Coleman Integration for Hyperelliptic Curves: Algorithms and Applications

by

Jennifer Sayaka Balakrishnan

A.B., Harvard University (2006)
A.M., Harvard University (2006)

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2011

Author ....
Department of Mathematics
April 26, 2011

Certified by ....
Kiran S. Kedlaya
Associate Professor
Thesis Supervisor

Accepted by ....
Bjorn Poonen
Chairman, Department Committee on Graduate Theses

Coleman Integration for Hyperelliptic Curves: Algorithms and Applications

by

Jennifer Shyamala Sayaka Balakrishnan

Submitted to the Department of Mathematics
on April 26, 2011, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

The Coleman integral is a p-adic line integral that can be used to encapsulate several quantities relevant to a study of the arithmetic of varieties. In this thesis, I describe algorithms for computing Coleman integrals on hyperelliptic curves and discuss some immediate applications. I give algorithms to compute single and iterated integrals on odd models of hyperelliptic curves, as well as the necessary modifications to implement these algorithms for even models. Furthermore, I show how these algorithms can be used in various situations. The first application is the method of Chabauty to find rational points on curves of genus greater than 1. The second is Minhyong Kim's recent nonabelian analogue of the Chabauty method for elliptic curves. The last two applications concern p-adic heights on Jacobians of hyperelliptic curves, necessary to formulate a p-adic analogue of the Birch and Swinnerton-Dyer conjecture. I conclude by stating the analogue of the Mazur-Tate-Teitelbaum conjecture in our setting and presenting supporting data.

Thesis Supervisor: Kiran S. Kedlaya
Title: Associate Professor

Acknowledgments

It is a pleasure to thank my advisor, Kiran Kedlaya, for his support of the efforts that went into this thesis. He has been incredibly generous with his time and ideas, patiently answering my numerous questions, suggesting many interesting problems, and encouraging several collaborations. One such collaboration led to the results in Chapter 3, which form the backbone of this thesis.

I would also like to thank a few others who have had a direct impact on this thesis. During my first year in college, I happened to take a seminar with William Stein, who introduced me to computational approaches in number theory. Over the years, we have worked on a few things together – most recently, a portion of the material that forms Chapter 9 of this thesis. Special thanks must also go out to two of my coauthors, Minhyong Kim and Amnon Besser, who kindly explained their work to me; collaborations with them led to Chapters 7 and 8, respectively, of this thesis. Thanks are also due to Barry Mazur, Bjorn Poonen, Alice Silverberg, Michael Stoll, Drew Sutherland, and Liang Xiao, for several productive discussions, and Robert Bradshaw and David Roe for laying much of the p-adic groundwork in Sage.

I must also thank Steffen Müller for visiting MIT last summer and carefully computing (and recomputing) many things in Magma, despite the many ill-posed queries I came up with during the process. It would have been impossible to assemble the data in Chapter 9 without his efforts. Repeating names, I would also like to thank Bjorn Poonen, Abhinav Kumar, and Kiran Kedlaya for agreeing to serve on my thesis committee, William Stein for access to his cluster of computers (chief among them {`mod,boxen,sage`}`.math.washington.edu`, funded by NSF grant DMS-0821725), and Kiran Kedlaya for access to `dwork.mit.edu`.

Finally, to my dear friends and family, thank you for your love, laughter, and support throughout the years. Kartik and Liz, I have thoroughly enjoyed our adventures in baking and ballet. And above all, Bala, Shizuko, Stephanie, and Vivek, thank you for always cheering me on, regardless of the time or time zone.

This research was supported by the National Science Foundation Graduate Research Fellowship and the National Defense Science and Engineering Graduate Fellowship.

For those in Yamada,
especially my grandmother Fumiko

Contents

1 Introduction **15**

1.0.1 Why hyperelliptic curves? 15

1.0.2 Beyond hyperelliptic curves? 16

1.0.3 Outline 16

2 Hyperelliptic curves and p-adic cohomology **19**

2.1 Hyperelliptic curves 19

2.2 p-adic cohomology 21

2.2.1 Frobenius 23

2.2.2 Kedlaya's algorithm 23

3 Coleman integration: the basic integrals **27**

3.1 Coleman's theory of p-adic integration 27

3.2 Explicit integrals for hyperelliptic curves 29

3.2.1 A basis for de Rham cohomology 30

3.2.2 Tiny integrals 30

3.2.3 Non-Weierstrass disks 31

3.2.4 Weierstrass endpoints of integration 34

3.3 Implementation notes and precision 36

3.3.1 Precision estimates 36

3.3.2 Complexity analysis 37

3.3.3 Numerical examples 38

4 Coleman integration: even degree models **41**

4.1 Introduction 41

4.2 A bit more p-adic cohomology 41

4.3 Coleman integration on even models 42

4.3.1 Local coordinates 42

4.3.2 Integrals 42

4.3.3 Using the linear system 44

5 Coleman integration: iterated integrals **47**

5.1 Introduction 47

5.2 Iterated path integrals 48

5.3 Tiny iterated integrals 50

5.3.1 Examples 51

5.4 Iterated integrals: linear system 55

5.5 Explicit double integrals 56

5.5.1 Tiny double integrals 56

5.5.2 The linear system for double integrals between Teichmüller points 57

5.5.3 Linking double integrals 59

5.5.4 Without Teichmüller points 60

5.5.5 Weierstrass points 62

5.6 Future work 65

5.6.1 Tangential basepoint at infinity 66

5.6.2 The fundamental linear system 66

5.6.3 The region of convergence in a Weierstrass disk 66

6 Explicit computations with the Chabauty method 67

6.1 Introduction 67

6.2 Explicit integrals to a parameter 69

6.3 Example: odd model 70

6.4 Future work 71

7 Kim's nonabelian Chabauty method 73

7.1 Introduction: the method 73

7.1.1 Elliptic curves 73

7.2 A few more explicit double integrals 74

7.2.1 Integrals to a parameter z 74

7.2.2 Double integrals to a parameter z 74

7.3 Carrying out the nonabelian Chabauty method 76

7.3.1 An example with 65A 77

7.3.2 An example with 37A 78

7.4 Connection to p-adic heights 80

7.5 Future work 81

7.5.1 Tangential basepoint 81

7.5.2 Tamagawa number hypothesis 81

8 p-adic heights on Jacobians of hyperelliptic curves 83

8.1 Introduction 83

8.2 The p-adic height pairing 84

8.3 Hyperelliptic curves 89

8.4 Coleman integrals 90

8.4.1 Generalities on Coleman integrals and symbols 90

8.4.2 Integration of forms with poles outside Weierstrass discs . . . 90

8.5 The local height pairing at primes above p 93

8.5.1 Computing cup products 99

8.5.2 The map Ψ 99

8.5.3 Decomposing a divisor D into D^{w} and D^{nw} 100

8.5.4 A form with the required residue divisor 100

8.5.5 Finding ω_D for a Weierstrass divisor D 101
8.5.6 Finding ω_D for a non-Weierstrass divisor D 101
8.5.7 Integration when D_2 reduces to Weierstrass points 101
8.5.8 Computation when D_1 is Weierstrass and D_2 is not 101
8.5.9 Computation when both divisors are non-Weierstrass 101
8.6 Implementation notes 101
8.6.1 Auxiliary choices 102
8.6.2 Precision 102
8.7 Examples 106
8.7.1 Local heights: genus 2, general divisors 106
8.7.2 Local heights: genus 2, anti-symmetric divisors 107
8.7.3 Global heights: genus 1 109
8.7.4 Global heights: genus 2 110
8.8 Future work 110
8.8.1 Global height pairings 110
8.8.2 Optimizations 111
8.8.3 Comparison with the work of Mazur-Stein-Tate 111

9 A p-adic Birch and Swinnerton-Dyer conjecture 113
9.1 Introduction 113
9.2 p-adic height pairings and regulators 115
9.3 p-adic L-series 116
9.3.1 Inert case 116
9.3.2 Split case 118
9.4 Data for rank 2 Jacobians of genus 2 curves 119
9.4.1 Auxiliary data 119
9.4.2 Evidence for Conjecture 9.1.4 121
9.4.3 Future work 141

A Auxiliary p-adic BSD data 143
A.1 $N = 67$ 143
A.2 $N = 73$ 146
A.3 $N = 85$ 147
A.4 $N = 93$ 148
A.5 $N = 103$ 150
A.6 $N = 107$ 152
A.7 $N = 115$ 154
A.8 $N = 125, A$ 156
A.9 $N = 133, B$ 157
A.10 $N = 147$ 159
A.11 $N = 161$ 160
A.12 $N = 165$ 162
A.13 $N = 177$ 165
A.14 $N = 188$ 167
A.15 $N = 191$ 169

List of Figures

3.1.1 Residue disks on an elliptic curve 28
3.1.2 A wide open subspace 28
3.2.1 A tiny integral between P and Q. 31
3.2.2 Coleman integration between the points P, Q 33

