambda_p(\rho(Q)) + \lambda_{\mathfrak{q}}(Q) = \lambda_p(\rho(Q)) - \log 11.$$

Similarly to Example 4.4.1, the appearance of $\rho(Q)$ in $\phi(-\log 11)$ is also justified by Proposition 4.3.4 (1).

Example 4.4.3 (Remark 4.3.8). Consider the elliptic curve 14112.q1 [90]

$$E\colon y^2 = x^3 - 9261x \tag{4.13}$$

and the prime $p = 5$, which is of good ordinary reduction. Note that p splits in $K = \mathbb{Q}(\sqrt{21})$ and by Remark 4.3.8, the localisations of the point $Q^{\pm} = (\pm 21\sqrt{21}, 0)$ belong to $\mathcal{X}(\mathbb{Z}_p)_2$ provided that (1/2) times the sum of its local heights at bad primes is in $||W||$. Both at 3 and 7, the curve has bad reduction of additive type III* with Tamagawa number 2; at 2 the curve has reduction of type III with Tamagawa number 2. Thus, $W = W_2 \times W_3 \times W_7$, with $W_q = \{0, -\frac{3}{2}\log q\}$ for each $q \in \{3, 7\}$ and $W_2 = \{0, -\frac{1}{2}\log 2\}$.

A global minimal model for the base change of E to K is given by $y^2 = x^3 - 21x$. Furthermore, 2 is inert in K and its reduction type does not change. The primes 3 and 7 become of type I_0^* with Tamagawa number 4. By Proposition 4.2.3 and Proposition 4.3.4 (1) (see also Remark 4.3.8), we then find that $Q^{\pm}$ is indeed in $\mathcal{X}(\mathbb{Z}_p)_2$.

Our computation of $\mathcal{X}(\mathbb{Z}_p)_2$ recovers precisely the integral points and the ones coming from $Q^{\pm}$.

Example 4.4.4 (Proposition 4.3.4 (1)). Consider the elliptic curve 11025.y2 [90], whose reduced minimal model is

$$E\colon y^2 + y = x^3 + 15006$$

and let $p = 13$, which is the smallest prime of good ordinary reduction for E. Note that E has vanishing j-invariant. We find that

$$\mathcal{X}(\mathbb{Z}_p)_2 = \{\pm(0, 122)\} \cup \{\pm(\zeta_3^i \sqrt[3]{120050}, 367) : 0 \le i \le 2\}, \tag{4.14}$$

where ζ_3 is a primitive third root of unity and we assume that we have fixed an embedding of $\mathbb{Q}(\zeta_3, \sqrt[3]{120050})$ into $\mathbb{Q}_p$. As usual, the equality (4.14) is deduced from computations combined with theoretical results. In this particular example, the theory needed is that the Galois group of $\mathbb{Q}(\zeta_3, \sqrt[3]{120050})/\mathbb{Q}$ acts on the order-6 points $\pm(\zeta_3^i \sqrt[3]{120050}, 367)$ by automorphisms. We leave the reader to check that these points also have the right local heights at bad primes.

Example 4.4.5 (Corollary 4.3.5, Corollary 4.3.9). Consider the elliptic curve 900.g3 [90] with reduced minimal model

$$E\colon y^2 = x^3 - 3375$$

and the prime 19, which is of good ordinary reduction for E. We have

$$\mathcal{X}(\mathbb{Z}_{19})_2 = \{(\zeta_3^i 15, 0), (-\zeta_3^i 30, \pm\sqrt{-30375}) : 0 \leq i \leq 2\}$$

where ζ_3 is a primitive third root of unity and we assume that we have fixed an embedding of $\mathbb{Q}(\zeta_3, \sqrt{-30375})$ into $\mathbb{Q}_{19}$.

4.4.3 Large-scale data

Using the database [90], we could run the code on all the $86,213$ elliptic curves over $\mathbb{Q}$ of rank 0 and conductor less than or equal to $30,000$; for each curve we let p be the smallest prime ≥ 5 of good ordinary reduction[5].

Out of these, we found exactly 470 pairs (E, p) for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. The 10 such pairs with E of conductor ≤ 100 are listed in Table 4.2.

We summarise the results of the computations in Propositions 4.4.6, 4.4.7, 4.4.9.

Proposition 4.4.6. *Let E be an elliptic curve of rank 0 and conductor less than or equal to $30,000$ and let $p \geq 5$ be the smallest prime of good ordinary reduction. Assume that $j(E) \notin \{0, 1728, -3375\}$. Then $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ is either empty or consists of localisations of points defined over the ring of integers of a quadratic field K on which the Galois group of $K/\mathbb{Q}$ acts as multiplication by ± 1.*

Proposition 4.4.7. *Let E be an elliptic curve of rank 0 and conductor less than or equal to $30,000$ and let $p \geq 5$ be the smallest prime of good ordinary reduction. If $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ contains localisations of points defined over a quadratic field K, these points satisfy the hypotheses of Proposition 4.3.4, i.e. the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts on them in the same way as an automorphism of E.*

[5] We could have allowed p to equal 3 and used the method of [6] to compute the quantities involved in the 3-adic heights. Some computations with supersingular primes were carried out for §4.4.4.

LMFDB	p	SS/CM	$\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$	Order	Explanation
17.a1	5	SS	$(-5, 2 \pm i)$	4	Cor. 4.3.7/Prop. 4.3.12
27.a3	7	$j = 0$	$\pm\left(\frac{-3\pm 3\sqrt{-3}}{2}, 4\right)$	3	Cor. 4.3.5/Prop. 4.3.12
32.a4	5	$j = 1728$	$(-2, \pm 4i)$	4	Prop. 4.3.4 (1)/Prop. 4.3.12
36.a3	7	$j = 0$	$\left(\frac{-3\pm 3\sqrt{-3}}{2}, 0\right)$	2	Cor. 4.3.5/Prop. 4.3.12
36.a4	7	$j = 0$	$\left(\frac{1\pm\sqrt{-3}}{2}, 0\right)$	2	Cor. 4.3.5/Prop. 4.3.12
			$\pm(-1 \pm \sqrt{-3}, 3)$	6	Cor. 4.3.5/Prop. 4.3.12
49.a2	11	$j = -3375$	$\pm\left(\frac{-7b^2+25}{2}, \frac{-49b^3+7b^2-49b-25}{4}\right)$	4	Prop. 4.3.14
49.a4	11	$j = -3375$	$\pm\left(\frac{b^2-3}{2}, \frac{b^3-b^2-7b+3}{4}\right)$	4	Prop. 4.3.14
75.b4	11	-	$(27, -14 \pm 5\sqrt{5})$	4	Prop. 4.3.4 (1)
75.b6	11	-	$\left(12, \frac{-13\pm 25\sqrt{5}}{2}\right)$	4	Prop. 4.3.4 (1)
			$\left(2, -\frac{3}{2}(1 \pm 5\sqrt{5})\right)$	4	Prop. 4.3.4 (1)
75.b7	11	-	$\left(2, \frac{1}{2}(-3 \pm 5\sqrt{5})\right)$	4	Prop. 4.3.4 (1)

Table 4.2: All curves of rank 0 and conductor ≤ 100 for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$ ($p \geq 5$ smallest good ordinary prime); b satisfies $x^4 + 7 = 0$. The curve is given in the first column as an LMFDB label [90]. In the third column, SS means 'semistable' and '-' neither semistable nor CM.

Remark 4.4.8. In view of the large data collected, it might have been tempting to expect that Propositions 4.4.6 and 4.4.7 would be true for arbitrary prime and conductor. It turns out that this is not the case: varying the prime for the curve 8712.u5 (which does not have CM), we found some quadratic points on which Galois does not act by automorphisms (cf. Example 4.4.11). We note nevertheless that in the latter case the extra points were explained by Proposition 4.3.12.

We now turn to the extra points in our data defined over number fields of degree[6] at least equal to 3. By Proposition 4.4.6, these can only show up if E has complex multiplication and, in fact, its j-invariant is one of $0, 1728, -3375$. There was only one curve besides the one of Example 4.4.4 where cubic points were recovered, namely the curve 19881.g2 [90]. As in Example 4.4.4, the curve has j-invariant equal to zero and the appearance of these points in $\mathcal{X}(\mathbb{Z}_p)_2$ is explained by Proposition 4.3.4.

Finally, we recovered points defined over number fields of degree 4 on the curve 14112.q2 ($j = 1728$) [90], which is explained by Proposition 4.3.4, and on all the twists of the modular curve $X_0(49)$, as predicted by Proposition 4.3.14. In fact the inclusion in the statement of Proposition 4.3.14 is an equality in all the following cases.

Proposition 4.4.9. *Let E be an elliptic curve of rank 0, conductor less than or equal to $30,000$ and $j(E) = -3375$. Then $\mathcal{X}(\mathbb{Z}_{11})_2 = \mathcal{X}(\mathbb{Z}) \cup \{\pm Q\}$, where Q has order 4 and comes from a point over the ring of integers of the smallest number field L over which $E(L)[4] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

4.4.4 Variation of the prime

In what follows, we assume that the rank of the elliptic curve is equal to zero. However, the discussion could easily go through word for word with $\mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{tors}}$ in place of $\mathcal{X}(\mathbb{Z}_p)_2$.

We have established that there exist curves of rank 0 and primes p for which $\mathcal{X}(\mathbb{Z}_p)_2 \supsetneq \mathcal{X}(\mathbb{Z})$. The next question we ask is whether there always exists a (not necessarily ordinary) prime for which the cohomologically global points of level 2 are precisely the global integral points. It turns out that the answer is negative, as we will see in Example 4.4.11 below.

[6]Note that by degree we mean the degree of the smallest number field over which a point in $\mathcal{X}(\mathbb{Z}_p)_2$ is defined and not the degree of the number field containing all the coordinates of the points in $\mathcal{X}(\mathbb{Z}_p)_2$, which could be larger.

Let us first gather some intuition on what is happening. Recall that, after having fixed all appropriate embeddings,

$$\phi(w) \subset \mathcal{E}(\overline{\mathbb{Z}})_{\mathrm{tors}} = E(\overline{\mathbb{Q}})_{\mathrm{tors}}.$$

Therefore, if $P \in E(F)_{\mathrm{tors}}$ for some minimal number field F, by picking p such that $[F_v \colon \mathbb{Q}_p] > 1$ for all $v \mid p$, we can guarantee that $P \notin \mathcal{X}(\mathbb{Z}_p)_2$. For instance in Example 4.4.1, if we pick $p' = 7$, which is of good ordinary reduction and which is inert in $\mathbb{Q}(i)$, we find $\mathcal{X}(\mathbb{Z}_{p'})_2 = \mathcal{X}(\mathbb{Z}) = \emptyset$.

Note that, in view of Corollary 4.3.5 and §4.3.3, there exist (infinitely many) curves for which $\mathcal{X}(\mathbb{Z}_p)_2$ is strictly larger than $\mathcal{X}(\mathbb{Z})$ for all odd primes p of good *ordinary* reduction. More generally, if E has complex multiplication by the quadratic field K and there exist points defined over K and satisfying the assumptions of Proposition 4.3.4 (1), then these points will show up in $\mathcal{X}(\mathbb{Z}_p)_2$ for any good ordinary odd prime p by Deuring's criterion. On the other hand, Deuring's criterion also implies that the good supersingular primes cannot split in K.

We ran the code on all the 470 curves of §4.4.3 for which we had found some extra points: this time, we varied the good ordinary prime until we found a prime for which no extra points showed up or we proved that such prime does not exist. If a good ordinary prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}_p)$ does not exist, we repeated the calculations with supersingular primes. We summarise the results in the following theorem (which includes also the statement of Theorem 4.1.5).

Theorem 4.4.10. *Let E be an elliptic curve over $\mathbb{Q}$ of rank 0 and conductor less than or equal to $30,000$. Then there exists a good ordinary odd prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z})$, unless:*

1. *E is 32.a4 ($j = 1728$) [90];*
2. *E is one of the 20 elliptic curves of rank 0 with $j = 0$ and $\mathbb{Z}/2\mathbb{Z} \subset E(\mathbb{Q})$ or E is 27.a3 ($j = 0$) [90];*
3. *E is 8712.u5 [90].*

Moreover, in cases (1) and (2), $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z}) \neq \emptyset$ for all good ordinary odd primes p, but there exists a supersingular prime p for which $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}_p)$; in case (3) $\mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z}) \neq \emptyset$ for all good (ordinary and supersingular) primes p.

Proof. That there exists a good ordinary prime for which Conjecture 4.1.1 holds at level 2 for all curves not in (1), (2) and (3) is shown computationally. The assertion of cases (1) and (2) follows from the discussion before the statement of the theorem together with explicit computations of $\mathcal{X}(\mathbb{Z}_p)_2$ at some supersingular primes p. Finally, we treat the curve 8712.u5 in detail in Example 4.4.11. □

Example 4.4.11. Consider the elliptic curve 8712.u5, given by

$$E\colon y^2 = x^3 + 726x + 9317. \tag{4.15}$$

K	q	Splitting	Reduction (Tamagawa)	$\lvert\Delta/\Delta_{\min}\rvert_{\mathfrak{q}}$	$\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$
$\mathbb{Q}(\sqrt{-11})$	2	inert	-	1	W_2
	3	split	-	1	W_3
	11	ramified	good	11^{-6}	W_{11}
$\mathbb{Q}(\sqrt{33})$	2	split	-	1	W_2
	3	ramified	non-split I_2 (2)	3^{-6}	W_3
	11	ramified	good	11^{-6}	W_{11}
$\mathbb{Q}(\sqrt{-3})$	2	inert	-	1	W_2
	3	ramified	non-split I_2 (2)	3^{-6}	W_3
	11	inert	I_0^* (4)	1	W_{11}

Table 4.3: Data for Example 4.4.11.

We have $S = \{2, 3, 11\}$: in particular, the reduction is of type III with Tamagawa number 2 at 2, of type I_1^* with Tamagawa number 4 at 3 and of type I_0^* with Tamagawa number 2 at 11. Thus $W = W_2 \times W_3 \times W_{11}$, where

$$W_2 = \left\{0, -\frac{1}{2}\log 2\right\}, \quad W_3 = \left\{0, -\log 3, -\frac{5}{4}\log 3\right\}, \quad W_{11} = \{0, -\log 11\}.$$

Consider

$$A := \left\{(-44, \pm 99\sqrt{-11}), (22, \pm 33\sqrt{33}), \left(\frac{11}{2}(1 \pm 3\sqrt{-3}), 0\right)\right\} \subset \mathcal{X}(\overline{\mathbb{Z}})_{\mathrm{tors}}.$$

If $p \notin S$, then p splits in at least one of $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{33})$ and $\mathbb{Q}(\sqrt{-3})$ and therefore $A \cap \mathcal{X}(\mathbb{Z}_p) \neq \emptyset$ (after having fixed embeddings). The fact that

$$A \cap \mathcal{X}(\mathbb{Z}_p)_2 \neq \emptyset,$$

then follows from Proposition 4.3.4 (1) (for the points over $\mathbb{Q}(\sqrt{-11})$ and $\mathbb{Q}(\sqrt{33})$), Proposition 4.3.12 (for the points over $\mathbb{Q}(\sqrt{-3})$) and Table 4.3, which shows how the reduction changes at the primes in S. The symbol - means that the reduction type has not changed. In the last column, there are the possible values of $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ where $\mathcal{O}_{\mathfrak{q}}$ is the ring of integers of the completion $K_{\mathfrak{q}}$ at a prime $\mathfrak{q}$ above q in the field K. We briefly explain how the table is computed. When the prime q splits in K, there is nothing to show: $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}})) = W_q$ if $\mathfrak{q} \mid q$. If q is inert, by Tate's algorithm, (4.15) is minimal at $\mathfrak{q} \mid q$ and the Kodaira symbol is unchanged. Once we know the Tamagawa number at $\mathfrak{q}$, we can find $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ directly from Proposition 4.2.3. Finally, if q ramifies in K, then $\lambda_{\mathfrak{q}}(\mathcal{X}(\mathcal{O}_{\mathfrak{q}}))$ may be deduced from Proposition 4.2.3, Lemma 2.2.2 (i) and (2.4). Note that some points in $\mathcal{X}(\mathcal{O}_{\mathfrak{q}})$ may map to non-integral points in a minimal model at $\mathfrak{q}$ (see also Lemma 4.6.4).

4.4.5 Further observations and analogies with the Strong Chabauty Conjecture

In view of the computations, we formulate the following conjecture. We add the assumption that p is ordinary simply because most of our computations were for ordinary primes; however, we expect no different behaviour for supersingular primes.

Conjecture 4.4.12. *Let $p \geq 5$ be a prime of good ordinary reduction for the elliptic curve $E/\mathbb{Q}$, which has rank 0 and whose Tate–Shafarevich group has finite p-primary part. Suppose that $z \in \mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ is the localisation of a torsion point over a number field K. Then, for each rational prime q, the local height $\lambda_{\mathfrak{q}}(z)$ is independent of the prime $\mathfrak{q} \mid q$ of K.*

Remark 4.4.13. The points of Propositions 4.3.4, 4.3.12 and 4.3.14 all satisfy Conjecture 4.4.12 (see also Remark 4.3.16).

Corollary 4.4.14. *If Conjecture 4.4.12 is true, then if $z \in \mathcal{X}(\mathbb{Z}_p)_2 \setminus \mathcal{X}(\mathbb{Z})$ is the localisation of a point defined over K, we have $z \in \mathcal{X}(\mathcal{O}_K)$.*

Proof. The proof is similar to that of Proposition 4.3.1. Note that a torsion point defined over an arbitrary number field can fail to be integral at $\mathfrak{q}$ only if its order is q^n for some n (where (q) is the prime of $\mathbb{Z}$ below $\mathfrak{q}$) and $\mathrm{ord}_{\mathfrak{q}}(q) \geq q^n - q^{n-1}$ (cf. [127, VIII, Theorem 7.1]). □

Conjecture 4.4.12 is in some sense a natural analogue of a conjecture of Stoll for the classical abelian Chabauty method [133, Conjecture 9.5], which appears in an unpublished draft of [134]. Let us restrict to the case when C is a hyperelliptic curve over $\mathbb{Q}$ of genus g, whose Jacobian J has rank $g-2$ over $\mathbb{Q}$ (for the conjecture in its full generality see Conjecture 5.4.4). Suppose that $\iota\colon C \hookrightarrow J$ is an embedding such that $\iota(C)$ generates J and that J is simple. Stoll's conjecture predicts the existence of a finite subscheme $Z \subset J$ and a set R of primes which has density 1 in the set of all primes such that, for each $\ell \in R$, we have $\overline{J(\mathbb{Q})} \cap \iota(C(\mathbb{Q}_\ell)) \subset Z(\mathbb{Q}_\ell)$, where $\overline{J(\mathbb{Q})}$ is the ℓ-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_\ell)$.

In Chapter 5 some evidence for Stoll's conjecture is collected when $g = 3$, with the scheme Z being the intersection of $\iota(C)$ with the saturation of $J(\mathbb{Q})$, that is

$$Z = \{\iota(P) \in J : n\iota(P) \in J(\mathbb{Q}) \text{ for some } n \in \mathbb{Z}_{\geq 1}\}.$$

In our setting of an elliptic curve of rank 0, it is clear that $\mathcal{X}(\mathbb{Z}_p)_2$ should be contained in the saturation of the Mordell–Weil group $E(\mathbb{Q})$, since $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}}$ and the equation $\operatorname{Log} z = 0$ cuts out the torsion points in $E(\mathbb{Q}_p)$. However, this is not a very strong requirement in the elliptic curve case, because the curve and the Jacobian are identified.

The conjecture asserts that the extra constraint $\lambda_p(z) = -||w||$, for some $w \in W$, leads to another type of "saturation", in the sense that we would be looking at those points for which the local heights behave as if the point were defined over $\mathbb{Q}$.

Note that Stoll's conjecture assumes that $g - r + l \geq 3$, where $l = 1$ is the level, in the sense that the Chabauty–Coleman method computes the cohomologically global points of level 1. In the situation discussed here we have $g = 1$, $r = 0$, $l = 2$, i.e. $g - r + l = 3$, so one could naively hope that for rank 1 similar conjectures could be formulated at level 3.

4.5 The rank 1 case

4.5.1 Algebraic non-rational points in $\mathcal{X}(\mathbb{Z}_p)'_2$ in rank 1

We retain the notation of Theorems 4.1.2 and 4.1.3. The set consisting of the torsion points in $\psi(w)$ is equal to $\phi(w)$. Therefore, the results of Section 4.3 translate into results for $\mathcal{X}(\mathbb{Z}_p)'_{2,\text{tors}}$.

Since each $\psi(w)$ is defined by a single p-adic equation, in most cases it is expected that $\mathcal{X}(\mathbb{Z}_p)'_2$ should be strictly larger than $\mathcal{X}(\mathbb{Z})$. The question we investigate in this subsection is which algebraic non-torsion points could arise in $\mathcal{X}(\mathbb{Z}_p)'_2$. The following

elementary lemma shows that if a non-torsion point in $\mathcal{X}(\mathbb{Z}_p)'_2$ comes from a quadratic point in the saturation of $E(\mathbb{Q})$, then its belonging to $\mathcal{X}(\mathbb{Z}_p)'_2$ cannot be explained by automorphisms (cf. §4.3.1).

Lemma 4.5.1. *Let E be an elliptic curve over $\mathbb{Q}$ and K a quadratic field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle\tau\rangle$. Let $P \in E(K) \setminus E(\mathbb{Q})$ such that $mP \in E(\mathbb{Q})$ for some non-zero integer m. Then, if $\psi(P) = \tau(P)$ for some $\psi \in \mathrm{Aut}(E/\overline{\mathbb{Q}})$, P has finite order.*

Proof. The hypotheses on P imply that $\psi \neq \mathrm{id}$. Since $mP \in E(\mathbb{Q})$, we have $O = mP - \tau(mP) = m(P - \tau(P))$. If $\psi = -\mathrm{id}$, then

$$\begin{cases} \tau(P) = -P \\ m(P - \tau(P)) = O \end{cases} \iff \begin{cases} \tau(P) = -P \\ 2mP = O; \end{cases}$$

thus, P has order dividing $2m$.

For more general ψ, let

$$[\,\cdot\,]\colon R \simeq \mathrm{End}(E)$$

where $R \subset \mathbb{C}$. Then there exists a root of unity ζ such that $\psi(P) = [\zeta]\,P$. Therefore,

$$\begin{cases} \tau(P) = [\zeta]\,P \\ m(P - \tau(P)) = O \end{cases} \iff \begin{cases} \tau(P) = [\zeta]\,P \\ [m(1-\zeta)]\,P = O \end{cases}$$

and so $P \in E(K)\left[mN_{\mathbb{Q}(\zeta)/\mathbb{Q}}(1-\zeta)\right]$. □

We could try and use non-cyclotomic idele class characters to motivate the existence of some algebraic points of infinite order in $\mathcal{X}(\mathbb{Z}_p)'_2$, following the ideas of §4.3.2. For example, what we could hope to prove is that at a certain $z \in \mathcal{X}(\overline{\mathbb{Z}})$ satisfying $mz \in E(\mathbb{Q})$ for some non-zero integer m, the quantity $2D_2(z) + C(\mathrm{Log}(z))^2 + ||w||$, for some $w \in W$, equals the value of *some* p-adic height function at z. If such a p-adic height comes from a character which restricts to the cyclotomic character on $\mathbb{A}_{\mathbb{Q}}^{\times}$ with the right normalisations, then looking at the equation defining $\psi(w)$ we see that this is enough to show $z \in \mathcal{X}(\mathbb{Z}_p)'_2$.

However, our computations (more on this in §4.5.2) also recovered some algebraic non-torsion points defined over real quadratic fields and we know that that the space of idele class characters of a real quadratic field is one-dimensional. Therefore, in the following proposition we present a sufficient condition for a point defined over a quadratic field to belong to $\mathcal{X}(\mathbb{Z}_p)'_2$, which looks less geometric or algebraic in nature compared to the results of Section 4.3. However, we then discuss in Remark 4.5.3 when we expect the hypotheses of the proposition to be satisfied.

Proposition 4.5.2. *Suppose that E satisfies the assumptions of Theorem 4.1.3 and that p is an odd prime of good ordinary reduction. Let K be a quadratic field in which p splits. Fix an embedding $\rho\colon K \hookrightarrow \mathbb{Q}_p$ and let τ be the non-trivial element in $\mathrm{Gal}(K/\mathbb{Q})$. Suppose that $z \in \mathcal{X}(\mathcal{O}_K)$ is such that $mz \in E(\mathbb{Q})\setminus\{O\}$ for some non-zero integer m and that*

$$f_m(z) = \zeta f_m(\tau(z)), \tag{4.16}$$

for some root of unity ζ. For each rational prime q, let $\mathfrak{q}$ be one (any) prime of K above q and $\lambda_{\mathfrak{q}}$ the local height at $\mathfrak{q}$ with respect to the model $\mathcal{E}$. If

$$\sum_{q\in S} \lambda_{\mathfrak{q}}(z) = ||w||$$

for some $w \in W$, then $\rho(z) \in \mathcal{X}(\mathbb{Z}_p)_2'$.

Proof. Let $\mathfrak{q} \nmid p$. By quasi-quadraticity (§2.2.1 (iv)) applied twice and the assumptions on z and m, we have

$$\begin{aligned}
\lambda_{\mathfrak{q}}(z) &= \frac{1}{m^2}\left(\lambda_{\mathfrak{q}}(mz) + 2\log|f_m(z)|_{\mathfrak{q}}\right)\\
&= \frac{1}{m^2}\left(\lambda_{\mathfrak{q}}(\tau(mz)) + 2\log|\zeta f_m(\tau(z))|_{\mathfrak{q}}\right)\\
&= \frac{1}{m^2}\left(\lambda_{\mathfrak{q}}(m\tau(z)) + 2\log|f_m(\tau(z))|_{\mathfrak{q}}\right)\\
&= \lambda_{\mathfrak{q}}(\tau(z)) = \lambda_{\tau(\mathfrak{q})}(z).
\end{aligned}$$

Similarly, if $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, then (without loss of generality)

$$\begin{aligned}
m^2\lambda_{\mathfrak{p}_1}(z) &= \lambda_p(mz) + 2\log(\rho(f_m(z)))\\
&= \lambda_p(mz) + 2\log(\rho(f_m(\tau(z)))) = m^2\lambda_{\mathfrak{p}_2}(z).
\end{aligned}$$

Therefore,

$$h_p(z) = \lambda_p(\rho(z)) + ||w||.$$

Since z is in the saturation of $E(\mathbb{Q})$ (i.e. $mz \in E(\mathbb{Q})$), then $z \in \psi(w)$. □

Remark 4.5.3. Let E, K and p be as in Proposition 4.5.2. Suppose that $z \in \mathcal{X}(\mathcal{O}_K)$ is such that $mz \in E(\mathbb{Q}) \setminus \{O\}$ and write $x(mz) = \frac{n(mz)}{d(mz)^2}$, for some coprime integers $n(mz)$ and $d(mz) > 0$. When can we expect (4.16) to hold? By [146, §2] and our assumptions, we know that

$$\frac{g_m(z)}{f_m(z)^2} = x(mz) = x(m\tau(z)) = \frac{g_m(\tau(z))}{f_m(\tau(z))^2},$$

where $g_m(z)$ can be written as a univariate polynomial in $x(z)$ over $\mathbb{Z}$. For $w \in \{z, \tau(z)\}$, define

$$\delta_m(w) = \frac{f_m(w)}{d(mw)}.$$

By Proposition 1 of *loc. cit.* $\delta_m(w)$ is a unit at all primes at which w has non-singular reduction. Furthermore, we have

$$\frac{\delta_m(z)}{\tau(\delta_m(\tau(z)))} = \frac{f_m(z)}{\tau(f_m(\tau(z)))} = 1.$$

Thus, if for example z has good reduction at all primes which are split in K, then $\tau(\delta_m(\tau(z))) = \delta_m(\tau(z))$ up to multiplication by elements of $\mathcal{O}_K^\times$: thus, in this case, $f_m(z) = uf_m(\tau(z))$ for some $u \in \mathcal{O}_K^\times$. If K is imaginary then u is a root of unity; otherwise u may or may not be. Note that if K is imaginary, we could have also avoided talking about division polynomials and followed a strategy similar to Proposition 4.3.12. Conversely, Proposition 4.5.2 is often not applicable for torsion points as it requires the existence of a *non-zero* multiple of z in $E(\mathbb{Q})$.

4.5.2 Computations in rank 1

The technique explained in §4.4.1 to compute $\mathcal{X}(\mathbb{Z}_p)_2$ in the rank 0 case can easily be adapted to compute $\mathcal{X}(\mathbb{Z}_p)'_2$ when the Mordell–Weil group has rank 1. As remarked in §4.5.1, the expectation is that $\mathcal{X}(\mathbb{Z}_p)'_2$ should generally be larger than $\mathcal{X}(\mathbb{Z})$.

We ran the code on all the 14,783 rank 1 elliptic curves of conductor at most 5,000 and let p be the smallest prime greater than or equal to 5 at which the curve has good ordinary reduction. The first observation is that it can happen that there are no points in $\mathcal{X}(\mathbb{Z}_p)'_2$ besides those in $\mathcal{X}(\mathbb{Z})$. For example, all the curves of conductor at most 500

- satisfying the assumptions of Theorem 4.1.3 (1) are 254.b1, 430.c1 [90];
- not satisfying Theorem 4.1.3 (1), but for which $\mathcal{X}(\mathbb{Z}_p)'_2 = \mathcal{X}(\mathbb{Z})$ are:

  297.b1, 325.b1 (see Example 4.A.1), 325.b2, 467.a1 [90].

Studying the torsion points of $\mathcal{X}(\mathbb{Z}_p)'_2$ morally provides more data on the extra points that can arise in $\mathcal{X}(\mathbb{Z}_p)_2$ when E has rank 0. No new phenomenon was observed, except that torsion points defined over some degree 4 number fields were also recovered on the two CM elliptic curves 576.e1 and 576.e2 [90] of j-invariant 54000.

The appearance of the latter points can be proved in a similar way to Proposition 4.3.14.

As far as algebraic non-torsion points are concerned, on 26 curves we identified non-torsion points defined over quadratic extensions of $\mathbb{Q}$. All of these were explained by Proposition 4.5.2 and only on two curves the points were defined over real quadratic fields. We now present an example in which some algebraic torsion and non-torsion points were recovered in $\mathcal{X}(\mathbb{Z}_p)'_2 \setminus \mathcal{X}(\mathbb{Z})$. Afterwards, we also include for completeness an example in which the extra algebraic non-torsion points are real.

Example 4.5.4. Consider the elliptic curve 576.e4 [90]

$$E\colon y^2 = x^3 + 8,$$

whose Mordell–Weil group over $\mathbb{Q}$ has rank 1 and is generated, modulo torsion, by the point $z_0 = (1, 3)$. Let $p = 7$, at which E has good ordinary reduction. We have $S = \{2, 3\}$ and $W = W_2 \times W_3$ where

$$W_2 = \{0, -\log 2\}$$
$$W_3 = \left\{0, -\frac{1}{2}\log 3\right\}.$$

Write

$$\mathcal{X}(\mathbb{Z}_p)'_2 = \mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{tors}} \cup \mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{nontors}},$$

where the subscripts tors and nontors have the obvious meaning. Let $K = \mathbb{Q}(\sqrt{-3})$ and let τ generate the Galois group of $K/\mathbb{Q}$. Assuming that we have fixed an embedding of $\mathbb{Q}(\sqrt{-3})$ into $\mathbb{Q}_p$, we find that

$$\mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{tors}} = \{(-2, 0), (1 \pm \sqrt{-3}, 0)\}$$
$$\mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{nontors}} = \pm\{(1, 3), (2, -4), (46, -312), (-5 \pm \sqrt{-3}, 6 \pm 6\sqrt{-3})\} \cup A^{\mathrm{nonalg?}}$$

where $A^{\mathrm{nonalg?}}$ denotes the set of points of $\mathcal{X}(\mathbb{Z}_p)'_2$ which have not been recognised as algebraic. Note that $A^{\mathrm{nonalg?}}$ modulo $\pm$ consists of 15 points. Corollary 4.3.5, together with the observation at the beginning of this section, proves why the two-torsion quadratic points $(1 \pm \sqrt{-3}, 0)$ belong to $\mathcal{X}(\mathbb{Z}_p)'_2$.

Consider now

$$Q \in \{\pm(-5 \pm \sqrt{-3}, 6 \pm 6\sqrt{-3})\}.$$

We will show why $Q \in \mathcal{X}(\mathbb{Z}_p)'_{2,\mathrm{nontors}}$. Without loss of generality we may assume that $Q = (-5 + \sqrt{-3}, 6 + 6\sqrt{-3})$. As

$$Q = -z_0 + (1 - \sqrt{-3}, 0),$$

$2Q \in E(\mathbb{Q})$. We have

$$f_2(Q) = 2y(Q) = \left(\frac{-1+\sqrt{-3}}{2}\right) f_2(\tau(Q)).$$

Therefore, in order to apply Proposition 4.5.2, it suffices to verify the condition on the local heights at the bad primes. For each prime $\mathfrak{q} \nmid p$, we could use the formula involving $f_2(Q)$ in order to compute $\lambda_{\mathfrak{q}}(Q)$, as in the proof of the proposition. We choose to compute it instead by the quasi-parallegram law

$$\begin{aligned}\lambda_{\mathfrak{q}}(Q) &= \lambda_{\mathfrak{q}}(z_0) + \lambda_{\mathfrak{q}}(1-\sqrt{-3}, 0) - \log|\sqrt{-3}|_{\mathfrak{q}} \\ &= \lambda_{\mathfrak{q}}(z_0) + \lambda_{\mathfrak{q}}(-2, 0) - \log|\sqrt{-3}|_{\mathfrak{q}},\end{aligned}$$

which gives

$$\lambda_{\mathfrak{q}}(Q) = \begin{cases} -\frac{1}{2}\log 3 & \text{if } \mathfrak{q} \mid 3, \\ -\log 2 & \text{if } \mathfrak{q} \mid 2, \\ 0 & \text{if } \mathfrak{q} \nmid 2, 3, p. \end{cases}$$

The fact that Q is in $\mathcal{X}(\mathbb{Z}_p)'_2$ then follows from Proposition 4.5.2.

Example 4.5.5. Consider the elliptic curve 525.c1 [90]

$$E\colon y^2 + xy = x^3 + x^2 - 450x + 3375.$$

Let p be an odd prime of good ordinary reduction split in $\mathbb{Q}(\sqrt{5})$ and fix an embedding $\mathbb{Q}(\sqrt{5}) \hookrightarrow \mathbb{Q}_p$. Then by Proposition 4.5.2 with $m = 2$, the infinite order points

$$\pm\left(10 \pm 5\sqrt{5}, \frac{5}{2}(23 \mp \sqrt{5})\right)$$

belong to $\mathcal{X}(\mathbb{Z}_p)'_2$.

4.6 Rational points on bielliptic curves

Let C be a smooth projective curve over $\mathbb{Q}$ of genus g and whose Jacobian J has Mordell–Weil rank equal to g. Assume in addition that the Néron–Severi group of J has rank at least equal to 2, that p is an odd prime of good reduction for C and that the p-adic closure of $J(\mathbb{Q})$ has finite index in $J(\mathbb{Q}_p)$. In [16, Theorem 1.2] Balakrishnan and Dogra use the Chabauty–Kim method to explicitly describe a finite set

$$C(\mathbb{Q}_p)_Z \subset C(\mathbb{Q}_p),$$

which depends upon the choice of a correspondence $Z \subset C \times C$ and which contains all the $\mathbb{Q}$-rational points of C. Note that one has $C(\mathbb{Q}_p)_2 \subset C(\mathbb{Q}_p)_Z$. The authors then make Theorem 1.2 algorithmic when C is a bielliptic curve of genus 2, under the extra assumption that J is ordinary at p (we remove this hypothesis here). Let

$$C\colon y^2 = x^6 + a_4x^4 + a_2x^2 + a_0, \qquad a_i \in \mathbb{Q},$$

be a genus 2 bielliptic curve with a rank-2 Jacobian and consider the associated maps $\varphi_i\colon C \to (E_i, O_{E_i})$, described affinely by

$$\begin{aligned} E_1\colon y^2 &= x^3 + a_4x^2 + a_2x + a_0, & \varphi_1(x,y) &= (x^2, y)\\ E_2\colon y^2 &= x^3 + a_2x^2 + a_4a_0x + a_0^2, & \varphi_2(x,y) &= (a_0x^{-2}, a_0yx^{-3}). \end{aligned}$$

Assume that each of E_1 and E_2 has rank 1. Then one may pick Z in such a way that $C(\mathbb{Q}_p)_Z$ can be described in terms of local and global p-adic heights of the images of the points of C in the two elliptic curves (we assume that the given equations for E_1 and E_2 are minimal at p). The superscript ^{E_i} indicates on which curve we are computing these quantities. Let P_i be a point of infinite order in $E_i(\mathbb{Q})$ and write

$$c_i = \frac{h_p^{E_i}(P_i)}{\mathrm{Log}^{E_i}(P_i)^2},$$

where, as usual, $h_p^{E_i}$ is the global p-adic height of Mazur–Tate or Bernardi depending on whether the reduction is ordinary or not. Let $Q_1 = (0, \sqrt{a_0}) \in E_1(\mathbb{Q}(\sqrt{a_0}))$ and $Q_2 = (0, a_0) \in E_2(\mathbb{Q})$. We assume that a_0 is a square in $\mathbb{Q}_p$. Furthermore, let

$$\begin{aligned} C^{(1)}(\mathbb{Q}_p) &= C(\mathbb{Q}_p) \setminus (]0, \sqrt{a_0})[\cup]0, -\sqrt{a_0})[)\\ C^{(2)}(\mathbb{Q}_p) &= C(\mathbb{Q}_p) \setminus (]\infty^+[\cup]\infty^-[)\\ C^{(i)}(\mathbb{Q}) &= C(\mathbb{Q}) \cap C^{(i)}(\mathbb{Q}_p) \quad \text{for } i = 1, 2, \end{aligned}$$

where the inverted square brackets denote the residue disk modulo p around the given point and $\infty^{\pm} = (1 : \pm 1 : 0) \in C(\mathbb{Q})$.

Theorem 4.6.1 (Balakrishnan–Dogra[7]). *For each $i \in \{1, 2\}$, the following set is finite*

$$W^i = \Bigg\{ \sum_{q \neq p} \left(\lambda_q^{E_i}(\varphi_i(z_q) + Q_i) + \lambda_q^{E_i}(\varphi_i(z_q) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z_q)) \right) : (z_q) \in \prod_{q \neq p} C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\} \Bigg\}.$$

[7]With a small correction: see Remark 4.6.2.

Furthermore,

$$C^{(i)}(\mathbb{Q}) \subset \big\{ z \in C^{(i)}(\mathbb{Q}_p) : 2\lambda_p^{E_{3-i}}(\varphi_{3-i}(z)) - \lambda_p^{E_i}(\varphi_i(z) + Q_i) - \lambda_p^{E_i}(\varphi_i(z) - Q_i) \\ -2c_{3-i}\,\mathrm{Log}^{E_{3-i}}(\varphi_{3-i}(z))^2 + 2c_i\,\mathrm{Log}^{E_i}(\varphi_i(z))^2 + 2h_p^{E_i}(Q_i) \in W^i \big\}.$$

The second assertion in Theorem 4.6.1 can be derived from the parallelogram law satisfied by the global p-adic height (Properties 2.2.7 (ii)) and the fact that there is at most one quadratic function (up to multiplication by a scalar) on each of $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$, due to the assumption on their ranks, in analogy with the proof of Theorem 4.1.3. The set of p-adic points described in the theorem is $C(\mathbb{Q}_p)_Z \cap C^{(i)}(\mathbb{Q}_p)$. We will explicitly determine the sets W^i for Example 4.6.3. For a general bielliptic curve we will give in Proposition 4.6.5 a description of a finite set containing W^i, hence giving a proof of finiteness of W^i. See Theorem 6.5.2 for an extension of this to general number fields.