List of Tables

9.4.1 Levels and integral models (Table 1, [FpS$^+$01]) 119

9.4.2 Levels and $y^2 = f(x)$ models 120

9.4.3 BSD data for rank 2 Jacobians of genus 2 curves (Table 2, [FpS$^+$01]) 120

9.4.4 Global generators and intersection data (computed by Steffen Müller) 121

9.4.5 p-adic regulators, $N = 67$ 123

9.4.6 p-adic special values, $N = 67$ 123

9.4.7 p-adic regulators, $N = 73$ 124

9.4.8 p-adic special values, $N = 73$ 124

9.4.9 p-adic regulators, $N = 85$ 125

9.4.10 p-adic special values, $N = 85$ 125

9.4.11 p-adic regulators, $N = 93$ 126

9.4.12 p-adic special values, $N = 93$ 126

9.4.13 p-adic regulators, $N = 103$ 127

9.4.14 p-adic special values, $N = 103$ 128

9.4.15 p-adic regulators, $N = 107$ 129

9.4.16 p-adic special values, $N = 107$ 129

9.4.17 p-adic regulators, $N = 115$ 130

9.4.18 p-adic special values, $N = 115$ 130

9.4.19 p-adic regulators, $N = 125, A$ 131

9.4.20 p-adic special values, $N = 125, A$ 131

9.4.21 p-adic regulators, $N = 133, B$ 132

9.4.22 p-adic special values, $N = 133, B$ 132

9.4.23 p-adic regulators, $N = 147$ 133

9.4.24 p-adic special values, $N = 147$ 133

9.4.25 p-adic regulators, $N = 161$ 134

9.4.26 p-adic special values, $N = 161$ 134

9.4.27 p-adic regulators, $N = 165$ 135

9.4.28 p-adic special values, $N = 165$ 136

9.4.29 p-adic regulators, $N = 177$ 137

9.4.30 p-adic special values, $N = 177$ 137

9.4.31 p-adic regulators, $N = 188$ 138

9.4.32 p-adic special values, $N = 188$ 139

9.4.33 p-adic regulators, $N = 191$ 140

9.4.34 p-adic special values, $N = 191$ 140

A.1.1 α factors for $N = 67$ 144

A.1.2 ϵ factors for $N = 67$ 145
A.2.1 α factors for $N = 73$ 146
A.2.2 ϵ factors for $N = 73$ 146
A.3.1 α factors for $N = 85$ 147
A.3.2 ϵ factors for $N = 85$ 147
A.4.1 α factors for $N = 93$ 148
A.4.2 ϵ factors for $N = 93$ 149
A.5.1 α factors for $N = 103$ 150
A.5.2 ϵ factors for $N = 103$ 151
A.6.1 α factors for $N = 107$ 152
A.6.2 ϵ factors for $N = 107$ 153
A.7.1 α factors for $N = 115$ 154
A.7.2 ϵ factors for $N = 115$ 155
A.8.1 α factors for $N = 125, A$ 156
A.8.2 ϵ factors for $N = 125, A$ 156
A.9.1 α factors for $N = 133, B$ 157
A.9.2 ϵ factors for $N = 133, B$ 158
A.10.1 α factors for $N = 147$ 159
A.10.2 ϵ factors for $N = 147$ 159
A.11.1 α factors for $N = 161$ 160
A.11.2 ϵ factors for $N = 161$ 161
A.12.1 α factors for $N = 165$ 163
A.12.2 ϵ factors for $N = 165$ 164
A.13.1 α factors for $N = 177$ 165
A.13.2 ϵ factors for $N = 177$ 166
A.14.1 α factors for $N = 188$ 167
A.14.2 ϵ factors for $N = 188$ 168
A.15.1 α factors for $N = 191$ 169
A.15.2 ϵ factors for $N = 191$ 169

Chapter 1

Introduction

The Coleman integral is an analytic tool that serves as the p-adic analogue of the usual (real-valued) line integral. These p-adic integrals help us understand the arithmetic and geometry of curves and abelian varieties. For example, certain integrals allow us to find rational points or torsion points; certain others give us p-adic height pairings.

Constructing this p-adic analogue is not at all obvious, as the totally disconnected topology of p-adic spaces makes it difficult to introduce a meaningful form of global antidifferentiation. Nevertheless, in a series of papers in the 1980s, Robert Coleman circumvented this problem using Dwork's principle of *Frobenius equivariance*. Using this idea, Coleman introduced a p-adic integration theory first on the projective line [Col82], then (partly jointly with de Shalit) on curves and abelian varieties [Col85], [CdS88]. Since then, alternative treatments have been given by Besser [Bes02a] using methods of p-adic cohomology, and by Berkovich [Ber07] using the nonarchimedean Gel'fand transform.

It was not immediately obvious that Coleman's p-adic integration theory was suitable for wide-scale computation. The first implementation (due to Besser and de Jeu [BdJ08]) was for curves of genus 0. In 2001, Kedlaya [Ked01] gave an algorithm computing the action of Frobenius on appropriate cohomology groups of hyperelliptic curves and in 2007 demonstrated [BCD$^+$08] that this algorithm could realize the Frobenius equivariance necessary for computing global Coleman integrals on such curves.

Motivating these algorithms is the fact that Coleman integration plays an important role in a study of the arithmetic of curves and abelian varieties. For example, appropriate integrals allow us to find torsion points and certain others describe integral points. Yet others give us a means to compute p-adic heights and regulators. Explicitly computing these quantities serves as motivation for several of our algorithms.

1.0.1 Why hyperelliptic curves?

The key input for all of our Coleman integration algorithms is the matrix of the action of Frobenius on an appropriate cohomology group of the variety. In particular, given a curve C, what is necessary is an algorithm that can compute the action of a p-power lift of Frobenius on a differential and then "reduce" it within the first de Rham cohomology group of the curve, $H^1_{dR}(C)$: that is, express it in terms of an exact differential plus a linear combination of basis (or pseudo-basis) differentials of $H^1_{dR}(C)$.

Since Kedlaya's algorithm [Ked01], which does precisely this, was originally purposed for hyperelliptic curves (and $p > 2$), the class of hyperelliptic curves was a natural starting point for our integration algorithms. Moreover, several applications of Coleman integration concern Jacobians of curves of genus greater than 1. Jacobians of hyperelliptic curves provide many interesting examples.

1.0.2 Beyond hyperelliptic curves?

Nevertheless, since Kedlaya's work, several generalizations have been formulated. Denef and Vercauteren [DV06] extended Kedlaya's algorithm to hyperelliptic curves in characteristic 2. Subsequent work by Gaudry and Gürel [GG01] treated the case of superelliptic curves. Castryck, Denef, and Vercauteren [CDV06] generalized Kedlaya's algorithm to nondegenerate curves. Any of these algorithms could be used to give Coleman integration algorithms on the relevant classes of curves. Moreover, the work of Abbott-Kedlaya-Roe [AKR09] (not to mention, David Harvey's recent optimized version [Har10b]), which does the analogous task for smooth hypersurfaces in projective space, could be used to extend Coleman integration beyond curves. It should also be possible to compute Coleman integrals using Frobenius structures on Picard-Fuchs (Gauss-Manin) connections, extending Lauder's *deformation method* for computing Frobenius matrices [Lau04].

1.0.3 Outline

This thesis presents several algorithms for p-adic integration on hyperelliptic curves. We begin with an introduction to hyperelliptic curves and Kedlaya's algorithm for computing the action of Frobenius on their cohomology. In Chapter 3, we use this to give algorithms to compute single Coleman integrals on odd models of hyperelliptic curves of good reduction over $\mathbb{C}_p$ for $p > 2$, as first appeared in joint work of the author with Bradshaw and Kedlaya [BBK10]. Chapter 4 builds on the work of Harrison [Har10a] to extend our techniques to even models of hyperelliptic curves. Chapter 5 presents algorithms to handle iterated Coleman integrals, with an emphasis on the particular case of double Coleman integrals.

The subsequent chapters of this thesis deal with applying these methods to study problems of interest in arithmetic geometry. In Chapter 6, we give an exposition of the method due to Chabauty and Coleman to find rational points on higher genus curves and demonstrate our algorithms in the case of hyperelliptic curves. Chapter 7 highlights Kim's recent work on a nonabelian analogue of this method as well as a few more algorithms and a behind-the-scenes look at numerical examples that first appeared in joint work of the author with Kedlaya and Kim in the Appendix and Erratum to [Kim10a]. In Chapter 8, we discuss the techniques of Coleman and Gross [CG89] studying p-adic local heights on curves. We present our algorithms appearing in joint work with Besser [BB] which adapt previous Coleman integration techniques to allow for differentials having residue divisors with non-Weierstrass support. This work gives the first algorithm to compute the Coleman-Gross local height pairing for Jacobians of hyperelliptic curves. Finally, we conclude in Chapter 9 with joint work of the author, Müller and Stein on explicit computations of p-adic regulators and p-adic L-series associated to Jacobians of hyperelliptic curves. We present some evidence toward a higher-dimensional analogue of the p-adic Birch and Swinnerton-Dyer conjecture.

Throughout, our algorithms have been implemented in the Sage computer algebra system [S$^+$11]. It is our hope that this thesis will serve as an introduction to the vast landscape of explicit methods involving p-adic integration.

Chapter 2

Hyperelliptic curves and p-adic cohomology

We begin by recalling some facts about hyperelliptic curves [CF05]. We continue with an introduction to some tools from p-adic cohomology, following the exposition in [CF05], as well as previous joint work of the author with Bradshaw and Kedlaya [BBK10]. These foundations will allow us to formulate the Coleman integration algorithms in subsequent chapters of this thesis.

2.1 Hyperelliptic curves

Let K be a field of characteristic not equal to 2.

Definition 2.1.1. A *hyperelliptic curve* C/K is a smooth projective curve of genus $g \geq 1$ such that an affine model of C can be written as

$$y^2 = f(x), f(x) \in K[x],$$

with $\deg(f) \leq 2g + 2$.

Let ι denote the *hyperelliptic involution* $\iota : (x, y) \mapsto (x, -y)$.

Definition 2.1.2. The *Weierstrass points* $P_1, \ldots, P_{2g+2}$ are the $\overline{K}$-rational fixed points of ι.

A point that is not a Weierstrass point is a *non-Weierstrass point.* If $\deg f(x) = 2g + 2$, then there are two distinct $\overline{K}$-rational non-Weierstrass points $P_{\infty^+}, P_{\infty^-}$ lying over ∞. If $\deg f(x) = 2g + 1$, then there is a single Weierstrass point P_∞ at ∞.

If $f(x)$ has a K-rational root, we may apply yet another change of coordinates to obtain a model of the form

$$y^2 = f(x), \quad \deg f(x) = 2g + 1.$$

We refer to this as an *odd model* for C. We distinguish between this case and that of the *even model*: when the curve is of the form $y^2 = f(x)$ with $\deg f(x) = 2g + 2$.