Remark 4.6.2. If Q_1 is not defined over $\mathbb{Q}$, with the notation $\lambda_q^{E_1}(\varphi_1(z) \pm Q_1)$ in Theorem 4.6.1 we mean $\lambda_{\mathfrak{q}}^{E_1}(\varphi_1(z) \pm Q_1)$, where $\mathfrak{q}$ is any prime of $\mathbb{Q}(\sqrt{a_0})$ lying above the rational prime q. Indeed, since $\tau(Q_1) = -Q_1$, where $\langle\tau\rangle = \mathrm{Gal}(\mathbb{Q}(\sqrt{a_0})/\mathbb{Q})$, there is no dependence on $\mathfrak{q} \mid q$ and

$$h_p^{E_1}(Q_1) = \sum_q \lambda_q^{E_1}(Q_1).$$

The equations defining the sets $C(\mathbb{Q}_p)_Z \cap C^{(1)}(\mathbb{Q}_p)$ in [16, Corollary 8.1] contain a typo in the case when Q_1 is not in the saturation of $E_1(\mathbb{Q})$, which we have corrected in Theorem 4.6.1. Their formula has the term $2c_1\,\mathrm{Log}^{E_1}(Q_1)^2$ in place of $2h_p^{E_1}(Q_1)$ and does not hold unless the two quantities are equal.

One of the advantages of computing rational points using Theorem 4.6.1 for a bielliptic curve, rather than the more general techniques developed in [18], is that we do not need to have prior knowledge of any affine point in $C(\mathbb{Q})$.

Balakrishnan–Dogra–Müller [16] use Theorem 4.6.1, combined with the Mordell–Weil sieve, to determine precisely the rational points of two bielliptic curves. As in §4.4.1, we suggest here that one can replace the computations of double Coleman integrals with computations involving the p-adic sigma function and division polynomials. We use the resulting algorithm to compute $C(\mathbb{Q}_p)_Z$ for a bielliptic curve whose rational points were already found using different Chabauty-type techniques by Wetherell [145, Proposition 5.1] and Flynn–Wetherell [61, Example 3.1]. Our methods lead to an alternative provable determination of $C(\mathbb{Q})$. We will consider this curve again in Chapter 6 (see Example 6.7.2).

Example 4.6.3. Consider the bielliptic curve

$$C\colon y^2 = x^6 + x^2 + 1;$$

the associated elliptic curves are 496.a1 and 248.a1 [90], given by the following minimal models

$$E_1\colon y^2 = x^3 + x + 1, \qquad E_2\colon y^2 = x^3 + x^2 + 1.$$

We have

$$Q_1 = (0,1) \in E_1(\mathbb{Q}), \qquad Q_2 = (0,1) \in E_2(\mathbb{Q}).$$

Both elliptic curves have rank 1. Let $p = 3$, which is a prime of good reduction for C. Since E_1 is supersingular at p, we use Bernardi's p-adic height for our calculations.

Claim 4.1. *If $q \neq p, 2$ and $z \in C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\}$, then*

$$w_{q,i}(z) := \lambda_q^{E_i}(\varphi_i(z) + Q_i) + \lambda_q^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) = 0.$$

Proof. The curves E_1 and E_2 have everywhere good reduction except at 2 and 31. At 31, the Tamagawa number of each E_i is trivial. Assume first that $\varphi_i(z) \neq O_{E_i}$. Then, for each $q \neq p$, the quasi-parallelogram law (2.3) gives

$$w_{q,i}(z) = 2\left(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) - \log|x(\varphi_i(z))|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\right);$$

thus, if $q \neq 2$, by Lemma 2.2.2 (i),

$$\begin{aligned} w_{q,i}(z) &= 2(\log(\max\{1, |x(\varphi_i(z))|_q\}) - \log(\max\{1, |x(\varphi_{3-i}(z))|_q\}) - \log|x(\varphi_i(z))|_q) \\ &= 2(\log(\max\{1, |x(\varphi_i(z))|_q\}) - \log(\max\{1, |x(\varphi_i(z))|_q^{-1}\}) - \log|x(\varphi_i(z))|_q) \\ &= 0. \end{aligned}$$

It remains to consider the case $\varphi_i(z) = O_{E_i}$. Then $\varphi_{3-i}(z) \in \{\pm Q_{3-i}\}$ and

$$w_{q,i}(z) = 2\lambda_q^{E_i}(Q_i) - 2\lambda_q^{E_{3-i}}(Q_{3-i}) = 0$$

by Proposition 4.2.1, since Q_i and Q_{3-i} are integral and the Tamagawa numbers at q are equal to 1. □

Claim 4.2. *We have*

$$W^1 = \{0, \log 2\}, \qquad W^2 = \{-\log 2, -2\log 2\}.$$

Proof. By Claim 4.1,

$$W^i = \{w_{2,i}(z) := \lambda_2^{E_i}(\varphi_i(z) + Q_i) + \lambda_2^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_2^{E_{3-i}}(\varphi_{3-i}(z)) : \\ z \in C(\mathbb{Q}_2) \setminus \{\varphi_i^{-1}(\pm Q_i)\}\}.$$

First note that the curve E_1 has Tamagawa number equal to 1 at 2, whereas E_2 has Tamagawa number equal to 2 and reduction type III. If $|x(z)|_2 \leq 1$, then $\varphi_2(z)$ has good reduction at 2 and $\lambda_2^{E_2}(\varphi_2(z)) = \log|x(z)^{-2}|_2$; otherwise $\varphi_2(z)$ reduces to a singular point modulo 2 and, by Proposition 4.2.3, $\lambda_2^{E_2}(\varphi_2(z)) = -\frac{1}{2}\log 2$. Furthermore $\lambda_2^{E_2}(Q_2) = -\frac{1}{2}\log 2$. Therefore, similarly to the proof of Claim 4.1, if $\varphi_1(z) \neq O_{E_1}$, then by the quasi-parallelogram law we have

$$w_{2,1}(z) = 2\left(\lambda_2^{E_1}(\varphi_1(z)) - \lambda_2^{E_2}(\varphi_2(z)) - \log|x(\varphi_1(z))|_2\right) = \begin{cases} 0 & \text{if } |x(z)|_2 \leq 1, \\ \log 2 & \text{if } |x(z)|_2 > 1; \end{cases}$$

for the remaining points $z = \infty^{\pm}$ we get

$$w_{2,1}(z) = -2\lambda_2^{E_2}(Q_2) = \log 2,$$

thus proving the claim for W^1. The set W^2 is determined in a very similar fashion and we leave the details to the reader. □

We can now compute $C(\mathbb{Q}_p)_Z$ as a union of the two $C(\mathbb{Q}_p)_Z \cap C(\mathbb{Q}_p)^{(i)}$. We find

$$C(\mathbb{Q}_p)_Z = \{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\} \sqcup A \tag{4.17}$$

where A is a set of size 4. Note, however, that up to the automorphisms $(x, y) \mapsto (-x, y)$, $(x, y) \mapsto (x, -y)$ and their composites, A actually consists of one point:

$$P = (2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 3^8 + O(3^9), 2 + 2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 3^6 + 2 \cdot 3^8 + O(3^9)).$$

We follow the same strategy to the one of the proof of [16, Theorem 8.6] to rule out the possibility that P could be rational. The image of the point P under φ_2 is a point in $E_2(\mathbb{Q}_p)$ whose x-coordinate has valuation $\mathrm{ord}_p(x(\varphi_2(P))) = -2$. On the other hand, the Mordell–Weil group $E_2(\mathbb{Q}) \cong \mathbb{Z}$ is generated by Q_2 and, thus, if $\varphi_2(P) \in E_2(\mathbb{Q})$, there must exist a multiple of Q_2 whose x-coordinate has p-adic valuation equal to -2. As the smallest multiple of Q_2 in the formal group at p is $6Q_2 = \left(\frac{55}{81}, -\frac{971}{729}\right)$, we have reached a contradiction, since the set of points in the formal group whose x-coordinate has valuation at most -4 is a group.

4.6.1 Explicit formulae for the sets W^i

Theorem 4.6.1 asserts that the sets W^i, for $i = 1, 2$, are finite, but does not describe them explicitly. In order to obtain an implementation for the computations of the sets $C(\mathbb{Q}_p)_Z \cap C^{(i)}(\mathbb{Q}_p)$ for an arbitrary genus 2 bielliptic curve C, it would be convenient to have a characterisation of W^i that can be made algorithmic, in analogy with that of the sets W_q of Theorems 4.1.2 and 4.1.3.

We assume in this subsection that the coefficients a_0, a_2, a_4 defining C are in $\mathbb{Z}$.

For $i = 1, 2$, let $W_q^{E_{i,\min}}$ be the set W_q from Section 4.1 for a global minimal model $E_{i,\min}$ of E_i if q is a prime of bad reduction and with non-trivial Tamagawa number. If $E_{i,\min}$ has good reduction at $q \in \{2, 3\} \setminus \{p\}$ and $\overline{E}_{i,\min}(\mathbb{F}_q) = \{O\}$ or $q = 2$ and $E_{i,\min}$ has split multiplicative reduction I_1 at q, let $W_q^{E_{i,\min}} = \emptyset$. For all other $q \neq p$, let $W_q^{E_{i,\min}} = \{0\}$.

Let $W_q^{E_i}$ be the set of values attained by $\lambda_q^{E_i}$ on the points of $E_i(\mathbb{Q}_q)$ of the form (x, y) with $x, y \in \mathbb{Z}_q$ and let

$$V_q^{E_i} = W_q^{E_i} \cup \{0\}.$$

Write

$$\delta^{E_i} = \frac{\Delta^{E_i}}{\Delta^{E_{i,\min}}},$$

where Δ^{E_i} and $\Delta^{E_{i,\min}}$ are the discriminants of E_i and $E_{i,\min}$.

For sets A, B of elements in a field F, we write $A+B$ for their Minkowski addition and $-A$ for the set consisting of the additive inverses of the elements in A. If $A = \{a\}$, we write $a + B$ for $A + B$.

Lemma 4.6.4.

$$W_q^{E_i} = \frac{1}{6}\log|\delta^{E_i}|_q + \left(W_q^{E_{i,\min}} \cup \left\{2k\log q : 1 \leq k \leq \frac{1}{12}\operatorname{ord}_q(\delta^{E_i})\right\}\right).$$

In particular, $W_q^{E_i}$ is finite; it equals $\{0\}$ for all but finitely many q.

Proof. Let x, y and $x_{\min}, y_{\min}$ be the Weierstrass coordinates for E_i and $E_{i,\min}$, respectively. Then there exist $u, r, s, t \in \mathbb{Q}$, $u \neq 0$, such that

$$x = u^2 x_{\min} + r, \qquad y = u^3 y_{\min} + s u^2 x_{\min} + t.$$

Since $\operatorname{ord}_q(\Delta^{E_{i,\min}}) \leq \operatorname{ord}_q(\Delta^{E_i})$ for each prime q, the scalars u, r, s, t are furthermore all integral (see [48, Lemma 5.3.1] or [127, VII, Proposition 1.3 (d)]).

Now let $P \in E_i(\mathbb{Q}_q)$ such that $x(P), y(P) \in \mathbb{Z}_q$. By (2.4), we have

$$\lambda_q^{E_i}(P) = \lambda_q^{E_{i,\min}}(P) + \frac{1}{6}\log|\delta^{E_i}|_q.$$

If $x_{\min}(P) \in \mathbb{Z}_q$, then $\lambda_q^{E_{i,\min}}(P) \in W_q^{E_{i,\min}}$ by Propositions 4.2.3, 4.2.1 and Lemma 4.2.2. Otherwise, by Lemma 2.2.2 (i), we have $\lambda_q^{E_{i,\min}}(P) = \log \left|\frac{x(P)-r}{u^2}\right|_q$, where by assumption $|x(P) - r|_q \leq 1$ and the valuation of $\frac{x(P)-r}{u^2}$ is an even negative integer. Since $\delta^{E_i} = u^{12}$, this completes the proof of $\subseteq$. To see why the inclusion is actually an equality, notice that the preimage of an integral point in $E_{i,\min}(\mathbb{Q}_q)$ is certainly an integral point on $E_i(\mathbb{Q}_q)$. Furthermore, the points on $E_{i,\min}(\mathbb{Q}_q)$ in the formal group are parametrised by $t \in q\mathbb{Z}_q$ as follows: $t \mapsto (x_{\min}(t), y_{\min}(t))$, where

$$x_{\min}(t) = \frac{1}{t^2} - \frac{a_{1,\min}}{t} - a_{2,\min} - a_{3,\min}t + \cdots \in \mathbb{Z}[a_{1,\min}, \ldots, a_{6,\min}]((t)),$$

where $a_{1,\min}, \ldots, a_{6,\min}$ are the Weierstrass coefficients of $E_{i,\min}$; in particular, we have $\mathrm{ord}_q(x_{\min}(t)) = -2\,\mathrm{ord}_q(t)$. Thus for each $1 \leq k \leq \frac{1}{12}\,\mathrm{ord}_q(\delta^{E_i})$, setting $t = q^k$ gives a point on $E_{i,\min}(\mathbb{Q}_q)$ whose preimage in $E_i(\mathbb{Q}_q)$ has integral x-coordinate. The second assertion of the lemma follows from the explicit description of the sets $W_q^{E_{i,\min}}$. $\square$

Proposition 4.6.5. *With the notation of Theorem 4.6.1, suppose that* $\mathrm{ord}_\ell(a_0) \in \{0, 1\}$ *for each prime* ℓ*. For each prime* $q \neq p$*, let*

$$W_q^{1\prime} = \left\{2v + 2\lambda_q^{E_1}(Q_1) : v \in V_q^{E_1} + (-W_q^{E_2})\right\} \cup \left\{2v + 2\lambda_q^{E_1}(Q_1) - 2\log|a_0|_q : v \in W_q^{E_1}\right\}$$
$$W_q^{2\prime} = \left\{2v + 2\lambda_q^{E_2}(Q_2) - 2\log|a_0|_q : v \in W_q^{E_2} + (-V_q^{E_1})\right\} \cup \left\{2v + 2\lambda_q^{E_2}(Q_2) : v \in -W_q^{E_1}\right\}.$$

Then W^i *is a subset of the finite set*

$$W^{i\prime} = \left\{\sum_{q\neq p} w'_{q,i} : w'_{q,i} \in W_q^{i\prime}\right\} = \left\{2h_p^{E_i}(Q_i) - 2\lambda_p^{E_i}(Q_i) + \sum_{q\neq p}(w'_{q,i} - 2\lambda_q^{E_i}(Q_i)) : w'_{q,i} \in W_q^{i\prime}\right\}.$$

Proof. By definition,

$$W^i = \left\{\sum_{q\neq p} w_{q,i} : w_{q,i} \in W_q^i\right\},$$

where

$$W_q^i = \left\{w_{q,i}(z) := \lambda_q^{E_i}(\varphi_i(z) + Q_i) + \lambda_q^{E_i}(\varphi_i(z) - Q_i) - 2\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) : z \in C(\mathbb{Q}_q) \setminus \left\{\varphi_i^{-1}(\pm Q_i)\right\}\right\}.$$

Let $z \in C(\mathbb{Q}_q) \setminus \{\varphi_i^{-1}(\pm Q_i)\}$. If $\varphi_i(z) = O_{E_i}$, then

$$w_{q,i}(z) = 2\lambda_q^{E_i}(Q_i) - 2\lambda_q^{E_{3-i}}(Q_{3-i}),$$

which belongs to $2\lambda_q^{E_i}(Q_i) - 2W_q^{E_{3-i}}$. When $i = 2$, note that, while it is not always the case that Q_1 is defined over $\mathbb{Q}_q$ (and hence that $\lambda_q^{E_1}(Q_1) \in W_q^{E_1}$), here this follows from the assumption that its preimage under φ_1 is in $C(\mathbb{Q}_q)$.

Otherwise, by the quasi-parallelogram law (2.3), we have

$$\begin{aligned} w_{q,i}(z) &= 2\left(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) - \log|x(\varphi_i(z))|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\right) \\ &= 2\left(\lambda_q^{E_i}(\varphi_i(z)) + \lambda_q^{E_i}(Q_i) + \log|x(\varphi_{3-i}(z))|_q - \log|a_0|_q - \lambda_q^{E_{3-i}}(\varphi_{3-i}(z))\right). \end{aligned}$$

Note that the assumption that $0 \leq \mathrm{ord}_q(a_0) \leq 1$ implies that, for each $i = 1, 2$,

$$|x(\varphi_i(z))|_q > 1 \Rightarrow |x(\varphi_{3-i}(z))|_q < 1 \tag{4.18}$$

$$|x(\varphi_{3-i}(z))|_q < 1 \Rightarrow |x(\varphi_i(z))|_q \geq 1. \tag{4.19}$$

If $|x(\varphi_i(z))|_q > 1$, then $\varphi_i(z)$ reduces to a non-singular point modulo q, with respect to the Weierstrass equation for E_i. Thus $\lambda_q^{E_i}(\varphi_i(z)) = \log|x(\varphi_i(z))|_q$. Furthermore, by (4.18), $\varphi_{3-i}(z)$ is integral with respect to the Weierstrass equation defining E_{3-i} and we have $\lambda_q^{E_{3-i}}(\varphi_{3-i}(z)) \in W_q^{E_{3-i}}$. Therefore

$$\frac{w_{q,i}(z)}{2} \in \lambda_q^{E_i}(Q_i) + (-W_q^{E_{3-i}}).$$

Similarly, if $|x(\varphi_{3-i}(z))|_q > 1$, then

$$\frac{w_{q,i}(z)}{2} \in (\lambda_q^{E_i}(Q_i) - \log|a_0|_q) + W_q^{E_i}.$$

It remains to consider the case when $|x(z)|_q = 1$. Then

$$\frac{w_{q,i}(z)}{2} \in W_q^{E_i} + (-W_q^{E_{3-i}}) + \begin{cases} \lambda_q^{E_i}(Q_i) & \text{if } i = 1, \\ \lambda_q^{E_i}(Q_i) - \log|a_0|_q & \text{if } i = 2. \end{cases}$$

□

Proposition 4.6.5 and Lemma 4.6.4 turn Theorem 4.6.1 into an algorithm for computing a finite set of p-adic points containing $C(\mathbb{Q})$, for an arbitrary genus 2 bielliptic curve C whose associated elliptic curves E_1 and E_2 have Mordell–Weil rank equal to 1. Furthermore, to improve the estimates of the sets W^i provided by Proposition 4.6.5 we may use the fact that the contributions at primes of potential good reduction for C are trivial (cf. [16, Theorem 1.2 (i)]). It seems unlikely to the author that the elementary approach of Proposition 4.6.5 could show the latter for an arbitrary curve, since it is hard to imagine how the proof could be made sensitive to the difference between C being of potential good reduction and its Jacobian only being of potential good reduction. Furthermore, even at primes not of potential good reduction, the sets $W_q^{i\prime}$ might be larger than W_q^i. Nevertheless, having fixed an explicit curve C, the steps of the proof of the proposition should guide the reader through computing W^i precisely.

Here we are instead interested in an algorithm which does not require prior computations of W^i. So let $W^{i\prime\prime}$ be obtained from $W^{i\prime}$ of Proposition 4.6.5 by replacing $W_q^{i\prime}$ with $\{0\}$ whenever q is a prime of potential good reduction. We implemented in `SageMath` the results of this section and could test them for several bielliptic curves, including the ones of [16] and the bielliptic curve

$$C\colon y^2 = (x^2+1)(x^2+3)(x^2+7), \tag{4.20}$$

which appears in [61, p. 532] as the only curve amongst 50 bielliptic curves for which the methods of Flynn and Wetherell to find rational points failed.

For instance, in Example 4.6.3 and for the curve of §8.3 in [16] we have $W^i = W^{i\prime} = W^{i\prime\prime}$ for each $i = 1$ and $i = 2$, but for the curve of [16, §8.4], the sets $W^{i\prime\prime}$ have size 3, whereas W^i has size 1.

We also remark that in Example 4.6.3, as well as the two examples of [16], the elliptic curve E_1 has trivial Tamagawa number at all primes and E_2 has trivial Tamagawa numbers everywhere except for at one prime where it has Tamagawa number equal to two or three. In other words, finding precise expressions for the sets W^i by hand is straightforward. In Example 4.6.3 as well as [16, §8.3] the task is further simplified by the fact that the Weierstrass equations for E_1 and E_2 have minimal discriminant. On the other hand, we cannot expect this for a generic curve. For example, the elliptic curves corresponding to (4.20) have Tamagawa numbers $(2, 1)$ respectively $(4, 2)$ at the primes not of potential good reduction and analysing what happens at each prime by hand might be rather tedious. In this case, we find $\#W^{1\prime\prime} = \#W^{2\prime\prime} = 18$ and in fact this results in many points in $C(\mathbb{Q}_p)$ that are probably not rational (142 when $p = 5$).

Appendix

4.A Using a sieve to compute $\mathcal{X}(\mathbb{Z})$ in rank 1

We give a few examples where computations of $\mathcal{X}(\mathbb{Z}_p)'_2$ for one, two or three primes p, provably find the set $\mathcal{X}(\mathbb{Z})$. Note that, by Remark 4.3.2, a point in $\mathcal{X}(\mathbb{Z}_p)'_2 \setminus \mathcal{X}(\mathbb{Z})$ is not defined over $\mathbb{Q}$.

For some curves we can prove that $\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \emptyset$ without performing any computation (see §4.5.2); we concentrate here on examples where the hypotheses of Theorem 4.1.3 (1) are not satisfied.

Example 4.A.1 (One prime). Consider the elliptic curve 325.b1 [90], which has reduced minimal model

$$E\colon y^2 + y = x^3 - x^2 - 53x - 132.$$

We have $||W|| = \{0\}$. The prime $p = 7$ is of good ordinary reduction and

$$\overline{E}(\mathbb{F}_p) = \{\overline{O}, \overline{(3,0)}, \overline{(3,6)}, \overline{(4,3)}\}.$$

Since the equation defining $\mathcal{X}(\mathbb{Z}_p)'_2$ is invariant under $z \mapsto -z$, it suffices to consider the residue disks $\overline{(3,0)}$ and $\overline{(4,3)}$. Thus, $\mathcal{X}(\mathbb{Z}_p)'_2/\langle\pm 1\rangle$ can be determined from the union of the roots of two p-adic equations. One of the two equations has a simple root which we identify as coming from the point $(-4,0)$; the other equation has two simple roots, corresponding to $\pm(18,-67)$. Thus,

$$\mathcal{X}(\mathbb{Z}_p)'_2/\langle\pm 1\rangle = \{(-4,0),(18,-67)\}.$$

When $\mathcal{X}(\mathbb{Z}_p)'_2$ is larger than the set $\mathcal{X}(\mathbb{Z})_{\text{known}}$ of known integral points, in [10] it is suggested that one might try to use information coming from the computation of $\mathcal{X}(\mathbb{Z}_p)'_2$ for several primes p to provably find $\mathcal{X}(\mathbb{Z})$. The idea is to look for sequences of distinct primes $(p_1,\dots,p_m)$ of good reduction with the property that $p_{i+1} \mid \#\overline{E}(\mathbb{F}_{p_i})$, where $i+1$ is taken modulo m. Such a sequence is called a *pseudo-aliquot cycle*. Suppose that $z \in \mathcal{X}(\mathbb{Z}_{p_1})'_2 \setminus \mathcal{X}(\mathbb{Z})_{\text{known}}$ is such that $z = nP$ where $E(\mathbb{Q}) = \langle P\rangle$. The fact that $p_{i+1} \mid \#\overline{E}(\mathbb{F}_{p_i})$ allows one to obtain a chain of congruence conditions on n which can sometimes lead to a contradiction.

Example A.1 of [10] shows a successful computation of $\mathcal{X}(\mathbb{Z})$ using a cycle of length 2. We implemented the sieve for cycles of arbitrary length, but so far have found examples where the sieve succeeds to rule out all the points in $\mathcal{X}(\mathbb{Z}_{p_1})'_2 \setminus \mathcal{X}(\mathbb{Z})_{\text{known}}$ only when the cycle has length 2 or 3. Since the idea for a cycle of length 3 easily generalises to length m, we prefer to work through the details of an example rather than outlining the general strategy (which is briefly sketched in [10]). Here is a list of curves, including the one of [10] and the ones of Examples 4.A.2 and 4.A.3, where a sieve with two or three primes succeeded in determining $\mathcal{X}(\mathbb{Z})$.

LMFDB [90]	primes	LMFDB [90]	primes
101.a1	$(5, 7)$	304.d2	$(7, 11)$
143.a1	$(5, 7)$	361.a2	$(5, 7)$
148.a1	$(7, 11)$	404.b1	$(5, 7)$
185.b1	$(11, 17)$	432.d1	$(7, 13)$
248.a1	$(7, 11)$	387.d1	$(5, 7, 11)$
304.b1	$(7, 11)$	141.d1	$(5, 7, 11)$

See also Example 6.7.2 (O2) for the use of a pseudo-aliquot cycle of length 1.

In the following examples, since we work with more than one prime p, we sometimes add the subscript p to previously introduced notation.

Example 4.A.2 (Two primes). Consider the elliptic curve 304.d2 [90], given by

$$E\colon y^2 = x^3 + x^2 - 76;$$

we have

$$||W|| = \left\{0, -\log 2, -\frac{13}{4}\log 2\right\}.$$

The primes 7 and 11 form a pseudo-aliquot cycle. The computation of $\mathcal{X}(\mathbb{Z}_p)'_2$ for $p \in \{7, 11\}$ gives

$$\mathcal{X}(\mathbb{Z})_{\text{known}} = \pm\{(4, 2), (10, 32), (187, -2564)\} \subseteq \mathcal{X}(\mathbb{Z});$$

to show the inclusion is an equality, we further need to prove that the points in $\mathcal{X}(\mathbb{Z}_p)'_2 \setminus \mathcal{X}(\mathbb{Z})_{\text{known}}$, for one of $p \in \{7, 11\}$, cannot belong to $\mathcal{X}(\mathbb{Z})$.

The point $P = (10, 32)$ generates $E(\mathbb{Q})$. Let $w \in ||W||$ and suppose that z_7 is a root of $\lambda_7(z) + w = c(\text{Log}_7(z))^2$. If $z_7 = nP$, then looking at the image of z_7 and P in $\overline{E}(\mathbb{F}_7)$ we can compute n modulo the order of the reduction of P, i.e. modulo 11; furthermore, we can compute n modulo 7 from $\text{Log}_7(P)^{-1}\,\text{Log}_7(z) \bmod 7$. We now run through all the roots of $\lambda_{11}(z) + w = c(\text{Log}_{11}(z))^2$; if a root z_{11} corresponds to the integral point z_7, then $\text{Log}_{11}(P)^{-1}\,\text{Log}_{11}(z_{11}) \equiv n \bmod 11$ and $n \equiv a \bmod 7$ where $\overline{z_{11}} = a\overline{P}$ in $\overline{E}(\mathbb{F}_{11})$, since $7\overline{P} = \overline{O} \in \overline{E}(\mathbb{F}_{11})$.

This argument leads to a contradiction for each of the 14 points in $\mathcal{X}(\mathbb{Z}_7)'_2 \setminus \mathcal{X}(\mathbb{Z})_{\text{known}}$.

Example 4.A.3 (Three primes). Consider the elliptic curve 387.d1 [90]

$$E\colon y^2 + xy = x^3 - x^2 - 15x - 46,$$

which has reduction III* at 3 with Tamagawa number 2, non-split multiplicative reduction of type I_1 (and thus Tamagawa number 1) at 43 and good reduction everywhere else. Therefore,

$$||W|| = \left\{0, -\frac{3}{2}\log 3\right\}.$$

The three smallest primes of good reduction for E are 5, 7, 11. Calculating $\mathcal{X}(\mathbb{Z}_p)'_2$ for $p \in \{5, 7, 11\}$, we find that

$$\pm(10, 22) \in \mathcal{X}(\mathbb{Z});$$

however, the computations at each p recover also some points which we cannot recognise as points in $\mathcal{X}(\mathbb{Z})$. The point $P = (10, 22)$ generates $E(\mathbb{Q})$. Note that

p	order of $\overline{P} \in \overline{E}(\mathbb{F}_p)$
5	7
7	11
11	15

For each $w \in ||W||$ we do the following:

Step (1) Compute the solutions z_5 to $\lambda_5(z)+w = c(\mathrm{Log}_5(z))^2$. If $z_5 \in \mathcal{X}(\mathbb{Z})$ then $z_5 = nP$ for some $n \in \mathbb{Z}$ with

- $n \equiv n_7 \bmod 7$ where $\overline{z_5} = n_7\overline{P}$ in $\overline{E}(\mathbb{F}_5)$.
- $n \equiv n_5 \bmod 5$ where $n_5 = \mathrm{Log}_5(z_5)(\mathrm{Log}_5(P))^{-1} \bmod 5$.

Step (2) The integral point z_5 must be a solution to $\lambda_7(z) + w = c(\mathrm{Log}_7(z))^2$. So, let $z_7^{(i)}$ be a root of the latter equation and suppose that $z_7^{(i)} = z_5$. Then

- n_7 must equal $n_7^{(i)} = \mathrm{Log}_7(z_7^{(i)})(\mathrm{Log}_7(P))^{-1} \bmod 7$; if this holds, then we must also have
- $n \equiv n_{11}^{(i)} \bmod 11$ where $\overline{z_7^{(i)}} = n_{11}^{(i)}\overline{P}$.

This produces a list of tuples $(n_5, n_7, n_{11}^{(i)})$ for each i that has survived the sieve.

Step (3) If the list is non-empty, we then use the fact that z_5 must also be a root of $\lambda_{11}(z) + w = c(\mathrm{Log}_{11}(z))^2$. For a root $z_{11}^{(j)}$ suppose that $z_{11}^{(j)} = z_5$. Then

- There must exist i such that $n_{11}^{(i)} = n_{11}^{(j)}$ where $n_{11}^{(j)} = \mathrm{Log}_{11}(z_{11}^{(j)})(\mathrm{Log}_{11}(P))^{-1} \bmod 11$. If such i exists, we must also have

– $n_5 \equiv n_{15}^{(j)} \bmod 5$ where $\overline{z_{11}^{(j)}} = n_{15}^{(j)}\overline{P}$.

Explicitly, we have that $w = 0$ does not contribute to any point in $\mathcal{X}(\mathbb{Z}_5)_2'$. On the other hand, for $w = -\frac{3}{2}\log 3$, we find, besides $\pm P$, the points

$$\pm\left(2\cdot 5 + 4\cdot 5^3 + O(5^6), 2 + 4\cdot 5 + 3\cdot 5^3 + 3\cdot 5^4 + O(5^6)\right)$$
$$\pm\left(2 + 2\cdot 5 + 5^2 + 3\cdot 5^3 + 2\cdot 5^4 + 4\cdot 5^5 + O(5^6), 1 + 5 + 3\cdot 5^2 + 5^3 + 5^4 + O(5^6)\right)$$
$$\pm\left(2 + 2\cdot 5 + 5^2 + 5^3 + 4\cdot 5^5 + O(5^6), 1 + 5 + 3\cdot 5^2 + 2\cdot 5^5 + O(5^6)\right)$$

Running through **Step (1)** for each of these points we obtain the following possibilities for $(n \bmod 5, n \bmod 7)$:

$$(1,6), (2,2), (2,5), (3,2), (3,5), (4,1).$$

Step (2) then gives the following possibilities for $(n \bmod 5, n \bmod 7, n \bmod 11)$:

$$(1,6,5), (2,2,6), (2,2,10), (2,5,1), (2,5,5), (3,2,6), (3,2,10), (3,5,1), (3,5,5), (4,1,6).$$

Finally, no tuple survives **Step (3)**.

Chapter 5

Chabauty–Coleman experiments for genus 3 hyperelliptic curves

This chapter is joint work with Jennifer Balakrishnan, Victoria Cantoral-Farfán, Mirela Çiperiani and Anastassia Etropolski. It is essentially the article [11], with some minor changes.

5.1 Introduction

Let C be a non-singular curve over $\mathbb{Q}$ of genus $g \geq 2$. The Mordell conjecture, proved by Faltings in 1983 [58], implies that $C(\mathbb{Q})$ is finite. Our main motivation is to compute $C(\mathbb{Q})$ explicitly in this case. We will focus our attention on hyperelliptic curves of genus 3 such that the group of rational points of the Jacobian of C has Mordell–Weil rank $r = 1$. This falls into the special case where $r < g$ which was considered by Chabauty in 1941 [41] and techniques developed by Coleman in the 1980s allow us to use p-adic integration to often in practice compute the set of rational points [43, 42].

In addition to these methods, we will also use the algorithm of Balakrishnan, Bradshaw and Kedlaya [13] and its implementation in `SageMath` [131] to explicitly compute the relevant Coleman integrals by computing analytic continuation of Frobenius on curves. Nonetheless, we note that the algorithms presented in this chapter (see Section 5.3) have not been implemented previously by other authors or carried out on a large collection of curves. (See, however, [37] for related work in genus 2.) Our code is available at [12].

We consider the case of genus 3 hyperelliptic curves for two reasons:

1. When $g = 3$, we can impose the condition that $0 < r < g - 1$, i.e. $r = 1$, which, by a dimension argument, makes the method more effective. Indeed, in

this case, the set $C(\mathbb{Q})$ is contained in the intersection of the zero sets of the integrals of two linearly independent regular 1-forms on the base change of C to $\mathbb{Q}_p$, where p is any odd prime of good reduction.

2. When $g = 2$, the Jacobian of C is a surface and its geometry and arithmetic is better understood. In particular, methods developed by Flynn [60] (see also [40]) have been implemented by Stoll in `Magma` to make the computations needed much more efficient. More precisely, in this case, one can simplify the algorithm further by working with the quotient of the Jacobian by $\langle \pm 1 \rangle$, which is a quartic surface in $\mathbb{P}^3$, known as the Kummer surface. In order to make the search of rational points more effective, the Chabauty method can also be combined with the Mordell–Weil sieve, which uses information at different primes (see also [38]).

We begin with an overview of the Chabauty–Coleman method and explicit Coleman integration in Section 5.2. In Section 5.3, we present an algorithm to find a finite set of p-adic points containing the rational points of a hyperelliptic curve[1] $C/\mathbb{Q}$ of genus 3 that admits an odd model and whose Jacobian J has rank 1. We fix a prime p and work under the assumption that we know a $\mathbb{Q}$-rational point whose image in the Jacobian has infinite order (here the embedding of C into J is via a chosen base point ∞). Besides $\mathbb{Q}$-rational points, the output will include all points in $C(\mathbb{Q}_p)$ which are in the preimage of the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$.

We then proceed to run our code on a list of relevant curves taken from the forthcoming database of genus 3 hyperelliptic curves [34]. Our list consists of 16,977 curves and we separately do a point search in `Magma` to find all $\mathbb{Q}$-rational points whose x-coordinates with respect to a fixed integral affine model have naive height at most 10^5 (cf. Section 5.4). Our Chabauty–Coleman computations then show that there are no $\mathbb{Q}$-rational points of larger height on any of these curves.

In some cases, our algorithm outputs points in $C(\mathbb{Q}_p) \setminus C(\mathbb{Q})$. Besides $\mathbb{Q}_p$-rational (but non-$\mathbb{Q}$-rational) Weierstrass points, on 75 curves we find that the local point is the localisation of a point $P \in C(K)$ where K is a quadratic field in which the prime p splits. In all these cases we are able to explain why these points appear in the zero locus that we are studying. The following three scenarios occur and we discuss representative examples of each in Section 5.4:

[1] We focus on hyperelliptic curves defined over $\mathbb{Q}$ because `SageMath` has an implementation of Coleman integration precisely for odd degree hyperelliptic curves given by a monic equation defined over $\mathbb{Z}_p$ for odd primes p of good reduction.

- Case 1: It may happen that $[P - \infty]$ is a torsion point in the Jacobian (see Example 5.4.1). In this case, the integral of any 1-form would vanish between ∞ and P.
- Case 2: As in Example 5.4.2, it may happen that some multiple of the image of $[P - \infty]$ in the Jacobian actually belongs to $J(\mathbb{Q})$: the vanishing here follows by linearity in the endpoints of integration.
- Case 3: The Jacobian J may decompose over $\mathbb{Q}$ as a product of an elliptic curve and an abelian surface. Then, if the subgroup H generated by $J(\mathbb{Q})$ and the point $[P - \infty]$ comes from the elliptic curve, the dimension of the p-adic closure of H in $J(\mathbb{Q}_p)$ must be equal to 1, even if $[P - \infty]$ is a point of infinite order (see Example 5.4.3).

We conclude in §5.4.2 by describing some follow-up computations in Cases 1 and 2 in light of Stoll's Strong Chabauty Conjecture [133, Conj. 9.5].

5.2 The Chabauty–Coleman method and Coleman integration

In this section we review the Chabauty–Coleman method, used to compute rational points in our main algorithm. For further details, see Section 5.3. We also give a brief overview of explicit Coleman integration on hyperelliptic curves.

5.2.1 Chabauty–Coleman method

Let C be a smooth projective curve over the rationals of genus $g \geq 2$ and let J be its Jacobian. Approximately 40 years before Faltings's non-constructive proof of the finiteness of $C(\mathbb{Q})$, Chabauty considered the following set-up. Let p be a prime and suppose that there exists $P \in C(\mathbb{Q})$, so the embedding

$$\begin{aligned} \iota_P \colon C &\hookrightarrow J \\ Q &\mapsto [Q - P] \end{aligned}$$

maps $C(\mathbb{Q})$ in $J(\mathbb{Q})$. Let $\overline{J(\mathbb{Q})}$ denote the p-adic closure of $J(\mathbb{Q})$ in the g-dimensional p-adic Lie group $J(\mathbb{Q}_p)$ and define

$$C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})} := \iota_P(C(\mathbb{Q}_p)) \cap \overline{J(\mathbb{Q})}.$$

Chabauty proved the following case of Mordell's conjecture:

Theorem 5.2.1 ([41]). *Let $C/\mathbb{Q}$ be a curve of genus $g \geq 2$ such that the Mordell–Weil rank of the Jacobian J of C over $\mathbb{Q}$ is less than g and let p be a prime. Then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite.*

Chabauty's result was later reinterpreted and made effective by Coleman, who showed the following:

Theorem 5.2.2 ([42]). *Let C be as above and suppose that p is a prime of good reduction for C. If $p > 2g$, then*

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2g - 2.$$

To obtain an explicit upper bound on the size of $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ and hence of $C(\mathbb{Q})$, Coleman used his theory of p-adic integration on curves to construct p-adic integrals of 1-forms on $J(\mathbb{Q}_p)$ that vanish on $J(\mathbb{Q})$ and restrict them to $C(\mathbb{Q}_p)$. Here, we follow the exposition in [145] in defining the Coleman integral.

Denote by $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ (resp. $H^0(C_{\mathbb{Q}_p}, \Omega^1)$) the $\mathbb{Q}_p$-vector space of regular 1-forms on $J_{\mathbb{Q}_p} := J \times_{\mathbb{Q}} \mathbb{Q}_p$ (resp. $C_{\mathbb{Q}_p} := C \times_{\mathbb{Q}} \mathbb{Q}_p$). Let $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ and let λ_{ω_J} be the unique analytic homomorphism $\lambda_{\omega_J} \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p$ such that its derivative $d(\lambda_{\omega_J})$ is exactly ω_J (cf. [145, §3 and §4] and [101, §4.1]). Consider the map

$$\iota^* \colon H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(C_{\mathbb{Q}_p}, \Omega^1)$$

induced by ι_P and let $\omega := \iota^*(\omega_J)$. Observe that ι^* is an isomorphism of g-dimensional vector spaces [102, Proposition 2.2], which is independent of the choice of $P \in C(\mathbb{Q}_p)$ [145, Lemma 4.2].

On the Jacobian we have the natural pairing

$$\begin{aligned} \lambda \colon H^0(J_{\mathbb{Q}_p}, \Omega^1) \times J(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ (\omega_J, R) &\mapsto \lambda_{\omega_J}(R) =: \int_0^R \omega_J, \end{aligned}$$

which induces a local diffeomorphism from $J(\mathbb{Q}_p)$ to the dual of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Note that since λ_{ω_J} is a homomorphism, it vanishes on $J(\mathbb{Q}_p)_{\mathrm{tors}}$. Now given $P, Q \in C(\mathbb{Q}_p)$ we define

$$\int_P^Q \omega := \int_0^{[Q-P]} \omega_J;$$

for a fixed point $P \in C(\mathbb{Q}_p)$ and $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ we then get a function $\lambda_{\omega,P} \colon C(\mathbb{Q}_p) \to \mathbb{Q}_p$ with

$$\lambda_{\omega,P}(Q) := \int_P^Q \omega = \int_0^{[Q-P]} \omega_J = \lambda_{\omega_J}([Q-P]).$$

We now restrict to $g = 3$ and $r = \text{rank}(J(\mathbb{Q})) = 1$, in which case $g - r = 2$. The exposition below can be generalised whenever $r < g$, or, more generally, when the dimension of the p-adic Lie group $\overline{J(\mathbb{Q})}$ is less than g. See also Section 6.3 for an extension to general number fields. Let

$$\text{Ann}(J(\mathbb{Q})) := \left\{ \omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1) : \lambda_{\omega_J}(R) = \int_0^R \omega_J = 0 \text{ for all } R \in J(\mathbb{Q}) \right\}.$$

This is a 2-dimensional $\mathbb{Q}_p$-vector space. Indeed, it is at most 2-dimensional because there is an $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ such that λ_{ω_J} is non-trivial on $J(\mathbb{Q})$ since $J(\mathbb{Q})$ is not torsion (cf. [43, Proposition 3.1]); it is at least 2-dimensional because the dimension of $\overline{J(\mathbb{Q})}$ is less than or equal to the rank of $J(\mathbb{Q})$ ([101, Lemma 4.2]), or, more straightforwardly, because there can exist at most one $\mathbb{Q}_p$-valued linear functional on the one-dimensional $J(\mathbb{Q}) \otimes \mathbb{Q}_p$ up to multiplication by a scalar. Hence there exist two linearly independent differentials $\alpha_J, \beta_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$ such that

$$\lambda_{\alpha_J}(R) = \lambda_{\beta_J}(R) = 0 \quad \text{for all } R \in J(\mathbb{Q}).$$

Let D be a $\mathbb{Q}$-rational divisor on C of degree d and consider the map $\iota_D \colon C \to J$ defined by $Q \mapsto [dQ - D]$. Let

$$\lambda_{\omega,D}(Q) := \lambda_{\omega_J} \circ \iota_D(Q) = \lambda_{\omega_J}([dQ - D])$$

and consider the set

$$\begin{aligned} Z &:= \{Q \in C(\mathbb{Q}_p) : \lambda_{\omega,D}(Q) = 0 \text{ for all } \omega \in \text{Ann}(J(\mathbb{Q}))\} \\ &= \ker(\lambda_{\alpha,D}) \cap \ker(\lambda_{\beta,D}). \end{aligned} \tag{5.1}$$

By construction, $C(\mathbb{Q}) \subset Z$. Note that the set Z is independent of the choice of the divisor D [145, §1.6].

The above discussion indicates how we would handle the case when our hyperelliptic curve has an even degree model. However, since we restrict our attention to hyperelliptic curves C with an odd degree model, we are guaranteed a rational point $\infty \in C(\mathbb{Q})$ and we use $D = \infty$. Hence, we have two $\mathbb{Q}_p$-valued functions $\lambda_{\alpha,\infty}, \lambda_{\beta,\infty}$ on $C(\mathbb{Q}_p)$ whose common zeros capture the rational points of C.

5.2.2 Computing Coleman integrals

We now specialise to our case of interest, where C is a genus 3 hyperelliptic curve given by an odd degree model, i.e. described affinely by

$$C \colon y^2 = F(x)$$

where $F(x) \in \mathbb{Q}[x]$ is monic of degree 7. The curve also possesses one point at infinity $\infty = (1:0:0)$. In order to compute Z, we need a way to evaluate $\int_P^Q \omega$ for an arbitrary $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ and arbitrary $P, Q \in C(\mathbb{Q}_p)$. Suppose that p is a prime of good reduction for C and let $\overline{C}$ be the reduction of C modulo p, i.e. the special fibre of a minimal regular proper model of C over $\mathbb{Z}_p$. To compute $\int_P^Q \omega$, we now consider two cases: either P and Q lie in the same residue disk, or they do not.

5.2.2.1 Coleman integral within a residue disk

Let $P \in C(\mathbb{Q}_p)$. By a *local coordinate* for P we mean a rational function $t \in \mathbb{Q}_p(C)$ such that

1. t is a uniformiser at P;
2. the reduction of t to a rational function for $\overline{C}$ is a uniformiser at $\overline{P}$.

Hence, a local coordinate t at P establishes a bijection

$$\begin{aligned} p\mathbb{Z}_p &\leftrightarrow \{Q \in C(\mathbb{Q}_p) : \overline{Q} = \overline{P}\} \\ t &\leftrightarrow (x(t), y(t)), \end{aligned}$$

where $x(t), y(t)$ are Laurent series and $(x(0), y(0)) = P$.

Suppose now that $\omega \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$ is normalised by an element of $\mathbb{Q}_p^\times$ in such a way that its reduction modulo p exists and is not identically zero. We will often use the fact that the expansion of ω in terms of t has the form $w(t)dt$, for some $w(t) \in \mathbb{Z}_p[[t]]$ converging on the entire residue disk. Hence, if $\overline{Q} = \overline{P}$, we can compute $\int_P^Q \omega$ by formally integrating a power series in the local coordinate t ([145, Lemma 7.2]). Such definite integrals are referred to as *tiny integrals*.

A local coordinate at a given point $P \in C(\mathbb{Q}_p)$ can be found using [5, Algorithms 2-4]. In particular,

1. If $y(\overline{P}) \neq 0$, then $x(t) = t + x(P)$ and $y(t)$ is the unique solution to $y^2 = F(x(t))$ such that $y(0) = y(P)$.
2. If $y(\overline{P}) = 0$ and $\overline{P} \neq \overline{\infty}$, then $y(t) = t + y(P)$ and $x(t)$ is the unique solution to $F(x) = y(t)^2$ such that $x(0) = x(P)$.
3. If $\overline{P} = \overline{\infty}$, one first finds $x(t) = t^{-2} + O(1)$ by solving $F(x) = \frac{x^6}{t^2}$. Then $y(t) = \frac{x(t)^3}{t}$.

In practice, in all three cases one can explicitly compute $(x(t), y(t))$ up to arbitrary p-adic and t-adic precision by Newton's method.

5.2.2.2 Coleman integral between different residue disks

In our intended application of computing rational points, we will fix a base point as one endpoint of integration and consider the various Coleman integrals given by varying the other endpoint of integration over all residue disks. This makes it essential that the tiny integrals constructed in §5.2.2.1 are consistent across the set of residue disks: in other words, we need a notion of analytic continuation between different residue disks.

Coleman solved this problem by using Frobenius to write down a unique "path" between different residue disks and presented a theory of p-adic line integration on curves [43] satisfying a number of natural properties, among which linearity in the integrand, additivity in endpoints, change of variables via rigid analytic maps (e.g. Frobenius) and the fundamental theorem of calculus. This was made algorithmic in [13] for hyperelliptic curves by solving a linear system induced by the action of Frobenius on Monsky-Washnitzer cohomology, with an implementation available in `SageMath`.

Thus given two points $P, Q \in C(\mathbb{Q}_p)$, one can compute the definite Coleman integral from P to Q as $\int_P^Q \omega$ directly via [13], as well as the Coleman integral from P to the residue disk of Q, by further computing a local coordinate t_Q at Q (such that $t_Q|_{t=0} = Q$), which gives:

$$\int_P^{t_Q} \omega = \int_P^Q \omega + \int_Q^{t_Q} \omega = \int_P^Q \omega + \int_0^t \omega,$$

where $\int_P^Q \omega$ now plays the role of the constant of integration between different residue disks.

5.3 The algorithm

Let C be as in §5.2.2. We further assume that the Jacobian J of C has Mordell–Weil rank 1 over $\mathbb{Q}$ and that we have computed a point $P_0 \in C(\mathbb{Q})$ with the property that $[P_0 - \infty]$ is of infinite order in $J(\mathbb{Q})$. (This last assumption is straightforward to remove for a particular choice of curve, see §5.3.4.1)

Fix an odd prime p of good reduction for C and let $C(\mathbb{Q})_{\text{known}}$ denote a list of known points in $C(\mathbb{Q})$. Given this input, the algorithm in this section returns the set Z of common zeros of $\lambda_{\alpha,\infty}$ and $\lambda_{\beta,\infty}$, as defined in §5.2.1, excluding the known rational points $C(\mathbb{Q})_{\text{known}}$.

5.3.1 Upper bounds in residue disks

Define $\omega_i = (x^i/2y)dx$ for $i \in \{0, 1, 2\}$. These differentials form a basis for $H^0(C_{\mathbb{Q}_p}, \Omega^1)$. Let α and β be 1-forms in $H^0(C_{\mathbb{Q}_p}, \Omega^1)$ such that α_J and β_J form a basis for $\mathrm{Ann}(J(\mathbb{Q}))$ and such that α and β are not identically zero modulo p. We may assume that we are in one of the following two situations:

1. $\alpha = \omega_0$ and β is a $\mathbb{Z}_p$-linear combination of ω_1 and ω_2, or
2. α is a $\mathbb{Z}_p$-linear combination of ω_0 and ω_1 and β is a $\mathbb{Z}_p$-linear combination of ω_0 and ω_2.

Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$. Ultimately we want to compute the zeros in $p\mathbb{Z}_p$ of a particular antiderivative $f(t)$, up to a desired p-adic precision. In certain cases, we will be able to avoid this calculation by obtaining an upper bound for the number of zeros of $f(t)$ in $p\mathbb{Z}_p$ which we know to be sharp. To do this, we use the theory of Newton polygons for p-adic power series (see e.g. [81, IV.4]).

Given $f(t) \in \mathbb{Q}_p[[t]]$ such that $f'(t) \in \mathbb{Z}_p[[t]]$, let $\overline{f'}(t) := f'(t) \bmod p$ and define

$$m_f := \mathrm{ord}_{t=0}\overline{f'}(t). \tag{5.2}$$

The following result is [101, Lemma 5.1] and can be viewed as a corollary of the p-adic Weierstrass Preparation Theorem.

Lemma 5.3.1. *Let $f(t) \in \mathbb{Q}_p[[t]]$ such that $f'(t) \in \mathbb{Z}_p[[t]]$. If $m_f < p - 2$, then the number of roots of f in $p\mathbb{Z}_p$ is less than or equal to $m_f + 1$.*

Remark 5.3.2. Note that if $p > 2g = 6$ and $f'(t)$ is the local expansion of a regular 1-form, then the Riemann-Roch Theorem implies that $m_f \leq 4$ and hence the condition $m_f < p - 2$ of Lemma 5.3.1 is always satisfied (cf. [101, Theorem 5.3]).

The following lemmas give a refinement of this result for our particular choice of f. We refer to a point of C or $\overline{C}$ as a *Weierstrass point* if it is fixed by the hyperelliptic involution and as a *finite Weierstrass point* if it is furthermore different from the point at infinity.

Lemma 5.3.3. *Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$. If $\overline{Q}$ is non-Weierstrass, then*

$$m_f \leq \begin{cases} 1 & \text{if } x(\overline{Q}) \neq 0, \\ 2 & \text{otherwise.} \end{cases}$$

Moreover, the minimum of the orders of vanishing of α and β at $\overline{Q}$ is less than or equal to 1 for all non-Weierstrass $\overline{Q}$.

Proof. By construction, the differential f' is a linear combination of two of the differentials $\omega_i = (x^i/2y)dx$, $i = 0, 1, 2$, and f' is non-trivial modulo p. The assumption that $\overline{Q}$ is non-Weierstrass implies that $t = x - x(Q)$ is a local coordinate, where Q is any lift of $\overline{Q}$ to characteristic zero. Write $f' = ((Ax^i + Bx^j)/2y)dx$, where $A, B \in \mathbb{Z}_p$, $i, j \in \{0, 1, 2\}$, $i < j$. Then in local coordinates we have

$$f'(t) = \frac{A(t + x(Q))^i + B(t + x(Q))^j}{2y(t)}dt$$

where $y(t)$ has no zeros or poles in the residue disk. Since $A(t+x(Q))^i+B(t+x(Q))^j$ is a polynomial of degree less than or equal to 2 in t, the first part of the first claim is proved. Furthermore, the polynomial has a double root modulo p at $\overline{Q}$ if and only if $A \equiv 0 \bmod p$, $j = 2$, $B \not\equiv 0$, and $x(\overline{Q}) = 0$; i.e. if and only if $f' \equiv \frac{x^2}{2y}dx$ (up to rescaling) and $x(\overline{Q}) = 0$. The last statement also follows, since by construction α is a linear combination of ω_0 and ω_1 (see the beginning of §5.3.1). □

Proposition 5.3.4. *Let $p \geq 5$ be a prime of good reduction for C. Let $\overline{Q} \in \overline{C}(\mathbb{F}_p)$ be a non-Weierstrass point. Then the set*

$$\left\{P \in C(\mathbb{Q}_p) : \overline{P} = \overline{Q} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0\right\}$$

has size less than or equal to 2.

Proof. Follows from Lemma 5.3.1 and Lemma 5.3.3. □

Lemma 5.3.5. *Let $f'(t)$ be the local expansion of α or β in the residue disk of the point $\overline{\infty} \in \overline{C}(\mathbb{F}_p)$. Then $m_f \in \{0, 2, 4\}$. In particular, the minimum of the orders of vanishing of α and β at $\overline{\infty}$ is less than or equal to 2.*

Proof. We may take $x(t) = t^{-2} + O(1)$, $y(t) = t^{-7} + O(t^{-5})$ (cf. [5, Algorithm 4]). Then $x^i dx/2y$ has a zero of order $4 - 2i$ at $t = 0$. □

Proposition 5.3.6. *Let $p \geq 5$ be a prime of good reduction for C. Then the set*

$$\left\{P \in C(\mathbb{Q}_p) : \overline{P} = \overline{\infty} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0\right\}$$

has size less than or equal to 3. In particular, there are at most two points different from the point at infinity and reducing to it modulo p in the above set.

Lemma 5.3.7. *Let $f'(t)$ be the local expansion of α or β in the residue disk of a point $\overline{Q} \in \overline{C}(\mathbb{F}_p)$. If $\overline{Q}$ is a finite Weierstrass point, then*

$$m_f \in \begin{cases} \{0,2\} & \text{if } x(\overline{Q}) \neq 0, \\ \{0,2,4\} & \text{else.} \end{cases}$$

Moreover, the minimum of the orders of vanishing of α and β at $\overline{Q}$ is less than or equal to 2.

Proof. In this case we may take $y = t$ and solve for x using $y^2 = F(x)$. In particular, we have that $x(t) = x(Q) + \frac{t^2}{F'(x(Q))} + O(t^4) \bmod p$ (cf. [5, Algorithm 3]). Therefore, $dx/2y$ has no zero or pole at $t = 0$ and $x^i dx/2y$ has either no zero or pole or a zero of order $2i$ if $\overline{Q} = (0,0)$. Now consider

$$f'(t) = \left(A \left(x(Q) + \frac{t^2}{F'(x(Q))} + O(t^4) \right)^i + B \left(x(Q) + \frac{t^2}{F'(x(Q))} + O(t^4) \right)^j \right) u(t)dt,$$

where $u(t)$ is a unit power series and A is non-zero modulo p. For any choice of $i, j \in \{0,1,2\}$, $i < j$, it can be verified that $m_f \in \{0,2\}$ by distinguishing between the cases $x(\overline{Q}) = 0$ or $x(\overline{Q}) \neq 0$. If $A \equiv 0 \bmod p$ when $i = 0$ or 1 and $j = 2$ then m_f equals 4 if $x(\overline{Q}) = 0$. However, by construction, α and β cannot both be of this form. □

Proposition 5.3.8. *Let $p \geq 5$ be a prime of good reduction for C. Let $\overline{Q} \in \overline{C}(\mathbb{F}_p)$ be a finite Weierstrass point. Then the set*

$$\left\{ P \in C(\mathbb{Q}_p) : \overline{P} = \overline{Q} \text{ and } \int_\infty^P \alpha = \int_\infty^P \beta = 0 \right\}$$

has size less than or equal to 3.

5.3.2 Roots of p-adic power series

Let $f'(t)$ be the local expansion of α (resp. β) in a residue disk and let $f(t)$ be an antiderivative of $f'(t)$ whose constant term is either zero or equal to the Coleman integral of α (resp. β) between ∞ and a $\mathbb{Q}_p$-rational point on C. To provably determine the roots of $f(t)$ lying in a residue disk up to a desired p-adic precision, we need to do the following:

- truncate at a p-adic precision p^N that is able to detect all the roots (up to $O(p^n)$ where $n = \lfloor (N-k)/2 \rfloor$, see Proposition 5.3.11), i.e. such that any two distinct roots of $f(t)$ reduce to different roots modulo p^n;

- determine M such that to compute a root up to $O(p^n)$, we only need to consider the power series up to $O(t^M)$ where the coefficient of t^i has p-adic valuation greater than or equal to $2n$ for all $i \geq M$ if the roots are simple and f is suitably normalised (i.e. $f \in \mathbb{Z}_p[[t]] \setminus p\mathbb{Z}_p[[t]]$).

Write $f(t) = f_M(t) + O(t^M)$ where M is an integer greater than or equal to $m_f + 2$ and $f_M(t)$ is a polynomial of degree less than or equal to $M - 1$. If $m_f < p - 2$, then $f(t)$ and $f_M(t)$ have the same number of roots in $\mathbb{C}_p$ of p-adic valuation greater than or equal to 1, as can be deduced from the same considerations on the Newton polygon of $f(t)$ which imply Lemma 5.3.1 (for more details, see the proof of [101, Lemma 5.1]). We are interested in the zeros of $f(pt)$ in $\mathbb{Z}_p$. Note that

$$f(pt) - f_M(pt) \in O(p^n t^M) \quad \text{for some } n \geq 2.$$

Hence, $f(pt)$ and $f_M(pt)$ have exactly the same zeros in $\mathbb{Z}/p^{n-k}\mathbb{Z}$ (including multiplicities), where k is the minimal valuation of the coefficients of $f(pt)$; see below for an upper bound on k and a lower bound on n which guarantee that $n - k \geq 1$. Furthermore, if a zero of $p^{-k}f(pt)$ (and $p^{-k}f_M(pt)$) modulo p^{n-k} is *simple* (i.e. its derivative is non-zero modulo $p^{\lceil (n-k)/2 \rceil}$), then it lifts to a root of $f(pt)$ in $\mathbb{Z}_p$ by an inductive application of Hensel's lemma.

To compute a suitable choice of M, we require two more lemmas.

Lemma 5.3.9. *Let $\omega_i = (x^i/2y)dx$ for some $i \in \{0, 1, 2\}$, and $\lambda_i = \int_\infty^{P_0} \omega_i$. If $\overline{[P_0 - \infty]} \in \overline{J}(\mathbb{F}_p)$ has order prime to p, then $\mathrm{ord}_p(\lambda_i) \geq 1$. In particular, this holds if p does not divide $\#\overline{J}(\mathbb{F}_p)$.*

Proof. Let n be the order of the reduction of $[P_0 - \infty]$ modulo p. Then $Q = n[P_0 - \infty] \in J_1(\mathbb{Q}_p)$, the kernel of reduction at p, and we have $\int_\infty^{P_0} \omega_i = \frac{1}{n} \int_0^Q \omega_{J,i}$, where $\iota^*(\omega_{J,i}) = \omega_i$. Now $\int_0^Q \omega_{J,i}$ can be computed by first writing $\omega_{J,i}$ as a power series in $\mathbb{Z}_p[[z_1, z_2, z_3]]$ where z_1, z_2, z_3 is a local coordinate system for $J_1(\mathbb{Q}_p)$ around 0 which identifies $J_1(\mathbb{Q}_p)$ with $(p\mathbb{Z}_p)^3$, and then formally integrating and evaluating at $z_1(Q), z_2(Q), z_3(Q)$. □

Lemma 5.3.10. *We have $f(pt) = \sum_{i=0}^\infty b_i t^i = \sum_{j=0}^\infty \frac{a_j p^{j+1}}{j+1} t^{j+1} + c$, where $c \in \mathbb{Q}_p$, $a_j \in \mathbb{Z}_p$ for all $j \geq 0$. Therefore for all $i \geq 1$, $\mathrm{ord}_p(b_i) \geq i - \mathrm{ord}_p(i)$. Furthermore if $p^2 \nmid \#\overline{J}(\mathbb{F}_p)$ then $c \in \mathbb{Z}_p$.*

Proof. The first assertion is clear. For the latter, recall that c is either 0 or of the form $\int_\infty^Q \gamma$, for some $Q \in C(\mathbb{Q}_p)$ and $\gamma \in \{\alpha, \beta\}$. The proof is then similar to Lemma 5.3.9. □

By Lemma 5.3.10, we know that $f(pt)$ has coefficients in $\mathbb{Z}_p$, except possibly when $p^2 \mid \#\overline{J}(\mathbb{F}_p)$. Let k be the minimum of the valuations of the coefficients of $f(pt)$. Note that, since $f'(t) \bmod p$ has order of vanishing equal to m_f, if $m_f < p-2$, it follows that the valuation of the coefficient of t^{m_f+1} in $f(pt)$ is precisely $m_f + 1$. Therefore $k \leq m_f + 1$. Furthermore, for $i > m_f + 1$, we have $\mathrm{ord}_p(b_i) \geq i - \mathrm{ord}_p(i) > i - (i - m_f - 1) = m_f + 1$.

Proposition 5.3.11. *Let $f(t)$ be an antiderivative of α or β, let $m_f < p-2$, and let k be the minimal valuation of the coefficients of $f(pt)$. Fix an integer N such that $m_f + 2 \leq N \leq p^p - p$. Let ap^e be the smallest integer greater than or equal to N with $p \nmid a$ and $e \geq 1$; set*

$$M = \begin{cases} ap^e + 1 & \text{if } ap^e - e < N, \\ N & \text{otherwise.} \end{cases}$$

Then each simple root of $p^{-k} f_M(pt)$ in $\mathbb{Z}/p^{N-k}\mathbb{Z}$ equals the approximation modulo $p^{\lfloor (N-k)/2 \rfloor}$ of a root of $f(pt)$. Furthermore, if all such roots are simple, then these are all the roots of $f(pt)$ in $\mathbb{Z}_p$.

Proof. It suffices to show that

$$\mathrm{ord}_p(b_i) \geq N \tag{5.3}$$

for all $i \geq M$. Indeed, if that is the case then

$$p^{-k} f_M(pt) = p^{-k} f(pt) \bmod p^{N-k} \quad \text{for all } t \in \mathbb{Z}_p.$$

Thus, if $t_0 \in \mathbb{Z}_p$ is a root of $f(pt)$ then t_0 modulo p^{N-k} is a root of $p^{-k} f_M(pt)$ modulo p^{N-k}. Conversely, if t_0 is a simple root of $p^{-k} f_M(pt)$ modulo p^{N-k} then by Hensel's lemma this lifts to a root in $\mathbb{Z}_p$ of $f_M(pt)$ congruent to t_0 modulo $p^{\lfloor (N-k)/2 \rfloor}$.

Since $M \geq N$, the statement (5.3) is clear for $p \nmid i$ by Lemma 5.3.10. Now suppose $p \mid i$ for some $i \geq M$. Hence, $i = bp^r$ where $p \nmid b$, $r \geq 1$ and $bp^r \geq M \geq N$. Then by the definition of ap^e, we know that

$$bp^r \geq ap^e \quad \text{and} \quad 0 \leq ap^e - N < p.$$

We now have two cases to consider:

Case 1: Assume that $bp^r = ap^e$. It follows that $M = N$ which in turn implies that $ap^e - e \geq N$. Then since $(a, e) = (b, r)$, we have that

$$\mathrm{ord}_p(b_i) \geq bp^r - r \geq N.$$

Case 2: Assume that $bp^r > ap^e$. It follows that $bp^r - ap^e \geq p$. Thus

$$\mathrm{ord}_p(b_i) \geq bp^r - r = (bp^r - ap^e) + (ap^e - r).$$

So if $\mathrm{ord}_p(b_i) < N$ then $r > (bp^r - ap^e) + (ap^e - N) \geq p$ and hence $p^p - p \leq bp^r - r < N$, contradicting our assumption on N. □

Remark 5.3.12. In order to apply Proposition 5.3.11 we need to meet the condition $m_f < p-2$; assuming that $p > 2g$ guarantees that this always holds, as a consequence of the Riemann-Roch Theorem (see Remark 5.3.2). Furthermore, in this case $p^p - p$ is large enough that the hypothesis on N of Proposition 5.3.11 is always met in practice.

5.3.3 Outline of the algorithm

We retain the notation of the beginning of Section 5.3. The algorithm will always work if $p \geq 7$. If $p = 3$ or 5, the algorithm will return an error if it is not able to give a provably correct output (see Remark 5.3.2 and the comments in the main steps of the algorithm below). We now list the input and output of our algorithm followed by its main steps.

Input:

- C: a hyperelliptic curve of genus 3 over $\mathbb{Q}$ given by a model $y^2 = F(x)$ where $F \in \mathbb{Q}[x]$ is monic of degree 7, such that its Jacobian J has rank 1;
- p: an odd prime of good reduction for C not dividing the leading coefficient of F;
- P_0: a point in $C(\mathbb{Q})$ such that $[P_0 - \infty] \in J(\mathbb{Q})$ has infinite order;
- $C(\mathbb{Q})_{\mathrm{known}}$: a list of all known rational points on $C(\mathbb{Q})$;
- a p-adic precision N.

Output: The set $Z \subseteq C(\mathbb{Q}_p)$ defined in (5.1) modulo the action of the hyperelliptic involution. In our code, this set is split into the following:

- a list of points of Z which can be recognised as points in $C(\mathbb{Q}) \setminus C(\mathbb{Q})_{\mathrm{known}}$ up to the hyperelliptic involution;

- a list of points $P \in Z$ such that $[P - \infty] \in J(\mathbb{Q}_p)_{\mathrm{tors}}$, up to the hyperelliptic involution. Here, if P is not 2-torsion and is the localisation of a point defined over a quadratic extension $K/\mathbb{Q}$ then the coordinates in K are given as the corresponding minimal polynomials over $\mathbb{Q}$; in all other cases, the p-adic expansion of P is returned.

- a list of all remaining points $P \in Z$ (as above, if P is the localisation of a point defined over a quadratic extension of $K/\mathbb{Q}$ then the coordinates in K are given as the corresponding minimal polynomials over $\mathbb{Q}$; in all other cases, the p-adic expansion of P is returned).

Main steps of the algorithm:

1. *A basis for the annihilator.*

   For each basis differential $\omega_i = (x^i/2y)dx$ $(i = 0, 1, 2)$, compute

   $$\lambda_i = \int_\infty^{P_0} \omega_i \bmod p^n,$$

   where n may be less than N if some precision is lost in computing the Coleman integrals. Set $k_{ij} := \min\{\mathrm{ord}_p(\lambda_i), \mathrm{ord}_p(\lambda_j)\}$ and

   $$(\alpha, \beta) = \begin{cases} \big(\omega_0,\, p^{-k_{12}}(\lambda_1\omega_2 - \lambda_2\omega_1)\big) & \text{if } \lambda_0 = 0, \\ \big(p^{-k_{01}}(\lambda_0\omega_1 - \lambda_1\omega_0),\, p^{-k_{02}}(\lambda_0\omega_2 - \lambda_2\omega_0)\big) & \text{else.} \end{cases}$$

   In either case, α and β are reductions modulo $p^{n'}$ of the pullback ι^* of a basis for the annihilator of $J(\mathbb{Q})$, where

   $$n' = \begin{cases} n - k_{12} & \text{if } \lambda_0 = 0, \\ n - \max\{k_{01}, k_{02}\} & \text{else.} \end{cases}$$

   By Lemma 5.3.9, $n' \leq n - 1$ if $p \nmid \#\overline{J}(\mathbb{F}_p)$. If $n' \geq 6$ we are guaranteed to be able to carry out all computations in the next steps when $p \geq 7$.

2. *Ruling out residue disks.* Observe that we only need to consider residue disks up to the hyperelliptic involution.

   Reduce α and β modulo p. For each $\overline{P} \in \overline{C}(\mathbb{F}_p)$, expand α and β in a local coordinate s around $\overline{P}$, calculate the orders of vanishing of α and β at $s = 0$ and let $m(\overline{P})$ denote their minimum. Note that $m(\overline{P}) \leq 2$ by Lemmas 5.3.3,

5.3.5 and 5.3.7; hence it suffices to compute $\alpha(s)$ and $\beta(s)$ up to $O(s^2)$ to find $m(\overline{P})$.

If $m(\overline{P})+1$ equals the number of $\mathbb{Q}$-rational points in $C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$ modulo p and $m(\overline{P}) < p-2$, then by Lemma 5.3.1 the set $C(\mathbb{Q})_{\text{known}}$ contains all $\mathbb{Q}$-rational points in the residue disk of $\overline{P}$. Otherwise, proceed to the next step.

3. *Searching for the remaining disks.*

   If, for a given point $\overline{P} \in \overline{C}(\mathbb{F}_p)$, the number of $\mathbb{Q}$-rational points in $C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$ modulo p is strictly smaller that $m(\overline{P})+1$, then we need to compute the set of $\mathbb{Q}_p$-rational points P reducing to $\overline{P}$ such that $\int_Q^P \alpha = \int_Q^P \beta = 0$ for a (any) rational point Q. For computational convenience we distinguish between two cases:

   (i) If there exists $P \in C(\mathbb{Q})_{\text{known}}$ reducing to $\overline{P}$, let t be a uniformiser at P. Then expand α and β in t and formally integrate to obtain two power series $f(t)$, $g(t)$, which parametrise the integrals of α and β between P and any other point in the residue disk.

   (ii) If we do not know any $\mathbb{Q}$-rational point in the residue disk of $\overline{P}$, then we may assume that $\overline{P} \neq \overline{\infty}$ and hence write $\overline{P} = (\overline{x_0}, \overline{y_0})$. If $\overline{y_0} = 0$, let $P = (x_0, 0)$ where x_0 is the Hensel lift of $\overline{x_0}$ to a root of $f(x)$. Otherwise, if $\overline{P}$ is not a Weierstrass point, we take $P = (x_0, y_0)$ where x_0 is any lift to $\mathbb{Z}_p$ of $\overline{x_0}$ (the Teichmüller lift of $\overline{x_0}$ is a particularly convenient choice for x_0, as it simplifies some of the underlying Coleman integration computations [13]) and y_0 is obtained from $\overline{y_0}$ using Hensel's Lemma on $y^2 = F(x_0)$. Let $\tilde{f}(t)$ and $\tilde{g}(t)$ be the integrals between P and any other point reducing to $\overline{P}$ in terms of a local parameter t at P. Then write $f(t) = \tilde{f}(t) + \int_\infty^P \alpha$ and $g(t) = \tilde{g}(t) + \int_\infty^P \beta$.

   Recall that in (1), we have computed the coefficients of the ω_i in α and β modulo n'. To provably compute the set of common zeros, we require that each common root is a simple zero of at least one of f and g at our working precision.

   Assume without loss of generality that f has only simple roots. The t-adic precision we should compute $f(t)$ to in order to find provably correct approximations of its simple zeros is determined by Proposition 5.3.11. In practice, we truncate $f(t)$ at $O(t^M)$ where $M = n'$, unless the smallest multiple r of

p greater than or equal to n' satisfies $r - \mathrm{ord}_p(r) < n'$, in which case take $M = r + 1$. For the p-adic precision, the coefficients are computed modulo $p^{n'}$. Then the simple roots are correct[2] up to $O(p^{\lfloor (n'-k)/2 \rfloor})$ where k is the minimal valuation of the known coefficients of $f(pt)$ (by an argument analogous to the discussion preceding Proposition 5.3.11). To compute the roots we use the function `polrootspadic` implemented in `PARI/GP`. Finally, we take the list of roots which lie in $p\mathbb{Z}_p$ and check whether they are also roots of g.

If $p = 3$ or $p = 5$ and the order of vanishing of $f(t)$ or $g(t)$ modulo p is greater than or equal to $p - 2$, then we cannot provably find the zeros of $f(pt)$ and $g(pt)$.

4. *Identifying the remaining disks.*

   Once we have found the common zeros of $f(pt)$ and $g(pt)$, we recover the corresponding $\mathbb{Q}_p$-rational points that do not come from points in $C(\mathbb{Q})_{\mathrm{known}}$. We now break this set of points into sublists.

   If we fail to recognise a point Q as $\mathbb{Q}$-rational, we can check whether the integral between ∞ and Q of any non-zero differential γ not in the span of α and β also vanishes. If this is the case, the point $[Q - \infty] \in J(\mathbb{Q}_p)$ is torsion (cf. [43, Proposition 3.1]) and the analogue of the Lutz–Nagell Theorem for hyperelliptic curves [63, Theorem 3], combined with reductions modulo primes, provides an effective procedure to determine which points of $C(\mathbb{Q})$ give rise to torsion points in $J(\mathbb{Q})$ and thus to verify whether Q is $\mathbb{Q}$-rational or not. Furthermore, by increasing the degree in `algdep`, we may even try to identify the number field over which the coordinates of Q are defined[3]. This may require high p-adic precision; however, it was possible for every curve we considered.

   If the integral of the differential γ is non-zero and we have not recognised Q as a $\mathbb{Q}$-rational point, we can still check whether the point Q is defined over some number field K. For instance $[Q - \infty]$ could equal a point in $J(\mathbb{Q})$ plus some torsion element in $J(K)$, with $[K\colon \mathbb{Q}] > 1$ (see Example 5.4.1).

[2]Note that when the derivative of $p^{-k} f_M(pt)$ at the root is non-zero modulo p which happens quite often, then the roots that we find are in fact correct modulo $p^{n'-k}$.

[3]The hyperelliptic curve C is defined over $\mathbb{Q}$. Thus the fact that $[Q - \infty] \in J(\mathbb{Q}_p)_{\mathrm{tors}}$ forces Q to have coordinates in $\overline{\mathbb{Q}} \cap \mathbb{Q}_p$.

5.3.4 Generalisations of the algorithm

5.3.4.1 What if we do not know $P_0 \in C(\mathbb{Q})$ such that $[P_0 - \infty] \notin J(\mathbb{Q})_{\text{tors}}$?

The hyperelliptic curve we input in the algorithm is assumed to have rank 1. Calculation of the rank is attempted by `Magma` [36] by working out both an upper bound and a lower bound, the former coming from computation of the 2-Selmer group and the latter from an explicit search for linearly independent points on the Jacobian. The success of the rank computation relies on the two bounds being equal. In particular, if we suppose that we know provably that the rank of the Jacobian is one, we may as well assume that we know a point $Q \in J(\mathbb{Q})$ of infinite order and a divisor E on C representing it. Then we may proceed as follows. The first task is to write $Q = [E]$ in the form $[D - d\infty]$, where D is an effective $\mathbb{Q}$-rational divisor. In order to achieve this, we follow step by step the proof of [135, Corollary 4.14]. That is, we compute the dimension of $\mathcal{L}(E + n\infty)$ for $n = 0, 1, 2, \ldots$ (here $\mathcal{L}(E + n\infty)$ denotes the Riemann-Roch space of $E + n\infty$), until we find the smallest $n = m$ for which the dimension is 1. Then $[D - d\infty] = [E + \text{div}(\phi)]$, where ϕ generates $\mathcal{L}(E + m\infty)$. By [135, Lemma 4.17], D is then the unique $\mathbb{Q}$-rational divisor in general position and of degree less than or equal to $g = 3$ such that Q can be represented in the form $[D - d\infty]$.

Let K be the smallest Galois extension of $\mathbb{Q}$ over which the support of D is defined. Furthermore, let p be a prime of good reduction for C that splits completely in $K/\mathbb{Q}$. Then K can be realised as a subfield of $\mathbb{Q}_p$ and hence the support of D can be seen as lying in $C(\mathbb{Q}_p)$. Write $D = \sum_{i=1}^{d} P_i$ (some P_i possibly being equal). Then we may proceed exactly as before, just replacing λ_i in (1) by

$$\lambda_i = \sum_{i=1}^{d} \int_{\infty}^{P_i} \omega_i.$$

5.3.4.2 Even degree model

The algorithm relies heavily on computations of Coleman integrals, for which one needs the hyperelliptic curve considered to have a model of the form $y^2 = F(x)$, where $F(x)$ is monic. In particular, if one were to work with an even degree model, the two points at infinity would necessarily be defined over $\mathbb{Q}$. Therefore we could proceed as in the odd degree case with the single point at infinity being replaced by one of these two points. If $F(x)$ is not monic, the issue is that Coleman integration is not implemented in `SageMath`, though an implementation is available in `Magma`

[21, 20]. Hence, general even models could be handled by computing the set of local points Z as defined in (5.1), using the sum of the two points at infinity as the divisor D.

5.3.4.3 Other ranks and genera

Our assumptions on g and r are somewhat arbitrary. With minor modifications, our code can be used in more general cases, provided that $0 < r < g$.

5.4 Curve analysis

Once we implemented in `SageMath` the algorithm described in the previous section, we ran it over $16,977$ hyperelliptic curves of genus $g = 3$ satisfying the following properties:

1. the curve admits an odd degree model over $\mathbb{Q}$;
2. the Jacobian of the curve has Mordell–Weil rank equal to 1;
3. there is a $\mathbb{Q}$-rational point P_0 such that $[P_0 - \infty]$ has infinite order in $J(\mathbb{Q})$.

In order to obtain those curves, we sorted the $67,879$ genus 3 hyperelliptic curves from a forthcoming database of genus 3 curves over $\mathbb{Q}$ [34]. (For each hyperelliptic curve, this database has its absolute minimal discriminant, the conductor of its Jacobian and an equation giving a minimal model for the curve.) Out of these, $19,254$ curves satisfy conditions (1) and (2).

Running our code for the $16,977$ curves for which we could further find a P_0 as in (3), we found 75 curves where the zero set Z contains something other than the rational points we had already computed and Weierstrass points defined over $\mathbb{Q}_p$ for our chosen prime p. Note that in all $16,977$ computations, the prime p used was the smallest prime greater than $2g = 6$ which divided neither the discriminant nor the leading coefficient of the hyperelliptic polynomial defining the curve.

Let C be one of these 75 curves, let W denote the set of Weierstrass points in $C(\mathbb{Q}_p) \setminus C(\mathbb{Q})$ and let $P \in Z \setminus (C(\mathbb{Q}) \cup W)$. In all cases, we identified P as a point defined over a quadratic extension K of $\mathbb{Q}$ in which p splits. Even so, these 75 curves split up into 3 distinct cases:

(1) $[P - \infty] \in J(K)_{\mathrm{tors}}$;

(2) $[P - \infty] \notin J(K)_{\mathrm{tors}}$ but $n[P - \infty] \in J(\mathbb{Q})$ for some positive integer n;

(3) $\langle J(\mathbb{Q}), [P-\infty]\rangle_{\mathbb{Z}}$ is a rank 2 subgroup of $J(K)$.