Unless otherwise mentioned, for simplicity, we present our algorithms for odd models of hyperelliptic curves and shall henceforth assume that $\deg f(x) = 2g+1$. In Chapter 4, we suspend this restriction and specifically address the situation of even models.

Let $K(C)$ denote the field of rational functions of C. Recall that a *local parameter* or a *local coordinate* at a $\overline{K}$-rational point P is a function $t \in K(C)$ such that $\operatorname{ord}_P(t) = 1$. Having explicit local coordinates at points on C is crucial to our integration algorithms. Here we record our local coordinate algorithms:

Algorithm 2.1.3 (Local coordinate at a non-Weierstrass point).
Input: A non-Weierstrass point $P = (a,b)$ on C (with $b \neq 0$) and precision n.
Output: A parametrization $(x(t), y(t))$ at P in terms of a local coordinate.

1. Let $x(t) = t + a$, where t is a local coordinate.

2. Solve for $y(t) = \sqrt{f(x(t))}$ by Newton's method: take $y_0 = b$, then set
$$y_i = \frac{1}{2}\left(y_{i-1} + \frac{f(x(t))}{y_{i-1}}\right), \quad i \geq 1$$
with $y_i(t) \to y(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n \rceil$.

Example 2.1.4. Let C be the hyperelliptic curve $y^2 = x^5 - 23x^3 + 18x^2 + 40x$ and consider the point $P = (1,6)$ on C. Then the local coordinates $(x(t), y(t))$ at P are
$$\begin{aligned} x(t) &= 1 + t, \\ y(t) &= 6 + t - \frac{7}{2}t^2 - \frac{1}{2}t^3 - \frac{25}{48}t^4 + O(t^5). \end{aligned}$$

Algorithm 2.1.5 (Local coordinate at a finite Weierstrass point).
Input: A finite Weierstrass point $P = (a,0)$ on C and precision n.
Output: A parametrization $(x(t), y(t))$ at P in terms of a local coordinate.

1. Let $y(t) = t$ where t is a local coordinate.

2. Iteratively solve for $x(t)$. One way is as follows: since $f(a) = 0$, note that
$$g(x) := f(x)/(x-a)$$
is a polynomial in x. Take
$$x_0 = a + \frac{1}{g(a)}t^2,$$
let $h(x,t) = f(x) - t^2$, and compute $h'(x,t) = \frac{\partial h(x,t)}{\partial x}$. Newton's method yields
$$x_{i+1}(t) = x_i(t) - \frac{h(x_i(t),t)}{h'(x_i(t),t)},$$

with $x_i(t) \to x(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n \rceil$

Example 2.1.6. Let C be the hyperelliptic curve $y^2 = x^5 - 23x^3 + 18x^2 + 40x$ and let $P = (4, 0)$ on C. Then the local coordinates $(x(t), y(t))$ at P are

$$\begin{aligned} x(t) &= 4 + \frac{1}{360}t^2 - \frac{191}{23328000}t^4 + \frac{7579}{188956800000}t^6 + O(t^7), \\ y(t) &= t. \end{aligned}$$

Finally for the case of infinity, since $y^2 = f(x)$, where $\deg f(x) = 2g + 1$, we have that x has a pole of order 2 at ∞, while y has a pole of order $2g+1$ at ∞. Let $t = \frac{x^g}{y}$ be the local parameter at ∞. To find the parametrization, we do as follows:

Algorithm 2.1.7 (Local coordinate at infinity).
Input: The point P_∞ above $x = \infty$ on C and precision n.
Output: A local coordinate $(x(t), y(t))$ at P_∞ such that t has a zero at ∞.

1. Take
$$x_0 = t^{-2},$$
let $h(x,t) = \left(\frac{x^g}{t}\right)^2 - f(x)$ and compute $h'(x,t) = \frac{\partial h(x,t)}{\partial x}$. Newton's method yields
$$x_{i+1}(t) = x_i(t) - \frac{h(x_i(t), t)}{h'(x_i(t), t)},$$
with $x_i(t) \to x(t)$. The number of iterates i to be taken depends on the necessary power series precision; for n digits of precision in t, i can be taken to be $\lceil \log_2 n \rceil$.

2. Take $y(t) = \frac{(x(t))^g}{t}$.

Example 2.1.8. Let C be the hyperelliptic curve $y^2 = x^5 - 23x^3 + 18x^2 + 40x$. At ∞, we have

$$\begin{aligned} x(t) &= t^{-2} + 23t^2 - 18t^4 - 569t^6 + O(t^7), \\ y(t) &= t^{-5} + 46t^{-1} - 36t - 609t^3 + 1656t^5 + O(t^6). \end{aligned}$$

2.2 p-adic cohomology

To discuss the differentials we will be integrating, we briefly introduce the necessary p-adic cohomology and some core definitions from [Ked01]. Let $p > 2g-1$ be a prime and K an unramified extension of $\mathbb{Q}_p$. Let C/K be a curve with good reduction. We will assume in addition that we have been given a model of C of the form $y^2 = f(x)$, with $f(x)$ having coefficients in the valuation ring $\mathcal{O}_K$ of K. We will assume that the leading coefficient of f is a unit, that $\deg f(x) = 2g + 1$, and that f has no repeated roots modulo p. Let C' be the affine curve obtained by deleting the Weierstrass points from C. Let $A = K[x, y, z]/(y^2 - f(x), yz - 1)$ be the coordinate ring of C'.

Definition 2.2.1. The Monsky-Washnitzer (MW) weak completion of A is the ring $A^\dagger$ consisting of infinite sums of the form

$$\left\{ \sum_{i=-\infty}^{\infty} \frac{B_i(x)}{y^i},\ B_i(x) \in K[x], \deg B_i \leq 2g \right\},$$

further subject to the condition that $v_p(B_i(x))$ grows faster than a linear function of i as $i \to \pm\infty$. We make a ring out of these by using the relation $y^2 = f(x)$.

Associated to each element $h \in A^\dagger$ is a differential dh such that the Leibniz rule holds: $d(hg) = h\,dg + g\,dh$ and such that $da = 0$ for each $a \in K$. Let Ω be the module of these differentials; then the operator d defines a K-derivation from $A^\dagger$ to Ω. Since $y^2 - f(x) = 0$, we conclude that

$$dy = f'(x)\,\frac{dx}{2y} \quad \text{and thus} \quad \Omega = A^\dagger \,\frac{dx}{2y}.$$

Let

$$H^0_{dR}(C) = \ker(d) = \{h \in A^\dagger | dh = 0\}, \quad H^1_{dR}(C) = \operatorname{coker}(d) = \left(A^\dagger \,\frac{dx}{2y}\right)/(dA^\dagger).$$

Thus elements of $H^1_{dR}(C)$ are differentials modulo exact differentials dh for some $h \in A^\dagger$. The next lemma [Ked01, §3] gives a basis for $H^1_{dR}(C')$.

Lemma 2.2.2. *The first de Rham cohomology $H^1_{dR}(C')$ splits into eigenspaces under the hyperelliptic involution ι:*

- *a positive eigenspace $H^1_{dR}(C')^+$ with basis $\{x^i \frac{dx}{y^2}\}$ for $i = 0, \ldots, 2g$.*
- *a negative eigenspace $H^1_{dR}(C')^-$ with basis $\{x^i \frac{dx}{2y}\}$ for $i = 0, \ldots, 2g-1$.*

For reasons which will become clear in the next chapter, we focus our attention on 1-forms that are *odd*, i.e., which are negated by the hyperelliptic involution. Let

$$\omega_i = x^i \,\frac{dx}{2y} \qquad (i = 0, \ldots, 2g-1). \tag{2.2.1}$$

By the lemma above, any odd differential $\omega \in \Omega$ can be written uniquely as

$$\omega = df + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1} \tag{2.2.2}$$

with $f \in A^\dagger$ and $c_i \in K$, since the ω_i form a basis of the odd part of the de Rham cohomology of $A^\dagger$. The process of putting ω in the form (2.2.2), using the relations

$$y^2 = f(x),$$
$$d(x^i y^j) = \left(2ix^{i-1}y^{j+1} + jx^i f'(x) y^{j-1}\right) \frac{dx}{2y},$$

can be made algorithmic; this is Kedlaya's algorithm, which we describe below. (Briefly, one uses the first relation to reduce high powers of x, and the second to reduce large positive and negative powers of y.)

2.2.1 Frobenius

Since K is an unramified extension of $\mathbb{Q}_p$, it carries a unique automorphism ϕ_K lifting the Frobenius automorphism $x \mapsto x^p$ on its residue field. Extend ϕ_K to a Frobenius lift ϕ on $A^\dagger$ by setting

$$\begin{aligned}
\phi(x) &= x^p, \\
\phi(y) &= y^p \left(1 + \frac{\phi_K(f)(x^p) - f(x)^p}{f(x)^p}\right)^{1/2} \\
&= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(\phi_K(f)(x^p) - f(x)^p)^i}{y^{2pi}}.
\end{aligned}$$

We will also need $\phi(y)^{-1}$, which can be computed as

$$\phi(y)^{-1} = y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{y^{2pi}}.$$

Remark 2.2.3. Note that one needs y^{-1} as an element of $A^\dagger$, which explains why we compute with C' instead of C.

Note also that for ease of exposition, we describe all of our algorithms as if it were possible to compute exactly in $A^\dagger$. This is not possible for two reasons: the elements of $A^\dagger$ correspond to infinite series, and the coefficients of these series are polynomials with p-adic coefficients. In practice, each computation will be made with suitable p-adic approximations of the truly desired quantities, so one must keep track of how much p-adic precision is needed in these estimates in order for the answers to bear a certain level of p-adic accuracy. We postpone this discussion to §3.3.1.