In Cases (1) and (2), it is clear why $P \in Z$. On the other hand, justifying Case (3) requires investigating more closely the geometry of the Jacobian of the curve, as is carried out in detail in Example 5.4.3.

5.4.1 Examples

For each of the curves below we give a list of known rational points, which are all of the rational points up to a height[4] of 10^5. Following the algorithm outlined in §5.3.3, we produce the set Z of local points for the prime $p = 7$ or $p = 11$, which in each case returns no new $\mathbb{Q}$-rational points, hence concluding that the set of known rational points $C(\mathbb{Q})_{\text{known}}$ is all of $C(\mathbb{Q})$. In each of the examples below, however, Z contains a $\mathbb{Q}_p$-point which is not a Weierstrass point and falls into one of the cases outlined above.

Example 5.4.1. Consider the hyperelliptic curve

$$y^2 + x^3 y = x^7 + 2x^6 - 2x^5 - 9x^4 - 4x^3 + 8x^2 + 8x + 2$$

(given above by a minimal model) which has absolute minimal discriminant 544256 and whose Jacobian has conductor $544256 = 2^9 \cdot 1063$. We work with an odd degree model

$$C\colon y^2 = 4x^7 + 9x^6 - 8x^5 - 36x^4 - 16x^3 + 32x^2 + 32x + 8,$$

which has the following five known rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (-1,-1), (-1,1), (1,-5), (1,5)\}.$$

Running the code on C together with the prime $p = 7$ and the point $P_0 = (-1,-1)$, we find that

$$Z = C(\mathbb{Q})_{\text{known}} \cup W \cup \{(0, \pm 2\sqrt{2})\},$$

where the set W of non-$\mathbb{Q}$-rational Weierstrass points has size 3. Moreover, the points $[(0, \pm 2\sqrt{2}) - \infty] \in J(\mathbb{Q}(\sqrt{2}))$ have order 12.

[4]Our computations show that the $\mathbb{Q}$-rational points of highest absolute logarithmic height (with respect to an odd degree model) on a curve among the 16,977 hyperelliptic curves that we considered, are

$$\left(-\frac{49}{18}, -\frac{339563}{11664}\right), \left(-\frac{49}{18}, -\frac{1600445}{52488}\right)$$

on the hyperelliptic curve

$$C\colon y^2 + (x^4 + x^2 + x)y = x^7 - x^6 - 5x^5 + 5x^3 - 3x^2 - x,$$

which has absolute minimal discriminant 5326597 and whose Jacobian has conductor 5326597.

Example 5.4.2. Consider the hyperelliptic curve

$$y^2 + (x^4 + 1)y = 2x^3 + 2x^2 + x$$

(given above by a minimal model) which has absolute minimal discriminant 48519 and whose Jacobian J has conductor $48519 = 3^4 \cdot 599$. We work with an odd degree model

$$C\colon y^2 = -4x^7 + 24x^6 - 56x^5 + 72x^4 - 56x^3 + 28x^2 - 8x + 1.$$

This curve has the following five known rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (0,-1), (0,1), (1,-1), (1,1)\}.$$

For this example we will give a more detailed outline of the algorithm. Following §5.2.1 we know that there exist functions $\lambda_{\alpha,\infty}$, $\lambda_{\beta,\infty}$ on $C(\mathbb{Q}_p)$, corresponding to differentials $\alpha, \beta \in H^0(C_{\mathbb{Q}_p}, \Omega^1)$. These two functions vanish on the rational points of C, i.e.

$$C(\mathbb{Q}) \subseteq \ker(\lambda_{\alpha,\infty}) \cap \ker(\lambda_{\beta,\infty}) = Z.$$

We would like to know whether this zero set Z contains anything other than the $\mathbb{Q}$-rational points on C.

If we take $p = 11$, we find that $Z = C(\mathbb{Q})_{\text{known}} \cup W$. Observe that 11 is inert in $K = \mathbb{Q}(\sqrt{-3})$. If we take $p = 7$, which splits in $K = \mathbb{Q}(\sqrt{-3})$, we find

$$\left\{\left((1+\sqrt{-3})/2, \pm\sqrt{-3}\right), \left((1-\sqrt{-3})/2, \pm\sqrt{-3}\right)\right\} \subseteq Z.$$

Indeed, if P denotes any of the above points, then $5[P - \infty] \in J(\mathbb{Q})$ and so $5\lambda_\alpha(P) = 0$.

We now run through the algorithm to see that for $p = 7$ we actually have precisely

$$C(\mathbb{Q})_{\text{known}} \cup \left\{\left((1+\sqrt{-3})/2, \pm\sqrt{-3}\right), \left((1-\sqrt{-3})/2, \pm\sqrt{-3}\right)\right\} = Z.$$

First we apply the change of variables $x \mapsto -4x$, $y \mapsto 4^4 y$ to obtain an equation for C for which the defining polynomial $F(x)$ is monic. The $\mathbb{F}_p$-points of C with respect to the resulting equation are

$$\overline{C}(\mathbb{F}_p) = \{\overline{\infty}, \overline{(0,2)}, \overline{(0,5)}, \overline{(1,4)}, \overline{(1,3)}, \overline{(2,4)}, \overline{(2,3)}, \overline{(4,4)}, \overline{(4,3)}, \overline{(5,2)}, \overline{(5,5)}\}.$$

Of these eleven points, five of them arise as reductions of known $\mathbb{Q}$-rational points and an order of vanishing calculation shows that these are the only rational points in those residue disks. For the remaining six $\mathbb{F}_p$-points of C, the same order of vanishing calculation shows that there is at most one $\mathbb{Q}_p$-point in each residue disk corresponding to these points on which $\lambda_{\alpha,\infty}$ and $\lambda_{\beta,\infty}$ vanish.

We know that the four quadratic points above reduce to

$$\{\overline{(1,4)}, \overline{(1,3)}, \overline{(4,4)}, \overline{(4,3)}\}$$

in some order (note that the quadratic points listed above are on the original curve and these $\mathbb{F}_p$-points are the images after the change of variables of their reductions). Hence, our task is now reduced to the analysis of the residue disks of $\overline{(2,4)}$ and $\overline{(2,3)}$, which moreover map to each other under the hyperelliptic involution. To show that $\lambda_\alpha, \lambda_\beta$ have no common zeros in these residue disks, we explicitly write down the power series and compute their zeros using `PARI/GP`, as outlined in §5.2.1.

As usual, let $\omega_i = x^i/2y$. Then the annihilator of $J(\mathbb{Q})$ under the integration pairing is spanned by

$$\begin{aligned}\alpha &= (1 + 2\cdot 7 + 7^2 + 2\cdot 7^3 + 5\cdot 7^4 + O(7^5))\,\omega_0 + (4 + 7^2 + 5\cdot 7^4 + O(7^5))\,\omega_1,\\ \beta &= (6 + 3\cdot 7 + 2\cdot 7^2 + 5\cdot 7^4 + O(7^5))\,\omega_0 + (4 + 7^2 + 5\cdot 7^4 + O(7^6))\,\omega_2.\end{aligned}$$

It suffices to consider the residue disk of $\overline{(2,4)}$, where we obtain the two power series

$$\begin{aligned}f(t) &= 2\cdot 7 + 4\cdot 7^2 + O(7^3) + (2 + 7 + 2\cdot 7^2 + O(7^3))t + (6 + 5\cdot 7 + 4\cdot 7^2 + O(7^3))t^2 + \cdots,\\ g(t) &= 7 + 6\cdot 7^2 + O(7^3) + (1 + 5\cdot 7 + 2\cdot 7^2 + O(7^3))t + (3 + 4\cdot 7 + 7^2 + O(7^3))t^2 + \cdots.\end{aligned}$$

Each of these has one zero in $p\mathbb{Z}_p$, but not the same zero. The two zeros are $6\cdot 7 + 5\cdot 7^2 + O(7^3)$ and $6\cdot 7 + 2\cdot 7^2 + O(7^3)$, respectively.

Example 5.4.3. Consider the hyperelliptic curve

$$y^2 + (x^3 + x)y = x^7 - 4x^6 + 8x^5 - 10x^4 + 8x^3 - 4x^2 + x,$$

(given above by a minimal model) which has absolute minimal discriminant 1573040 and whose Jacobian J has conductor $786520 = 2^3 \cdot 5 \cdot 7 \cdot 53^2$. We work with the odd degree model

$$C\colon y^2 = 4x^7 - 15x^6 + 32x^5 - 38x^4 + 32x^3 - 15x^2 + 4x,$$

on which we know the following rational points:

$$C(\mathbb{Q})_{\text{known}} = \{\infty, (0,0), (1,-2), (1,2)\}.$$

The point $R = [(1,-2) - \infty]$ has infinite order in $J(\mathbb{Q})$ and can thus be used to initiate the algorithm of §5.3.3 with $p = 11$, which is the smallest prime greater than 6 of good reduction for C. We find that

$$Z = C(\mathbb{Q})_{\text{known}} \cup W \cup \{(-1, \pm 2\sqrt{-35})\},$$

where the set W of non-$\mathbb{Q}$-rational Weierstrass points has size 2. In particular, we have $C(\mathbb{Q}) = C(\mathbb{Q})_{\text{known}}$.

Perhaps more interestingly, we now explain[5] why $\{(-1, \pm 2\sqrt{-35})\} \subseteq Z$. Let $K = \mathbb{Q}(\sqrt{-35})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and fix an embedding $K \hookrightarrow \mathbb{Q}_p$. The point

$$Q = [(-1, 2\sqrt{-35}) - \infty] \in J(K)$$

is of infinite order, as there exists a non-zero differential in $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ whose integral does not vanish on Q. Suppose that $nQ \in J(\mathbb{Q})$ for some integer $n \neq 0$. Then $nQ = (nQ)^\tau = nQ^\tau$ and hence $2Q = Q - Q^\tau \in J(K)_{\text{tors}}$, a contradiction. It follows that $J(\mathbb{Q})$ and Q generate a subgroup of rank 2 in $J(K)$. A computation in `Magma` shows that the rank of $J(K)$ itself is equal to 2. Therefore, the image of $Z \setminus W$ in $J(K)$ generates a subgroup of finite index. Showing that $(-1, \pm 2\sqrt{-35}) \in Z$ is then equivalent to proving that the dimension of the p-adic closure of $J(K)$ in $J(\mathbb{Q}_p)$ is 1, i.e. that the $\mathbb{Z}$-linear independence of Q and $J(\mathbb{Q})$ is not preserved under the base change of J to $\mathbb{Q}_p$.

To explain this phenomenon, we compute the automorphism group of C using `Magma`. We have that $\mathrm{Aut}(C) \cong C_2 \times C_2$, where the first copy of C_2 is generated by the hyperelliptic involution $i\colon C \to C$ and the second one is generated by $\varphi\colon C \to C$, $\varphi(x, y, z) = (z, y, x)$ which in affine coordinates corresponds to $(x, y) \mapsto (1/x, y/x^4)$. The quotient $C/\langle \varphi \rangle$ is the elliptic curve

$$E\colon y^2 + xy + y = x^3 - x^2,$$

whereas the quotient $C/\langle \varphi \circ i \rangle$ is the genus 2 hyperelliptic curve

$$y^2 + (x^2 + 1)y = x^5 + x^4 - 4x^3 + 3x^2 - x - 1,$$

which has the following odd degree model

$$H\colon y^2 = 4x^5 + 5x^4 - 16x^3 + 14x^2 - 4x - 3.$$

It follows that J decomposes, over $\mathbb{Q}$, as a product of E and the Jacobian of H, which is an abelian surface A [109, Theorem 4] .

[5] We are grateful to Andrew Sutherland for kindly computing real endomorphism algebras (using the techniques of [35, 68]) for a number of curves that produced Chabauty–Coleman output similar to this example, which greatly assisted in understanding the structure of their Jacobians. (Work by Costa et al. [51] provides further data on endomorphisms, can be made rigorous and is freely available on GitHub.) We would also like to thank Bjorn Poonen for a very helpful discussion about this phenomenon.

Since $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}(J(\mathbb{Q})) = 1$ and the p-adic closure of $E(L)$ in $J(\mathbb{Q}_p)$ can have dimension at most one for any number field L where p splits completely and any embedding $L \hookrightarrow \mathbb{Q}_p$, in order to determine which points of $C(\overline{\mathbb{Q}})$ can appear in Z, we then need to search for points that map to torsion points in A, under the quotient map $C \to H \to A$.

An explicit computation using Coleman integrals on H shows that $H(\mathbb{Q}_p) \cap A(\mathbb{Q}_p)_{\mathrm{tors}} \subseteq A(\mathbb{Q}_p)[2]$, where, as usual, the embedding of H into A is via the base point ∞. Moreover, the quotient map $C \to H$ maps ∞ and $(0,0)$ to ∞ and is defined elsewhere by

$$(x, y) \mapsto \left(\frac{x^2 - x + 1}{x}, \frac{x^2 y - y}{x^3} \right).$$

Let $T \in C(\mathbb{Q}_p)$. Then T maps into $A(\mathbb{Q}_p)_{\mathrm{tors}}$ if and only if either $T \in \{(0,0), \infty\}$ or $T = (x, y)$ with $y(x^2 - 1) = 0$. The latter condition is equivalent to $T \in W$ or $x^2 = 1$. This shows both why $\{(-1, \pm 2\sqrt{-35})\} \subset Z$ and why no other non-torsion point in $C(\overline{\mathbb{Q}})$ can occur in Z besides $(1, \pm 2)$ and $(-1, \pm 2\sqrt{-35})$.

5.4.2 Variation of the prime and the Strong Chabauty Conjecture

We also carried out an additional set of computations in light of the following conjecture:

Conjecture 5.4.4 (Stoll [133, Conj. 9.5]). *Let C be a smooth, projective, geometrically connected curve of genus ≥ 2 over a number field K. Assume that there is a non-constant morphism $\iota\colon C \to A$ into an abelian variety such that $\iota(C)$ generates A. Assume that the rank r of $A(K)$ is at most $\dim A - 2$. Then there is a finite subscheme $S \subset A$ and a set of places v of K of density 1 such that the topological closure of $A(K)$ in $A(K_v)$ meets $\iota(C)$ in a subset of $S(K_v)$.*

Remark 5.4.5. We thank Michael Stoll and Felipe Voloch for bringing this to our attention. As communicated to us by Stoll, the conjecture above should also have the hypothesis that the abelian variety A is simple.

With the hypothesis in the above conjecture that the abelian variety is simple, our Case 1 and 2 examples are of particular interest. We carried out the algorithm of §5.3.3 for each of these curves and all good primes between 7 and 1000 not dividing the leading coefficient of the curve's defining polynomial F. For each curve C and prime ℓ, we found that the output was just as expected, as we now explain. In what follows,

the subscript ℓ (or p) added to previously defined sets emphasises the dependence on the prime used.

Recall that for the smallest prime p satisfying the above assumptions, we had previously found that $Z_p \setminus (C(\mathbb{Q}) \cup W_p)$ was the p-adic localisation of a set of points $T \subset C(K)$, for some quadratic field K. Our additional computations showed that $Z_\ell \setminus (C(\mathbb{Q}) \cup W_\ell)$ is either empty (if ℓ is inert or ramified in K) or is the ℓ-adic localisation of the set T (if ℓ splits in K). In particular, this provides evidence for Conjecture 5.4.4 with the subscheme $S \subset J$ being the intersection of $\iota(C)$ with the saturation of $J(\mathbb{Q})$, as conjectured by Stoll.

To extend these computations to larger primes, we note that the recent work of Best [27] improving the complexity of Coleman integration algorithms would be useful for improving the speed of these computations.

Chapter 6

Quadratic Chabauty for (bi)elliptic curves over number fields

This chapter is based on joint work with Jennifer Balakrishnan, Amnon Besser and Steffen Müller, available at [8]. We include here only the results that can be phrased in terms of p-adic heights on elliptic curves, to avoid introducing p-adic heights on Jacobians of curves of higher genus, which appear nowhere else in this thesis. For a method to compute integral points over number fields on hyperelliptic curves of genus > 1 we refer the reader to [8].

6.1 Introduction

Let K be a number field and let X/K be a smooth projective curve of genus $g \geq 2$. When the Mordell–Weil rank r of the Jacobian J/K is less than g, the method of Chabauty [41], made effective by Coleman [42], can be used to compute a finite subset of $X(K_{\mathfrak{p}})$ containing $X(K)$, for any prime $\mathfrak{p}$ of good reduction for X. This often suffices to compute $X(K)$ exactly, as we saw in Chapter 5, or, more generally, when used in conjunction with the Mordell–Weil sieve. In principle, this method can be used also to compute rational points on elliptic curves, but it only applies to the trivial case $r = 0$.

Recall that the method of Chabauty–Coleman relies on the image of the map[1]

$$\log\colon J(K) \otimes K_{\mathfrak{p}} \to H^0(X_{K_{\mathfrak{p}}}, \Omega_1)^* \tag{6.1}$$

having positive codimension, which is used to write down abelian integrals vanishing at the rational points. Following an unpublished idea of Wetherell, Siksek [122] proposed to consider, instead of just one place $\mathfrak{p}$, all primes $\mathfrak{p}$ of K above a fixed

[1]Note that log is still also our notation for the p-adic logarithm $\mathbb{Q}_p^\times \to \mathbb{Q}_p$.

rational prime p simultaneously and, instead of $K_\mathfrak{p}$-valued functionals, $\mathbb{Q}_p$-valued ones. That is, he replaced the map (6.1) with

$$\log\colon J(K)\otimes\mathbb{Q}_p \to \mathrm{Res}_{K/\mathbb{Q}}(J)(\mathbb{Q}_p) \to \mathrm{Lie}(\mathrm{Res}_{K/\mathbb{Q}}(J))_{\mathbb{Q}_p}, \tag{6.2}$$

where $\mathrm{Res}_{K/\mathbb{Q}}$ is the Weil restriction. This often allows one to p-adically approximate $X(K)$ when

$$r \leq [K\colon\mathbb{Q}](g-1),$$

which improves Chabauty–Coleman's $r < g$. The first goal of this chapter is to extend the quadratic Chabauty method for elliptic curves described in Chapter 4 to general number fields, using a similar approach to Siksek's. Let E be an elliptic curve over K, fix a prime number p such that E has good reduction at all $\mathfrak{p} \mid p$ and let $\chi\colon \mathbb{A}_K^\times/K^\times \to \mathbb{Q}_p$ be a non-trivial idele class character (cf. Definition 4.3.10). This choice induces $\mathbb{Q}_p$-linear maps $t_\mathfrak{p}^\chi\colon K_\mathfrak{p}\to\mathbb{Q}_p$ for all $\mathfrak{p}\mid p$ and a $\mathbb{Q}_p$-valued p-adic height h_p^χ on $E(K)$, which can be decomposed into a weighted sum $[K\colon\mathbb{Q}]^{-1}\sum n_v\lambda_v^\chi$ of local heights. The local heights $\lambda_\mathfrak{p}^\chi$ are of the form $t_\mathfrak{p}^\chi\circ\tau_\mathfrak{p}$ for some Coleman functions $\tau_\mathfrak{p}$.

Let $\psi\colon E(K)\hookrightarrow E(K\otimes\mathbb{Q}_p)$ denote the embedding induced by the product of the completion maps $K\hookrightarrow K\otimes\mathbb{Q}_p=\prod_{\mathfrak{p}\mid p}K_\mathfrak{p}$ and let $\mathcal{X}$ be the complement of the origin of a fixed model for E/K. If (6.2) is injective for E, then we can find a set of $\mathbb{Q}_p$-valued functions on $E(K\otimes\mathbb{Q}_p)$ which restricts to a basis of $\mathbb{Q}_p$-valued quadratic forms on $E(K)$. From this, we deduce

Theorem 6.1.1. *Suppose that* (6.2) *is injective for E. Then there exists an explicitly computable finite set $T^\chi\subset\mathbb{Q}_p$ and an explicitly computable non-constant locally analytic function $\rho^\chi\colon\mathcal{X}(\mathcal{O}_K\otimes\mathbb{Z}_p)\to\mathbb{Q}_p$, both dependent on χ, such that $\rho^\chi(\psi(\mathcal{X}(\mathcal{O}_K)))\subset T^\chi$.*

See Theorem 6.4.2 below and its proof. Our approach to Theorem 6.1.1 can be used to extend the elementary proof of Theorem 4.6.1 given in Section 4.6 to general number fields K. In particular, let C be a bielliptic curve of genus 2 over K. Then C admits degree 2 maps φ_1,φ_2 to two elliptic curves E_1 and E_2 respectively.

Theorem 6.1.2. *Suppose that* (6.2) *is an injection for E_1 and E_2; for $i\in\{1,2\}$ let $\mathcal{Q}_i$ denote a set of $\mathbb{Q}_p$-valued functions on $E_i(K\otimes\mathbb{Q}_p)$ which restricts to a basis of quadratic forms on $E_i(K)$. For every non-trivial idele class character χ, there exist explicitly computable constants $\alpha_{q_1}^\chi,\beta_{q_2}^\chi\in\mathbb{Q}_p$, indexed by $q_1\in\mathcal{Q}_1$ and $q_2\in\mathcal{Q}_2$, and an explicitly computable finite set $T^\chi\subset\mathbb{Q}_p$ such that the function*

$$\rho^\chi\colon \tilde{C}(K\otimes\mathbb{Q}_p)\to\mathbb{Q}_p$$

defined by

$$\rho^\chi(z) := \sum_{\mathfrak{p}|p} (n_\mathfrak{p}^\chi \lambda_\mathfrak{p}^\chi(\varphi_1(z_\mathfrak{p})) - n_\mathfrak{p}^\chi \lambda_\mathfrak{p}^\chi(\varphi_2(z_\mathfrak{p})) - 2\chi_\mathfrak{p}(x(z_\mathfrak{p})))$$
$$- \sum_{q_1 \in \mathcal{Q}_1} \alpha_{q_1}^\chi q_1(\varphi_1(z)) + \sum_{q_2 \in \mathcal{Q}_2} \beta_{q_2}^\chi q_2(\varphi_2(z))$$

satisfies

$$\rho^\chi(\psi(\tilde{C}(K))) \subset T^\chi;$$

here $\tilde{C}(K \otimes \mathbb{Q}_p)$ *is the subset of* $C(K \otimes \mathbb{Q}_p)$ *where* ρ^χ *is well-defined and* $\psi(\tilde{C}(K))$ *is its intersection with* $\psi(C(K))$.

See Theorem 6.5.2 for a more precise formulation. If we want to use Theorem 6.1.1 (resp. Theorem 6.1.2) to actually compute integral (resp. rational) points of $X = E$ (resp. $X = C$), then we need enough functions ρ^χ so that their common zero set is finite. In order to achieve this, we require at least $[K\colon \mathbb{Q}]$ such functions, since this is the dimension of the Weil restriction of X over $\mathbb{Q}$.

Over the rational numbers the space of $\mathbb{Q}_p$-valued idele class characters has dimension 1, so up to a scalar factor, Theorem 6.1.1 (resp. Theorem 6.1.2) only leads to one locally analytic function which vanishes at the integral (resp. rational) points. In general, the dimension of this space is at least $r_2 + 1$, where r_2 is the number of conjugate pairs of non-real embeddings of K into $\mathbb{C}$ (with equality if Leopoldt's conjecture holds). Combining the resulting functions with Siksek's work, we expect that, generically, we get a method to compute integral or rational points whenever

$$r + \operatorname{rank}(\mathcal{O}_K^\times) \leq [K\colon \mathbb{Q}]g. \tag{6.3}$$

As in Siksek's work, this cannot be true in general, for instance because of base change obstructions: if X can be defined over a subfield F of K and if

$$\operatorname{rank}(\operatorname{Jac}(X)(F)) + \operatorname{rank}(\mathcal{O}_F^\times) > [F\colon \mathbb{Q}]g,$$

then our approach might fail. See also Question 6.4.4.

However, the focus of this work is on developing explicit methods for computing integral or rational points, not on theoretical conditions guaranteeing finiteness. See recent work of Dogra [56] for a discussion of finiteness issues related to ours, but working directly with Kim's approach.

It would certainly be interesting to extend the explicit results in [17] and [18] to general number fields. We have not attempted this, but rather focused on extending those explicit quadratic Chabauty results which do not require p-adic Hodge theory.

To illustrate the practicality of our method, we give several examples over quadratic fields. In particular, we compute

- the $\mathbb{Q}(i)$-rational points on the bielliptic modular curve $X_0(91)^+$, see Example 6.7.1. The Mordell–Weil rank of the Jacobian of $X_0(91)^+$ over $\mathbb{Q}(i)$ is 4 and its rank over $\mathbb{Q}$ is 2.

- the $\mathbb{Q}(\sqrt{34})$-rational points on the curve C of Example 4.6.3, arising from the work of Diophantus and considered by Wetherell. The Jacobian of C has rank 3 over $\mathbb{Q}(\sqrt{34})$. See Example 6.7.2.

The chapter is structured as follows. In Section 6.2 we review the part of the theory of $\mathbb{Q}_p$-valued idele class characters which is relevant to our applications. In Section 6.3, we recall Siksek's work on classical Chabauty over number fields. In Sections 6.4 and 6.5 we present our extension to number fields of quadratic Chabauty for elliptic and bielliptic curves. Algorithms and examples over quadratic fields in which the prime p splits are then the subject of Sections 6.6 and 6.7. Finally, in Appendix 6.A, we discuss how to compute solutions to systems of p-adic equations in several variables, as this is a technical tool used in our algorithms.

6.1.1 Notation

In addition to the notation listed at the beginning of this thesis, we fix here the following conventions specific to this chapter.

K	a number field,
d	the extension degree $[K\colon \mathbb{Q}]$,
(r_1, r_2)	the signature of K,
r_K	the rank $r_1 + r_2 - 1$ of the unit group $\mathcal{O}_K^\times$,
$\varepsilon_1, \dots, \varepsilon_{r_K} \in K$	fundamental units of K,
h_K	the class number of K,
ξ_v	a generator of v^{h_K} if $v \subset K$ is a prime ideal,
n_v	the degree $[K_v\colon \mathbb{Q}_p]$ if $v \subset K$ is a prime ideal,
p	an odd prime number, unramified in K,
$\mathfrak{p}_1, \dots, \mathfrak{p}_m \subset K$	the primes of $\mathcal{O}_K$ lying above p,
$K_j = K_{\mathfrak{p}_j}$	the completion of K at $\mathfrak{p}_j$,
$\mathcal{O}_j$	the ring of integers of K_j,
$\psi_j\colon K \hookrightarrow K_j$	an embedding $K \hookrightarrow K_j$,
$n_j = n_{\mathfrak{p}_j}$	the degree $[K_j\colon \mathbb{Q}_p]$,
$\log_j\colon K_j^\times \to K_j$	a branch of the logarithm.

6.2 Idele class characters and p-adic heights

In this section, we recall the structure of the idele class characters

$$\chi = \sum_v \chi_v\colon \mathbb{A}_K^\times / K^\times \to \mathbb{Q}_p$$

of Definition 4.3.10 (note in particular that we require that χ be continuous) and discuss in more detail how to construct them explicitly. These characters are of great importance in Iwasawa theory, as they correspond to $\mathbb{Z}_p$-extensions of K (see also Chapter 7). We shall not use this interpretation; for us, the main application is the explicit construction of p-adic heights.

First we note the following:

- For any prime $\mathfrak{q} \nmid p$ we have $\chi_\mathfrak{q}(\mathcal{O}_\mathfrak{q}^\times) = 0$ because of continuity. So if $\pi_\mathfrak{q}$ is a uniformiser in $K_\mathfrak{q}$, then $\chi_\mathfrak{q}$ is completely determined by $\chi_\mathfrak{q}(\pi_\mathfrak{q})$. Equivalently, we can use instead $\chi_\mathfrak{q}(q)$, where q is the underlying prime number, or $\chi_\mathfrak{q}(\xi_\mathfrak{q})$.

- For any $j \in \{1, \dots, m\}$, there is a $\mathbb{Q}_p$-linear map t_j such that we can decompose

$$\begin{array}{ccc} \mathcal{O}_j^\times & \xrightarrow{\quad\chi_{\mathfrak{p}_j}\quad} & \mathbb{Q}_p, \\ & {\scriptstyle \log_j} \searrow \quad \nearrow {\scriptstyle t_j} & \\ & K_j & \end{array} \tag{6.4}$$

  because $\chi_{\mathfrak{p}_j}$ takes values in the torsion-free group $(\mathbb{Q}_p, +)$. We call the t_j *additive characters.*

Remark 6.2.1. If an idele class character χ is ramified at $\mathfrak{p}_j$, that is, if the local character $\chi_{\mathfrak{p}_j}$ does not vanish on $\mathcal{O}_j^\times$, then we can extend $\log_j$ to

$$\log_j \colon K_j^\times \to K_j \tag{6.5}$$

in such a way that the diagram (6.4) remains commutative.

Henceforth, we shall write

$$(K \otimes \mathbb{Q}_p)^* = \prod_{i=1}^m \mathrm{Hom}_{\mathbb{Q}_p}(K_i, \mathbb{Q}_p)$$

for the $\mathbb{Q}_p$-linear forms on $K \otimes \mathbb{Q}_p$. By the above, an idele class character of K determines an element t^χ of $(K \otimes \mathbb{Q}_p)^*$.

Lemma 6.2.2. *The choice of*

$$t^\chi = (t_1, \dots, t_m) \in (K \otimes \mathbb{Q}_p)^*$$

as in (6.4) *uniquely determines the character* χ.

Proof. We first show that t^χ determines $\chi_{\mathfrak{p}_j}$ for $1 \le j \le m$. Indeed, since $\chi_{\mathfrak{p}_j}(u) = t_j(\log_j(u))$ for all $u \in \mathcal{O}_j^\times$ and since $\psi_i(\xi_{\mathfrak{p}_j})$ is a unit in $\mathcal{O}_i$ for $i \ne j$, we have

$$\chi_{\mathfrak{p}_j}(\psi_j(\xi_{\mathfrak{p}_j})) = -\sum_{i \ne j} \chi_{\mathfrak{p}_i}(\psi_i(\xi_{\mathfrak{p}_j})) = -\sum_{i \ne j} t_i(\log_i(\psi_i(\xi_{\mathfrak{p}_j}))),$$

so $\chi_{\mathfrak{p}_j}$ is completely determined.

Now let $\mathfrak{q}$ be a prime not dividing p. Then $\chi_\mathfrak{q}$ is determined by its value on $\xi_\mathfrak{q}$ (embedded into $K_\mathfrak{q}$ via $\psi_\mathfrak{q}$) and vanishes on $\mathcal{O}_\mathfrak{q}^\times$. Hence we find

$$\chi_\mathfrak{q}(\psi_\mathfrak{q}(\xi_\mathfrak{q})) = -\sum_{i=1}^m \chi_{\mathfrak{p}_i}(\psi_i(\xi_\mathfrak{q})) = -\sum_{i=1}^m t_i(\log_i(\psi_i(\xi_\mathfrak{q}))). \qquad \square$$

So in order to construct idele class characters, we need to determine which elements $t \in (K \otimes \mathbb{Q}_p)^*$ lead to such characters.

Lemma 6.2.3. *A homomorphism*

$$t = (t_1, \ldots, t_m) \in (K \otimes \mathbb{Q}_p)^*$$

gives rise to an idele class character χ if and only if

$$t_1(\log_1(\psi_1(\varepsilon_i))) + \cdots + t_m(\log_m(\psi_m(\varepsilon_i))) = 0 \tag{6.6}$$

for all $1 \leq i \leq r_K$.

Proof. Suppose that χ is an idele class character, determined by $t \in (K \otimes \mathbb{Q}_p)^*$ as in Lemma 6.2.2. Note that for a unit $\varepsilon \in \mathcal{O}_K^\times$ the value $\chi_v(\varepsilon)$ depends only on t_v for $v \mid p$ and is 0 otherwise. Hence (6.6) must be satisfied for all $i \in \{1, \ldots, r_K\}$.

On the other hand, suppose that $t \in (K \otimes \mathbb{Q}_p)^*$ and let χ denote the character $\chi\colon \mathbb{A}_K^\times \to \mathbb{Q}_p$ associated to t as in Lemma 6.2.2. Given $\beta \in K^\times$, we need to show that $\chi(\beta) = 0$. Suppose that $(\beta) = \prod v_i^{e_i}$ is the decomposition of the fractional ideal (β). Then

$$(\beta^{h_K}) = \prod v_i^{h_K e_i} = \prod (\xi_{v_i})^{e_i} = \left(\prod \xi_{v_i}^{e_i}\right)$$

so that $\beta^{h_K} = \prod \xi_{v_i}^{e_i} u$ for some unit u. But since the construction of χ was done so that $\chi(\xi_v) = 0$ for every v and $\chi(u) = 0$ for every unit, we see that $\chi(\beta^{h_K}) = 0$ and hence $\chi(\beta) = 0$. □

We deduce the following result:

Corollary 6.2.4. *The idele class characters of K form a $\mathbb{Q}_p$-vector space V_K of dimension $\geq r_2+1$, with equality if Leopoldt's conjecture [89] holds for K. In particular, if $K/\mathbb{Q}$ is an abelian extension, then we have* $\dim_{\mathbb{Q}_p} V_K = r_2 + 1$.

Proof. The space V_K has dimension precisely $d - r_K = r_2 + 1$ if the equations (6.6) are independent; otherwise its dimension is larger. Leopoldt's conjecture [89] predicts that the p-adic regulator of K is non-zero, which is equivalent to independence of the equations (6.6). Brumer [39] proved Leopoldt's conjecture for abelian $K/\mathbb{Q}$. □

Remark 6.2.5. For our applications it suffices that $\dim_{\mathbb{Q}_p} V_K \geq r_2 + 1$.

Remark 6.2.6. Corollary 6.2.4 is classical [95], but our proof yields a method for actually determining a basis of V_K, provided that we know the class number h_K, fundamental units and a method for computing, for each prime v of K, a generator $\xi_v \in K^\times$ of the principal ideal v^{h_K}.

Example 6.2.7. If $t = (t_1, \dots, t_m) \in (K \otimes \mathbb{Q}_p)^*$, where $t_j = \mathrm{tr}_{K_j/\mathbb{Q}_p}$, then equation (6.6) translates into the trivially satisfied $\log(N_{K/\mathbb{Q}}(\varepsilon_i)) = 0$. This choice of t gives rise to an idele class character χ^{cyc}, which one obtains by composing the usual idele class character over $\mathbb{Q}$ (corresponding to $t_1 = \mathrm{id}_{\mathbb{Q}_p}$) with the norm on the idele class group. We call χ^{cyc} the *cyclotomic* character; it cuts out the cyclotomic $\mathbb{Z}_p$-extension of K (cf. [96, §2.1]). Note that every idele class character of a totally real abelian number field is a scalar multiple of χ^{cyc} by Corollary 6.2.4.

Example 6.2.8. If p is totally split in K, then the additive characters correspond to scalar multiplication on $K_j \cong \mathbb{Q}_p$, so by Lemma 6.2.3, the space V_K of idele class characters is isomorphic to the subspace of all $(c_1, \dots, c_d) \in \mathbb{Q}_p^d$ such that

$$c_1 \log_1(\psi_1(\varepsilon_k)) + \cdots + c_d \log_d(\psi_d(\varepsilon_k)) = 0 \tag{6.7}$$

for all $1 \leq k \leq r_K$.

Example 6.2.9. Suppose that K is imaginary quadratic. Denote by $c\colon \mathbb{A}_K^\times/K^\times \to \mathbb{A}_K^\times/K^\times$ the involution induced by complex conjugation in K. We say that an idele class character $\chi \in V_K$ is *anticyclotomic* if $\chi \circ c = -\chi$. Any non-trivial anticyclotomic character cuts out the anticyclotomic $\mathbb{Z}_p$-extension of K and plays an important role in Iwasawa theory. Together with the cyclotomic character, it spans the two-dimensional space V_K.

If we assume, in addition, that p splits completely in K, then it turns out that $\chi \in V_K$ is anticyclotomic if and only if

$$c_1 + c_2 = 0$$

in the notation of Example 6.2.8. In this case, we call the character χ^{anti} corresponding to the choice $c_1 = 1$ and $c_2 = -1$ *the anticyclotomic* character. See [14, §1] for an explicit construction of χ^{anti}.

Let E/K be an elliptic curve of rank r, with good reduction at $\mathfrak{p}_1, \dots, \mathfrak{p}_m$. We fix a Weierstrass equation for E with coefficients in $\mathcal{O}_K$ and minimal at all $\mathfrak{p}_i$; we denote by O the point at infinity of E and for $P \in E(K) \setminus \{O\}$ we let $x(P)$ be the x-coordinate of P with respect to our fixed equation. Recall from §4.3.2 that, given $\chi \in V_K$, we can define a p-adic height

$$h_p^\chi\colon E(K) \to \mathbb{Q}_p$$

by $h_p^\chi = \frac{1}{[K\colon \mathbb{Q}]} \sum_v n_v \lambda_v^\chi$, for some functions $\lambda_v^\chi\colon E(K_v) \setminus \{O\} \to \mathbb{Q}_p$ and by setting $h_p^\chi(O) = 0$.

For instance, if $\mathfrak{q} \nmid p$ and $P \in E(K_\mathfrak{q}) \setminus \{O\}$ reduces to a non-singular point, then

$$\lambda_\mathfrak{q}^\chi(P) = -\frac{\chi_\mathfrak{q}}{n_\mathfrak{q}}(\max\{1, |x(P)|_\mathfrak{q}\}), \tag{6.8}$$

whereas if $P \in E(K_j)$, $\overline{P} \neq \overline{O}$,

$$\lambda_{\mathfrak{p}_j}^\chi(P) = \frac{1}{n_j} t_j \left(2 \int_b^P \psi_j(\omega_0)(\psi_j(\eta_0) + \beta_j \psi_j(\omega_0)) \right) =: \frac{1}{n_j} t_j(\tau_j^{(\beta_j)}(P))$$

for some fixed $\beta_j \in K_j$; here b is a tangential base point at O, ω_0 is an invariant differential and $\eta_0 = x\omega_0$. As usual, the local height $\lambda_{\mathfrak{p}_j}^\chi$ can be interpreted in terms of $\mathfrak{p}_j$-adic sigma functions (see Chapter 2 and (4.6)). For any K, we write h_p^{cyc} for $h_p^{\chi^{\mathrm{cyc}}}$, which is the usual cyclotomic p-adic height; if K is imaginary quadratic, we let h_p^{anti} be the anticyclotomic p-adic height $h_p^{\chi^{\mathrm{anti}}}$.

Denote by $\mathcal{B}$ the space of $\mathbb{Q}_p$-valued quadratic forms on $E(K) \otimes_\mathbb{Z} \mathbb{Q}_p$. The function $V_K \to \mathcal{B}$ mapping χ to h_p^χ is $\mathbb{Q}_p$-linear. The dimension of its image is bounded from above by

$$\min\left\{\dim_{\mathbb{Q}_p} V_K, \frac{r(r+1)}{2}\right\} \geq \min\left\{r_2 + 1, \frac{r(r+1)}{2}\right\},$$

where the inequality is an equality if Leopoldt's conjecture holds for K (see Corollary 6.2.4). Lower bounds on the dimension are much more difficult (cf. Chapter 3).

6.3 Chabauty over number fields

In this section we recall the method of Chabauty and Coleman over number fields. This was first proposed by Wetherell at an MSRI talk in 2000, but his ideas were never published. Then Siksek [122] showed how to p-adically approximate the rational points on a curve over a number field K using p-adic integrals, provided that the curve satisfies certain conditions. He also discussed how this can be combined with the Mordell–Weil sieve to compute the set of K-rational points. See also Triantafillou's work [139] for a recent application to hyperbolic curves of genus 0 and S-unit equations.