2.2.2 Kedlaya's algorithm

To compute in $H^1_{dR}(C)$, we need to express an arbitrary differential form as the sum of a K-linear combination of the basis in Lemma 2.2.2 and an exact differential. We refer to this process as *reduction in cohomology* and carry it out as follows.

First note that any differential form can be written as

$$\sum_{k=-\infty}^{\infty} \sum_{i=0}^{2g} a_{i,k} \frac{x^i}{y^k} dx, \quad a_{i,k} \in K.$$

Indeed, using the equation of the curve, we can replace $h(x)f(x)$ with $h(x)y^2$ as many times as needed. Next, a differential $\frac{P(x)}{y^s} dx$ with $P(x) \in K[x]$ and $s \in \mathbb{N}$

can be reduced as follows. Since $f(x)$ has no repeated roots, we can always write $P(x) = U(x)f(x) + V(x)f'(x)$. Since $d\left(\frac{V(x)}{y^{s-2}}\right)$ is exact, we obtain

$$\frac{P(x)}{y^s}\,dx \equiv \left(U(x) + \frac{2V'(x)}{s-2}\right)\frac{dx}{y^{s-2}},$$

where $\equiv$ means equality modulo exact differentials. This congruence can be used to reduce a differential form involving negative powers of y to the case $s = 1$ and $s = 2$. Moreover, a differential $\frac{P(x)}{y}\,dx$ with $\deg P = n \geq 2g$ can be reduced by repeatedly subtracting appropriate multiples of the exact differential $d(x^{i-2g}y)$ for $i = n, \dots, 2g$. Finally, note that the differential $\frac{P(x)}{y^2}\,dx$ is congruent to $\frac{P(x) \bmod f(x)}{y^2}\,dx$ modulo exact differentials. A differential of the form $P(x)y^s\,dx$ with $P(x) \in K[x]$ and $s \in \mathbb{N}$ is exact if s is even and equal to $\frac{P(x)f(x)^{\lceil s/2 \rceil}}{y}\,dx$ if s is odd and thus can be reduced using the above reduction formula.

Since the q-power Frobenius ϕ_q is ϕ^d, it suffices to compute the matrix M through which the p-power Frobenius acts on the anti-invariant part $H^1_{dR}(C)^-$ of $H^1_{dR}(C)$; the matrix of the q-power Frobenius can then be obtained as $M_{\phi_q} = M\phi(M)\cdots\phi^{d-1}(M)$. The action of ϕ on the basis of $H^1_{dR}(C)^-$ can be computed as

$$\phi\left(\frac{x^i}{2y}\,dx\right) = \frac{px^{p(i+1)-1}}{2\phi(y)}\,dx,$$

for $i = 0, \dots, 2g-1$. Given a sufficiently precise approximation to $\frac{1}{\phi(y)}$, we can use reduction in cohomology to express $\phi(\omega_i)$ on the basis of $H^1_{dR}(C)^-$ and compute the matrix M. This is Kedlaya's algorithm:

Algorithm 2.2.4 (Kedlaya's algorithm).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$.
Output: Functions $f_i \in A^\dagger$ and a $2g \times 2g$ matrix M over K such that

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j$$

for all i.

1. Compute $\phi(x), \phi(y)$ as infinite series in $A^\dagger$.

2. Use a Newton iteration to compute $\frac{y}{\phi(y)}$. Then for $i = 0, \dots, 2g-1$, proceed as in §2.2.2 to write

$$\phi^*(\omega_i) = px^{pi+p-1}\frac{y}{\phi(y)}\frac{dx}{2y} = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j \qquad (2.2.3)$$

   for some $f_i \in A^\dagger$ and some $2g \times 2g$ matrix M over K.

For some applications, it may be convenient to use a different basis of de Rham cohomology. For instance, the basis $\frac{x^i}{2y^3}\,dx\,(i = 0, \dots, 2g-1)$ is *crystalline* (see [Har10a], as well as the erratum to [Ked01]), so Frobenius will act via a matrix with p-adically integral entries.

Chapter 3

Coleman integration: the basic integrals

Most of the material in this chapter originally appeared in joint work of the author with Bradshaw and Kedlaya [BBK10].

3.1 Coleman's theory of p-adic integration

In this section, we recall Coleman's p-adic integration theory in the case of curves with good reduction. This theory involves some concepts from rigid analytic geometry which it would be hopeless to introduce in such limited space; some standard references are [BGR84] and [FvdP04]. (See also [Col85, §1].)

Let $\mathbb{C}_p$ be a completed algebraic closure of $\mathbb{Q}_p$, and let $\mathcal{O}$ be the valuation subring of $\mathbb{C}_p$. Choose once and for all a *branch of the p-adic logarithm*, i.e., a homomorphism $\mathrm{Log} : \mathbb{C}_p^\times \to \mathbb{C}_p$ whose restriction to the disk $\{x \in \mathbb{C}_p : |x-1| < 1\}$ is given by the logarithm series $\log(x) = -\sum_{i=1}^{\infty}(1-x)^i/i$. (The choice of branch will have no effect on the integrals of differentials of the second kind, i.e., everywhere meromorphic differentials with all residues zero.)

We first introduce integrals on disks and annuli within $\mathbb{P}^1$.

Definition 3.1.1. Let I be an open subinterval of $[0, +\infty)$. Let $A(I)$ denote the annulus (or disk) $\{t \in \mathbb{A}^1_{\mathbb{C}_p} : |t| \in I\}$. For $\sum_{i\in\mathbb{Z}} c_i t^i\, dt \in \Omega^1_{A(I)/\mathbb{C}_p}$ and $P, Q \in A(I)$, define

$$\int_P^Q \sum_{i\in\mathbb{Z}} c_i t^i\, dt = c_{-1}\mathrm{Log}(Q/P) + \sum_{i\neq -1} \frac{c_i}{i+1}(Q^{i+1} - P^{i+1}).$$

This is easily shown not to depend on the choice of the coordinate t.

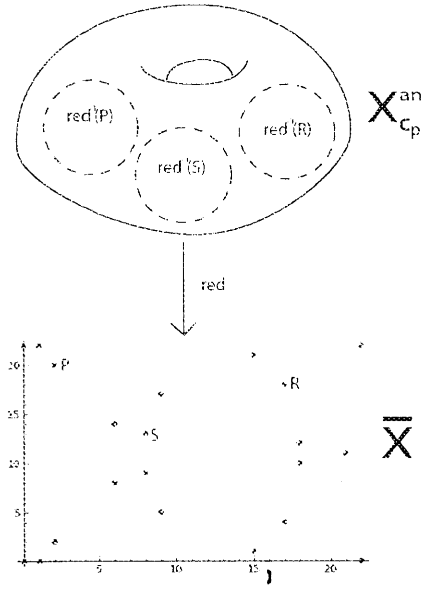
Remark 3.1.2. Note that because of the division by $i+1$ in the formula for the integral, we are unable to integrate on *closed* disks or annuli (as this affects convergence on the "boundary").

We next turn to curves of good reduction.

Definition 3.1.3. By a *curve* over $\mathcal{O}$, we will mean a smooth proper connected scheme X over $\mathcal{O}$ of relative dimension 1. Equip the function field $K(X)$ with the p-adic absolute value, so that the elements of $K(X)$ of norm at most 1 constitute the local ring in X of the generic point of the special fibre $\overline{X}$ of X.

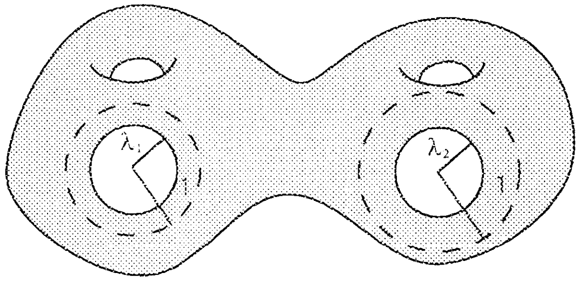
Let $X^{\mathrm{an}}_{\mathbb{C}_p}$ denote the generic fibre of X as a rigid analytic space. There is a natural reduction map from $X^{\mathrm{an}}_{\mathbb{C}_p}$ to $\overline{X}(\overline{F}_p)$; the inverse image of any closed point of $\overline{X}$ is a subspace of $X^{\mathrm{an}}_{\mathbb{C}_p}$ isomorphic to an open unit disk. We call such a disk a *residue disk* of X.

Figure 3.1.1: Residue disks on an elliptic curve



Definition 3.1.4. Let X be a curve over $\mathcal{O}$. By a *wide open subspace* of $X^{\mathrm{an}}_{\mathbb{C}_p}$, we will mean a rigid analytic subspace of $X^{\mathrm{an}}_{\mathbb{C}_p}$ that is the complement of the union of a finite collection of disjoint closed disks of radius $\lambda_i < 1$.

Figure 3.1.2: A wide open subspace



Coleman made the surprising discovery that there is a well-behaved integration theory on wide open subspaces of curves over $\mathcal{O}$, exhibiting no phenomena of path dependence. (One needs to consider wide open subspaces even to integrate differentials which are holomorphic or meromorphic on the entire curve.) In the case of hyperelliptic curves, Coleman's construction of these integrals using Frobenius lifts will be reflected in our technique for computing the integrals. For the general case, see [Col85, §2], [Bes02a, §4], or [Ber07, Theorem 1.6.1].

Let $\mathrm{Div}(W)$ denote the free group on the elements of W and $\mathrm{Div}^0(W)$ denote the kernel of the degree map $\deg : \mathrm{Div}(W) \to \mathbb{Z}$ taking each element of W to 1

Theorem 3.1.5 (Coleman). *We may assign to each curve X over $\mathcal{O}$ and each wide open subspace W of $X^{\mathrm{an}}_{\mathbb{C}_p}$ a map $\mu_W : \mathrm{Div}^0(W) \times \Omega^1_{W/\mathbb{C}_p} \to \mathbb{C}_p$, subject to the following conditions.*

(a) (Linearity) The map μ_W is linear on $\mathrm{Div}^0(W)$ and $\mathbb{C}_p$-linear on $\Omega^1_{W/\mathbb{C}_p}$.