Let X/K be a smooth, projective, geometrically irreducible curve of genus $g > 0$ with good reduction at $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$; let J denote its Jacobian and let $r = \mathrm{rank}(J(K))$. We also assume that there is a rational point $P_0 \in X(K)$ and we let $\iota\colon X \hookrightarrow J$ denote the Abel–Jacobi map corresponding to it. We write $X(K \otimes \mathbb{Q}_p)$ for the subset $X(K_1) \times \cdots \times X(K_m)$ of $X(\overline{\mathbb{Q}}_p)^m$ and $\psi\colon X(K) \hookrightarrow X(K \otimes \mathbb{Q}_p)$ for the embedding induced by $\psi_j\colon X(K) \hookrightarrow X(K_j)$.

Recall that the classical method of Chabauty–Coleman (see [42, 101]) over $K = \mathbb{Q}$ can be used to compute a finite subset of $X(\mathbb{Q}_p)$ which contains $X(\mathbb{Q})$ and that the idea is to construct a non-trivial locally analytic function $\rho\colon X(\mathbb{Q}) \to \mathbb{Q}_p$ which vanishes on $X(\mathbb{Q})$. For general K, the goal is to find d explicitly computable locally analytic functions

$$\rho_1, \dots, \rho_d\colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

such that

(i) we have $\rho_l(\psi(X(K))) = 0$ for all $1 \leq l \leq d$;

(ii) the intersection

$$B := \{z \in X(K \otimes \mathbb{Q}_p) : \rho_l(z) = 0 \text{ for all } 1 \leq l \leq d\}$$

is finite.

The reason for requiring (at least) d such functions is that we can identify $X(K)$ with $W(\mathbb{Q})$, where W is the Weil restriction of X over $\mathbb{Q}$, which has dimension d; hence at least d functions are needed to cut out a finite subset of $X(K \otimes \mathbb{Q}_p)$.

With a view towards explicit computations and generalisations, we now discuss how the functions ρ_l can be constructed in terms of Coleman integrals. Let $j \in \{1, \dots, m\}$ and let $z_j \in X(K_j)$. If ω is a holomorphic 1-form on X/K_j, then the integral $\int_{\psi_j(P_0)}^{z_j} \omega$ is an element of K_j. We can compose it with an additive character $t_j \in \mathrm{Hom}_{\mathbb{Q}_p}(K_j, \mathbb{Q}_p)$ to get a locally analytic function

$$X(K_j) \to \mathbb{Q}_p; \qquad z_j \mapsto t_j\left(\int_{\psi_j(P_0)}^{z_j} \omega\right).$$

For every $j \in \{1, \dots, m\}$, we fix a basis $(t_{j,1}, \dots, t_{j,n_j})$ of $\mathrm{Hom}_{\mathbb{Q}_p}(K_j, \mathbb{Q}_p)$; we also fix a basis $(\omega_0, \dots, \omega_{g-1})$ of $H^0(X/K, \Omega^1)$.

Definition 6.3.1. Let $i \in \{0, \dots, g-1\}$, let $j \in \{1, \dots, m\}$ and let $k \in \{1, \dots, n_j\}$. We define

$$f_i^{(j,k)}(z) := t_{j,k}\left(\int_{\psi_j(P_0)}^{z_j} \psi_j(\omega_i)\right)$$

for $z = (z_1, \dots, z_m) \in X(K \otimes \mathbb{Q}_p)$. For $Q \in X(K)$, we set

$$f_i^{(j,k)}(Q) := f_i^{(j,k)}(\psi(Q)).$$

The maps $f_i^{(j,k)}$ define locally analytic functions $X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$. We fix an arbitrary ordering and label their restrictions to $X(K)$ by

$$f_0, \ldots, f_{dg-1} \colon X(K) \to \mathbb{Q}_p.$$

Extending these by additivity, we obtain $\mathbb{Q}_p$-valued linear functionals

$$f_0, \ldots, f_{dg-1} \colon J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathbb{Q}_p. \tag{6.9}$$

We fix some more notation. Let $(J(K) \otimes \mathbb{Q}_p)^* = \mathrm{Hom}_{\mathbb{Q}_p}(J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p, \mathbb{Q}_p)$, let

$$U = \mathrm{Span}_{\mathbb{Q}_p}(f_0, \ldots, f_{dg-1}) \subset (J(K) \otimes \mathbb{Q}_p)^*,$$

and let

$$n = dg - \dim_{\mathbb{Q}_p}(U)$$

denote the maximal number of independent relations between the f_i.

Suppose that

$$n \geq d \tag{6.10}$$

and fix a set of d independent relations in U. These, pulled back via the Abel–Jacobi map ι, extend to explicitly computable locally analytic functions

$$\rho_1, \ldots, \rho_d \colon X(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

such that

$$\rho_l(\psi(X(K))) = 0$$

for all $l = 1, \ldots, d$. Then, provided that the common zero set B of $\rho_1, \ldots, \rho_d$ is finite, we can explicitly determine $X(K)$, by first computing B (to suitable p-adic precision) and then identifying $\psi(X(K)) \subset B$ using the Mordell–Weil sieve. See [122] for details.

As mentioned previously, over $\mathbb{Q}$ the condition $r < g$ is a sufficient criterion for the method of Chabauty–Coleman to work. But when $K \neq \mathbb{Q}$, it is much more delicate to predict whether the zero set B is finite, as we have to deal with systems of multivariate power series (see also Appendix 6.A). Since $\dim_{\mathbb{Q}_p}(J(K) \otimes \mathbb{Q}_p)^* = r$, we have $n \geq dg - r$. Therefore one might guess that for finiteness of B it could be sufficient that

$$r \leq d(g-1). \tag{6.11}$$

This is not the case, as one can find examples where B is infinite because X can be defined over some subfield F of K over which $\mathrm{rank}(J(F)) > [F \colon \mathbb{Q}](g-1)$; see [122] for a discussion. Siksek asks whether B is finite whenever

$$\mathrm{rank}(\mathrm{Jac}(\tilde{X})(F)) \leq [F \colon \mathbb{Q}](g-1) \tag{6.12}$$

for all subfields F and for every smooth projective curve $\tilde{X}/F$ such that $\tilde{X} \times_F K \cong_K X$. This was shown to be false by Dogra [56]. In particular, he constructs a hyperelliptic genus 3 curve X with minimal field of definition $K := \mathbb{Q}(\sqrt{33})$ covering a genus 2 curve $X_0/\mathbb{Q}$ whose Jacobian J_0 satisfies $\mathrm{rank}(J_0(\mathbb{Q})) = 2$. This X satisfies the condition (6.12), but the functions ρ_l vanish in the preimage of $X_0(\mathbb{Q}_p)$ in $X(K \otimes \mathbb{Q}_p)$, so B is infinite. Dogra also shows that B is finite whenever $r \leq d(g-1)$ and $\mathrm{Hom}(J(K)_{\overline{\mathbb{Q}},\psi_1}, J(K)_{\overline{\mathbb{Q}},\psi_2})$ is trivial for any two distinct embeddings $\psi_1, \psi_2 \colon K \hookrightarrow \overline{\mathbb{Q}}$, i.e. whenever J and its conjugates do not share an isogeny component over $\overline{\mathbb{Q}}$.

When $r > d(g-1)$, the method of Siksek is in general not applicable. In the following two sections, we discuss how to extend it using p-adic heights.

6.4 Quadratic Chabauty for integral points on elliptic curves over number fields

Let E/K be as at the end of Section 6.2 and let $\mathcal{X}$ be the complement of the origin in our fixed model for E over $\mathcal{O}_K$. For the case $K = \mathbb{Q}$, we saw in Chapter 4 how to define a finite subset of $\mathcal{X}(\mathbb{Z}_p)$ containing $\mathcal{X}(\mathbb{Z})$ when $r \leq 1$, using locally analytic functions constructed in terms of the cyclotomic p-adic height. We now show how to generalise this idea to arbitrary number fields. Generically, we expect our method to work when

$$r + r_K \leq d. \tag{6.13}$$

More precisely, we try to construct explicitly computable functions

$$\rho_1, \ldots, \rho_d \colon E(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$$

which are locally analytic on p-integral points, and explicitly computable finite subsets $T^{(1)}, \ldots, T^{(d)} \subset \mathbb{Q}_p$ such that

(i) we have $\rho_l(\psi(\mathcal{X}(\mathcal{O}_K))) \subset T^{(l)}$ for all $1 \leq l \leq d$;

(ii) the intersection

$$B := \left\{ z \in \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) : \ \rho_l(z) \in T^{(l)} \ \text{ for all } \ 1 \leq l \leq d \right\}$$

is finite.

We show how to construct such functions $\rho_1, \ldots, \rho_d$ when (6.13) and the following condition for $J = E$ are satisfied:

Condition 6.4.1. We have

$$(J(K) \otimes \mathbb{Q}_p)^* = U,$$

where U is defined as in Section 6.3.

If Condition 6.4.1 is satisfied for E, then we have $\dim_{\mathbb{Q}_p} U = r$ and hence

$$n + r = d; \tag{6.14}$$

in particular, we need $r \leq d$ for Condition 6.4.1 to hold and, in fact, it is even necessary that

$$\operatorname{rank}(\tilde{E}(F)) \leq [F\colon \mathbb{Q}]$$

for all subfields F of K and for all $\tilde{E}/F$ isomorphic to E over K. If $r = d$, Condition 6.4.1 is equivalent to surjectivity of the map in (6.2) with $J = E$.

We can order the f_i so that $(f_0, \ldots, f_{r-1})$ is a basis of $(E(K) \otimes \mathbb{Q}_p)^*$. For $0 \leq i \leq j \leq r-1$, we define the quadratic form $g_{ij}\colon E(K) \otimes \mathbb{Q}_p \to \mathbb{Q}_p$ by

$$g_{ij}(P) = f_i(P) f_j(P).$$

Thus $(g_{ij} : 0 \leq i \leq j \leq r-1)$ is a basis for the space of $\mathbb{Q}_p$-valued quadratic forms on $E(K) \otimes \mathbb{Q}_p$. Let χ be a non-trivial idele class character of K and let h_p^χ be the global p-adic height of Section 6.2 on E with respect to χ. Embed $E(K)$ in $E(K \otimes \mathbb{Q}_p)$ via ψ. Note that, while h_p^χ only makes sense on $E(K)$, each g_{ij} is the restriction of a function on $E(K \otimes \mathbb{Q}_p)$, which we also denote by g_{ij}. On the other hand, on $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$, we also have the function $\sum_{j=1}^m n_j \lambda_{\mathfrak{p}_j}^\chi(z_j)$, for $z = (z_1, \ldots, z_m)$.

Theorem 6.4.2. *Suppose that Condition 6.4.1 is satisfied. Then there are explicitly computable constants $\alpha_{ij}^\chi \in \mathbb{Q}_p$ and an explicitly computable finite set $T^\chi \subset \mathbb{Q}_p$ such that the locally analytic function*

$$\rho^\chi\colon \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p,$$

defined by

$$\rho^\chi(z) := \sum_{j=1}^m n_j \lambda_{\mathfrak{p}_j}^\chi(z_j) - \sum_{0 \leq i \leq j \leq r-1} \alpha_{ij}^\chi g_{ij}(z),$$

satisfies

$$\rho^\chi(\psi(\mathcal{X}(\mathcal{O}_K))) \subset T^\chi.$$

Proof. Since h_p^χ is a $\mathbb{Q}_p$-valued quadratic form on $E(K)$, we can find $\alpha_{ij}^\chi \in \mathbb{Q}_p$ such that

$$[K\colon \mathbb{Q}]h_p^\chi = \sum_{0\le i\le j\le r-1} \alpha_{ij}^\chi g_{ij}. \tag{6.15}$$

Let $\mathfrak{q}$ be a prime of K not dividing p. When χ is the cyclotomic character and $\mathcal{X}$ is minimal at $\mathfrak{q}$, we saw in §4.2.1 that $\lambda_\mathfrak{q}^\chi(\mathcal{X}(\mathcal{O}_\mathfrak{q}))$ is a finite set which only depends on the reduction type at $\mathfrak{q}$ and is $\{0\}$ for almost all $\mathfrak{q}$. Because of (2.4), this holds also when $\mathcal{X}$ is not minimal at some primes (see also Lemma 4.6.4). In view of the definition of $\lambda_\mathfrak{q}^\chi$, all this remains true for arbitrary χ and $\lambda_\mathfrak{q}^\chi(\mathcal{X}(\mathcal{O}_\mathfrak{q}))$ can be computed using Propositions 4.2.1, 4.2.3 and (2.4), upon replacing log with $-\frac{\chi_\mathfrak{q}}{n_\mathfrak{q}}$.

Now suppose that $Q \in \mathcal{X}(\mathcal{O}_K)$. We conclude that

$$\begin{aligned}\rho^\chi(\psi(Q)) &= \sum_{j=1}^m n_j \lambda_{\mathfrak{p}_j}^\chi(\psi_j(Q)) - \sum_{0\le i\le j\le r-1} \alpha_{ij}^\chi g_{ij}(\psi(Q)) \\ &= \sum_{j=1}^m n_j \lambda_{\mathfrak{p}_j}^\chi(Q) - [K\colon\mathbb{Q}]h_p^\chi(Q) \\ &= -\sum_{\mathfrak{q}\nmid p} n_\mathfrak{q}\lambda_\mathfrak{q}^\chi(Q)\end{aligned}$$

indeed takes values in an explicitly computable finite set. □

Remark 6.4.3. This is a more precise version of Theorem 6.1.1. Since a global minimal model for E/K might not exist if the class number of K is non-trivial, we do not explicitly write down here the sets T^χ. The proof of Theorem 6.4.2 shows how to compute these sets and precise expressions were given in Chapter 4 for $K = \mathbb{Q}$ and $\chi = \chi^{\mathrm{cyc}}$.

We can expect at most $\min\left(\dim_{\mathbb{Q}_p} V_K, \frac{r(r+1)}{2}\right)$ independent height pairings h_p^χ. Recall that $\dim_{\mathbb{Q}_p} V_K \ge r_2 + 1$ (with equality if Leopoldt's conjecture holds for K). The set of all $z \in \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$ such that $\rho^\chi(z) \in T^\chi$ holds for the corresponding functions can only be finite when $r_2 + 1 = d$, i.e. when $K = \mathbb{Q}$ or K is an imaginary quadratic number field. In general, we need at least $d - (r_2 + 1) = r_K$ additional functions $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$ to cut out a finite subset of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$ containing $\psi(\mathcal{X}(\mathcal{O}_K))$. It is natural to take these from the relations among the functions f_i, as in Section 6.3. Therefore we need the maximal number n of independent relations to be at least r_K. Because of (6.14), this means that we want $r + r_K \le d$, which is precisely (6.13), to hold.

Let $\rho_1, \dots, \rho_{r_2+1}\colon \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) \to \mathbb{Q}_p$ be functions coming from p-adic heights associated to non-trivial idele class characters $\chi \in V_K$ above, with corresponding finite

sets $T^{(k)} \subset \mathbb{Q}_p$. Suppose that (6.13) holds and let $\rho_{r_2+2}, \ldots, \rho_d \colon E(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$ be induced by independent relations among the f_i. Set $T^{(l)} = \{0\} \subset \mathbb{Q}_p$ for $r_2+2 \leq l \leq d$. Then

$$B := \{z \in \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) : \rho_l(z) \in T^{(l)} \text{ for all } 1 \leq l \leq d\}$$

contains $\psi(\mathcal{X}(\mathcal{O}_K))$ and is explicitly computable. Thus, we get a method to p-adically approximate $\mathcal{X}(\mathcal{O}_K)$ in practice whenever B is finite.

The results of this section readily generalise to curves X of genus $g > 1$ with Jacobian J, by replacing the p-adic height h_p^χ with the p-adic height $J(K) \to \mathbb{Q}_p$ of Coleman–Gross [46] (see [8] for more details and [9, 10] for the case $K = \mathbb{Q}$). In analogy with the results of Dogra [56], we then raise the following

Question 6.4.4. Suppose that Condition 6.4.1 is satisfied and that we have

$$\operatorname{rank}(\operatorname{Jac}(Y)(F)) + r_F \leq [F \colon \mathbb{Q}]g \tag{6.16}$$

for every subfield $F \subset K$ and for every smooth projective curve Y/F such that $Y \times_F K \cong_K X$. Is it true that B can only be infinite for geometric reasons?

Remark 6.4.5. Siksek's method always succeeds in constructing a set B, provided that $r \leq d(g-1)$. As was explained at the end of Section 6.3, this assumption on the rank is however not sufficient to guarantee finiteness of B. On the contrary, even definability of a set B is not ensured by (6.16). If $K = \mathbb{Q}$ and (6.16) holds, then either Condition 6.4.1 is satisfied or classical Chabauty is applicable (or both). For general K, it is instead possible to construct examples where (6.16) holds, but we are neither in the situation of Condition 6.4.1 nor in Siksek's. Indeed, let X be a genus 2 hyperelliptic curve over an imaginary quadratic field K. Suppose that X does not not descend to $\mathbb{Q}$ and that its Jacobian splits as the product of two elliptic curves E_1 and E_2. If $\operatorname{rank}(E_1(K)) = 3$ and $\operatorname{rank}(E_2(K)) = 1$ and E_1 cannot be defined over $\mathbb{Q}$, then we expect that $\dim_{\mathbb{Q}_p}(U) = 3$. For example, consider the hyperelliptic curve over $\mathbb{Q}(i)$

$$X \colon y^2 = x^6 + \frac{1}{5}(8i-6)x^4 + (-4i-3)x^2 + 4i + 8.$$

Its Jacobian splits as the product of

$$E_1 \colon y^2 = x^3 + (-4i-3)x^2 + (8i-16)x + (64i+48)$$
$$E_2 \colon y^2 = x^3 + \frac{1}{5}(8i-6)x^2 + (-4i-3)x + (4i+8)$$

of respective ranks 3 and 1. Let $P = (4i+2, -2i), Q = (4i, 8) \in E_1(\mathbb{Q}(i))$ and let ω_0 be a non-zero invariant differential on E_1. Then, choosing $p = 5$, we get

$$\left(\int_O^{\psi_1(P)} \psi_1(\omega_0)\right)\left(\int_O^{\psi_2(Q)} \psi_2(\omega_0)\right) \neq \left(\int_O^{\psi_2(P)} \psi_2(\omega_0)\right)\left(\int_O^{\psi_1(Q)} \psi_1(\omega_0)\right),$$

so (6.2) is surjective for E_1. Thus the dimension of U for J is 3.

When $K = \mathbb{Q}$ it is conjectured by Waldschmidt that it is sufficient that J is simple of Mordell–Weil rank equal at most g for Condition 6.4.1 to hold (see [143]).

Remark 6.4.6. The equations attached by Theorem 6.4.2 to dependent height pairings can sometimes be independent. To see this, consider an elliptic curve E over $\mathbb{Q}$ of rank 0. Then all global height pairings are identically zero on $E(\mathbb{Q})$; nevertheless, the cyclotomic height (with respect to a choice of splitting) gives an equation whose zero set is, in general, not identical to $E(\mathbb{Q}_p)_{\mathrm{tors}}$, i.e. to the zero set of the p-adic logarithm on $E(\mathbb{Q}_p)$. See Chapter 4 for computational evidence and relations with a conjecture of Kim on effectiveness.

This phenomenon in rank 0 also provides us with an example of how different choices of splittings of the de Rham cohomology can lead to linearly independent equations. Indeed, recall that the cyclotomic p-adic height pairing on $E/\mathbb{Q}$ depends on a choice of subspace $W \subset H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$, complementary to the space of holomorphic forms, and that the local height at p is then given by

$$\lambda_p^{(W)}(z) = 2D_2(z) + \beta_W \operatorname{Log}(z)^2,$$

where $\beta_W \in \mathbb{Q}_p$ depends on W. Choosing two different subspaces W_1, W_2 we then get $\lambda_p^{(W_1)}(z) = 0 = \lambda_p^{(W_2)}(z)$ if and only if $\lambda_p^{(W)}(z) = 0 = \operatorname{Log}(z)$ for any W. Thus, for all $z \in \mathcal{X}(\mathbb{Z}_p)$ such that $\lambda_p^{(W_1)}(z) = 0$ but $\operatorname{Log}(z) \neq 0$, we have $\lambda_p^{(W_2)}(z) \neq 0$; examples of such z can be found in the computations for Chapter 4.

6.5 Quadratic Chabauty for rational points on bielliptic curves over number fields

Let C/K be the genus 2 bielliptic curve

$$y^2 = x^6 + a_4x^4 + a_2x^2 + a_0 \qquad (a_i \in \mathcal{O}_K \text{ and } \psi_j(a_0) \in \mathcal{O}_j^2 \text{ for all } 1 \leq j \leq m),$$

which has degree 2 maps φ_1, φ_2 to two elliptic curves:

$$\begin{aligned} E_1 &: y^2 = x^3 + a_4x^2 + a_2x + a_0, & \varphi_1(x,y) &= (x^2, y) \\ E_2 &: y^2 = x^3 + a_2x^2 + a_4a_0x + a_0^2, & \varphi_2(x,y) &= (a_0x^{-2}, a_0yx^{-3}). \end{aligned} \tag{6.17}$$

When K is either $\mathbb{Q}$ or an imaginary quadratic field and both E_1 and E_2 have Mordell–Weil rank 1 over K, it was shown in [16] that a suitable choice of idele class character of K gives rise to a locally analytic function on $C(K_j)$ which vanishes on $C(K)$, provided that $K_j \simeq \mathbb{Q}_p$ and C has good reduction at each $\mathfrak{p}_j$ (see Section 4.6 for the case $K = \mathbb{Q}$).

In this section, we combine the ideas of [16] with those of Section 6.4 to approximate $C(K)$ inside $C(K \otimes \mathbb{Q}_p)$ when K is an arbitrary number field and p is a prime, unramified in K, above which the given model for C has everywhere good reduction. As in Sections 6.3 and 6.4, we do not investigate here whether the systems of d equations in d variables that we define have finitely many zeros.

Embed C into its Jacobian J via the Abel–Jacobi map with respect to a point in $C(K)$ (for instance one of $\infty^{\pm} = (1 : \pm 1 : 0) \in C(K)$). For the construction it is sufficient to work under Assumption 6.5.1 below and

$$\operatorname{rank}(J(K)) + r_K \leq dg = 2d. \tag{6.18}$$

For each $A \in \{J, E_1, E_2\}$, let

$$f_0^A, \ldots, f_{dg(A)-1}^A \colon A(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p \to \mathbb{Q}_p$$

be the $\mathbb{Q}_p$-valued linear functionals of Section 6.3 on A (here by $g(J)$ we mean the genus of C) and define, for $0 \leq i \leq j \leq dg(A) - 1$, the quadratic form

$$g_{ij}^A \colon A(K) \otimes \mathbb{Q}_p \to \mathbb{Q}_p, \qquad g_{ij}^A(P) = f_i^A(P) f_j^A(P).$$

Let χ be a non-trivial idele class character of K and for each $k \in \{1, 2\}$ let h_p^{χ, E_k} be the global p-adic height of Section 6.2 on E_k with respect to χ. Similarly, for a prime v of K, denote by λ_v^{χ, E_k} the local height at v. We work under the following assumption:

Assumption 6.5.1. Condition 6.4.1 holds for each of E_1 and E_2.

Possibly after reordering the $g_{ij}^{E_k}$, we can then find α_{ij}^{χ, E_k}, $0 \leq i \leq j \leq \operatorname{rank}(E_k(K)) - 1$, such that

$$[K \colon \mathbb{Q}] h_p^{\chi, E_k} = \sum_{i,j} \alpha_{ij}^{\chi, E_k} g_{ij}^{E_k}. \tag{6.19}$$

Let $Q_1 = (0, \sqrt{a_0}) \in E_1(K(\sqrt{a_0}))$, $Q_2 = (0, a_0) \in E_2(K)$ and, for a point $P \in C(K_j)$, denote by $]P[$ the residue disk centred at P in $C(K_j)$. Define

$$C^{(k)}(K \otimes \mathbb{Q}_p) = \prod_{j=1}^{m} C(K_j) \setminus \left( ]\psi_j(\varphi_k^{-1}(Q_k))[\cup\,]\psi_j(\varphi_k^{-1}(-Q_k))[\right)$$
$$C^{(k)}(K) = \psi(C(K)) \cap C^{(k)}(K \otimes \mathbb{Q}_p),$$

where, if Q_1 is not defined over K, we let $\psi_j(\varphi_1^{-1}(\pm Q_1)) = (0, \pm\sqrt{\psi_j(a_0)})$.

If a_0 is not a square in K, let χ' be the idele class character of $L := K(\sqrt{a_0})$ defined by composing the additive characters of χ with the field traces $L_{\mathfrak{p}'}/K_{\mathfrak{p}_j}$ at each $\mathfrak{p}' \mid \mathfrak{p}_j$ and normalised so that it restricts to 2χ on $\mathbb{A}_K^\times/K^\times$ (cf. Lemma 4.3.13). Write $h_p^{\chi,E_1}(Q_1) = h_p^{\chi',E_1}(Q_1)$ and, for a prime v of K, $\lambda_v^{\chi,E_1}(Q_1) = \lambda_{v'}^{\chi',E_1}(Q_1)$ where v' is any prime of L above v. Since $\mathrm{Gal}(L/K)$ acts on Q_1 by multiplication by ± 1 and by definition of χ', the quantity $\lambda_v^{\chi,E_1}(Q_1)$ is well-defined and all properties of λ_v^{χ,E_1} for points over K hold for Q_1. The following result is a version of Theorem 6.1.2 which is computationally more useful, since the function of Theorem 6.1.2 is defined only on a proper subset of $C^{(k)}(K \otimes \mathbb{Q}_p)$ for each k.

Theorem 6.5.2. *Suppose that* $\mathrm{ord}_v(a_0) \leq 1$ *for all primes* v. *For each* $k \in \{1,2\}$, *there exists an explicitly computable finite set* $T^{\chi,k} \subset \mathbb{Q}_p$ *such that the locally analytic function* $\rho^{\chi,k}\colon C^{(k)}(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$, *defined by*

$$\begin{aligned}\rho^{\chi,k}(z) := \sum_{j=1}^{m} n_j \left(2\lambda_{\mathfrak{p}_j}^{\chi,E_{3-k}}(\varphi_{3-k}(z_j)) - \lambda_{\mathfrak{p}_j}^{\chi,E_k}(\varphi_k(z_j)+Q_k) - \lambda_{\mathfrak{p}_j}^{\chi,E_k}(\varphi_k(z_j)-Q_k)\right)\\ -2\sum_{i,j}\alpha_{ij}^{\chi,E_{3-k}} g_{ij}^{E_{3-k}}(\varphi_{3-k}(z)) + 2\sum_{i,j}\alpha_{ij}^{\chi,E_k} g_{ij}^{E_k}(\varphi_k(z)) + 2[K\colon\mathbb{Q}]h_p^{\chi,E_k}(Q_k),\end{aligned}$$

takes values in $T^{\chi,k}$ *when restricted to* $C^{(k)}(K)$.

Proof. Let v be any prime of K and $\ell \in \{1,2\}$. By [16, Lemma 7.4], the local height λ_v^{χ,E_ℓ} satisfies the quasi-parallelogram law, i.e. for all points $P, R \in E_\ell(K_v)$ such that $P, R, P \pm R \neq O_{E_\ell}$, we have

$$\lambda_v^{\chi,E_\ell}(P+R) + \lambda_v^{\chi,E_\ell}(P-R) = 2\lambda_v^{\chi,E_\ell}(P) + 2\lambda_v^{\chi,E_\ell}(R) - 2\frac{\chi_v}{n_v}(x(R)-x(P)). \quad (6.20)$$

This, together with (6.19), implies that $\rho^{\chi,k}(C^{(k)}(K))$ is contained in

$$T^{\chi,k} := \left\{\sum_{\mathfrak{q}\nmid p} n_{\mathfrak{q}}\left(\lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z_{\mathfrak{q}})+Q_k) + \lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z_{\mathfrak{q}})-Q_k) - 2\lambda_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z_{\mathfrak{q}}))\right) : (z_{\mathfrak{q}}) \in \prod_{\mathfrak{q}\nmid p} C(K_{\mathfrak{q}}) \setminus \{\varphi_k^{-1}(\pm Q_k)\}\right\}.$$

The elementary proof of finiteness of $T^{k,\chi}$ given in Proposition 4.6.5 when $K = \mathbb{Q}$ and χ is the cyclotomic character uses properties of the local heights away from p that hold also in this more general setting. Any detail that is omitted here can thus be deduced from there. Let $\mathfrak{q} \nmid p$ and define

$$W_{\mathfrak{q}}^{\chi,E_\ell} = \{n_{\mathfrak{q}}\lambda_{\mathfrak{q}}^{\chi,E_\ell}(P) : P \in E_\ell(K_{\mathfrak{q}}), x(P) \in \mathcal{O}_{\mathfrak{q}}\}.$$

As in the proof of Theorem 6.4.2, $W_{\mathfrak{q}}^{\chi,E_\ell}$ is finite and identically zero for almost all $\mathfrak{q}$. On the other hand, if $P \in E_\ell(K_{\mathfrak{q}})$ with $x(P) \notin \mathcal{O}_{\mathfrak{q}}$, then

$$\lambda_{\mathfrak{q}}^{\chi,E_\ell}(P) = \frac{\chi_{\mathfrak{q}}}{n_{\mathfrak{q}}}(x(P)) \tag{6.21}$$

(cf. (6.8)). Let $z \in C(K_{\mathfrak{q}}) \setminus \{\varphi_k^{-1}(\pm Q_k)\}$ and define

$$w_{\mathfrak{q}}^{\chi,E_k}(z) = n_{\mathfrak{q}} \left(\lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z) + Q_k) + \lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z) - Q_k) - 2\lambda_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)) \right).$$

If $\varphi_k(z) = O_{E_k}$, then $w_{\mathfrak{q}}^{\chi,E_k}(z) = 2n_{\mathfrak{q}}(\lambda_{\mathfrak{q}}^{\chi,E_k}(Q_k) - \lambda_{\mathfrak{q}}^{\chi,E_{3-k}}(Q_{3-k}))$; otherwise, by (6.20), we have

$$\begin{aligned} w_{\mathfrak{q}}^{\chi,E_k}(z) &= 2n_{\mathfrak{q}} \left(\lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z)) + \lambda_{\mathfrak{q}}^{\chi,E_k}(Q_k) - \frac{\chi_{\mathfrak{q}}}{n_{\mathfrak{q}}}(x(\varphi_k(z))) - \lambda_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)) \right) \\ &= 2n_{\mathfrak{q}} \left(\lambda_{\mathfrak{q}}^{\chi,E_k}(\varphi_k(z)) + \lambda_{\mathfrak{q}}^{\chi,E_k}(Q_k) + \frac{\chi_{\mathfrak{q}}}{n_{\mathfrak{q}}}(x(\varphi_{3-k}(z))) - \frac{\chi_{\mathfrak{q}}}{n_{\mathfrak{q}}}(a_0) - \lambda_{\mathfrak{q}}^{\chi,E_{3-k}}(\varphi_{3-k}(z)) \right). \end{aligned}$$

The assumption that $\mathrm{ord}_{\mathfrak{q}}(a_0) \leq 1$ implies that if $\mathrm{ord}_{\mathfrak{q}}(x(z)) \neq 0$, then exactly one of $x(\varphi_1(z))$ and $x(\varphi_2(z))$ is non-integral. Thus, by (6.21) and finiteness of $W_{\mathfrak{q}}^{\chi,E_\ell}$, we deduce that $w_{\mathfrak{q}}^{\chi,E_k}(z)$ takes values in a finite set $T_{\mathfrak{q}}^{\chi,k}$. Furthermore, since Q_ℓ is an integral point and a_0 divides the discriminant of E_2, $T_{\mathfrak{q}}^{\chi,k} \subseteq \{0\}$ for all primes $\mathfrak{q}$ that divide neither the discriminant of E_1 nor the one of E_2. □

Assuming Leopoldt's conjecture, we have $r_2 + 1$ choices of independent characters χ and then Theorem 6.5.2 gives at most $r_2 + 1$ independent locally analytic functions on $C^{(k)}(K \otimes \mathbb{Q}_p)$ vanishing on the global points $C^{(k)}(K)$. As in Section 6.4, we construct other r_K functions using the relations among the functionals f_i^J imposed by our assumption (6.18). In practice, each such relation can be reduced to a relation among the $f_i^{E_k}$ for some k.

Remark 6.5.3. As soon as $m > 1$, $C^{(1)}(K \otimes \mathbb{Q}_p) \cup C^{(2)}(K \otimes \mathbb{Q}_p) \subsetneq C(K \otimes \mathbb{Q}_p)$. Thus, in order to turn the method outlined in this section into a strategy to compute $C(K)$, one also needs to deal with the residue disks that are not covered by Theorem 6.5.2. If, for instance, there are no K-rational points in these disks, then we can use the Mordell–Weil sieve to prove this. Indeed, one obtains congruence conditions on the image on the Jacobian of a putative rational point in these disks. The Mordell–Weil sieve can be used to show that no rational point satisfying these conditions can exist. See also the following remark for a class of examples where we can immediately prove that there exist no K-rational points in such disks.

Remark 6.5.4. A quadratic Chabauty computation over number fields can sometimes be replaced with several quadratic Chabauty computations over $\mathbb{Q}$. For example, suppose that C is defined over $\mathbb{Q}$ and that we want to determine $C(K)$, where $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Q}$. Assume that $\mathrm{rank}(E_1(\mathbb{Q})) = \mathrm{rank}(E_2(\mathbb{Q})) = 1$, $\mathrm{rank}(E_1(K)) = 2$ and $E_2(K) = E_2(\mathbb{Q})$. If $P \in C(K)$, then $\varphi_2(P) \in E_2(K) = E_2(\mathbb{Q})$ and so $x(P)^2 \in \mathbb{Q}$, $y(P)/x(P) \in \mathbb{Q}$. It follows that computing $C(K)$ is equivalent to computing $C(\mathbb{Q})$ and $C'(\mathbb{Q})$ where

$$C' \colon y^2 = x^6 + \frac{a_4}{d}x^4 + \frac{a_2}{d^2}x^2 + \frac{a_0}{d^3}.$$

The curve C' is a genus 2 bielliptic curve whose corresponding elliptic curves are the quadratic twists $E_1^{d^{-1}} \cong_{\mathbb{Q}} E_1$ and $E_2^{d^{-2}} \cong_{\mathbb{Q}} E_2$. In particular, $\mathrm{rank}(E_1^{d^{-1}}(\mathbb{Q})) = 1$ and $\mathrm{rank}(E_2^{d^{-2}}(\mathbb{Q})) = 1$. Quadratic Chabauty can thus be used to determine both $C(\mathbb{Q})$ and $C'(\mathbb{Q})$.

We also note that, even when p is split in K, in this example we have $\psi(C(K)) = C^{(1)}(K) \cup C^{(2)}(K)$. Indeed, $C(K \otimes \mathbb{Q}_p) \setminus (C^{(1)}(K \otimes \mathbb{Q}_p) \cup C^{(2)}(K \otimes \mathbb{Q}_p))$ consists of those points $(z_1, z_2) \in C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ such that $\overline{z_i} \in \{\overline{(0, \pm\sqrt{a_0})}\}$, $z_j \in \{\overline{\infty^{\pm}}\}$ if $\{i, j\} = \{1, 2\}$, where $\sqrt{a_0}$ is a fixed square root of a_0 in $\mathbb{Q}_p$. Suppose that $(z_1, z_2) = \psi(z)$ for some $z \in C(K)$. Then $x(z_1)^2 = x(z_2)^2$ since $\varphi_2(z) \in E_2(\mathbb{Q})$. In particular, $\mathrm{ord}_p(x(z_1)) = \mathrm{ord}_p(x(z_2))$: a contradiction.

6.6 Algorithms and examples for integral points

Keep the notation of Section 6.4. Because of current limitations of our implementation, we restrict to the case where p is totally split in K, so that the Coleman integration really takes place over $\mathbb{Q}_p$.

Let E be an elliptic curve over K. Suppose we are given independent $\chi_1, \ldots, \chi_{r_2+1} \in V_K$. By Example 6.2.8, they correspond to tuples $c^{(k)} = (c_1^{(k)}, \ldots, c_d^{(k)})$ of p-adic numbers, respectively, such that $\lambda_{\mathfrak{p}_j}^{\chi_k}(Q) = c_j^{(k)} \tau_j^{(\beta_j)}(\psi_j(Q))$ for all $1 \leq j \leq d$ and $Q \in \mathcal{X}(\mathcal{O}_K)$. Writing

$$h_p^{\chi_k} = [K \colon \mathbb{Q}]^{-1} \sum_{0 \leq i \leq j \leq r-1} \alpha_{ij}^{(k)} g_{ij},$$

we get

$$\rho_k(z) := \rho^{\chi_k}(z) = \sum_{j=1}^{d} c_j^{(k)} \tau_j^{(\beta_j)}(z_j) - \sum_{i,j} \alpha_{ij}^{(k)} g_{ij}(z) \tag{6.22}$$

for $z \in \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$. We shall now fix choices of β_j following the conventions of §4.2.1 and henceforth remove β_j from the notation. Algorithms for the case $K = \mathbb{Q}$

are discussed in Chapter 4; most of them readily generalise to more general number fields K, since we assume that all K_j are isomorphic to $\mathbb{Q}_p$ and that the $c^{(k)}$ are given explicitly.

We give some examples for Section 6.4 when K is a quadratic field and p is a prime number such that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ is split. In this case, we want to find (at least) two functions ρ_1, ρ_2 which map

$$(\psi_1(\mathcal{X}(\mathcal{O}_K)), \psi_2(\mathcal{X}(\mathcal{O}_K))) \subset \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) = \psi_1(\mathcal{X})(\mathbb{Z}_p) \times \psi_2(\mathcal{X})(\mathbb{Z}_p)$$

into an explicitly computable finite set $T^{(1)}$ ($T^{(2)}$, respectively) and have a finite common solution set B. In order to compute B, we find the local expansion of ρ_1 and ρ_2 in each pair of residue disks in $(\overline{\psi_1(E)}(\mathbb{F}_p) \setminus \{\overline{O}\}) \times (\overline{\psi_2(E)}(\mathbb{F}_p) \setminus \{\overline{O}\})$ and use the strategy outlined in Appendix 6.A. Once we have approximated B, we have to check for each solution (z_1, z_2) whether it actually comes from a K-rational point, that is, if $z_1 = \psi_1(Q)$ and $z_2 = \psi_2(Q)$ for some $Q \in \mathcal{X}(\mathcal{O}_K)$. We can use, for instance, that if this is the case, then we must have $x(z_1)x(z_2) \in \mathbb{Q}$ and $x(z_1) + x(z_2) \in \mathbb{Q}$.

The linear functionals f_i in $(E(K) \otimes \mathbb{Q}_p)^*$ are given by

$$f_i(Q) = \int_O^{\psi_{i+1}(Q)} \psi_{i+1}(\omega_0) \quad \text{for } i = 0, 1.$$

By abuse of notation, g_{ij} denotes both the function $g_{ij} \colon E(K \otimes \mathbb{Q}_p) \to \mathbb{Q}_p$,

$$g_{ij}(z) = \left(\int_O^{z_{i+1}} \psi_{i+1}(\omega_0)\right)\left(\int_O^{z_{j+1}} \psi_{j+1}(\omega_0)\right),$$

and its restriction to $E(K) \otimes \mathbb{Q}_p$, which equals $f_i f_j$.