(b) (Compatibility) For any residue disk D of X and any isomorphism $\psi : W \cap D \to A(I)$ for some interval I, the restriction of μ_W to $\mathrm{Div}^0(W \cap D) \times \Omega^1_{W/\mathbb{C}_p}$ is compatible with Definition 3.1.1 via ψ.

(c) (Change of variables) Let X' be another curve over $\mathcal{O}$, let W' be a wide open subspace of X', and let $\psi : W \to W'$ be any morphism of rigid spaces relative to a continuous automorphism of $\mathbb{C}_p$. Then

$$\mu_{W'}(\psi(\cdot), \cdot) = \mu_W(\cdot, \psi^*(\cdot)). \tag{3.1.1}$$

(d) (Fundamental theorem of calculus) For any $Q = \sum_i c_i P_i \in \mathrm{Div}^0(W)$ and any $f \in \mathcal{O}(W)$, $\mu_W(Q, df) = \sum_i c_i f(P_i)$.

The map μ_W is uniquely determined by these conditions.

Example 3.1.6. The Frobenius ϕ defined in Chapter 2 may be interpreted a morphism from a wide open subspace of X to X^{an}.

Remark 3.1.7. One cannot expect path independence in the case of bad reduction. For instance, an elliptic curve over $\mathbb{C}_p$ with bad reduction admits a Tate uniformization, so its logarithm map has nonzero periods in general. In Berkovich's theory of integration, this occurs because the nonarchimedean analytic space associated to this curve X has nontrivial first homology.

3.2 Explicit integrals for hyperelliptic curves

We now specialize to the situation where $p > 2g - 1$ and X is a genus g hyperelliptic curve over an unramified extension K of $\mathbb{Q}_p$ having good reduction. (The assumption on p is so that the matrix of Frobenius with respect to our choice of basis is p-integral.) We will assume in addition that we have been given a model of X of the form $y^2 = f(x)$ such that $\deg f(x) = 2g + 1$ and f has no repeated roots modulo p. (This restriction is inherited from §2.2.2, where it is used to simplify the reduction procedure. One could reduce to this case after possibly replacing K by a larger unramified extension of $\mathbb{Q}_p$, by performing a linear fractional transformation in x to put one root at infinity, thus reducing the degree from $2g+2$ to $2g+1$. However, we will also directly formulate integration algorithms when $\deg f(x) = 2g+2$ in Chapter 4.) We will distinguish between *Weierstrass* and *non-Weierstrass* residue disks of X, which respectively correspond to Weierstrass and non-Weierstrass points of $\overline{X}$.

Let X' be the affine curve obtained by deleting the Weierstrass points from X, let $A = K[x, y, z]/(y^2 - f(x), yz - 1)$ be the coordinate ring of X', and let $A^\dagger$ be the MW weak completion of A (as in Chapter 2). These functions $g \in A^\dagger$ are holomorphic on wide opens, so we will integrate 1-forms

$$\omega = g(x,y)\frac{dx}{2y}, \quad g(x,y) \in A^\dagger. \tag{3.2.1}$$

Note that we only consider 1-forms which are *odd*. Even 1-forms can be written in terms of x alone, and so can be integrated directly as in Definition 3.1.1. (This last statement would fail if we had taken $A^\dagger$ to be the full p-adic completion of A, rather than the weak completion. This observation is the basis for Monsky-Washnitzer's formal cohomology, which is used in [Ked01].)

Note that the class of allowed forms includes those meromorphic differentials on X whose poles all belong to Weierstrass residue disks. For some applications (e.g., p-adic canonical heights), it is necessary to integrate meromorphic differentials with poles in non-Weierstrass residue disks. These will be discussed in Chapter 8.

3.2.1 A basis for de Rham cohomology

As observed in §2.2.2, any odd differential ω as in (3.2.1) can be written uniquely as

$$\omega = df + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1} \tag{3.2.2}$$

with $f \in A^\dagger$, $c_i \in K$, and

$$\omega_i = \frac{x^i\,dx}{2y} \qquad (i = 0, \ldots, 2g-1).$$

That is, the ω_i form a basis of the odd part of the de Rham cohomology of $A^\dagger$.

Using properties from Theorem 3.1.5 (linearity and the fundamental theorem of calculus), the integration of ω reduces effectively to the integration of the ω_i.

3.2.2 Tiny integrals

We refer to any Coleman integral of the form $\int_P^Q \omega$ in which P, Q lie in the same residue disk (Weierstrass or not) as a *tiny integral.* As an easy first case, we give an algorithm to compute tiny integrals of basis differentials.

Algorithm 3.2.1 (Tiny Coleman integrals).
Input: Points $P, Q \in X(\mathbb{C}_p)$ in the same residue disk and a basis differential ω_i

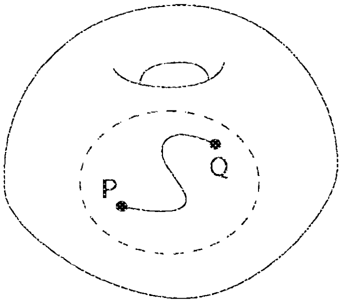
without poles in the disk.
Output: The integral $\int_P^Q \omega_i$.

1. Using the relevant algorithm (Algorithm 2.1.3, 2.1.5 or 2.1.7), compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t.

2. Formally integrate the power series in t:

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^{t(Q)} \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt.$$

Figure 3.2.1: A tiny integral between P and Q.



Remark 3.2.2. One can similarly integrate any ω holomorphic in the residue disk containing P and Q. If ω is only meromorphic in the disk, but has no pole at P or Q, we can first make a polar decomposition, i.e., write ω as a holomorphic differential on the disk plus some terms of the form $c/(t-r)^i dt$, and integrate the latter terms directly. (If ω is everywhere meromorphic, the integration of ω is achieved by a partial fractions decomposition.)

3.2.3 Non-Weierstrass disks

We next compute integrals of the form $\int_P^Q \omega_i$ in which $P, Q \in X(\mathbb{C}_p)$ lie in distinct non-Weierstrass residue disks. The method of tiny integrals is not available; we instead employ Dwork's principle of analytic continuation along Frobenius, in the form of Kedlaya's algorithm (Algorithm 2.2.4) for calculating the action of Frobenius on de Rham cohomology.

Our recipe is essentially Coleman's construction of the integrals in this case.

Algorithm 3.2.3 (Coleman integration in non-Weierstrass disks).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in X(\mathbb{C}_p)$ in non-Weierstrass residue disks, and a positive integer m such that the residue fields of P, Q are contained in $\mathbb{F}_{p^m}$.
Output: The integrals $\left(\int_P^Q \omega_i\right)_{i=0}^{2g-1}$.

1. Calculate the action of the m-th power of Frobenius on each basis element (see Remark 3.2.4):
$$(\phi^m)^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j. \tag{3.2.3}$$

2. By change of variables (see Remark 3.2.5 below), we obtain
$$\sum_{j=0}^{2g-1}(M-I)_{ij}\int_P^Q \omega_j = f_i(P) - f_i(Q) - \int_P^{\phi^m(P)} \omega_i - \int_{\phi^m(Q)}^Q \omega_i \tag{3.2.4}$$
(the *fundamental linear system*). Since the eigenvalues of the matrix M are algebraic integers of $\mathbb{C}$-norm $p^{m/2} \neq 1$ (see [Ked01, §2]), the matrix $M - I$ is invertible, and we may solve (3.2.4) to obtain the integrals $\int_P^Q \omega_i$.

Remark 3.2.4. To compute the action of ϕ^m, first perform Algorithm 2.2.4 to write
$$\phi^*\omega_i = dg_i + \sum_{j=0}^{2g-1} B_{ij}\omega_j.$$

If we view f, g as column vectors and M, B as matrices, induction on m shows that
$$\begin{aligned} f &= \phi^{m-1}(g) + B\phi^{m-2}(g) + \cdots + B\phi_K(B)\cdots\phi_K^{m-2}(B)g \\ M &= B\phi_K(B)\cdots\phi_K^{m-1}(B). \end{aligned}$$

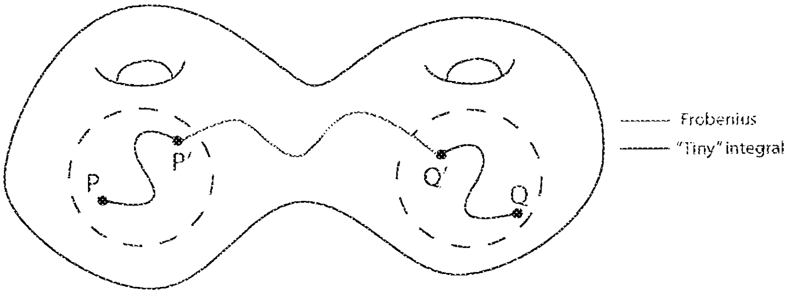
Remark 3.2.5. We obtain (3.2.4) as follows. By change of variables,
$$\begin{aligned} \int_{\phi^m(P)}^{\phi^m(Q)} \omega_i &= \int_P^Q (\phi^m)^*\omega_i \\ &= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j) \\ &= f_i(Q) - f_i(P) + \sum_{j=0}^{2g-1} M_{ij}\int_P^Q \omega_j. \end{aligned}$$

Adding $\int_P^{P'} \omega_i + \int_{Q'}^Q \omega_i$ to both sides of this equation yields
$$\int_P^Q \omega_i = \int_P^{P'} \omega_i + \int_{Q'}^Q \omega_i + f_i(Q) - f_i(P) + \sum_{j=0}^{2g-1} M_{ij}\int_P^Q \omega_j,$$
which is equivalent to (3.2.4).