6.6.1 Elliptic curves over real quadratic fields

Suppose that K is a real quadratic field[2]. Let E denote an elliptic curve defined over K such that E has good reduction at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

Equation (6.13) is satisfied if and only if $r = \mathrm{rank}(E(K)) = 0$ or 1; we assume that $r = 1$ – although the case $r = 0$ might be of some interest in terms of generalisations of Kim's conjecture (Conjecture 4.1.1) to this setting. It follows that there is a linear dependency $f_0 = bf_1$ between the functionals f_0 and f_1 on $E(K) \otimes \mathbb{Q}_p$. The first function ρ_1 is constructed using the cyclotomic p-adic height h_p^{cyc}. We have

$$\rho_1(z) := \rho^{\mathrm{cyc}}(z) = \tau_1(z_1) + \tau_2(z_2) - \alpha g_{00}(z)$$

[2]The algorithm described in this subsection works also when K is imaginary; however, while in the real case the rank assumption here is optimal, in the imaginary case we can work with curves of larger rank, as is explained in §6.6.2.

for $z \in \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$, where

$$2h_p^{\mathrm{cyc}} = \alpha g_{00} = \alpha f_0^2$$

on $E(K) \otimes \mathbb{Q}_p$. We can compute α by comparing $h_p^{\mathrm{cyc}}(Q)$ and $f_0^2(Q)$ for some non-torsion point $Q \in E(K)$. Letting $T := T^{(1)}$ denote the finite set of values that $-\sum_{\mathfrak{q}\nmid p} n_{\mathfrak{q}}\lambda_{\mathfrak{q}}(z_{\mathfrak{q}})$ can take for $(z_{\mathfrak{q}}) \in \prod_{\mathfrak{q}\nmid p}\mathcal{X}(\mathcal{O}_{\mathfrak{q}})$, we then must have

$$\rho_1(\psi_1(Q), \psi_2(Q)) \in T$$

for all $Q \in \mathcal{X}(\mathcal{O}_K)$.

The second function comes from the dependency between f_0 and f_1 on $E(K)$ and is given by

$$\rho_2(z) = \int_O^{z_1} \psi_1(\omega_0) - b\int_O^{z_2} \psi_2(\omega_0);$$

we have $\rho_2(\psi_1(Q), \psi_2(Q)) = 0$ for all $Q \in E(K)$. We can use any non-torsion $Q \in E(K)$ and compare $f_0(Q)$ to $f_1(Q)$ to find b.

Note that, if E is defined over $\mathbb{Q}$ and $w \in T$, we can always reduce the system

$$\begin{cases} \rho_1(z_1, z_2) = w \\ \rho_2(z_1, z_2) = 0 \end{cases}$$

to one equation in one variable. Indeed, first observe that

- if $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}(E(K)) = 1$, then for every $Q \in E(K)$ there exists n such that $nQ \in E(\mathbb{Q})$. Thus, by linearity, $f_0(Q) = f_1(Q)$;
- if $\mathrm{rank}(E(\mathbb{Q})) = 0$, then for every $Q \in E(K)$ we have $Q+Q^c \in E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}}$, where Q^c is the Galois conjugate of Q. Thus, since $\psi_2(Q) = \psi_1(Q^c)$, we deduce that $f_0(Q) + f_1(Q) = f_0(Q + Q^c) = 0$.

Furthermore,

$$\int_O^{R_1} \omega_0 = \int_O^{R_2} \omega_0 \iff R_1 - R_2 \in E(\mathbb{Q}_p)_{\mathrm{tors}}.$$

Suppose that $\mathrm{rank}(E(\mathbb{Q})) = 1$ and we want to find all $Q \in \mathcal{X}(\mathcal{O}_K)$ such that $(\overline{\psi_1(Q)}, \overline{\psi_2(Q)}) = (\overline{P_1}, \overline{P_2}) \in \overline{E}(\mathbb{F}_p) \times \overline{E}(\mathbb{F}_p)$. If there are no torsion points in $E(\mathbb{Q}_p)$ reducing to $\overline{P_1} - \overline{P_2}$, then the above shows that no such Q exists. Otherwise, we solve

$$\rho_1((x(s), y(s)), (x(s), y(s)) + R) = w$$

where $(x(s), y(s))$ is a parametrisation for the points in $E(\mathbb{Q}_p)$ reducing to $\overline{P_1}$ and R is the unique torsion point in $E(\mathbb{Q}_p)$ such that $\overline{P_2} - \overline{P_1} = \overline{R}$ (cf. Remark 6.6.1 and Example 6.6.3). The case $\mathrm{rank}(E(\mathbb{Q})) = 0$ is very similar.

Remark 6.6.1. Let E be defined over $\mathbb{Q}$. Since p is assumed odd, the group $E_1(\mathbb{Q}_p)$ of $\mathbb{Q}_p$-points on the formal group at p is torsion-free (cf. [127, IV, Proposition 3.2(b) and Theorem 6.1]). Therefore, $E(\mathbb{Q}_p)_{\text{tors}}$ can be realised as a subgroup of $\overline{E}(\mathbb{F}_p)$. Hence, if $\overline{P} \in \overline{E}(\mathbb{F}_p)$ then there is at most one point $R \in E(\mathbb{Q}_p)_{\text{tors}}$ such that $\overline{R} = \overline{P}$.

For an example in which $E(\mathbb{Q}_p)_{\text{tors}}$ is a proper subgroup of $\overline{E}(\mathbb{F}_p)$, consider the elliptic curve 38.b1 [90]

$$E\colon y^2 + xy + y = x^3 + x^2 - 70x - 279,$$

for which $\#\overline{E}(\mathbb{F}_5) = 10$, but $\#E(\mathbb{Q}_5)_{\text{tors}} = 2$.

If $p \nmid \overline{E}(\mathbb{F}_p)$, however, one always has $E(\mathbb{Q}_p)_{\text{tors}} \cong \overline{E}(\mathbb{F}_p)$. Indeed, let $\overline{P} \in \overline{E}(\mathbb{F}_p)$ of order n. We need to show that there exists $R \in E(\mathbb{Q}_p)_{\text{tors}}$ such that $\overline{R} = \overline{P}$. If $\overline{P} = \overline{O}$, this is trivial. Otherwise, let $P \in E(\mathbb{Q}_p)$ be any lift of $\overline{P}$. Then $P \notin E_1(\mathbb{Q}_p)$ but $nP \in E_1(\mathbb{Q}_p) \cong \mathbb{Z}_p$. Since n is coprime to p by assumption, n is invertible in $\mathbb{Z}_p$ and thus there exists $Q \in E_1(\mathbb{Q}_p)$ such that $nQ = nP$. Then $R = P - Q$ satisfies the requirements.

Example 6.6.2. Consider the elliptic curve 199.1-c1 [90] over $K = \mathbb{Q}(a)$, where a is a root of $x^2 - x - 1$. It admits the global minimal model

$$E\colon y^2 + y = x^3 + (a+1)x^2 + ax.$$

The prime $p = 11$ is the smallest prime splitting in K. The curve has everywhere good reduction, except at $(-3a+16)$, where it has Kodaira symbol I_1: thus, $T = \{0\}$. The common zero set of ρ_1 and ρ_2 contains the integral points

$$\pm(-1,0), \pm(0,0), \pm(a,2a), \pm(-2a+3, 4a-7), \pm(a+1, 3a+1), \pm(-a,0),$$
$$\pm(42a+27, -420a-259), \pm(-6a+8, -18a+29), \pm(-a+1, a-2)$$

and 138 other pairs of points in $\psi_1(E)(\mathbb{Q}_p) \times \psi_2(E)(\mathbb{Q}_p)$, where $\psi_i(E)/\mathbb{Q}_p$ is the curve obtained from the Weierstrass equation for E via the embedding $\psi_i\colon K \hookrightarrow \mathbb{Q}_p$.

Example 6.6.3. Consider the elliptic curve with LMFDB label 192.a3 [90]

$$E\colon y^2 = x^3 - x^2 - 4x - 2$$

and let $K = \mathbb{Q}(\sqrt{3})$. We have that $\operatorname{rank}(E(K)) = \operatorname{rank}(E(\mathbb{Q})) = 1$ and that $p = 13$ is of good ordinary reduction for E and is split in K. As explained above, in this setting we can reduce our computations to finding solutions to power series equations in one

variable. Note in particular that $\#\overline{E}(\mathbb{F}_p) = 12$, so by Remark 6.6.1 each residue disk contains precisely one torsion point of $E(\mathbb{Q}_p)$.

The only inputs in this computation which come from our specific choice of quadratic field K are the reduction type of E at the bad primes (and consequently the set T) and the choice of prime p, since we require that two primes lie above it.

For this reason, it is not surprising that, besides recovering the integral points

$$\pm(3,2), (-1,0), (1 \pm \sqrt{3}, 0), \pm(25 \pm 15\sqrt{3}, 180 \pm 104\sqrt{3}),$$

we also recognise in our zero set the points

$$\pm\left(\frac{-1 \pm \sqrt{-3}}{2}, \frac{-3 \pm \sqrt{-3}}{2}\right), \pm(-1 \pm i, 2),$$

all of which belong to the 2-saturation of $E(\mathbb{Q})$.

6.6.2 Elliptic curves over imaginary quadratic fields

Let K be an imaginary quadratic number field and let E be an elliptic curve defined over K with $r = \mathrm{rank}(E(K)) = 2$, such that E has good reduction at both $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Suppose that f_0 and f_1 are linearly independent. Note that:

Lemma 6.6.4. *Suppose that E as above can be defined over $\mathbb{Q}$. Then f_0 and f_1 are linearly independent if and only* $\mathrm{rank}(E(\mathbb{Q})) = 1$.

Proof. If $\mathrm{rank}(E(\mathbb{Q})) = r$ (resp. $\mathrm{rank}(E(\mathbb{Q})) = 0$), then $f_0 = f_1$ (resp. $f_0 = -f_1$) on $E(K)$ (cf. also the discussion before Remark 6.6.1). Conversely, suppose that $\mathrm{rank}(E(\mathbb{Q})) = 1$ and that f_0 and f_1 are linearly dependent on $E(K) \otimes \mathbb{Q}_p$. Since neither of f_0 and f_1 is identically zero on $E(K)$ (as $E(K)$ contains points of infinite order), then there exists $\alpha \in \mathbb{Q}_p$ such that $f_0 = \alpha f_1$. Let $P \in E(\mathbb{Q})$ of infinite order. Then $f_0(P) = f_1(P)$ and hence $\alpha = 1$. Thus, for all $Q \in E(K)$, we have $\int_O^{\psi_1(Q)} \omega_0 = \int_O^{\psi_2(Q)} \omega_0$, so that $\psi_1(Q - Q^c) \in E(\mathbb{Q}_p)_{\mathrm{tors}}$, where Q^c is the Galois conjugate of Q. Let $R \in E(K)_{\mathrm{tors}}$ such that $Q = Q^c + R$ and let n be the additive order of R. Then $nQ = nQ^c$, i.e. $nQ \in E(\mathbb{Q})$ for all $Q \in E(K)$, contradicting $\mathrm{rank}(E(K)) > \mathrm{rank}(E(\mathbb{Q}))$. □

Under our assumption, the quadratic forms g_{ij} $(0 \leq i \leq j \leq 1)$ generate $\mathcal{B}$, the space of $\mathbb{Q}_p$-valued quadratic forms on $E(K) \otimes \mathbb{Q}_p$. Hence the p-adic heights h_p^{cyc} and h_p^{anti} can be expressed as linear combinations $h_p^{\mathrm{cyc}} = \frac{1}{2}\sum \alpha_{ij}^{\mathrm{cyc}} g_{ij}$ and $h_p^{\mathrm{anti}} = \frac{1}{2}\sum \alpha_{ij}^{\mathrm{anti}} g_{ij}$. Using independent non-torsion points $P, Q \in E(K)$, we can find all $\alpha_{ij}^{\mathrm{cyc}}$ (resp. $\alpha_{ij}^{\mathrm{anti}}$) by computing $f_0(P), f_1(P), f_0(Q), f_1(Q)$ and $h_p^{\mathrm{cyc}}(P), h_p^{\mathrm{cyc}}(Q), h_p^{\mathrm{cyc}}(P+Q)$ (resp. $h_p^{\mathrm{anti}}(P), h_p^{\mathrm{anti}}(Q), h_p^{\mathrm{anti}}(P+Q)$).

When E is defined over $\mathbb{Q}$, we have $\alpha_{00}^{\mathrm{cyc}} = \alpha_{11}^{\mathrm{cyc}}$ and $\alpha_{01}^{\mathrm{anti}} = 0$, $\alpha_{00}^{\mathrm{anti}} = -\alpha_{11}^{\mathrm{anti}}$. Indeed, since by definition the cyclotomic height of any $R \in E(K)$ equals the cyclotomic height of its Galois conjugate, we have

$$(\alpha_{00}^{\mathrm{cyc}} - \alpha_{11}^{\mathrm{cyc}})(f_0(R)^2 - f_1(R)^2) = 0;$$

the first claim then follows since the g_{ij} are a basis for $\mathcal{B}$. Similarly, the anticyclotomic height changes of sign if we first act by Galois, proving the second claim.

Let T^{cyc} (resp. T^{anti}) denote the set of possible values of $-\sum_{\mathfrak{q}\nmid p} n_{\mathfrak{q}}\lambda_{\mathfrak{q}}^{\mathrm{cyc}}(z_{\mathfrak{q}})$ (resp. $-\sum_{\mathfrak{q}\nmid p} n_{\mathfrak{q}}\lambda_{\mathfrak{q}}^{\mathrm{anti}}(z_{\mathfrak{q}})$) for $(z_{\mathfrak{q}}) \in \prod_{\mathfrak{q}\nmid p} \mathcal{X}(\mathcal{O}_{\mathfrak{q}})$.

Then every point in $\mathcal{X}(\mathcal{O}_K)$ must satisfy

$$\rho^{\mathrm{cyc}}(\psi_1(Q), \psi_2(Q)) \in T^{\mathrm{cyc}} \quad \text{and} \quad \rho^{\mathrm{anti}}(\psi_1(Q), \psi_2(Q)) \in T^{\mathrm{anti}},$$

where

$$\rho^{\mathrm{cyc}}(z) = \tau_1(z_1) + \tau_2(z_2) - \alpha_{00}^{\mathrm{cyc}}\left(\int_O^{z_1}\omega_0\right)^2 - \alpha_{01}^{\mathrm{cyc}}\int_O^{z_1}\omega_0\int_O^{z_2}\omega_0 - \alpha_{11}^{\mathrm{cyc}}\left(\int_O^{z_2}\omega_0\right)^2$$
$$\rho^{\mathrm{anti}}(z) = \tau_1(z_1) - \tau_2(z_2) - \alpha_{00}^{\mathrm{anti}}\left(\int_O^{z_1}\omega_0\right)^2 - \alpha_{01}^{\mathrm{anti}}\int_O^{z_1}\omega_0\int_O^{z_2}\omega_0 - \alpha_{11}^{\mathrm{anti}}\left(\int_O^{z_2}\omega_0\right)^2$$

(by abuse of notation, we wrote ω_0 for $\psi_i(\omega_0)$ with i clarified by the context).

We do not present an example of such a computation, as the ideas outlined here are implicitly used in the bielliptic example over imaginary quadratic fields of the next section.

6.7 Examples for rational points

In this section we present examples for Section 6.5, of which we retain the notation, when K is a quadratic field and C is defined over $\mathbb{Q}$. As for integral points on elliptic curves, it is again convenient to distinguish between the imaginary and real case. We let p be an odd prime which splits in K and such that C has good reduction at each prime above p. For simplicity we assume that a_0 is a square in K.

6.7.1 Rank 4 over imaginary quadratic fields

Let $C/\mathbb{Q}$ be as above and let K be an imaginary quadratic field. If $\mathrm{rank}(E_k(\mathbb{Q})) = 1$ and $\mathrm{rank}(E_k(K)) = 2$ for each k, then (6.18) and Assumption 6.5.1 are both satisfied in view of Lemma 6.6.4. Theorem 6.5.2 with $\chi = \chi^{\mathrm{cyc}}$ and $\chi = \chi^{\mathrm{anti}}$ provides us, for each $k \in \{1, 2\}$, with two locally analytic functions $\rho^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}$ on $C^{(k)}(K \otimes \mathbb{Q}_p)$

and finite sets $T^{\mathrm{cyc},k}$ and $T^{\mathrm{anti},k}$. Varying k and looking at the intersection B^k of the loci $\rho^{\mathrm{cyc},k}(z) \in T^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}(z) \in T^{\mathrm{anti},k}$, we obtain a set of points containing all the points in $(\psi_1(C(K)), \psi_2(C(K)))$ that do not map to $(\overline{\infty^{\pm}}, \overline{(0, \pm\sqrt{a_0})})$ or to $(\overline{(0, \pm\sqrt{a_0})}, \overline{\infty^{\pm}})$ under reduction to $\overline{C}(\mathbb{F}_p) \times \overline{C}(\mathbb{F}_p)$.

As already mentioned, the algorithm of §6.6.2 is used in the computation of the constants of Theorem 6.5.2. To p-adically approximate the set B^k, we need to compute roots of systems of two equations in two variables. We do so using Algorithm 6.A.2, Lemma 6.A.4 and the discussion in Appendix 6.A. Note that $\rho^{\mathrm{cyc},k}$ and $\rho^{\mathrm{anti},k}$ are both invariant under the automorphism $\theta\colon (x, y) \mapsto (\pm x, \pm y)$ of C. Thus, from the points in B^k reducing to $(\overline{P}, \overline{Q}) \in \overline{C}(\mathbb{F}_p) \times \overline{C}(\mathbb{F}_p)$ we can deduce the points in B^k reducing to $(\theta(\overline{P}), \theta(\overline{Q}))$. This cuts down the number of pairs of residue disks that we need to consider.

Example 6.7.1. Consider the modular curve

$$C = X_0(91)^+\colon y^2 = x^6 - 3x^4 + 19x^2 - 1.$$

The associated elliptic curves E_1 ([90, 91.a1]) and E_2 ([90, 91.b2]) each have rank 1 over $\mathbb{Q}$ and applying the algorithm of Section 4.6 with $p = 5$ recovers the rational points

$$\{\infty^{\pm}, (\pm 1, \pm 4), (\pm 1/3, \pm 28/27)\} \tag{6.23}$$

and the following two p-adic points up to automorphisms:

$$(5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 + O(5^6), 3 + 3 \cdot 5 + 5^2 + 5^3 + 4 \cdot 5^4 + O(5^6))$$
$$(1 + 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 2 \cdot 5^5 + O(5^6), 4 + 4 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 + 5^4 + 5^5 + O(5^6)).$$

We now carry out quadratic Chabauty for p and $K = \mathbb{Q}(i)$, over which the elliptic curves E_1 and E_2 attain rank 2. Denote by $T^{\mathrm{cyc},k}$ and $T^{\mathrm{anti},k}$ the explicitly computable finite sets of Theorem 6.5.2 for $\chi = \chi^{\mathrm{cyc}}$ and $\chi = \chi^{\mathrm{anti}}$, respectively.

Claim 6.1. $T^{\mathrm{cyc},1} = T^{\mathrm{cyc},2} = T^{\mathrm{anti},1} = T^{\mathrm{anti},2} = \{0\}$.

Proof. $X_0(91)^+$ has bad but potentially good reduction at 2, and bad reduction at 7 and 13. Furthermore, E_1 and E_2 are minimal at the primes of $\mathbb{Q}(i)$ above 7 and 13 and the reduction type at all these primes is I_1. □

Besides the $\mathbb{Q}$-rational points listed above, in $B^1 \cup B^2$ we also recover the following points defined over $\mathbb{Q}(i)$:

$$(0, \pm i), (\pm(-2i + 1), \pm(-8i + 12)), (\pm(2i + 1), \pm(8i + 12)), \tag{6.24}$$

as well as 20 other p-adic points up to automorphisms $(x, y) \mapsto (\pm x, \pm y)$. We apply the Mordell–Weil sieve to show that these p-adic points do not correspond to $\mathbb{Q}(i)$-rational points and that there are no $\mathbb{Q}(i)$-rational points mapping to the pairs of residue disks

$$(\overline{\infty^{\pm}}, \overline{(0, \pm\sqrt{-1})}), (\overline{(0, \pm\sqrt{-1})}, \overline{\infty^{\pm}}).$$

This proves that all rational points on $X_0(91)^+$ are either listed in (6.23) or in (6.24).

A technical remark (with reference to Appendix 6.A): there are four pairs of residue disks in $\overline{C}(\mathbb{F}_p) \times \overline{C}(\mathbb{F}_p)$, up to automorphism, such that a root in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ of the corresponding system of equations is also a root modulo p of the determinant of the Jacobian matrix. Of these, two correspond to the global points $(0, i)$ and ∞ (and thus the determinant of the Jacobian matrix has a zero at those points by Remark 6.A.3), another one lifts to no root in $\mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$ for sufficiently large n and for the remaining one we can apply the multivariate Hensel's lemma after lifting the root modulo some small power of p (cf. Algorithm 6.A.2). Furthermore, the strategy outlined after Remark 6.A.3 also shows that there are no other points in the residue disks of $(0, i)$ and ∞. Therefore, we conclude that the approximations that we have computed are in one-to-one correspondence with the elements in $B^1 \cup B^2$ (up to automorphism). Amongst the 20 extra points, we recognise the pair of rational points $z = ((1, 4), (-1, 4))$. Indeed, z_1 and z_2 both map to $(1, 4)$ in $E_1(\mathbb{Q})$ and map to the torsion points $(-1, -4)$ and $(-1, 4)$ in $E_2(\mathbb{Q})$. Thus $g_{ij}^{E_2}(\varphi_2(z)) = 0$. The claim then follows since the local heights are invariant under pre-multiplication by -1.

Finally, note that, since $T^{\mathrm{anti},k} = \{0\}$, in this case $B^1 \cup B^2$ is closed under $(z_1, z_2) \mapsto (z_2, z_1)$. Quotienting by this symmetry, the 20 extra pairs of points become 14.

6.7.2 Rank 3 over real quadratic fields

Keep the notation of the beginning of Section 6.7 and let K now be a real quadratic field[3]. Then (6.18) forces $\mathrm{rank}(J(K)) \leq 3$. Since we need Assumption 6.5.1 to also hold, we suppose here that $\mathrm{rank}(E_1(K)) = 2$, $\mathrm{rank}(E_1(\mathbb{Q})) = 1$ and $\mathrm{rank}(E_2(K)) = 1$. This is sufficient by Lemma 6.6.4 and by the non-degeneracy of the p-adic logarithm on an elliptic curve.

For a fixed $k \in \{1, 2\}$, Theorem 6.5.2 determines only one function ρ_1^k and one finite set T^k in this case; the second function ρ_2 that we need comes from the dependency of $f_0^{E_2}$ and $f_1^{E_2}$ (see also §6.6.1). Let

$$B^k = \{z \in C^{(k)}(K \otimes \mathbb{Q}_p) : \rho_1^k(z) \in T^k, \rho_2(z) = 0\}.$$

[3]The strategy also works if K is imaginary. See also footnote 2 in §6.6.1.

Note that it suffices to run through $\overline{C}(\mathbb{F}_p) \times \overline{C}(\mathbb{F}_p)/\sim$ where $(P,Q) \sim (R,T)$ if and only if $P = T$ and $Q = R$, as our equations are symmetric with respect to the two embeddings of K into $\mathbb{Q}_p$ (cf. the discussion of §6.6.2). As before, we can also use the invariance of our zero sets under the hyperelliptic and bielliptic automorphisms of C to reduce even further the number of pairs of disks that we need to consider.

In view of Remark 6.5.4, the resulting algorithm is often an alternative to a series of quadratic Chabauty computations over the rationals. This is in particular the case in the following example.

Example 6.7.2. Consider

$$C\colon y^2 = x^6 + x^2 + 1.$$

We provided in Example 4.6.3 an alternative proof of Wetherell's result [145] that

$$C(\mathbb{Q}) = \{\infty^{\pm}, (0, \pm 1), (\pm 1/2, \pm 9/8)\}.$$

Let $K = \mathbb{Q}(\sqrt{34})$. We have $\operatorname{rank}(E_1(\mathbb{Q})) = 1$, $\operatorname{rank}(E_1(K)) = 2$ and $\operatorname{rank}(E_2(\mathbb{Q})) = \operatorname{rank}(E_2(K)) = 1$. We now determine $C(K)$ exactly, by applying quadratic Chabauty over K with the split prime $p = 3$. We may choose

$$\rho_2(z) = \int_O^{\varphi_2(z_1)} \omega_0^{E_2} - \int_O^{\varphi_2(z_2)} \omega_0^{E_2},$$

where $O := O_{E_2}$. Denote by T^k the explicitly computable finite set of Theorem 6.5.2 for $\chi = \chi^{\mathrm{cyc}}$.

Claim 6.2. $T^1 = \left\{0, 2\log 2, \frac{5}{2}\log 2\right\}$, $T^2 = \left\{-2\log 2, -4\log 2, -\frac{9}{2}\log 2\right\}$.

Proof. The elliptic curves E_1 and E_2 have everywhere good reduction except at the primes above 2 and 31. Furthermore, the models

$$E_1\colon y^2 = x^3 + x + 1, \qquad E_2\colon y^2 = x^3 + x^2 + 1$$

are globally minimal also over K. The prime 31 is inert in K and E_1 and E_2 have reduction type I_1 with Tamagawa number 1 at $31\mathcal{O}_K$. Thus, the only non-trivial contributions to T^k can come from the unique prime $\mathfrak{q}$ of K above 2. The curve E_1 has Tamagawa number 1 (and Kodaira symbol I_0^*) at $\mathfrak{q}$, so $\lambda_{\mathfrak{q}}^{E_1}$ is identically zero on integral points. The curve E_2 has reduction type I_1^* with Tamagawa number 4 at $\mathfrak{q}$ and we have

$$\lambda_{\mathfrak{q}}^{E_2}(x,y) = \begin{cases} 0 & \text{if } |x|_{\mathfrak{q}} = 1, \\ -\frac{1}{2}\log 2 \text{ or } -\frac{5}{8}\log 2 & \text{if } |x|_{\mathfrak{q}} < 1 \end{cases}$$

by Proposition 4.2.3; as we saw in Example 4.6.3, $\lambda_{\mathfrak{q}}^{E_2}(Q_2) = -\frac{1}{2}\log 2$.

For $z \in C(K_{\mathfrak{q}})$, $\varphi_1(z) \neq \pm Q_1$ resp. $\varphi_2(z) \neq \pm Q_2$, let

$$w_{\mathfrak{q}}^{E_1}(z) = 2(\lambda_{\mathfrak{q}}^{E_1}(\varphi_1(z) + Q_1) + \lambda_{\mathfrak{q}}^{E_1}(\varphi_1(z) - Q_1) - 2\lambda_{\mathfrak{q}}^{E_2}(\varphi_2(z)))$$
$$w_{\mathfrak{q}}^{E_2}(z) = 2(\lambda_{\mathfrak{q}}^{E_2}(\varphi_2(z) + Q_2) + \lambda_{\mathfrak{q}}^{E_2}(\varphi_2(z) - Q_2) - 2\lambda_{\mathfrak{q}}^{E_1}(\varphi_1(z))).$$

Using the quasi-parallelogram law (2.3), we find

- If $|x(z)|_{\mathfrak{q}} \leq 1$, then $w_{\mathfrak{q}}^{E_1}(z) = 0$ and $w_{\mathfrak{q}}^{E_2}(z) = -2\log 2$.
- If $|x(z)|_{\mathfrak{q}} > 1$, then $w_{\mathfrak{q}}^{E_1}(z) \in \left\{2\log 2, \frac{5}{2}\log 2\right\}$ and $w_{\mathfrak{q}}^{E_2}(z) \in \left\{-4\log 2, -\frac{9}{2}\log 2\right\}$.

□

Since $E_2(K) = E_2(\mathbb{Q})$ (as $\mathrm{rank}(E_2(K)) = \mathrm{rank}(E_2(\mathbb{Q}))$ and $E_2(K)_{\mathrm{tors}} = \{O\}$), Remark 6.5.4 tells us that $C(K) \subset C^{(1)}(K \otimes \mathbb{Q}_p) \cup C^{(2)}(K \otimes \mathbb{Q}_p)$ and, in particular, $C(K) \subseteq B^1 \cup B^2$. We have

$$\overline{C}(\mathbb{F}_3) = \{\overline{\infty^{\pm}}, \overline{(0, \pm 1)}, \overline{(\pm 1, 0)}\}.$$

It follows from the observations at the beginning of §6.7.2 that it suffices to consider the points in $C^{(k)}(K \otimes \mathbb{Q}_p)$ reducing to one of the following pairs of residue disks in $\overline{C}(\mathbb{F}_3) \times \overline{C}(\mathbb{F}_3)$:

$$(\overline{\infty^+}, \overline{\infty^+}), (\overline{\infty^+}, \overline{\infty^-}), (\overline{\infty^+}, \overline{(1,0)}) \text{ with } k = 1,$$
$$(\overline{(0,1)}, \overline{(0,1)}), (\overline{(0,2)}, \overline{(0,1)}), (\overline{(0,2)}, \overline{(1,0)}), (\overline{(1,0)}, \overline{(1,0)}), (\overline{(1,0)}, \overline{(2,0)}) \text{ with } k = 2.$$

By Claim 6.2, the intersection of B^k with a residue pair (for k dependent on the pair and chosen as above) is given by the union of the zeros of three systems of two equations in two variables (by a similar argument to the one at the end of Remark 6.5.4, some pairs could be excluded a priori from containing points in $C(K)$ by valuation considerations, but we leave them all in the computation here). Using the algorithms of Appendix 6.A, we recover in $B^1 \cup B^2$ exactly the points in Table 6.1 (the residue pairs contained in $C^{(k)}(K \otimes \mathbb{Q}_p)$ that intersect B^k trivially are not listed).

Besides recovering representatives of the points in

$$C(\mathbb{Q}) \cup \left\{ \left(\frac{11}{204}\sqrt{34}, \pm\frac{44909}{249696}\sqrt{34} \right), \left(-\frac{11}{204}\sqrt{34}, \pm\frac{44909}{249696}\sqrt{34} \right) \right\}$$

up to automorphisms, our zero sets contain some points $z = (z_1, z_2) \in C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ which we do not recognise as points coming from $C(K)$. Using one of the following arguments, we can prove that each of these points is indeed not K-rational. Suppose that $z \in \psi(C(K))$. Then, since $E_2(K) = E_2(\mathbb{Q})$, the computed approximations of $\varphi_2(z_1)$ and $\varphi_2(z_2)$ must agree. If this holds, let $\varphi_2(z)$ be either of $\varphi_2(z_1)$ and $\varphi_2(z_2)$.

(O1) If $\varphi_2(z)$ is in the formal group at p, we showed in Example 4.6.3 that we must have $\mathrm{ord}_p(x(\varphi_2(z))) \leq -4$.

(O2) Else, since $E_2(\mathbb{Q})$ is generated by $Q_2 = (0,1)$, if $\varphi_2(z) = nQ_2$ for some $n \in \mathbb{Z}$, then

$$n \equiv n_1 := \frac{\int_O^{\varphi_2(z)} \omega_0^{E_2}}{\int_O^{Q_2} \omega_0^{E_2}} \bmod 3;$$

on the other hand, $\overline{Q_2} \in \overline{E_2}(\mathbb{F}_3)$ has order 6. Thus, if $\overline{\varphi_2(z)} = n_2\overline{Q_2}$, we also have

$$n \equiv n_2 \bmod 6.$$

If $n_1 \not\equiv n_2 \bmod 3$, then $z \notin \psi(C(K))$ (cf. also the discussion in Appendix 4.A).

The extra points in the residue pair $(\overline{(0,1)}, \overline{(0,1)})$ are precisely the extra points of the computation over $\mathbb{Q}$ (Example 4.6.3). Also note that the criterion (O1) could be deduced from (O2).

residue pair	k	recovered in B^k	if not in $C(K)$, why?
$(\overline{\infty^+}, \overline{\infty^+})$	1	∞^+ $\left(\frac{11}{204}\sqrt{34}, \frac{44909}{249696}\sqrt{34}\right)$ $\left(-\frac{11}{204}\sqrt{34}, -\frac{44909}{249696}\sqrt{34}\right)$	
$(\overline{(0,1)}, \overline{(0,1)})$	2	$(0,1)$ $x(z_1) = x(z_2) = \pm(2 \cdot 3 + 2 \cdot 3^3 + O(3^5))$	$\mathrm{ord}_p(x(\varphi_2(z))) = -2$
$(\overline{(0,2)}, \overline{(0,1)})$	2	$x(z_1) = \pm(2 \cdot 3 + 3^2 + 2 \cdot 3^3 + O(3^5)) = -x(z_2)$	$\mathrm{ord}_p(x(\varphi_2(z))) = -2$
$(\overline{(1,0)}, \overline{(1,0)})$	2	$\left(-\frac{1}{2}, \pm\frac{9}{8}\right)$	
$(\overline{(1,0)}, \overline{(2,0)})$	2	$x(z_1) = 1 + 3 + 3^3 + O(3^5) = -x(z_2)$, $y(z_1) = -y(z_2)$	(O2) with $n_1 = \pm 1$, $n_2 = 3$

Table 6.1: Computation of $B^1 \cup B^2$ for Example 6.7.2.

Appendix

6.A Roots of multivariate systems of p-adic equations

Some of the algorithms of Sections 6.6 and 6.7 require us to solve systems of two p-adic equations in two variables. In particular, in each pair of residue disks we reduce the problem to that of finding all $(t_1, t_2) \in \mathbb{Z}_p \times \mathbb{Z}_p$ such that

$$\begin{cases} \rho_1(pt_1, pt_2) = 0 \\ \rho_2(pt_1, pt_2) = 0 \end{cases} \tag{6.25}$$

for some $\rho_1(t_1, t_2), \rho_2(t_1, t_2) \in \mathbb{Q}_p[[t_1, t_2]]$.

The power series ρ_1 and ρ_2 are convergent on $p\mathbb{Z}_p \times p\mathbb{Z}_p$ and, possibly after multiplying by a power of p, we may assume that $\rho_1(pt_1, pt_2), \rho_2(pt_1, pt_2) \in \mathbb{Z}_p[[t_1, t_2]] \setminus p\mathbb{Z}_p[[t_1, t_2]]$.

A careful study of the valuation of the coefficients of ρ_1 and ρ_2 allows us to conclude that if $(\alpha, \beta) \in \mathbb{Z}_p \times \mathbb{Z}_p$ is a solution to (6.25), then $(\alpha \bmod p^n, \beta \bmod p^n)$ is a solution modulo (p^n) to the system

$$\begin{cases} \rho_1(pt_1, pt_2) + O(t_1, t_2)^{\tilde{n}} = 0 \\ \rho_2(pt_1, pt_2) + O(t_1, t_2)^{\tilde{n}} = 0 \end{cases} \tag{6.26}$$

for some integer $\tilde{n}$. How reversible is this process? In other words, if we find all the solutions of (6.26) mod p^n, how do we know if each such solution *lifts* to a *unique* solution to (6.25)?

In some cases, we can apply a multivariate version of Hensel's lemma (see Theorem 6.A.1 below). Let us first introduce some notation. Let $m \in \mathbb{N}$ and, for an element $\underline{a} = (a_1, \ldots, a_m) \in \mathbb{Q}_p^m$, define $\mathrm{ord}_p(\underline{a}) = \min_{1 \le i \le m}\{\mathrm{ord}_p(a_i)\}$. Then ord_p satisfies the following properties:

(a) For any $k \in \mathbb{Q}_p$, $\mathrm{ord}_p(k\underline{a}) = \mathrm{ord}_p(k) + \mathrm{ord}_p(\underline{a})$.

(b) $\mathrm{ord}_p(\underline{a} + \underline{b}) \ge \min\{\mathrm{ord}_p(\underline{a}), \mathrm{ord}_p(\underline{b})\}$ with equality if $\mathrm{ord}_p(\underline{a}) \ne \mathrm{ord}_p(\underline{b})$.

For $\underline{f} = (f_1, \ldots, f_m) \in \mathbb{Z}_p[[x_1, \ldots, x_m]]^m$ and $\underline{x} = (x_1, \ldots, x_m)$, define the Jacobian matrix

$$J_{\underline{f}}(\underline{x}) := \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_m} \\ \vdots & \ddots & \vdots & \\ \frac{\partial f_m}{\partial x_1} & \frac{\partial f_m}{\partial x_2} & \cdots & \frac{\partial f_m}{\partial x_m} \end{bmatrix} (\underline{x}).$$

Similarly to Chapter 3, denote by $\mathbb{Z}_p\langle x_1, \ldots, x_m\rangle$ the subring of $\mathbb{Z}_p[[x_1, \ldots, x_m]]$ consisting of those power series whose coefficients tend to 0 as the degree of the corresponding monomials tends to infinity.

Theorem 6.A.1 (Multivariate Hensel's lemma [49, Theorem 4.1]). *Let $\underline{f} = (f_1, \ldots, f_m) \in \mathbb{Z}_p\langle x_1, \ldots, x_m\rangle^m$. Assume that $\underline{a} \in \mathbb{Z}_p^m$ satisfies*

$$\mathrm{ord}_p(\underline{f}(\underline{a})) > 2\mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))).$$

Then there is a unique $\underline{\alpha} \in \mathbb{Z}_p^m$ such that $\underline{f}(\underline{\alpha}) = \underline{0}$ and $\mathrm{ord}_p(\underline{\alpha}-\underline{a}) > \mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a})))$. Furthermore, $\mathrm{ord}_p(\underline{\alpha} - \underline{a}) \geq \mathrm{ord}_p(\underline{f}(\underline{a})) - \mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a})))$.

Even though [49] is not the only reference for Theorem 6.A.1 (see for example also [83, Theorem 23]), the proof given by Conrad[4] in [49] has the advantage of being constructive: it shows how to explicitly find approximations of $\underline{\alpha}$ and how fast these converge to $\underline{\alpha}$. In particular, with the notation of the theorem, let $\underline{a}_1 = \underline{a}$ and define, for $N \geq 1$,

$$\underline{a_{N+1}} = \underline{a_N} - \underline{f}(\underline{a_N}) \cdot (J_{\underline{f}}(\underline{a_N})^T)^{-1}.$$

By [49, (3.9)], we have the inequality

$$\mathrm{ord}_p(\underline{a_{N+1}} - \underline{a_N}) \geq \mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\mathrm{ord}_p(\underline{f}(\underline{a})) - 2\mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a})))),$$

combining this with Property (b) and with the assumption that

$$\mathrm{ord}_p(\underline{f}(\underline{a})) - 2\mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))) > 0,$$

we obtain

$$\mathrm{ord}_p(\underline{a_M} - \underline{a_N}) \geq \mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\mathrm{ord}_p(\underline{f}(\underline{a})) - 2\mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))))$$

for all $M > N$. Thus, taking limits as $M \to \infty$,

$$\mathrm{ord}_p(\underline{\alpha} - \underline{a_N}) \geq \mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a}))) + 2^{N-1}(\mathrm{ord}_p(\underline{f}(\underline{a})) - 2\mathrm{ord}_p(\det(J_{\underline{f}}(\underline{a})))).$$

We sketch a possible strategy to compute roots of systems of equations of the form (6.25), omitting technicalities on precision.

Algorithm 6.A.2. *Computing roots of (6.25)*

Input: A system $\underline{\rho} = (\rho_1, \rho_2)$ of the form (6.25).

[4]We thank Keith Conrad for useful correspondence about his notes [49] and for consequently including a power series version of the lemma, which was needed for this work.

Output: L – *list of roots modulo* p^n *of* $\underline{\rho}$.

1. *Reduce to (6.26).*

2. *Compute* $R_p = \{(t_1, t_2) \in \{0, \dots, p-1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p\}$

3. *Let* $\underline{a} \in R_p$. *If* $\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{a}))) = 0$, *by Theorem 6.A.1 there exists a unique root* $\underline{\alpha} \in \mathbb{Z}_p^2$ *of (6.25) such that* $\mathrm{ord}_p(\underline{\alpha} - \underline{a}) > 0$. *Compute* $\underline{\alpha}$ *to the desired precision using the discussion following Theorem 6.A.1 and append it to* L.

4. *Let* $\underline{a} \in R_p$ *such that* $\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{a}))) \neq 0$. *Fix an* $r \geq 3$, $r \leq n$ *and naively find* $R_{p^r}(\underline{a}) = \{(t_1, t_2) \in \{0, \dots, p^r - 1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p^r$ *and* $(t_1, t_2) \equiv \underline{a} \bmod p\}$. *For each* $\underline{b} \in R_{p^r}(\underline{a})$ *do the following:*

   (i) *if* $2\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b}))) < r$, *compute using Theorem 6.A.1 an approximation of the unique root* $\underline{\beta} \in \mathbb{Z}_p^2$ *such that* $\mathrm{ord}_p(\underline{\beta} - \underline{b}) > \mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b})))$ *and append it to* L. *Remove from* $R_{p^r}(\underline{a})$ *all* $\underline{b}'$ *such that* $\mathrm{ord}_p(\underline{b}' - \underline{b}) > \mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b})))$.

   (ii) *if* $2\mathrm{ord}_p(\det(J_{\underline{\rho}}(\underline{b}))) \geq r$, *then if* $r = n$ *append* $\underline{b}$ *to* L; *if* $r < n$, *choose some* $s > r$, $s \leq n$, *naively find* $R_{p^s}(\underline{b}) = \{(t_1, t_2) \in \{0, \dots, p^s - 1\}^2 : \underline{\rho}(pt_1, pt_2) \equiv 0 \bmod p^s$ *and* $(t_1, t_2) \equiv \underline{b} \bmod p^r\}$ *and for each* $\underline{c} \in R_{p^s}(\underline{b})$ *repeat (i), (ii) with the appropriate modification in notation.*

Remark 6.A.3. If the algorithm never appends to L in 4 (ii), each element in L is the approximation of a unique root of (6.25) and, conversely, each root of (6.25) reduces to an element of L. Otherwise, we can try to increase n. However, there are some residue disks where the systems that we consider provably have roots at which the determinant of the Jacobian matrix also vanishes, so Theorem 6.A.1 is not applicable. Indeed, let C be as in Section 6.5. Then C admits the automorphisms $\theta\colon (x, y) \mapsto (\pm x, \pm y)$. Composing φ_k with θ we obtain either the identity or multiplication by -1 on E_k. Since local heights are even, it follows that if a function ρ comes from a height function as in Theorem 6.5.2, then all its partial derivatives vanish[5] at a K-rational point fixed by a non-trivial automorphism θ. A function coming from relations of the linear functionals f_i on E_k is odd and will thus have non-simple zeros in the above sense at those points (x, y) which are fixed by a non-trivial automorphism θ that projects to the identity on E_k.

[5]E.g. for the pair of disks containing a point fixed by $(x, y) \mapsto (-x, y)$, we can set $t_1 = x_1$, $t_2 = x_2$ as uniformisers. Then $\rho(t_1, t_2) = \rho(-t_1, -t_2)$ giving vanishing of the partial derivatives at $t_1 = t_2 = 0$.

We now explain how to deal with the disks of Remark 6.A.3 where Hensel is not applicable, for the explicit algorithms that we described in Section 6.7. Suppose first that we are in the situation of §6.7.1, of which we retain the notation. Let H be the subgroup of the automorphism group of C generated by the hyperelliptic involution and the bielliptic automorphism $(x, y) \mapsto (-x, y)$.

Lemma 6.A.4. *Let K and $C/\mathbb{Q}$ be as in §6.7.1. Let $P \in C(K)$ such that $\theta(P) = P$ for a non-trivial automorphism $\theta \in H$; if $y(P) = 0$, further assume that $x(P)^2 \in \mathbb{Q}$. Let $k \in \{1, 2\}$ such that $P \in C^{(k)}(K)$ and let $w \in T^{\mathrm{anti},k}$ such that $\rho^{\mathrm{anti},k}(\psi(P)) = w$. Then we can choose local coordinates[6] t_1 and t_2 for $\psi_1(P)$ and $\psi_2(P)$, such that, in the residue pair $\overline{\psi_1(P)} \times \overline{\psi_2(P)} \in \overline{C}(\mathbb{F}_p) \times \overline{C}(\mathbb{F}_p)$, we have*

$$\rho^{\mathrm{anti},k}(t_1, t_2) - w = \sum_{i=1}^{\infty} c_i(t_1^{2i} - t_2^{2i}) = (t_1^2 - t_2^2) \sum_{i=1}^{\infty} c_i \left(\sum_{j=0}^{i-1} t_1^{2j} t_2^{2i-2-2j} \right)$$

for some $c_i \in \mathbb{Q}_p$.

Proof. Write a point in $C(\mathbb{Q}_p) \times C(\mathbb{Q}_p)$ as $((x_1, y_1), (x_2, y_2))$. We fix the following choices for t_1 and t_2. If $\theta(x, y) = (-x, y)$, let $t_i = x_i$; if $\theta(x, y) = (x, -y)$, let $t_i = y_i$; finally, if $P = \infty^{\pm}$, let $t_i = 1/x_i$. As observed in Remark 6.A.3, we have

$$\rho^{\mathrm{anti},k}((x_1, y_1), (x_2, y_2)) = \rho^{\mathrm{anti},k}(\theta(x_1, y_1), \theta(x_2, y_2));$$

our choice of local coordinates then yields

$$\rho^{\mathrm{anti},k}(t_1, t_2) = \rho^{\mathrm{anti},k}(-t_1, -t_2).$$

Since by §6.6.2 we have $\alpha_{01}^{\mathrm{anti},E_j} = 0$ for each $j \in \{1, 2\}$, this implies that there exist some power series f_1 and f_2 such that

$$\rho^{\mathrm{anti},k}(t_1, t_2) = f_1(t_1^2) - f_2(t_2^2) + 4h_p^{\mathrm{anti},E_k}(Q_k).$$

In view of our assumptions, we also have that $x_1(t_1)^2 = x_2(t_2)^2|_{t_1}$ and thus that $\varphi_j(x_1(t_1), y_1(t_1)) = \pm\varphi_j(x_2(t_2), y_2(t_2))|_{t_1}$. Since $\alpha_{00}^{\mathrm{anti},E_j} = -\alpha_{11}^{\mathrm{anti},E_j}$ by §6.6.2, we conclude that $f_1 = f_2$. Finally, the lemma follows by definition of w. □

Remark 6.A.5. Since $h_p^{\mathrm{anti},E_k}(Q_k) = 0$, we must have $w = 0$.

In the notation of Lemma 6.A.4, the points $(z_1, z_2) \in C^{(k)}(K \otimes \mathbb{Q}_p)$ reducing to $\overline{\psi_1(P)} \times \overline{\psi_2(P)}$ and such that $\rho^{\mathrm{anti},k}(z_1, z_2) = w$ satisfy one of the following

[6] in the sense of §5.2.2.1

(i) $t_1(z_1) = t_2(z_2)$ and $\rho^{\mathrm{cyc},k}(t_1(z_1), t_1(z_1)) \in T^{k,\mathrm{cyc}}$;

(ii) $t_1(z_1) = -t_2(z_2)$ and $\rho^{\mathrm{cyc},k}(t_1(z_1), -t_1(z_1)) \in T^{k,\mathrm{cyc}}$;

(iii) $\begin{cases} \sum_{i=1}^{\infty} c_i \left(\sum_{j=0}^{i-1} t_1(z_1)^{2j} t_2(z_2)^{2i-2-2j} \right) = 0 \\ \rho^{\mathrm{cyc},k}(t_1(z_1), t_2(z_2)) \in T^{k,\mathrm{cyc}}. \end{cases}$

If $c_1 \neq 0$, then $(0,0)$ is not a root of (iii), so in Algorithm 6.A.2 we can hope for no root to be appended in 4 (ii). We also note that the one-variable power series of (i) and (ii) are power series in t_1^2.

In the setting of §6.7.2, we follow a similar strategy (and adopt some of the notation of the imaginary case). Recall that the second function ρ_2 is given by

$$\rho_2(z_1, z_2) = \int_O^{\varphi_2(z_1)} \omega_0^{E_2} - b \int_O^{\varphi_2(z_2)} \omega_0^{E_2},$$

where $b = 1$ or $b = -1$, depending on the rank of E_2 over $\mathbb{Q}$. We assume here that $b = 1$ as in Example 6.7.2. Let $P \in C^{(k)}(K)$ be fixed by $\theta \in H \setminus \{\mathrm{id}\}$ and let t_1 and t_2 be local coordinates chosen in the same way as in the proof of Lemma 6.A.4. Then, in the residue disk of $\psi(P)$, we have

$$\rho_2(-t_1, -t_2) = \begin{cases} \rho_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = \mathrm{id}, \\ -\rho_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = -\mathrm{id}. \end{cases}$$

Assume for simplicity that $P \in C(\mathbb{Q})$, so the local expansion of $\int_O^{\varphi_2(z_1)} \omega_0^{E_2}$ evaluated at t_2 gives the local expansion of $\int_O^{\varphi_2(z_2)} \omega_0^{E_2}$. We conclude that

$$\rho_2(t_1, t_2) = \begin{cases} (t_1^2 - t_2^2)\tilde{\rho}_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = \mathrm{id}, \\ (t_1 - t_2)\tilde{\rho}_2(t_1, t_2) & \text{if } \varphi_2 \circ \theta = -\mathrm{id}, \end{cases}$$

for some $\tilde{\rho}_2(t_1, t_2) \in \mathbb{Q}_p[[t_1, t_2]]$.

Chapter 7

Consequences of the functional equation of the p-adic L-function of an elliptic curve

This chapter (without the appendix) is essentially the article [30].

7.1 Introduction

In [148], Wuthrich proves a relation between the leading and sub-leading coefficients of the Taylor series expansion at $s = 1$ of the L-function of an elliptic curve over a number field, under the assumptions that the series admits an analytic continuation to $s = 1$ and satisfies a functional equation. Wuthrich remarks that a similar result can potentially be obtained for any L-function which satisfies a functional equation.

In this chapter, we consider the p-adic L-function of an elliptic curve over $\mathbb{Q}$ and its twist by a quadratic character and explore the analogue of Wuthrich's result. The prime p will be assumed to be odd and of semistable reduction for the curve. We start in Section 7.2 by reviewing the definition of the p-adic L-function and of its twists by Dirichlet characters ψ. Indeed, we define two p-adic L-functions, namely $L_p(E, \alpha, \psi, s)$, which is a function of $s \in \mathbb{Z}_p$, and $\mathcal{L}_p(E, \alpha, \psi, T)$, a power series in T. We state in Proposition 7.2.1 and Corollary 7.2.2 the functional equation for $L_p(E, \alpha, \psi, s)$ and the corresponding result for $\mathcal{L}_p(E, \alpha, \psi, T)$. Proofs of the interpolation property and of the functional equation satisfied, more generally, by the twists of the p-adic L-function of a weight k cuspidal eigenform of Nebentypus ϵ are provided in [100, Ch. I, §§13, 17].

Subsequently, in Section 7.3, we prove the analogue of [148, Theorem 1] for $L_p(E, \alpha, \psi, s)$ when ψ is a real character (i.e. when ψ is either the trivial character or

a quadratic character). In particular, we prove in Theorem 7.3.3 that the sub-leading coefficient in the Taylor expansion of $L_p(E, \alpha, \psi, s)$ at $s = 1$ is equal to the leading coefficient multiplied by a constant dependent exclusively on the conductor of E, on the conductor of ψ and on the prime p. The assumption that ψ is a real character is necessary, since the functional equation relates the values of $L_p(E, \alpha, \psi, s)$ to those of $L_p(E, \alpha, \overline{\psi}, 2 - s)$.

Although the latter result is perhaps of some interest on its own, when studying p-adic L-functions one is often concerned about the corresponding power series $\mathcal{L}_p(E, \alpha, \psi, T)$, because of its central importance in Iwasawa theory of elliptic curves. In Theorem 7.4.1 we thus translate the results of Section 7.3 into a relation between the first two leading coefficients of $\mathcal{L}_p(E, \alpha, \psi, T)$. In Section 7.4, we also prove another consequence of the relation between $\mathcal{L}_p(E, \alpha, \psi, T)$ and $\mathcal{L}_p(E, \alpha, \overline{\psi}, (1+T)^{-1}-1)$, namely that the μ-invariant of $\mathcal{L}_p(E, \alpha, \psi, T)$ is the same as that of $\mathcal{L}_p(E, \alpha, \overline{\psi}, T)$. This is Theorem 7.4.2.

We end the chapter with a generalisation of some of the results to the p-adic L-function of the base change of an elliptic curve to an abelian number field.

7.2 Notation and statement of the functional equation

In this section, we recall the definition of the p-adic L-function and the statement of the functional equation it satisfies. In Appendices 7.A and 7.B we will include a proof of the interpolation property and of the functional equation in some cases. We follow the notation of [132] for the modular symbols and measures as well as the construction of the p-adic L-function, but we also allow non-trivial twists. We fix once and for all an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and assume that p is an odd prime at which E has semistable reduction. Let $f(z)$ be the newform of weight 2 corresponding to E by modularity and denote its q-expansion $\sum_{n=1}^{\infty} a_n q^n$.

We now define a quantity α, dependent on the reduction type of E at p. In particular, if E has good ordinary reduction (cf. §2.2.2.1), we let α be the unique p-adic unit in $\mathbb{Z}_p$ which is a root of the characteristic polynomial of Frobenius $P(X) = X^2 - a_p X + p$. When E has good supersingular reduction, we denote by α an arbitrary fixed root of $P(X)$. Finally, if E has multiplicative reduction, we set $\alpha = a_p$, so that, in particular, $\alpha = 1$ (resp. $\alpha = -1$) if the reduction type is split (resp. non-split). We

call α an *allowable p-root (for E)* and we emphasise that α is uniquely determined, unless E has good supersingular reduction at p.

For $r \in \mathbb{Q}$, we let

$$\lambda^{\pm}(r) = \mp \pi i \left(\int_r^{i\infty} f(z)dz \pm \int_{-r}^{i\infty} f(z)dz \right).$$

Normalising $\lambda^+(r)$ (resp. $\lambda^-(r)$) by the real period Ω_E^+ (resp. imaginary period Ω_E^-) of E gives the rational numbers $[r]^{\pm} = \frac{\lambda^{\pm}(r)}{\Omega_E^{\pm}}$ (cf. [92]).

Any unit x in $\mathbb{Z}_p$ has a unique decomposition as a product of the form $\omega(x)\langle x \rangle$ where $\omega(x)$ is a $(p-1)$-st root of unity and $\langle x \rangle \in 1+p\mathbb{Z}_p$ (note the running assumption that p is odd).

As in [100, Ch. I, §§11, 13], for a positive integer M coprime to p, we let

$$\mathbb{Z}_{p,M} = \varprojlim_n (\mathbb{Z}/p^n M\mathbb{Z}) \qquad \mathbb{Z}_{p,M}^{\times} = \varprojlim_n (\mathbb{Z}/p^n M\mathbb{Z})^{\times}$$

and define a *p-adic character* as a continuous homomorphism $\mathbb{Z}_{p,M}^{\times} \to \mathbb{C}_p^{\times}$. In particular, since we have fixed an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$, we may regard the notion of a finite order p-adic character and a Dirichlet character as equivalent and hence, even in the p-adic setting, we may use the notation $\overline{\psi}$ for the inverse of the finite order character ψ and say ψ is *real-valued* if it is real-valued as a Dirichlet character, i.e. $\psi = \overline{\psi}$.

We then define the measures

$$\mu_{\alpha}^{\pm}(a + p^k M\mathbb{Z}_{p,M}) = \frac{1}{\alpha^k} \left[\frac{a}{Mp^k} \right]^{\pm} - \frac{(1-\delta)}{\alpha^{k+1}} \left[\frac{a}{Mp^{k-1}} \right]^{\pm},$$

where $\delta = 0$ if E has good reduction and 1 otherwise.

Let ψ be a finite order p-adic character (possibly the identity) of conductor $p^k M$, with $(M,p) = 1$, and write $\langle x \rangle^{s-1} = \exp\left((s-1)\log\langle x \rangle\right) = \sum_{n=0}^{\infty} \frac{(s-1)^n}{n!} (\log\langle x \rangle)^n$, where exp and log are the p-adic exponential and logarithm maps. Then we define

$$L_p(E, \alpha, \psi, s) = \int_{\mathbb{Z}_{p,M}^{\times}} \psi(x)\langle x \rangle^{s-1} d\mu_{\alpha}(x),$$

where $\mu_{\alpha} = \mu_{\alpha}^+$ if the sign of ψ is $+1$ and $\mu_{\alpha} = \mu_{\alpha}^-$ otherwise. The p-adic L-function $L_p(E, \alpha, \psi, s)$ is a locally analytic function of $s \in \mathbb{Z}_p$ (see the first proposition in [100, Ch. I, §13]).

We now perform a change of variable in the definition of $L_p(E, \alpha, \psi, s)$. Consider the extension $\mathbb{Q}(\mu_{p^\infty})$ of $\mathbb{Q}$, obtained by adjoining to $\mathbb{Q}$ all roots of unity of p-power order. Furthermore, let Γ denote the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}^{\infty}$

of $\mathbb{Q}$ and let $\mathbb{Q}^n$ be the n-th layer in the cyclotomic tower, that is, the unique subfield of $\mathbb{Q}^\infty$ whose Galois group over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. More precisely, there is a canonical homomorphism

$$\kappa\colon \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to \mathbb{Z}_p^\times$$

defined by the relation $\sigma(\zeta) = \zeta^{\kappa(\sigma)}$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ and $\zeta \in \mu_{p^\infty}$. The homomorphism κ is called the *cyclotomic character* and it induces an isomorphism $\Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$. Indeed, the group Γ is naturally identified with the quotient of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ by the subgroup which is mapped, under κ, to $(\mathbb{Z}/p\mathbb{Z})^\times \times \{0\} < (\mathbb{Z}/p\mathbb{Z})^\times \times (1+p\mathbb{Z}_p) \cong \mathbb{Z}_p^\times$. We may choose a topological generator $\gamma \in \Gamma$ and define $T = \kappa(\gamma)^{s-1} - 1$. The result is a power series in T, with coefficients in $\mathbb{Q}_p[\psi](\alpha)$,

$$\mathcal{L}_p(E, \alpha, \psi, T) = \int_{\mathbb{Z}_{p,M}^\times} \psi(x)(1+T)^{\frac{\log\langle x\rangle}{\log \kappa(\gamma)}} d\mu_\alpha(x).$$

When the character ψ is trivial, we write simply $L_p(E, \alpha, s)$ and $\mathcal{L}_p(E, \alpha, T)$.

Denote by Q the largest divisor of N coprime to pM. Then there exists $c_Q = \pm 1$ such that $w_Q(f) = c_Q f$, where

$$w_Q(f) = f|_{\left(\begin{smallmatrix} Qa & b \\ Nc & Qd \end{smallmatrix}\right)}(z) := \frac{Q}{(Ncz + Qd)^2} \cdot f\left(\frac{Qaz + b}{Ncz + Qd}\right)$$

for some integers a, b, c, d satisfying $Qad - (N/Q)bc = 1$ (see [4]). Note that, when $Q = N$, we have $w_E = -c_Q$ where w_E is the sign in the functional equation of the complex L-function $L(E, s)$.

Proposition 7.2.1 (Functional equation). *Let E be an elliptic curve of conductor N with semistable reduction at the odd prime p and let ψ be a Dirichlet character of conductor $p^k M$, for some non-negative integers k and M, with $(M, p) = 1$. For each allowable p-root α, the p-adic L-function $L_p(E, \alpha, \psi, s)$ satisfies the functional equation*

$$L_p(E, \alpha, \psi, 2 - s) = -c_Q \cdot \overline{\psi}(-Q)\langle Q\rangle^{s-1} L_p(E, \alpha, \overline{\psi}, s),$$

where Q is the largest divisor of N coprime to pM.

Proof. See [100, Ch. I, §17, Corollary 2] for the general case and Appendix 7.B for a proof under the assumptions that $Q = N$ and that p is ordinary. □

Corollary 7.2.2. *With the assumptions as in Proposition 7.2.1, we have*

$$\mathcal{L}_p(E, \alpha, \psi, T) = -c_Q \cdot \overline{\psi}(-Q)(1+T)^{-\frac{\log\langle Q\rangle}{\log \kappa(\gamma)}} \mathcal{L}_p(E, \alpha, \overline{\psi}, (1+T)^{-1} - 1).$$

7.3 Relation between the leading and sub-leading coefficients of the p-adic L-function of an elliptic curve

We adopt the same notation as in Section 7.2.

Lemma 7.3.1. *Let ψ be a real-valued Dirichlet character. Then*

$$-c_Q \cdot \psi(-Q) = (-1)^{\mathrm{ord}_{s=1} L_p(E,\alpha,\psi,s)}.$$

Proof. This is a standard exercise given the functional equation. Indeed, since ψ is assumed to be real-valued, Proposition 7.2.1 becomes

$$\Lambda_p(E,\alpha,\psi,2-s) = -c_Q \cdot \psi(-Q)\Lambda_p(E,\alpha,\psi,s), \tag{7.1}$$

where we put $\Lambda_p(E,\alpha,\psi,s) = f(s) \cdot L_p(E,\alpha,\psi,s)$ with $f(s) = \langle Q \rangle^{s/2}$.

Let $m = \mathrm{ord}_{s=1} L_p(E,\alpha,\psi,s)$, so that $\frac{d^i}{ds^i} L_p(E,\alpha,\psi,s)\big|_{s=1} = 0$ for all $i < m$ and $\frac{d^m}{ds^m} L_p(E,\alpha,\psi,s)\big|_{s=1} \neq 0$. Then differentiating both sides of (7.1) and evaluating at $s = 1$ yields

$$((-1)^m + c_Q \cdot \psi(-Q)) \frac{d^m}{ds^m} \Lambda_p(E,\alpha,\psi,s)\big|_{s=1} = 0.$$

By the definition of m, one has

$$\frac{d^m}{ds^m} \Lambda_p(E,\alpha,\psi,s)\big|_{s=1} = f(1) \frac{d^m}{ds^m} L_p(E,\alpha,\psi,s)\big|_{s=1} \neq 0, \tag{7.2}$$

which forces $-c_Q \cdot \psi(-Q) = (-1)^m$. □

Remark 7.3.2. Assume that E has good ordinary or multiplicative reduction at p and that ψ is either trivial or a quadratic character of conductor M (i.e. coprime with p) such that $\frac{N}{p^{\mathrm{ord}_p(N)} Q} \mid M$. The p-adic Birch and Swinnerton-Dyer conjecture (cf. [100, Ch. II, §§10, 11] and Appendix 7.C) then predicts that

$$\mathrm{ord}_{s=1} L_p(E,\alpha,\psi,s) = \mathrm{rank}(E^\psi(\mathbb{Q})) + \upsilon,$$

where E^ψ is the twist of E by ψ and υ vanishes except for when $\psi(p) = \alpha$, in which case $\upsilon = 1$.

We now state and prove the result analogous to Wuthrich [148, Theorem 1].

Theorem 7.3.3. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and p an odd prime of semistable reduction for E. Let ψ be either the trivial character or a quadratic character. Let α be an allowable p-root and denote by m the order of vanishing at $s = 1$ of $L_p(E, \alpha, \psi, s)$. Then*

$$L_p(E, \alpha, \psi, s) = a_m(s-1)^m + a_{m+1}(s-1)^{m+1} + \cdots$$

with

$$a_{m+1} = -\frac{a_m}{2} \log \langle Q \rangle,$$

where Q is the largest divisor of N coprime to p and to the conductor of ψ.

Proof. By Lemma 7.3.1, we have

$$\Lambda_p(E, \alpha, \psi, 2-s) = (-1)^m \Lambda_p(E, \alpha, \psi, s),$$

where, as in the proof of the lemma, $\Lambda_p(E, \alpha, \psi, s) = f(s) \cdot L_p(E, \alpha, \psi, s)$ with $f(s) = \langle Q \rangle^{s/2}$. We can now follow Wuthrich's proof nearly identically. In particular, for $i \equiv m+1 \bmod 2$, one has

$$\frac{d^i}{ds^i} \Lambda_p(E, \alpha, \psi, s)\big|_{s=1} = 0. \tag{7.3}$$

Choosing $i = m+1$, this gives

$$\begin{aligned}
0 &= \frac{d^{m+1}}{ds^{m+1}} \left(f(s) L_p(E, \alpha, \psi, s) \right) \big|_{s=1} \\
&= \left(\sum_{k=0}^{m+1} \binom{m+1}{k} \frac{d^{m+1-k}}{ds^{m+1-k}} f(s) \cdot \frac{d^k}{ds^k} L_p(E, \alpha, \psi, s) \right) \Bigg|_{s=1} \\
&= \left((m+1) f'(s) \cdot \frac{d^m}{ds^m} L_p(E, \alpha, \psi, s) + f(s) \cdot \frac{d^{m+1}}{ds^{m+1}} L_p(E, \alpha, \psi, s) \right) \Bigg|_{s=1} \\
&= (m+1)! (f'(1) \cdot a_m + f(1) \cdot a_{m+1}).
\end{aligned}$$

Therefore, $a_{m+1} = -\frac{f'(1)}{f(1)} a_m = -\frac{a_m}{2} \log \langle Q \rangle$. □

Let E be as in Theorem 7.3.3. The twist of E by a quadratic character ψ of conductor coprime to p can be realised as an elliptic curve $E'/\mathbb{Q}$ which has semistable reduction at p. Therefore, if the conductor of ψ is coprime to p and E' has additive reduction at all primes of additive reduction for E, the statement of Theorem 7.3.3 for $L_p(E, \alpha, \psi, s)$ is implicitly included in the statement of Theorem 7.3.3 for the p-adic L-function of E' with trivial twist. On the other hand, the twist of E by a quadratic character of conductor divisible by p is an elliptic curve E' with additive reduction

at p. In other words, the quadratic character case in Theorem 7.3.3 is not completely exhausted by the result for the trivial character.

Note that Wuthrich's method can be generalised to obtain the coefficient a_{m+k} for every positive odd k in terms of the coefficients a_{m+j}, where $0 \leq j < k$, just by considering (7.3) for $i = m + k$. Recursively, this gives a way of expressing a_{m+k} for *odd* k in terms of $a_{m+\ell}$ for *even* ℓ with $\ell < k$. In particular, we may consider Theorem 7.3.3 as a special case of the following result.

Theorem 7.3.4. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and p an odd prime of semistable reduction for E. Let ψ be either the trivial character or a quadratic character and let Q be the largest divisor of N coprime to p and to the conductor of ψ. Denote by m the order of vanishing at $s = 1$ of $L_p(E, \alpha, \psi, s)$. Then*

$$L_p(E, \alpha, \psi, s) = a_m(s-1)^m + a_{m+1}(s-1)^{m+1} + \cdots,$$

where, for odd $k > 0$, we have

$$a_{m+k} = -\sum_{i=0}^{k-1} \frac{1}{(k-i)!} \cdot \left(\frac{\log\langle Q\rangle}{2}\right)^{k-i} a_{m+i}.$$

Therefore, for odd k, a_{m+k} can be expressed as a linear combination of $a_{m+\ell}$ for even ℓ, $0 \leq \ell < k$.

Proof. Using (7.3) with $i = m + k$ and the fact that $\frac{d^k}{ds^k} L_p(E, \alpha, \psi, s)\big|_{s=1} = 0$ for all $k < m$ gives

$$\sum_{r=m}^{m+k} \frac{(m+k)!}{(m+k-r)!} f^{(m+k-r)}(1) a_r = 0.$$

It remains to notice that, for all $j \geq 0$, $f^{(j)}(s) = \left(\frac{\log\langle Q\rangle}{2}\right)^j \langle Q\rangle^{s/2}$. □

Remark 7.3.5. Although Theorem 7.3.4 is more general than Theorem 7.3.3, the latter is perhaps the more interesting result. Indeed, when ψ is the trivial character, the p-adic version of the Birch and Swinnerton-Dyer conjecture gives an explicit expression for a_m (see Conjecture (BSD(p)) in [100, Ch. II, §10] for the ordinary case, and [23], [47, Conjecture 0.12] for the supersingular case). Thus, a similar observation to Wuthrich's in [148] holds here: assuming the p-adic BSD, Theorem 7.1.5 provides an arithmetic interpretation also of the sub-leading coefficient of $L_p(E, \alpha, s)$.

In the quadratic character case, a BSD-type formula is given in [100] only when the conductor of ψ equals M with $(M, p) = 1$ and $\frac{N}{p^{\mathrm{ord}_p(N)}Q} \mid M$; once again, this is equivalent to BSD(p) for the semistable twisted curve (see Proposition in Ch. II §11 of *loc. cit.*).

7.4 Results for $\mathcal{L}_p(E, \alpha, \psi, T)$

The starting point for this section is Corollary 7.2.2. The first result is then

Theorem 7.4.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and p an odd prime of semistable reduction for E. Let ψ be either the trivial character or a quadratic character and let Q be the largest divisor of N coprime to p and to the conductor of ψ. Let α be an allowable p-root and denote by m the order of vanishing at $T = 0$ of $\mathcal{L}_p(E, \alpha, \psi, T)$. Then*

$$\mathcal{L}_p(E, \alpha, \psi, T) = c_m T^m + c_{m+1} T^{m+1} + \cdots$$

where

$$c_{m+1} = -\frac{c_m}{2}\left(\frac{\log\langle Q\rangle}{\log(\kappa(\gamma))} + m\right).$$

Proof. By Corollary 7.2.2, we have

$$\mathcal{L}_p(E, \alpha, \psi, (1+T)^{-1} - 1) = (-c_Q)\psi(-Q)(1+T)^{\frac{\log\langle Q\rangle}{\log\kappa(\gamma)}}\mathcal{L}_p(E, \alpha, \psi, T). \tag{7.4}$$

Differentiating m times and evaluating at $T = 0$ yields the equality $-c_Q\psi(-Q) = (-1)^m$, similarly to Lemma 7.3.1.

Then, differentiating $m + 1$ times the right hand side resp. the left hand side of (7.4) and evaluating at $T = 0$ gives

$$(-1)^m(m+1)!\left(\frac{\log\langle Q\rangle}{\log\kappa(\gamma)}c_m + c_{m+1}\right)$$

resp.

$$(-1)^{m+1}(m+1)!(c_{m+1} + mc_m). \qquad \square$$

Assume now that E has ordinary semistable reduction at the odd prime p, that is, either good ordinary or multiplicative reduction. Since, in this case, there is a unique p-admissible root α for E, we may drop α from the notation and simply write $\mathcal{L}_p(E, \psi, T)$ for the p-adic L-function of E, twisted by ψ. By [147], $\mathcal{L}_p(E, \psi, T) \in \Lambda = \mathbb{Z}_p[\psi][[T]]$ and we define the *μ-invariant* of $\mathcal{L}_p(E, \psi, T)$ as the p-adic valuation of the highest power of π dividing $\mathcal{L}_p(E, \psi, T)$, where π is a uniformiser for $\mathbb{Z}_p[\psi]$. From the relation between $\mathcal{L}_p(E, \psi, T)$ and $\mathcal{L}_p(E, \overline{\psi}, (1+T)^{-1} - 1)$ we deduce equality of the μ-invariants of $\mathcal{L}_p(E, \psi, T)$ and $\mathcal{L}_p(E, \overline{\psi}, T)$:

Theorem 7.4.2. *Let E be an elliptic curve over $\mathbb{Q}$ and p an odd prime of ordinary semistable reduction for E. Let ψ be a character of conductor $p^k M$. The μ-invariant of $\mathcal{L}_p(E, \psi, T)$ equals the μ-invariant of $\mathcal{L}_p(E, \overline{\psi}, T)$.*

Proof. By Corollary 7.2.2,

$$\mathcal{L}_p(E,\psi,T) = -c_Q \cdot \overline{\psi}(-Q)(1+T)^{-\frac{\log\langle Q\rangle}{\log\kappa(\gamma)}}\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1).$$

Now $c_Q = \pm 1$, $\overline{\psi}(-Q)$ is a root of unity and $(1+T)^{-\frac{\log\langle Q\rangle}{\log\kappa(\gamma)}}$ is a unit power series. Therefore the μ-invariant of $\mathcal{L}_p(E,\psi,T)$ is the same as the μ-invariant of $\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)$.

The theorem then follows if we show that the μ-invariant of a power series in Λ is unchanged under the substitution $T \mapsto (1+T)^{-1}-1$. For this purpose, let $f(T) = \sum_{k=0}^{\infty} a_k T^k$ and $g(T) = f((1+T)^{-1}-1)$. Since $(1+T)^{-1}-1 = \sum_{i=1}^{\infty}(-1)^i T^i$, if $\pi^\nu \mid f(T)$ then $\pi^\nu \mid g(T)$, so that the μ-invariant of $g(T)$ is at least equal to the μ-invariant of $f(T)$. By applying the same argument to $g(T)$ and $g((1+T)^{-1}-1) = f(T)$, we conclude that the μ-invariant of $g(T)$ is indeed equal to the one of $f(T)$. □

7.5 Generalisations to the base change of an elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Let K be an abelian number field such that the additive primes for $E/\mathbb{Q}$ remain additive in the base change of E to K. Denote by p an odd prime of semistable reduction for E and assume[1] further that the field K is disjoint from the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Fix a choice of an allowable p-root α for $E/\mathbb{Q}$ as in Section 7.2. We can then define the p-adic L-function for the base-changed curve E/K as (cf. [97, §9.2] and [93, §2])

$$\mathcal{L}_p(E/K,\alpha,T) = \prod_{\psi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}} \mathcal{L}_p(E,\alpha,\psi,T), \tag{7.5}$$

where $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$ is the group of characters on $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathcal{L}_p(E,\alpha,\psi,T)$ is the p-adic L-function of $E/\mathbb{Q}$ twisted by ψ, as defined in Section 7.2. From the interpolation property for each $\mathcal{L}_p(E,\alpha,\psi,T)$ and the assumption on the behaviour of the additive places in $K/\mathbb{Q}$, it is easy to see that $\mathcal{L}_p(E/K,\alpha,T)$ interpolates the values at $s=1$ of the complex L-function $L(E/K,s)$, twisted by characters of the $\mathbb{Z}_p$-cyclotomic extension of K (cf. Remark 7.A.5).

[1] Let χ be the character factoring through $\mathbb{Q}^n$ sending $\kappa(\gamma)$ to the p^n-th root of unity ζ. Then $\mathcal{L}_p(E,\alpha,\chi,T) = \mathcal{L}_p(E,\alpha,\zeta(T+1)-1)$, so that it is really meaningful to consider only extensions that are disjoint from the $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Furthermore, using Corollary 7.2.2 on each factor of the right hand side of (7.5), we find the following transformation property for $\mathcal{L}_p(E/K, \alpha, T)$

$$\mathcal{L}_p(E/K, \alpha, T) = \left[\prod_{\psi}(-c_{Q_\psi}) \cdot \prod_{\psi}\overline{\psi}(-Q_\psi)\right] \cdot \left[\prod_{\psi}(1+T)^{-\frac{\log\langle Q_\psi\rangle}{\log\kappa(\gamma)}}\right] \cdot \\ \cdot \mathcal{L}_p(E/K, \alpha, (1+T)^{-1} - 1), \tag{7.6}$$

where the products run over all characters ψ of $\widehat{\mathrm{Gal}(K/\mathbb{Q})}$ and Q_ψ is the largest divisor of N coprime with p and with the conductor of ψ.

Recall from Section 7.2 that the variables T and s are related by the identity $T = \kappa(\gamma)^{s-1} - 1$. The analogue of Proposition 7.2.1 for E/K is then

$$L_p(E/K, \alpha, 2-s) = \left[\prod_{\psi}(-c_{Q_\psi}) \cdot \prod_{\psi}\overline{\psi}(-Q_\psi)\right] \cdot \left[\prod_{\psi}\langle Q_\psi\rangle^{s-1}\right] L_p(E/K, \alpha, s). \tag{7.7}$$

Equations (7.7) and (7.6) allow us to deduce analogues of Theorem 7.3.3 and Theorem 7.4.1 for E/K. The proofs are essentially identical, so we include only the statements of the results.

Theorem 7.5.1. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and p an odd prime of semistable reduction for E. Denote by E/K the base change of E to an abelian number field K, where K is assumed to be disjoint from the $\mathbb{Z}_p$-extension of $\mathbb{Q}$ and such that additive reduction is preserved everywhere in the extension $K/\mathbb{Q}$. For each allowable p-root α, let m be the order of vanishing of $L_p(E/K, \alpha, s)$ at $s = 1$. Then*

$$L_p(E/K, \alpha, s) = a_m(s-1)^m + a_{m+1}(s-1)^{m+1} + \cdots$$

with

$$a_{m+1} = -\frac{\sum_\psi \log\langle Q_\psi\rangle}{2} a_m,$$

where ψ runs through the characters of $\mathrm{Gal}(K/\mathbb{Q})$ and Q_ψ is the largest divisor of N which is coprime with p and with the conductor of ψ.

Theorem 7.5.2. *With the assumptions of Theorem 7.5.1, we have*

$$\mathcal{L}_p(E/K, \alpha, T) = c_m T^m + c_{m+1} T^{m+1} + \cdots$$

with

$$c_{m+1} = -\frac{c_m}{2}\left(\frac{\sum_\psi \log\langle Q_\psi\rangle}{\log\kappa(\gamma)} + m\right).$$

Appendix

In this appendix we include proofs of the interpolation property and functional equation of the p-adic L-functions considered in this chapter. These are of course just special cases of the results of [100], which is our main reference, but we have found it useful to work out the details to gain better understanding. See also [1] and [142] for the good reduction case. We also state the p-adic analogue of the Birch and Swinnerton-Dyer conjecture, which provides a bridge to the rest of the thesis.

7.A The interpolation property

We retain the notation of Section 7.2. In particular, E is an elliptic curve over $\mathbb{Q}$ of conductor N and $f \in S_2(\Gamma_0(N))$ is the associated newform. Suppose f has q-expansion $\sum_{n=1}^{\infty} a_n q^n$ and let χ be a Dirichlet character of conductor $m > 1$. Then $L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$ and we further set

$$L(E,\chi,s) := \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}.$$

Lemma 7.A.1. *Let χ be a Dirichlet character of conductor m. We have*

$$L(E,\chi,1) = \frac{\tau(\chi)}{m} \sum_{a \bmod m} \overline{\chi}(a) \cdot (-2\pi i) \int_{-a/m}^{i\infty} f(z)dz,$$

where $\tau(\chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i a/m}$ is the Gauss sum.

Proof. Let $\tau(n,\chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i n a/m}$ be the generalised Gauss sum, so $\tau(1,\chi) = \tau(\chi)$. We have the equality[2] $\tau(n,\chi) = \overline{\chi}(n)\tau(\chi)$. Denoting by f_χ the twist of f by χ, we see that

$$\begin{aligned} f_\chi(z) &= \sum_n \chi(n) a_n e^{2\pi i n z} = \sum_n \left(\frac{\tau(n,\overline{\chi})}{\tau(\overline{\chi})} a_n e^{2\pi i n z} \right) \\ &= \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod m} \overline{\chi}(a) \sum_n a_n e^{2\pi i n(z+a/m)} = \frac{1}{\tau(\overline{\chi})} \sum_{a \bmod m} \overline{\chi}(a) f\left(z + \frac{a}{m}\right). \end{aligned}$$

[2] If $(n,m) = 1$, then it is clear. Otherwise, in order to show equality we have to prove that $\tau(n,\chi) = 0$. Write $m = m'g$, $n = n'g$ with $g = \gcd(n,m)$. Then

$$\tau(n,\chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i n'(a \bmod m')/m'} = \sum_{a \bmod m'} \left(\sum_{\substack{b \bmod m \\ b \equiv a \bmod m'}} \chi(b) \right) e^{2\pi i n' a/m'}$$

and the inner sum is zero for each a (note χ is assumed to be primitive modulo m), proving the claim.