Definition 3.2.6. A *Teichmüller point* of $X_{\mathbb{C}_p}^{\text{an}}$ is a point fixed by some power of ϕ. Each non-Weierstrass residue disk contains a unique such point: if $(\overline{x}, \overline{y}) \in \overline{X}$ is a non-Weierstrass point, the Teichmüller point in its residue disk has x-coordinate equal to the usual Teichmüller lift of x. This leaves two choices for the y-coordinate, exactly one of which has the correct reduction modulo p. Note that Teichmüller points are always defined over finite *unramified* extensions of $\mathbb{Q}_p$.

A variant of Algorithm 3.2.3 is to first find the Teichmüller points P', Q' in the residue disks of P, Q, then use the fundamental system to calculate integrals between these points, and employ additivity to correct endpoints. We illustrate this with a figure below.

Figure 3.2.2: Coleman integration between the points P, Q



More precisely, we have the following:

Algorithm 3.2.7 (Coleman integration via Teichmüller points).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in X(\mathbb{C}_p)$ in non-Weierstrass residue disks, and a positive integer m such that the residue fields of P, Q are contained in $\mathbb{F}_{p^m}$.
Output: The integrals $\left(\int_P^Q \omega_i\right)_{i=0}^{2g-1}$.

1. Compute Teichmüller points P', Q' in the disks of P and Q, respectively.
2. Use the fundamental linear system to obtain
$$\sum_{j=0}^{2g-1}(M-I)_{ij}\int_{P'}^{Q'}\omega_j = f_i(P') - f_i(Q').$$
3. Use additivity to correct the endpoints and recover the integral from P to Q:
$$\int_P^Q \omega_i = \int_P^{P'}\omega_i + \int_{P'}^{Q'}\omega_i + \int_Q^{Q'}\omega_i.$$

Finally, given an arbitrary odd differential ω, we use the previous algorithms, linearity, and the fundamental theorem of calculus to recover the integral of ω between non-Weierstrass points P and Q:

Algorithm 3.2.8 (Coleman integral of an odd ω).
Input: Non-Weierstrass points $P, Q \in X(\mathbb{C}_p)$ and an odd differential ω holomorphic outside Weierstrass disks.
Output: The integral $\int_P^Q \omega$.

1. Use Kedlaya's algorithm (Algorithm 2.2.4) to write ω in the form

$$\omega = df + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1}$$

2. For each ω_i, compute $\int_P^Q \omega_i$.

3. Use the fundamental theorem of calculus and linearity to obtain the integral

$$\int_P^Q \omega = f(Q) - f(P) + c_0 \int_P^Q \omega_0 + \cdots + c_{2g-1} \int_P^Q \omega_{2g-1}.$$

3.2.4 Weierstrass endpoints of integration

Suppose now that P, Q lie in different residue disks, at least one of which is Weierstrass. Since a differential ω of the form (3.2.1) is not meromorphic on Weierstrass residue disks, we cannot always even define $\int_P^Q \omega$, let alone compute it. We will thus assume (to cover most cases arising in applications) that ω is everywhere meromorphic, with no poles in the residue disks of P and Q.

Lemma 3.2.9. *Let $P, Q \in X(\mathbb{C}_p)$, with P a Weierstrass point. Let ω be an odd, everywhere meromorphic differential on X with no poles in the residue disks of P and Q. Then for ι the hyperelliptic involution, $\int_P^Q \omega = \frac{1}{2}\int_{\iota(Q)}^Q \omega$. In particular, if Q is also a Weierstrass point, then $\int_P^Q \omega = 0$.*

Proof. Let $I := \int_P^Q \omega = \int_P^{\iota(Q)} (-\omega) = \int_{\iota(Q)}^P \omega$. Then by additivity in the endpoints, we have $\int_{\iota(Q)}^Q \omega = 2I$, from which the result follows. □

If P belongs to a Weierstrass residue disk while Q does not, we find the Weierstrass point P' in the disk of P, then apply Lemma 3.2.9 to write

$$\int_P^Q \omega = \int_P^{P'} \omega + \frac{1}{2}\int_{\iota(Q)}^Q \omega. \tag{3.2.5}$$

The first integral on the right side of (3.2.5) is tiny, while the second integral involves two points in non-Weierstrass residue disks, and so may be computed as in the previous section. The situation is even better if P, Q both belong to residue disks containing respective Weierstrass points P', Q': in this case, by Lemma 3.2.9, $\int_P^Q \omega$ equals the sum $\int_P^{P'} \omega + \int_{Q'}^Q \omega$ of tiny integrals.

Beware that Lemma 3.2.9 does not generalize to iterated integrals. For instance, for double integrals, if both integrands are odd, the total integrand is even, so the argument of Lemma 3.2.9 tells us nothing. It is thus worth considering alternate approaches for dealing with Weierstrass disks, which may generalize better to the iterated case. We concentrate on the case where P lies in a Weierstrass residue disk but Q does not, since we may reduce to this case by splitting $\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega$ for some auxiliary point R in a non-Weierstrass residue disk.

In Algorithm 3.2.3, the form f_i belongs to $A^\dagger$, so it need not converge at P. However, it does converge at any point R near the boundary of the disk, i.e., in the complement of a certain smaller disk which can be bounded explicitly. We may thus write $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$ for suitable R in the disk of P, to obtain an analogue of the fundamental linear system (3.2.4). Similarly, when we write ω as in (3.2.2), we can find R close enough to the boundary of the disk of P so that f converges at R, use Algorithm 3.2.3 to evaluate $\int_R^Q \omega$, then compute $\int_P^R \omega$ as a tiny integral. One defect of this approach is that forcing R to be close to the boundary of the residue disk of P forces R to be defined over a highly ramified extension of $\mathbb{Q}_p$, over which computations are more expensive.

An alternate approach exploits the fact that for P in the infinite residue disk but distinct from ∞, we may compute $\int_P^Q \omega$ directly using Algorithm 3.2.3. This works because both the Frobenius lift and the reduction process respect the subring of $A^\dagger$ consisting of functions which are meromorphic at infinity. When P lies in a finite Weierstrass residue disk, we may reduce to the previous case using a change of variables on the x-line to move P to the infinite disk. However, one still must use the approach of the previous paragraph to reduce evaluation of $\int_P^Q \omega$ to evaluation of the $\int_P^Q \omega_i$.

We have the following algorithms:

Algorithm 3.2.10 (Finding a near-boundary point in a finite Weierstrass disk).
Input: A finite Weierstrass point P, and a positive integer d.
Output: A point $R = (x(p^{1/d}), p^{1/d})$ in the disk of P defined over the totally ramified extension $\mathbb{Q}_p(p^{1/d})$.

1. Compute a parametrization $(x(t), t)$ at P in terms of the local coordinate t.

2. Evaluate local coordinates at $t = p^{1/d}$. This is R.

Algorithm 3.2.11 (Coleman integration in a finite Weierstrass disk).
Input: A finite Weierstrass point P, a positive integer d, a non-Weierstrass point Q, and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.

1. Use Algorithm 3.2.10 to find R. Keep the local coordinate $(x(t), t)$ at P.

2. Compute $\int_P^R \omega_i$ as a tiny integral: $\int_P^R \omega_i = \int_0^{p^{1/d}} \frac{x(t)^i dx(t)}{2t} dt$.

3. Use the fundamental linear system to compute $\int_R^Q \omega_i$.

4. Use additivity in endpoints to recover $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$.

3.3 Implementation notes and precision

We have implemented the above algorithms in Sage [S+11] for curves defined over $\mathbb{Q}_p$. In doing so, we made the following observations.

3.3.1 Precision estimates

For a tiny integral, the precision of the result depends on the truncation of the power series computed. Here is the analysis for a non-Weierstrass disk; the analysis for a Weierstrass disk, using a different local interpolation, is similar. (For points over ramified extensions, one must also account for the ramification index in the bound, but it should be clear from the proof how this is done.)

Proposition 3.3.1. *Let $\omega = g(x,y)\,dx$ be a differential of the second kind such that $h(t) = g(x(t), y(t))$ belongs to $\mathcal{O}[[t]]$. Let $\int_P^Q \omega$ be a tiny integral in a non-Weierstrass residue disk, with P, Q defined over an unramified extension of K and accurate to n digits of precision. Let $(x(t), y(t))$ be the local interpolation between P and Q defined by*

$$\begin{aligned} x(t) &= x(P)(1-t) + x(Q)t = x(P) + t(x(Q) - x(P)) \\ y(t) &= \sqrt{f(x(t))}. \end{aligned}$$

If we truncate $h(t)$ modulo t^m and modulo p^n, then the computed value of the integral $\int_P^Q \omega$ will be correct to $\min\{n, m+1-\lfloor \log_p(m+1)\rfloor\}$ digits of (absolute) precision.

Proof. Let $t' = t(x(Q) - x(P))$. As P, Q are in the same residue disk and are defined over an unramified extension of K, we have $v_p(x(Q) - x(P)) \geq 1$. If we expand $g(x(t'), y(t')) = \sum_{i=0}^{\infty} c_i (t')^i$, then by hypothesis $c_i \in \mathcal{O}$. Thus

$$\begin{aligned} \int_P^Q \omega &= \int_P^Q g(x,y)\,dx \\ &= \int_0^1 g(x(t), y(t))\,dx(t) \\ &= \int_0^{x(Q)-x(P)} g(x(t'), y(t'))\,dt' \\ &= \int_0^{x(Q)-x(P)} \sum_{i=0}^{\infty} c_i (t')^i\,dt' \\ &= \sum_{i=0}^{\infty} \frac{c_i}{i+1}(x(Q) - x(P))^{i+1}. \end{aligned}$$

The effect of omitting $c_i(t')^i$ from the expansion of $g(x(t'), y(t'))$ for some $i \geq m$ is to change the final sum by a quantity of valuation at least $i + 1 - \lfloor \log_p(i+1)\rfloor \geq m + 1 - \lfloor \log_p(m+1)\rfloor$. The effect of the ambiguity in P and Q is that the computed value of $(x(Q) - x(P))^{i+1}$ differs from the true value by a quantity of valuation at least $i + 1 - \lfloor \log_p(i + 1) \rfloor + n - 1 \geq n$. □

For Coleman integrals between different residue disks, which we may assume are non-Weierstrass thanks to §3.2.4, one must first account for the precision loss in Algorithm 2.2.4. According to [Ked01, Lemmas 2,3] and the erratum to [Ked01] (or [Har07]), working to precision p^N in Algorithm 2.2.4 produces the f_i and M_{ij} accurately modulo p^{N-n} for $n = 1 + \lfloor \log_p \max\{N, 2g + 1\} \rfloor$.