Now $L(E,\chi,1) = L(f_\chi,1) = (-2\pi i)\int_0^{i\infty} f_\chi(z)dz$. Thus, substituting the expression for f_χ found above, using

$$\sum_{a \bmod m} \overline{\chi}(a) \int_0^{i\infty} f\left(z + \frac{a}{m}\right) dz = \overline{\chi}(-1) \sum_{a \bmod m} \overline{\chi}(a) \int_{-a/m}^{i\infty} f(z)dz$$

and the elementary identity $\chi(-1)\tau(\chi)\tau(\overline{\chi}) = m$, we obtain the required result. □

If E has good reduction at p, the modular form f is an eigenform with eigenvalue a_p for the Hecke operator T_p defined by

$$f|_{T_p}(z) = \frac{1}{p}\sum_{a=0}^{p-1} f\left(\frac{z+a}{p}\right) + pf(pz);$$

if E has bad reduction at p, then f is an eigenform for the Atkin operator U_p, defined by

$$f|_{U_p}(z) = \frac{1}{p}\sum_{a=0}^{p-1} f\left(\frac{z+a}{p}\right).$$

Lemma 7.A.2. *Let* $\Lambda(f,\chi) = \sum_{a \bmod m} \chi(a)\left[\frac{a}{m}\right]^{\mathrm{sign}(\chi)}$. *Then*

$$L(f_{\overline{\chi}},1) = \frac{\Omega_E^{\mathrm{sign}(\chi)}}{m}\tau(\overline{\chi})\Lambda(f,\chi).$$

Proof. It suffices to show that the right hand side is equal to the formula for $L(f_{\overline{\chi}},1)$ given in Lemma 7.A.1, with χ replaced by $\overline{\chi}$. By definition of Λ, we have

$$\begin{aligned}
\mathrm{RHS} &= \frac{\tau(\overline{\chi})}{m}\sum_{a \bmod m} \chi(a)\lambda^{\mathrm{sign}(\chi)}\left(\frac{a}{m}\right) \\
&= \frac{\tau(\overline{\chi})}{m}\sum_{a \bmod m} \chi(-a)(-\pi i)\left(\int_{a/m}^{i\infty} f(z)dz + \mathrm{sign}(\chi)\int_{-a/m}^{i\infty} f(z)dz\right) \\
&= (-\pi i)\frac{\tau(\overline{\chi})}{m}\left(\sum_{a \bmod m} \chi(-a)\int_{a/m}^{i\infty} f(z)dz + \sum_{a \bmod m} \chi(a)\int_{-a/m}^{i\infty} f(z)dz\right) \\
&= (-2\pi i)\frac{\tau(\overline{\chi})}{m}\sum_{a \bmod m} \chi(a)\int_{-a/m}^{i\infty} f(z)dz.
\end{aligned}$$

□

Let now $\mathcal{L}_p(E,\alpha,\psi,T)$ be the p-adic L-function defined in Section 7.2 and define the *p-adic multiplier* (see [100, Ch. I, §14])

$$e_p(\alpha,\psi) = \frac{1}{\alpha^k}\left(1 - \frac{\overline{\psi}(p)(1-\delta)}{\alpha}\right)\left(1 - \frac{\psi(p)}{\alpha}\right),$$

where ψ is of conductor p^kM with $(p,M) = 1$ and δ is, as in Section 7.2, equal to zero unless E has bad reduction, in which case it is 1.

Proposition 7.A.3 (Interpolation Property I). *Let ψ be a character of conductor m. Then*

$$\mathcal{L}_p(E,\alpha,\psi,0) = e_p(\alpha,\psi)\cdot\frac{m}{\tau(\overline{\psi})}\cdot\frac{L(E,\overline{\psi},1)}{\Omega_E^{\mathrm{sign}(\psi)}}.$$

Proof. We treat the cases $m=1$ and $m>1$ separately. Assume first that $m=1$, so that ψ is the trivial character. Then

$$\mathcal{L}_p(E,\alpha,0) = \int_{\mathbb{Z}_p^\times} d\mu_\alpha^+ = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times}\mu_\alpha^+(a+p\mathbb{Z}_p) = \sum_{a=1}^{p-1}\left(\frac{1}{\alpha}\left[\frac{a}{p}\right]^+ - \frac{1-\delta}{\alpha^2}[a]^+\right).$$

Since $f(z+n)=f(z)$ for all $n\in\mathbb{Z}$, we have

$$-\frac{1}{\alpha^2}\sum_{a=1}^{p-1}[a]^+ = -\frac{(p-1)}{\alpha^2\Omega_E^+}L(E,1).$$

As for the first sum in $\mathcal{L}_p(E,\alpha,0)$, if E has good reduction at p, we use the following fact

$$\int_0^{i\infty} f|_{T_p}dz = \sum_{a=0}^{p-1}\int_0^{i\infty} f\left(\frac{z+a}{p}\right)\frac{dz}{p} + \int_0^{i\infty} f(pz)pdz = \sum_{a=1}^{p-1}\int_{a/p}^{i\infty} f(z)dz + 2\int_0^{i\infty} f(z)dz,$$

which, combined with $f|_{T_p} = a_p f$, gives

$$\frac{1}{\alpha}\sum_{a=1}^{p-1}\left[\frac{a}{p}\right]^+ = \frac{(a_p-2)}{\alpha\Omega_E^+}L(E,1).$$

Similarly, if E has bad reduction at p, f is an eigenform for U_p with eigenvalue $\alpha=a_p$ and we have $\frac{1}{\alpha}\sum_{a=1}^{p-1}\left[\frac{a}{p}\right]^+ = \frac{(\alpha-1)}{\alpha\Omega_E^+}L(E,1)$. Putting things together and using the fact that, in the good reduction case, $a_p\alpha^{-1}-p\alpha^{-2}=1$, since α is a root of X^2-a_pX+p, we obtain

$$\mathcal{L}_p(E,\alpha,0) = \left(1-\frac{1}{\alpha}\right)^{2-\delta}\frac{L(E,1)}{\Omega_E^+}.$$

Assume now that ψ is non-trivial, of conductor p^kM with $k\geq 1$. Then ψ is a locally constant function on $\mathbb{Z}_{p,M}^\times$ and we can evaluate $\mathcal{L}_p(E,\alpha,\psi,0)$ as a Riemann sum:

$$\begin{aligned}\mathcal{L}_p(E,\alpha,\psi,0) &= \sum_{a\in(\mathbb{Z}/p^kM\mathbb{Z})^\times}\psi(a)\mu_\alpha^{\mathrm{sign}(\psi)}(a+p^kM\mathbb{Z}_{p,M})\\ &= \frac{1}{\alpha^k}\sum_{a\in(\mathbb{Z}/p^kM\mathbb{Z})^\times}\psi(a)\left[\frac{a}{Mp^k}\right]^{\mathrm{sign}(\psi)} - \frac{(1-\delta)}{\alpha^{k+1}}\sum_{a\in(\mathbb{Z}/Mp^k\mathbb{Z})^\times}\psi(a)\left[\frac{a}{Mp^{k-1}}\right]^{\mathrm{sign}(\psi)}.\end{aligned} \tag{7.8}$$

The first term in (7.8) is just $\frac{1}{\alpha^k}\Lambda(f,\psi)$ and we can apply Lemma 7.A.2. As for the second one, note that the integrals appearing in $\left[\frac{a}{Mp^{k-1}}\right]^{\mathrm{sign}(\psi)}$ depend on a modulo Mp^{k-1} only. Indeed, suppose that $b = a + l(Mp^{k-1})$ for some $l \in \mathbb{Z}$. Then

$$\int_{b/Mp^{k-1}}^{i\infty} f(z)dz = \int_{b/Mp^{k-1}}^{i\infty} f(z+l)dz = \int_{a/Mp^{k-1}}^{i\infty} f(z)dz.$$

Thus $\sum_{a\in(\mathbb{Z}/Mp^k\mathbb{Z})^\times} \psi(a)\left[\frac{a}{Mp^{k-1}}\right]^{\mathrm{sign}(\psi)}$ may be rewritten as

$$\frac{(-\pi i)}{\Omega_E^{\mathrm{sign}(\psi)}} \sum_{a=0}^{Mp^{k-1}-1} \left(\sum_{\substack{b=0 \\ b\equiv a(Mp^{k-1})}}^{Mp^k-1} \psi(-b) \right) \left(\int_{a/p^{k-1}}^{i\infty} f(z)dz + \mathrm{sign}(\psi) \int_{-a/p^{k-1}}^{i\infty} f(z)dz \right).$$

Now $\sum_{\substack{b=0 \\ b\equiv a(Mp^{k-1})}}^{p^k-1} \psi(-b) = 0$ for each a. Indeed, for each $(n, Mp^k) = 1$, $n \equiv 1 \bmod Mp^{k-1}$, we have

$$\psi(n) \sum_{\substack{b=0 \\ b\equiv a(Mp^{k-1})}}^{Mp^k-1} \psi(-b) = \sum_{\substack{b=0 \\ b\equiv a(Mp^{k-1})}}^{Mp^k-1} \psi(-nb) = \sum_{\substack{b=0 \\ b\equiv a(Mp^{k-1})}}^{Mp^k-1} \psi(-b)$$

and since $\psi(n)$ cannot be 1 for all such n (otherwise ψ would not be primitive modulo Mp^k [2, Theorem 8.16]), this implies the claim, which, in turn, completes the proof when $k \geq 1$.

Finally, we treat the case when ψ is non-trivial of conductor M, where M is coprime with p. We then have

$$\mathcal{L}_p(E,\alpha,\psi,0) = \sum_{\substack{a \bmod M \\ (a,M)=1}} \int_{\mathbb{Z}_{p,M}^\times \cap (a+M\mathbb{Z}_{p,M})} \psi(x) d\mu_\alpha^{\mathrm{sign}(\psi)}.$$

The intersection $\mathbb{Z}_{p,M}^\times \cap (a + M\mathbb{Z}_{p,M})$ is equal to $(a + M\mathbb{Z}_{p,M}) - (pap' + pM\mathbb{Z}_{p,M})$, where $pp' \equiv 1 \mod M$. Therefore,

$$\mathcal{L}_p(E,\alpha,\psi,0) = \sum_{a \bmod M} \psi(a)(\mu_\alpha^{\mathrm{sign}(\psi)}(a + M\mathbb{Z}_{p,M}) - \mu_\alpha^{\mathrm{sign}(\psi)}(pap' + pM\mathbb{Z}_{p,M}))$$

and, using Lemma 7.A.2 repeatedly, we get the right interpolation. □

Let χ be a character of $\mathrm{Gal}(\mathbb{Q}^n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ such that χ does not factor through $\mathrm{Gal}(\mathbb{Q}^{n-1}/\mathbb{Q})$. Through the identification $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}$, we can regard χ as a Dirichlet character of conductor p^{n+1} which is trivial on the $\mathbb{Z}/(p-1)\mathbb{Z}$

part. Moreover, since χ does not factor through lower layers in the $\mathbb{Z}_p$-cyclotomic tower, χ must send a generator of $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ to a primitive p^n-th root of unity. Since all elements of $\mathbb{Z}/p^n\mathbb{Z}$ have odd order, $-1 \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ has trivial $\mathbb{Z}/p^n\mathbb{Z}$-component through the above isomorphism, so $\chi(-1) = 1$.

By a slight abuse of notation, we may rephrase this by saying that $\chi\colon \mathbb{Z}_p^\times \to \mathbb{C}_p^\times$ is the p-adic character defined by $\chi(\kappa(\gamma)) = \zeta$, where ζ is a root of unity of exact order p^n, and $\chi(x) = \chi(\langle x\rangle)$ (here κ is, as before, the cyclotomic character).

The converse is also true, i.e. given ζ, there is a unique character of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, that factors through $\mathrm{Gal}(\mathbb{Q}^n/\mathbb{Q})$, and such that $\chi(\kappa(\gamma)) = \zeta$.

Proposition 7.A.4 (Interpolation Property II). *Let ζ be a primitive p^n-th root of unity, for some $n \geq 1$, and let ψ be of conductor m. Then*

$$\mathcal{L}_p(E, \alpha, \psi, \zeta - 1) = e_p(\alpha, \chi\psi)\frac{\mathfrak{f}}{\tau(\overline{\chi}\overline{\psi})} \cdot \frac{L(E, \overline{\chi}\overline{\psi}, 1)}{\Omega_E^{\mathrm{sign}(\psi)}},$$

where χ is the Dirichlet character of conductor p^{n+1} described above and $\mathfrak{f}$ is the conductor of $\chi\psi$.

Proof. We have

$$\mathcal{L}_p(E, \alpha, \psi, \zeta - 1) = \int_{\mathbb{Z}_{p,M}^\times} \psi(x)\zeta^{\frac{\log\langle x\rangle}{\log\kappa(\gamma)}} d\mu_\alpha(x) = \int_{\mathbb{Z}_{p,M}^\times} \psi(x)\chi(x) d\mu_\alpha(x).$$

Now, as shown above, the sign of χ is $+1$ so that $\chi\psi$ has the same sign as ψ and then the proof is the same as the proof of Proposition 7.A.3 with ψ replaced by $\chi\psi$. □

Remark 7.A.5. In Section 7.5 we defined the p-adic L-function of the base change of E to an abelian number field K, disjoint from the cyclotomic tower of $\mathbb{Q}$, and such that the additive primes of $E/\mathbb{Q}$ remain additive over K, as a product of twisted p-adic L-functions of $E/\mathbb{Q}$. Let K^∞ be the cyclotomic $\mathbb{Z}_p$-extension of K and let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \overline{\mathbb{Q}}$ be the character which factors through the n-th layer K^n of the cyclotomic tower of K and maps a topological generator for $\mathrm{Gal}(K^\infty/K)$ to a p^n-th root of unity ζ. By inductivity in the Artin formalism, the twisted complex L-function $L(E/K, \rho, s)$ is equal to $L(E/\mathbb{Q}, \mathrm{Ind}_K^{\mathbb{Q}}\rho, s)$, where $\mathrm{Ind}_K^{\mathbb{Q}}\rho$ is the $[K\colon \mathbb{Q}]$-dimensional representation obtained by inducing ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let χ be the character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sending a topological generator of $\mathrm{Gal}(\mathbb{Q}^\infty/\mathbb{Q})$ to ζ. Then, by Frobenius reciprocity, $\mathrm{Ind}_K^{\mathbb{Q}}\rho = \oplus_\psi \chi\psi$, where the sum is over all irreducible characters of $\mathrm{Gal}(K/\mathbb{Q})$ (inflated to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). Additivity in the Artin formalism and

Proposition 7.A.4 then show that

$$\mathcal{L}_p(E/K,\alpha,\zeta-1)=\left(\prod_{\psi\in\widehat{\mathrm{Gal}(K/\mathbb{Q})}}\frac{e_p(\alpha,\chi\psi)}{\Omega_E^{\mathrm{sign}(\psi)}}\frac{\mathfrak{f}_\psi}{\tau(\bar{\chi}\bar{\psi})}\right)\cdot L(E/K,\bar{\rho},1),$$

where $\mathfrak{f}_\psi$ is the conductor of $\chi\psi$.

7.B The functional equation

We provide a proof of the functional equation for $\mathcal{L}_p(E,\alpha,\psi,T)$ in the case when the conductor of ψ and the conductor N of E are coprime, and p is a prime of good ordinary reduction. As in Section 7.4, we may omit α from the notation as it is completely determined. We use Proposition 7.A.4 and the functional equation satisfied by the complex L-function of E twisted by characters to relate values of $\mathcal{L}_p(E,\psi,T)$ and of $\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)$.

For a Dirichlet character ρ of conductor $\mathfrak{f}$ coprime to N, define the completed L-function

$$\Lambda(E,\rho,s)=\left(\frac{\mathfrak{f}\sqrt{N}}{2\pi}\right)^s\Gamma(s)L(E,\rho,s),$$

where $\Gamma(s)$ is the gamma function. Then $\Lambda(E,\rho,s)$ satisfies the functional equation (see [119, Theorem 3.66])

$$\Lambda(E,\rho,s)=\mathfrak{f}^{-1}w_E\rho(N)\tau(\rho)^2\Lambda(E,\overline{\rho},2-s);$$

here $w_E=\pm1$ is determined by $w_N(f)=-w_Ef$, where

$$w_N(f)=f|_{\left(\begin{smallmatrix}0&-1\\N&0\end{smallmatrix}\right)}(z)=\frac{1}{Nz^2}f\left(-\frac{1}{Nz}\right).$$

This gives a relation between the central values $L(E,\rho,1)$ and $L(E,\overline{\rho},1)$, which reads as follows

$$L(E,\rho,1)=\mathfrak{f}^{-1}w_E\rho(N)\tau(\rho)^2L(E,\overline{\rho},1). \tag{7.9}$$

With the notation of Proposition 7.A.4 and by (7.9) with $\rho=\overline{\chi}\overline{\psi}$, we have

$$\mathcal{L}_p(E,\psi,T)\big|_{T=\zeta-1}=e_p(\chi\psi)w_E\tau(\overline{\chi}\overline{\psi})\overline{\chi}\overline{\psi}(N)\cdot\frac{L(E,\chi\psi,1)}{\Omega_E^{\mathrm{sign}(\psi)}},$$

which, using the elementary identity $\tau(\overline{\chi}\overline{\psi})=\frac{\mathfrak{f}}{\tau(\chi\psi)}\cdot\overline{\chi}\overline{\psi}(-1)$, where $\mathfrak{f}$ is the conductor of $\chi\psi$, and Proposition 7.A.4 again, yields

$$\mathcal{L}_p(E,\psi,T)\big|_{T=\zeta-1}=w_E\cdot\overline{\chi}\overline{\psi}(-N)\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)\big|_{T=\zeta-1}. \tag{7.10}$$

Since $\overline{\chi}(-N) = \overline{\chi}(N) = \overline{\chi}(\langle N\rangle) = (\overline{\chi}(\kappa(\gamma)))^{\frac{\log\langle N\rangle}{\log\kappa(\gamma)}} = \zeta^{-\frac{\log\langle N\rangle}{\log\kappa(\gamma)}} = (1+T)^{-\frac{\log\langle N\rangle}{\log\kappa(\gamma)}}\big|_{T=\zeta-1}$ we may rewrite (7.10) as

$$\mathcal{L}_p(E,\psi,T)\big|_{T=\zeta-1} = w_E\cdot\overline{\psi}(-N)(1+T)^{-\frac{\log\langle N\rangle}{\log\kappa(\gamma)}}\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)\big|_{T=\zeta-1}.$$

Now let $g(T) = \mathcal{L}_p(E,\psi,T) - w_E\overline{\psi}(-N)(1+T)^{-\frac{\log\langle N\rangle}{\log\kappa(\gamma)}}\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)$. Then we have just shown that $g(T)\in\mathbb{Z}_p[\psi][[T]]$ has infinitely many zeros of p-adic absolute value strictly less than 1. Thus, by the p-adic Weierstrass Preparation Theorem, $g(T)$ must be identically zero, that is, we have proved the following proposition.

Proposition 7.B.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, p an odd prime of good ordinary reduction for E and ψ a character of conductor coprime to N. Then*

$$\mathcal{L}_p(E,\psi,T) = w_E\cdot\overline{\psi}(-N)(1+T)^{-\frac{\log\langle N\rangle}{\log\kappa(\gamma)}}\mathcal{L}_p(E,\overline{\psi},(1+T)^{-1}-1)$$

as power series in T.

Corollary 7.B.2 (Functional equation). *With the assumptions as in Proposition 7.B.1, $L_p(E,\psi,s)$ satisfies the following functional equation*

$$L_p(E,\psi,2-s) = w_E\cdot\overline{\psi}(-N)\langle N\rangle^{s-1}L_p(E,\overline{\psi},s).$$

7.C Statement of p-adic BSD

We state the p-adic analogue of the Birch and Swinnerton-Dyer conjecture formulated in [100]. We choose to give the formula for $\mathcal{L}_p$ rather than L_p and restrict to the good ordinary case, since we have not defined the p-adic regulator in the multiplicative setting. Given an elliptic curve $E/\mathbb{Q}$ with good ordinary reduction at p, let Reg_p be its p-adic regulator, defined as in (2.10) of Chapter 2. Let $Ш_{E/\mathbb{Q}}$ be the Tate–Shafarevich group, c_q the Tamagawa number at the prime q, r the algebraic rank of $E(\mathbb{Q})$ and

$$r^{\mathrm{an}} := \mathrm{ord}_{T=0}\,\mathcal{L}_p(E,T).$$

Also note that

$$e_p := e_p(\alpha) = \left(1-\frac{1}{\alpha}\right)^2.$$

Conjecture 7.C.1 (Mazur–Tate–Teitelbaum). *Let E be an elliptic curve with good ordinary reduction at the odd prime p. Then*

(i) $r^{\mathrm{an}} = r$.

(ii) Moreover,

$$\lim_{T\to 0} T^{-r^{\mathrm{an}}} \mathcal{L}_p(E,T) = e_p \cdot \frac{\prod_q c_q \cdot \#Ш_{E/\mathbb{Q}}}{\#E(\mathbb{Q})^2_{\mathrm{tors}}} \cdot \frac{\mathrm{Reg}_p}{\log(\kappa(\gamma))^r}.$$

By Proposition 7.A.3, if $r = 0$, then Conjecture 7.C.1 is equivalent to the classical Birch and Swinnerton-Dyer Conjecture. If $r \geq 1$, however, the conjectures are different. Schneider [117] and Perrin-Riou [110] showed that the analogous statement to Conjecture 7.C.1 holds[3] for the *algebraic* p-adic L-function of $E/\mathbb{Q}$, provided that $\#Ш_{E/\mathbb{Q}} < \infty$ and $\mathrm{Reg}_p \neq 0$. The Main Conjecture of Iwasawa Theory for elliptic curves then implies Conjecture 7.C.1 (i) and Conjecture 7.C.1 (ii) up to a p-adic unit. Many cases of the Main Conjecture are known, for instance thanks to work of Kato [72] and Skinner–Urban [129].

[3]Strictly speaking, the analogue of (ii) can only be formulated up to multiplication by a p-adic unit.

Bibliography

[1] Y. Amice and J. Vélu. Distributions p-adiques associées aux séries de Hecke. In *Journées arithmétiques de Bordeaux*, number 24–25 in Astérisque, pages 119–131. Soc. Math. France, Paris, 1975.

[2] T. M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1976.

[3] S. Arms, Á. Lozano-Robledo, and S. J. Miller. Constructing one-parameter families of elliptic curves with moderate rank. *J. Number Theory*, 123(2):388–402, 2007.

[4] A. O. L. Atkin and W. W. Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[5] J. S. Balakrishnan. Explicit p-adic methods for elliptic and hyperelliptic curves. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 260–285. IOS, Amsterdam, 2015.

[6] J. S. Balakrishnan. On 3-adic heights on elliptic curves. *J. Number Theory*, 161:119–134, 2016.

[7] J. S. Balakrishnan and A. Besser. Coleman-Gross height pairings and the p-adic sigma function. *J. Reine Angew. Math.*, 698:89–104, 2015.

[8] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller. Explicit quadratic Chabauty over number fields. *arXiv:1910.04653*, 2019.

[9] J. S. Balakrishnan, A. Besser, and J. S. Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.*, 720:51–79, 2016.

[10] J. S. Balakrishnan, A. Besser, and J. S. Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86(305):1403–1434, 2017.

[11] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski. Chabauty–Coleman experiments for genus 3 hyperelliptic curves. In *Research Directions in Number Theory*, Women in Numbers IV, to appear.

[12] J. S. Balakrishnan, F. Bianchi, V. Cantoral-Farfán, M. Çiperiani, and A. Etropolski. SageMath code. *https://github.com/jbalakrishnan/WIN4*.

[13] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory (ANTS-IX)*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010.

[14] J. S. Balakrishnan, M. Çiperiani, J. Lang, B. Mirza, and R. Newton. Shadow lines in the arithmetic of elliptic curves. In *Directions in Number Theory*, volume 3 of *Assoc. Women Math. Ser.*, pages 33–55. Springer, Cham, 2016.

[15] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.*, 372(1-2):369–428, 2018.

[16] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. With an appendix by J. S. Müller.

[17] J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *arXiv:1705.00401*, 2018.

[18] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty—Kim for the split Cartan modular curve of level 13. *Ann. of Math.*, 189(3):885–944, 2019.

[19] J. S. Balakrishnan, K. S. Kedlaya, and M. Kim. Appendix and erratum to "Massey products for elliptic curves of rank 1". *J. Amer. Math. Soc.*, 24(1):281–291, 2011.

[20] J. S. Balakrishnan and J. Tuitman. Magma code. *https://github.com/jtuitman/Coleman*.

[21] J. S. Balakrishnan and J. Tuitman. Explicit Coleman integration for curves. *arXiv:1710.01673*, 2017.

[22] D. Bernardi. Hauteur p-adique sur les courbes elliptiques. In *Séminaire de Théorie des Nombres, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 1–14. Birkhäuser, Boston, Mass., 1981.

[23] D. Bernardi and B. Perrin-Riou. Variante p-adique de la conjecture de Birch et Swinnerton-Dyer (le cas supersingulier). *C.R. Acad. Sci. Paris Sér. I Math.*, 317(3):227–232, 1993.

[24] D. Bertrand. Valeurs de fonctions thêta et hauteurs p-adiques. In *Séminaire de Théorie des Nombres, Paris 1980-81*, volume 22 of *Progr. Math.*, pages 1–12. Birkhäuser, Boston, Mass., 1982.

[25] A. Besser. Coleman integration using the Tannakian formalism. *Math. Ann.*, 322(1):19–48, 2002.

[26] A. Besser. The p-adic height pairings of Coleman-Gross and of Nekovář. In *Number theory*, volume 36 of *CRM Proc. Lecture Notes*, pages 13–25. Amer. Math. Soc., Providence, RI, 2004.

[27] A. J. Best. Explicit Coleman integration in larger characteristic. In *Proceedings of ANTS XIII*, to appear.

[28] S. Bettin, C. David, and C. Delaunay. Non-isotrivial elliptic surfaces with non-zero average root number. *J. Number Theory*, 191:1–84, 2018.

[29] F. Bianchi. SageMath code. *https://github.com/bianchifrancesca/quadratic_chabauty*.

[30] F. Bianchi. Consequences of the functional equation of the p-adic l-function of an elliptic curve. *Funct. Approx. Comment. Math.*, 2018. Advance publication.

[31] F. Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture. *arXiv:1904.04622*, 2019.

[32] H. Billard. Sur la répartition des points rationnels de surfaces elliptiques. *J. Reine Angew. Math.*, 505:45–71, 1998.

[33] S. Bloch. A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 58(1):65–76, 1980.

[34] A. Booker, D. Platt, J. Sijsling, and A. V. Sutherland. Genus 3 hyperelliptic curves. *http://math.mit.edu/~drew/lmfdb_genus3_hyperelliptic.txt*.

[35] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight, and D. Yasaki. A database of genus-2 curves over the rational numbers. *LMS J. Comput. Math.*, 19(suppl. A):235–254, 2016.

[36] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[37] N. Bruin and M. Stoll. Deciding existence of rational points on curves: An experiment. *Experiment. Math.*, 17(2):181–189, 2008.

[38] N. Bruin and M. Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010.

[39] A. Brumer. On the units of algebraic number fields. *Mathematika*, 14:121–124, 1967.

[40] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[41] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C.R. Acad. Sci. Paris*, 212:882–885, 1941.

[42] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[43] R. F. Coleman. Torsion points on curves and p-adic abelian integrals. *Ann. of Math. (2)*, 121(1):111–168, 1985.

[44] R. F. Coleman. The universal vectorial bi-extension and p-adic heights. *Invent. Math.*, 103(3):631–650, 1991.

[45] R. F. Coleman and E. de Shalit. p-adic regulators on curves and special values of p-adic L-functions. *Invent. Math.*, 93(2):239–266, 1988.

[46] R. F. Coleman and B. H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, Mass., 1989.

[47] P. Colmez. La conjecture de Birch et Swinnerton-Dyer p-adique. In *Séminaire Bourbaki : volume 2002/2003, exposés 909-923*, number 294 in Astérisque, pages 251–319. Soc. Math. France, Paris, 2004.

[48] I. Connell. Elliptic Curve Handbook. `http://webs.ucm.es/BUCM/mat/doc8354.pdf`, February 1999.

[49] K. Conrad. A multivariable Hensel's lemma. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`.

[50] K. Conrad. Infinite series in p-adic fields. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/infseriespadic.pdf`.

[51] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[52] D. A. Cox and S. Zucker. Intersection numbers of sections of elliptic surfaces. *Invent. Math.*, 53(1):1–44, 1979.

[53] J. E. Cremona. Numerical evidence for the Birch—Swinnerton-Dyer conjecture. `http://homepages.warwick.ac.uk/staff/J.E.Cremona/papers/bsd50.pdf`.

[54] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[55] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[56] N. Dogra. Unlikely intersections and the Chabauty-Kim method over number fields. *arXiv:1903.05032*, 2019.

[57] E. V. Eikenberg. *Rational points on some families of elliptic curves*. ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–University of Maryland, College Park.

[58] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[59] G. Faltings. Erratum: "Finiteness theorems for abelian varieties over number fields". *Invent. Math.*, 75(2):381, 1984.

[60] E. V. Flynn. A flexible method for applying Chabauty's theorem. *Compositio Math.*, 105(1):79–94, 1997.

[61] E. V. Flynn and J. L. Wetherell. Finding rational points on bielliptic genus 2 curves. *Manuscripta Math.*, 100(4):519–533, 1999.

[62] F. Q. Gouvêa. *p-adic numbers: An Introduction*. Universitext. Springer-Verlag, Berlin, 1993.

[63] D. Grant. On an analogue of the Lutz-Nagell theorem for hyperelliptic curves. *J. Number Theory*, 133(3):963–969, 2013.

[64] R. Greenberg. Introduction to Iwasawa theory for elliptic curves. In *Arithmetic algebraic geometry*, volume 9 of *IAS/Park City Math. Ser.*, pages 407–464. Amer. Math. Soc., Providence, RI, 2001.

[65] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[66] M. C. Harrison. An extension of Kedlaya's algorithm for hyperelliptic curves. *J. Symbolic Comput.*, 47(1):89–101, 2012.

[67] D. Harvey. Efficient computation of p-adic heights. *LMS J. Comput. Math.*, 11:40–59, 2008.

[68] D. Harvey and A. V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II. In *Frobenius distributions: Lang-Trotter and Sato-Tate conjectures*, volume 663 of *Contemp. Math.*, pages 127–147. Amer. Math. Soc., Providence, RI, 2016.

[69] H. A. Helfgott. *Root numbers and the parity problem*. ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–Princeton University.

[70] H. Hubrechts. *Elliptic and hyperelliptic curve point counting through deformation*. PhD thesis, Katholieke Universiteit Leuven, 2007.

[71] H. Hubrechts. Point counting in families of hyperelliptic curves. *Found. Comput. Math.*, 8(1):137–169, 2008.

[72] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. In *Cohomologies p-adiques et applications arithmétiques. III*, number 295 in Astérisque, pages ix, 117–290. Soc. Math. France, Paris, 2004.

[73] N. M. Katz. p-adic properties of modular schemes and modular forms. In *Modular Functions of One Variable III*, volume 350 of *Lecture Notes in Mathematics*, pages 69–190. Springer, Berlin, 1973.

[74] N. M. Katz. p-adic interpolation of real analytic Eisenstein series. *Ann. of Math. (2)*, 104(3):459–571, 1976.

[75] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[76] K. S. Kedlaya. Computing zeta functions via p-adic cohomology. In *Algorithmic number theory (ANTS-VI)*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 1–17. Springer, Berlin, 2004.

[77] K. S. Kedlaya. p-adic cohomology: from theory to practice. In *p-adic geometry*, volume 45 of *Univ. Lecture Ser.*, pages 175–203. Amer. Math. Soc., Providence, RI, 2008.

[78] M. Kim. The motivic fundamental group of $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[79] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[80] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010.

[81] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1984.

[82] V. A. Kolyvagin. Finiteness of $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[83] F.-V. Kuhlmann. Maps on ultrametric spaces, Hensel's lemma, and differential equations over valued fields. *Comm. Algebra*, 39(5):1730–1776, 2011.

[84] E. E. Kummer. Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.*, 44:93–146, 1852.

[85] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[86] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[87] A. G. B. Lauder. Counting solutions to equations in many variables over finite fields. *Found. Comput. Math.*, 4(3):221–267, 2004.

[88] A. G. B. Lauder. Deformation theory and the computation of zeta functions. *Proc. London Math. Soc. (3)*, 88(3):565–602, 2004.

[89] H.-W. Leopoldt. Zur Arithmetik in abelschen Zahlkörpern. *J. Reine Angew. Math.*, 209:54–71, 1962.

[90] The LMFDB Collaboration. The L-functions and Modular forms database (2018), 2018. `http://lmfdb.org`.

[91] Ju. I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.

[92] Ju. I. Manin. Parabolic points and zeta functions of modular curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 36:19–66, 1972.

[93] K. Matsuno. An analogue of Kida's formula for the p-adic L-functions of modular elliptic curves. *J. Number Theory*, 84(1):80–92, 2000.

[94] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44(2):129–162, 1978. With an appendix by D. Goldfeld.

[95] B. Mazur. Modular curves and arithmetic. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983)*, pages 185–211. PWN, Warsaw, 1984.

[96] B. Mazur, W. Stein, and J. Tate. Computation of p-adic heights and log convergence. *Doc. Math.*, (Extra Vol.):577–614, 2006.

[97] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[98] B. Mazur and J. Tate. Canonical height pairings via biextensions. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 195–237. Birkhäuser, Boston, Mass., 1983.

[99] B. Mazur and J. Tate. The p-adic sigma function. *Duke Math. J.*, 62(3):663–688, 1991.

[100] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.

[101] W. McCallum and B. Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[102] J. S. Milne. Jacobian varieties. In *Arithmetic geometry*, pages 167–212. Springer-Verlag, New York, 1986.

[103] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922.

[104] M. R. Murty and V. K. Murty. *Non-vanishing of L-functions and applications*, volume 157 of *Progr. Math.* Birkhäuser Verlag, Basel, 1997.

[105] K. Nagao. $\mathbf{Q}(T)$-rank of elliptic curves and certain limit coming from the local points. *Manuscripta Math.*, 92(1):13–32, 1997. With an appendix by N. Ishida, T. Ishikawa and the author.

[106] A. Néron. Quasi-fonctions et hauteurs sur les variétés abéliennes. *Ann. of Math. (2)*, 82(2):249–331, 1965.

[107] A. Néron. Fonctions thêta p-adiques et hauteurs p-adiques. In *Séminaire de Théorie des Nombres, Paris 1980-81*, volume 22 of *Progr. Math.*, pages 149–174. Birkhäuser, Boston, Mass., 1982.

[108] K. Oguiso and T. Shioda. The Mordell-Weil lattice of a rational elliptic surface. *Comment. Math. Univ. St. Paul.*, 40(1):83–99, 1991.

[109] J. Paulhus. Decomposing Jacobians of curves with extra automorphisms. *Acta Arith.*, 132(3):231–244, 2008.

[110] B. Perrin-Riou. Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe. *Invent. Math.*, 70(3):369–398, 1982/83.

[111] B. Perrin-Riou. Hauteurs p-adiques. In *Séminaire de Théorie des Nombres, Paris 1982–83*, volume 51 of *Progr. Math.*, pages 233–257. Birkhäuser, Boston, Mass., 1984.

[112] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[113] M. Rosen and J. H. Silverman. On the rank of an elliptic surface. *Invent. Math.*, 133(1):43–67, 1998.

[114] C. Salgado. On the rank of the fibers of rational elliptic surfaces. *Algebra Number Theory*, 6(7):1289–1314, 2012.

[115] N. Schappacher. Diophantus of Alexandria : a Text and its History. `http://irma.math.unistra.fr/~schappa/NSch/Publications_files/1998cBis_Dioph.pdf`.

[116] P. Schneider. p-adic height pairings. I. *Invent. Math.*, 69(3):401–409, 1982.

[117] P. Schneider. p-adic height pairings. II. *Invent. Math.*, 79(2):329–374, 1985.

[118] M. Schütt and T. Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[119] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[120] T. Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990.

[121] C. L. Siegel. Über einige Anwendungen Diophantischer Approximationen. *Abh. Preus. Acad. Wiss.*, 1, 01 1929.

[122] S. Siksek. Explicit Chabauty over number fields. *Algebra Number Theory*, 7(4):765–793, 2013.

[123] J. H. Silverman. Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.

[124] J. H. Silverman. Computing heights on elliptic curves. *Math. Comp.*, 51(183):339–358, 1988.

[125] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[126] J. H. Silverman. The average rank of an algebraic family of elliptic curves. *J. Reine Angew. Math.*, 504:227–236, 1998.

[127] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[128] C. Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. *arXiv:1405.7294*, 2014.

[129] C. Skinner and E. Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[130] N. P. Smart. S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 116(3):391–399, 1994.

[131] W. Stein et al. *Sage Mathematics Software (Version 7.5.1 and later, up to 8.8)*. The Sage Development Team, 2017-2019. `http://www.sagemath.org`.

[132] W. Stein and C. Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Math. Comp.*, 82(283):1757–1792, 2013.

[133] M. Stoll. Finite descent obstructions and rational points on curves. *Algebra Number Theory*, 1(4):349–391, 2007. version of `http://www.mathe2.uni-bayreuth.de/stoll/papers/covers8.pdf`.

[134] M. Stoll. Finite descent obstructions and rational points on curves. *Algebra Number Theory*, 1(4):349–391, 2007.

[135] M. Stoll. Arithmetic of Hyperelliptic Curves. *Lecture notes Summer Semester, University of Bayreuth*, 2014. `http://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2014/Skript-ArithHypCurves-pub-screen.pdf`.

[136] R. J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.*, 67(2):177–196, 1994.

[137] P. Tadić. On the family of elliptic curves $Y^2 = X^3 - T^2X + 1$. *Glas. Mat. Ser. III*, 47(67)(1):81–93, 2012.

[138] Y. Tian. Lectures on algebraic number theory. `http://www.mcm.ac.cn/faculty/tianyichao/201409/W020140919372982540194.pdf`.

[139] N. Triantafillou. *Restriction of Scalars, the Chabauty-Coleman Method, and* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$. PhD thesis, MIT, 2019.

[140] M. van der Put. The cohomology of Monsky and Washnitzer. In *Introductions aux cohomologies p-adiques (Luminy, 1984)*, number 23, pages 4, 33–59. Mém. Soc. Math. France (N.S.), 1986.

[141] M.-F. Vignéras. Valeur au centre de symétrie des fonctions L associées aux formes modulaires. In *Séminaire de Théorie des Nombres, Paris 1979-80*, volume 12 of *Progr. Math.*, pages 331–356. Birkhäuser, Boston, Mass., 1981.

[142] M. M. Višik. Nonarchimedean measures associated with Dirichlet series. *Mat. Sb. (N.S.)*, 99(141)(2):248–260, 296, 1976.

[143] M. Waldschmidt. On the p-adic closure of a subgroup of rational points on an Abelian variety. *Afr. Mat.*, 22(1):79–89, 2011.

[144] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

[145] J. L. Wetherell. *Bounding the number of rational points on certain curves of high rank*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley.

[146] C. Wuthrich. On p-adic heights in families of elliptic curves. *J. London Math. Soc. (2)*, 70(1):23–40, 2004.

[147] C. Wuthrich. On the integrality of modular symbols and Kato's Euler system for elliptic curves. *Doc. Math.*, 19:381–402, 2014.

[148] C. Wuthrich. The sub-leading coefficient of the L-function of an elliptic curve. *Publ. Math. Besançon Algèbre Théorie Nr*, 2016:95–96, 2017.

[149] W. Zhang. Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.*, 2(2):191–253, 2014.