We must then take into account the objects involved in the linear system (3.2.4), as follows.

Proposition 3.3.2. *Let $\int_P^Q \omega$ be a Coleman integral, with ω a differential of the second kind and with P, Q in non-Weierstrass residue disks, defined over an unramified extension of $\mathbb{Q}_p$. Suppose that P, Q, and ω are accurate to n digits of precision. Let* Frob *be the matrix of the action of Frobenius on the basis differentials, and let* Frob^T *denote its transpose. Set $B = \mathrm{Frob}^T - I$, and let $m = v_p(\det(B))$. Then the computed value of the integral $\int_P^Q \omega$ will be accurate to $n - \max\{m, \lfloor \log_p n \rfloor\}$ digits of precision.*

Proof. By the linear system (3.2.4), the Coleman integral is expressed in terms of tiny integrals, integrals of exact forms evaluated at points. and a matrix inversion. Suppose that the entries of $B = \mathrm{Frob}^T - I$ are computed to precision n. Then taking B^{-1}, we have to divide by $\det(B)$, which lowers the precision by $m = v_p(\det(B))$. By Proposition 3.3.1, computing tiny integrals (with the series expansions truncated modulo t^{n-1}) gives a result precise up to $n - \lfloor \log_p n \rfloor$ digits. Thus the value of the integral $\int_P^Q \omega$ will be correct to $n - \max\{m, \lfloor \log_p n \rfloor\}$ digits of precision. □

3.3.2 Complexity analysis

We assume that asymptotically fast integer and polynomial multiplication algorithms are used; specifically addition, subtraction, multiplication, and division take $\widetilde{O}(\log N)$ bit operations in $\mathbb{Z}/N\mathbb{Z}$ and $\widetilde{O}(n)$ basering operations in $R[x]/x^n R[x]$. In particular, this allows arithmetic operations in $\mathbb{Q}_p$ to n (relative) digits of precision, hereafter called field operations, in time $\widetilde{O}(n \log p)$. Using Newton iteration, both square roots and the Teichmüller character can be computed to n digits of precision using $\widetilde{O}(\log n)$ arithmetic operations. (We again consider only points in non-Weierstrass disks defined over unramified fields.)

Proposition 3.3.3. *Let $\int_P^Q \omega$ be a Coleman integral on an odd degree hyperelliptic curve of genus g over $\mathbb{Q}_p$, with $\omega = df_\omega + \sum_{i=1}^{2g-i} c_i \omega_i$ a differential of the second kind and with P, Q in non-Weierstrass residue disks, defined over $\mathbb{Q}_p$, and accurate to n digits of precision. Let* Frob *be the matrix of the action of Frobenius on the basis differentials, and let $m = v_p(\det(\mathrm{Frob}^T - I))$. Let $F(n)$ be the running time of evaluating f_ω at P and Q to n digits of precision. The value of the integral $\int_P^Q \omega$ can be computed to $n - \max\{m, \lfloor \log_p n \rfloor\}$ digits of precision in time $F(n) + \widetilde{O}(pn^2g^2 + g^3 n \log p)$. (Over a degree N unramified extension of $\mathbb{Q}_p$, the analysis is the same with the runtime multiplied by a factor of N.)*

Proof. An essential input to the algorithm is the matrix of the action of Frobenius, which can be computed by Kedlaya's algorithm to n digits of precision in running time $\widetilde{O}(pn^2g^2)$. Inverting the resulting matrix can be (naïvely) done with $O(g^3)$ arithmetic operations in $\mathbb{Q}_p$. It remains to be shown that no other step exceeds these running times. For the tiny integral on the first basis differential, the power series $x(t)/y(t) = x(t)f(x(t))^{-1/2}$ can be computed modulo t^{n-1} using Newton iteration, requiring $\widetilde{O}(n \log n)$ field operations. Each other basis differential can be computed from the first by multiplication by the linear polynomial $x(t)$ and the definite integral evaluated with $\widetilde{O}(n)$ field operations, for a total of $\widetilde{O}(gn^2)$ bit operations. Computing $\phi(P)$ and $\phi(Q)$ to n digits of precision is cheap; directly using the formula in Algorithm 2.2.4 uses $\widetilde{O}(g + \log p)$ field operations. The last potentially significant step is computing and evaluating the f_i at each P and/or Q. The coefficients of the f_i can be read off in the reduction phase of Kedlaya's algorithm, and have $O(png)$ terms each. Evaluating (or even recording) all g of these forms takes $\widetilde{O}(png^2)$ field operations, or $\widetilde{O}(pn^2g^2)$ bit operations, which is proportional to the cost of doing the reduction. □

3.3.3 Numerical examples

Here are some sample computations made using our Sage implementation.

Example 3.3.4. Leprévost [Lep95] showed that the divisor $(1, -1) - \infty^+$ on the genus 2 curve $y^2 = (2x-1)(2x^5 - x^4 - 4x^2 + 8x - 4)$ over $\mathbb{Q}$ is torsion of order 29. Consequently, the integrals of holomorphic differentials against this divisor must vanish. We may observe this vanishing numerically, as follows. Indeed, let

$$C : y^2 = x^5 + \frac{33}{16}x^4 + \frac{3}{4}x^3 + \frac{3}{8}x^2 - \frac{1}{4}x + \frac{1}{16}$$

be an odd degree model of Leprévost's curve, obtained via the linear fractional transformation $x \mapsto (1-2x)/(2x)$ taking ∞ to $1/2$. The original points $(1, -1), \infty^+$ correspond to the points $P = (-1, 1)$, $Q = (0, \frac{1}{4})$ on C. The curve C has good reduction at $p = 11$, and we compute

$$\int_P^Q \omega_0 = \int_P^Q \omega_1 = O(11^6), \int_P^Q \omega_2 = 7 \cdot 11 + 6 \cdot 11^2 + 3 \cdot 11^3 + 11^4 + 5 \cdot 11^5 + O(11^6),$$

consistent with the fact that $Q - P$ is torsion and ω_0, ω_1 are holomorphic but ω_2 is not.

Example 3.3.5. Let $C : y^2 = (x^4 - 2x^2 - 8x + 1)(x^3 + x + 1)$ (from [Wet97, §1.9]). The Jacobian of this genus 3 curve has Mordell-Weil rank 1. Let $P = \infty$ and $Q = (0, -1)$.

The curve has good reduction at $p = 3$, and we compute

$$\begin{aligned}
a &:= \int_P^Q \omega_0 = 2 \cdot 3 + 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6 + 3^7 + O(3^8), \\
b &:= \int_P^Q \omega_1 = 2 \cdot 3 + 3^2 + 3^4 + O(3^8), \\
c &:= \int_P^Q \omega_2 = 2 \cdot 3^3 + 3^5 + 3^6 + 3^7 + O(3^8).
\end{aligned}$$

Taking

$$\begin{aligned}
\alpha &= b\omega_0 - a\omega_1 \\
\beta &= c\omega_0 - a\omega_2,
\end{aligned}$$

one can use these differentials in the Chabauty method to show that the points P, Q, along with the point $(0, 1)$ are the only three rational points on the curve. We will return to this example in Chapter 6.

Chapter 4

Coleman integration: even degree models

4.1 Introduction

In this chapter, we extend the algorithms in Chapter 3 to even degree models of hyperelliptic curves over unramified extensions of $\mathbb{Q}_p$. Throughout this chapter, we assume that the genus g hyperelliptic curve C is given by a model of the form $y^2 = f(x)$, where f is a separable polynomial with $\deg f = 2g+2$. This allows us to make explicit constructions requiring Coleman integration for both odd and even models of hyperelliptic curves.

A few remarks are in order about computing with even degree models of hyperelliptic curves. We begin with some notation. Let C' be the affine curve obtained by taking C and deleting the Weierstrass points (which are now just the support of the divisor of y). Since $d = 2g+2$, recall that C has a pair of non-Weierstrass points, P_{∞^+} and P_{∞^-}, which are swapped by the hyperelliptic involution. From a computational perspective, we prefer that f is monic. So we shall henceforth assume that f is monic, $d = 2g+2$, and C has two rational points at infinity. For technical reasons which shall become clear in §4.2, we further require that the prime p be a prime of good reduction such that $p > g$.

4.2 A bit more p-adic cohomology

Let $H^1_{dR}(C')$ and $H^1_{dR}(C')^-$ be as in [Har10a]. We begin with a basis for $H^1_{dR}(C')^-$:

Lemma 4.2.1. *The space $H^1_{dR}(C')^-$ has basis $\{x^i \frac{dx}{2y}\}$ for $i = 0, \ldots, 2g$.*

Proof. See [Har10a, §3.2]. □

This gives us one extra element than before, and the matrix of the Frobenius action on this space will now be a $(2g+1) \times (2g+1)$ matrix. Nevertheless, Kedlaya's algorithm works in essentially the same way in this situation. The reductions described in §2.2.2

are just applied to an extra differential. The key is how the eigenvalues of Frobenius on $H^1_{dR}(C')^-$ change when one introduces this extra differential.

More precisely, let $P_C(t)$ be the numerator of the zeta function of C, with $P_C(t) = t^{2g} + c_{2g-1}t^{2g-1} + \cdots + c_0$, a monic polynomial over $\mathbb{Z}$. Denote its roots by $(\alpha_i)_{i=1}^{2g}$.

Proposition 4.2.2 (Harrison, § 3.1). *The eigenvalues of Frobenius on $H^1_{dR}(C')^-$ are*

$$\{\alpha_1, \ldots, \alpha_{2g}, q\}.$$

Harrison also proves a lemma on p-integrality of the matrix of Frobenius: namely, if $p > g$, the matrix of the action of Frobenius with respect to the basis in Lemma 4.2.1 is p-integral as before.

These two results have the following consequence for us: if $p > g$, the characteristic polynomial $P(t)$ of the action of Frobenius on the set $\{\frac{dx}{2y}, \ldots \frac{x^{2g}dx}{2y}\}$ is

$$P(t) = (t-q)P_C(t),$$

where $P_C(t)$ is the characteristic polynomial of Frobenius acting on the Tate module of the Jacobian of C. In particular, as this merely introduces an extra eigenvalue $\neq 1$, one can still compute the linear system of Frobenius on these differentials as before and recover Coleman integrals on the pseudo-basis.

4.3 Coleman integration on even models

4.3.1 Local coordinates

The previous algorithms (Algorithms 2.1.3, 2.1.5) for computing local coordinates at finite non-Weierstrass points and finite Weierstrass points, respectively, apply verbatim to even models as well.

Our previous integration algorithms are essentially unchanged. However, we require a bit of notation. Let B_1 be the set of differentials

$$B_1 = \left\{\frac{dx}{2y}, x\frac{dx}{2y}, \ldots, x^{2g}\frac{dx}{2y}\right\}.$$

Let $\omega_i = x^i\frac{dx}{2y}$. An odd differential ω on C can be represented as a linear combination of elements of B_1 . The computation of $\int_P^Q \omega$ thus can be reduced to the computation of Coleman integrals on B_1, and we have the following algorithms:

4.3.2 Integrals

Algorithm 4.3.1 (Tiny Coleman integrals).
Input: Points $P, Q \in C(\mathbb{C}_p)$ in the same residue disk (neither equal to points above ∞) and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.

1. Compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t.

2. Formally integrate the power series in t:

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^{t(Q)} \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt.$$

Algorithm 4.3.2 (Coleman integration in finite non-Weierstrass disks).
Input: The differentials $(\omega_i)_{i=0}^{2g}$, points $P, Q \in C(\mathbb{C}_p)$ in finite non-Weierstrass residue disks, and a positive integer m such that the residue fields of P, Q are contained in $\mathbb{F}_{p^m}$.
Output: The integrals $\left(\int_P^Q \omega_i\right)_{i=0}^{2g}$.

1. Calculate the action of the m-th power of Frobenius on each pseudo-basis element (see Remark 4.3.3 below):

$$(\phi^m)^* \omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j. \tag{4.3.1}$$

2. By change of variables (see Remark 4.3.4), we obtain

$$\sum_{j=0}^{2g} (M - I)_{ij} \int_P^Q \omega_j = f_i(P) - f_i(Q) - \int_P^{\phi^m(P)} \omega_i - \int_{\phi^m(Q)}^Q \omega_i \tag{4.3.2}$$

(the *fundamental linear system*). As the eigenvalues of the matrix M are algebraic integers of $\mathbb{C}_p$-norm not equal to 1, the matrix $M - I$ is invertible, and we may solve (4.3.2) to obtain the integrals $\int_P^Q \omega_i$.

Remark 4.3.3. To compute the action of ϕ^m, first perform Algorithm 2.2.4 to write

$$\phi^* \omega_i = dg_i + \sum_{j=0}^{2g} B_{ij}\omega_j.$$

If we view f, g as column vectors and M, B as matrices, we then have

$$\begin{aligned} f &= \phi^{m-1}(g) + B\phi^{m-2}(g) + \cdots + B\phi_K(B) \cdots \phi_K^{m-2}(B)g \\ M &= B\phi_K(B) \cdots \phi_K^{m-1}(B). \end{aligned}$$

Remark 4.3.4. We obtain (4.3.2) as follows. By change of variables,

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

Adding $\int_P^{\phi^m(P)} \omega_i + \int_{\phi^m(Q)}^Q \omega_i$ to both sides of this equation yields

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

which is equivalent to (4.3.2).

Algorithm 4.3.5 (Finding a near-boundary point in a Weierstrass disk).
Input: A Weierstrass point P, and a positive integer d.
Output: A point $R = (x(p^{1/d}), p^{1/d})$ in the disk of P defined over the totally ramified extension $\mathbb{Q}_p(p^{1/d})$.

1. Compute a parametrization $(x(t), t)$ at P in terms of the local coordinate t.

2. Evaluate local coordinates at $t = p^{1/d}$. This is R.

Algorithm 4.3.6 (Coleman integration in a Weierstrass disk).
Input: A Weierstrass point P, a positive integer d, a non-Weierstrass point Q, and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.

1. Use Algorithm 4.3.5 to find R. Keep the local coordinate $(x(t), t)$ at P.

2. Compute $\int_P^R \omega_i$ as a tiny integral: $\int_P^R \omega_i = \int_0^{p^{1/d}} \frac{x(t)^i dx(t)}{2t} dt$.

3. Use the fundamental linear system to compute $\int_R^Q \omega_i$.

4. Use additivity in endpoints to recover $\int_P^Q \omega_i = \int_P^R \omega_i + \int_R^Q \omega_i$.

4.3.3 Using the linear system

Here we show how in direct analogue to [BBK10], one can compute the matrix of Frobenius on a pseudo-basis to recover the global integrals.

Example 4.3.7. Modifying the Leprévost example (Example 3.3.4), let C_{even} be the hyperelliptic curve

$$y^2 = x^6 - x^5 + \frac{1}{4}x^4 - 2x^3 + 5x^2 - 4x + 1$$

given by a *monic* sextic let and C_{odd} the hyperelliptic curve

$$y^2 = x^5 + \frac{33}{16}x^4 + \frac{3}{4}x^3 + \frac{3}{8}x^2 - \frac{1}{4}x + \frac{1}{16}$$

given by a monic quintic. Note that $p = 11$ is a prime of good reduction.

We have inverse isomorphisms

$$\begin{aligned} \psi : C_{\text{even}} &\longrightarrow C_{\text{odd}} \\ (x, y) &\mapsto \left(\frac{1}{1-2x}, \frac{2y}{(1-2x)^3}\right), \end{aligned}$$

and

$$\begin{aligned} \psi^{-1} : C_{\text{odd}} &\longrightarrow C_{\text{even}} \\ (x, y) &\mapsto \left(\frac{x-1}{2x}, \frac{y}{2x^3}\right), \end{aligned}$$

so

$$\begin{aligned} \int_{C_{\text{even}}} \frac{dx}{y} &= \int_{\psi^{-1}\circ\psi(C_{\text{even}})} \frac{dx}{y} \\ &= \int_{\psi(C_{\text{even}})} (\psi^{-1})^* \left(\frac{dx}{y}\right) \\ &= \int_{C_{\text{odd}}} \frac{1}{2x^2}\frac{2x^3}{y} dx \\ &= \int_{C_{\text{odd}}} \frac{x dx}{y} \end{aligned}$$

and similarly

$$\int_{C_{\text{even}}} \frac{x dx}{y} = \int_{C_{\text{odd}}} \frac{x-1}{2}\frac{dx}{y}.$$

We illustrate this further with a numerical example. Take the following points on C_{even}:

$$\begin{aligned} P_0 &= \left(1 + 11 + O(11^5), 5 + 3 \cdot 11 + 9 \cdot 11^2 + 7 \cdot 11^3 + 3 \cdot 11^4 + O(11^5)\right) \\ Q_0 &= \left(11 + O(11^6), 1 + 9 \cdot 11 + 5 \cdot 11^2 + 5 \cdot 11^3 + 5 \cdot 11^4 + O(11^5))\right) \end{aligned}$$

whose respective images under ψ are

$$\begin{aligned}P_1 &= \big(10 + 11 + 7 \cdot 11^2 + 7 \cdot 11^3 + 6 \cdot 11^4 + O(11^5), 1 + 9 \cdot 11 + 2 \cdot 11^2 + 4 \cdot 11^3 + 3 \cdot 11^4 + O(11^5)\big)\\ Q_1 &= \big(1 + 2 \cdot 11 + 4 \cdot 11^2 + 8 \cdot 11^3 + 5 \cdot 11^4 + O(11^5), 2 + 8 \cdot 11 + 3 \cdot 11^2 + 6 \cdot 11^3 + 3 \cdot 11^4 + O(11^5)\big)\end{aligned}$$

Then we have

$$\int_{P_0}^{Q_0} \frac{dx}{2y} = \int_{P_1}^{Q_1} \frac{xdx}{2y} = 7 \cdot 11 + 9 \cdot 11^2 + 3 \cdot 11^3 + 4 \cdot 11^4 + O(11^5)$$

and

$$\int_{P_0}^{Q_0} \frac{xdx}{2y} = \frac{1}{2} \int_{P_1}^{Q_1} \frac{x-1}{2} \frac{dx}{2y} = 11 + 7 \cdot 11^2 + 9 \cdot 11^3 + 11^4 + O(11^5).$$

Chapter 5

Coleman integration: iterated integrals

5.1 Introduction

We continue our discussion of algorithms for Coleman integrals on hyperelliptic curves by directly generalizing our work in Chapter 3 to formulate algorithms for iterated integrals.

Indeed, Coleman's theory of integration is not limited to single integrals; it gives rise to an entire class of locally analytic functions, the *Coleman functions*, on which antidifferentiation is well-defined. In other words, one can define iterated p-adic integrals [Col82], [Bes02b]

$$\int_P^Q \omega_n \cdots \omega_1$$

which behave formally like iterated path integrals

$$\int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1.$$

These appear in several applications of Coleman integration, e.g., p-adic regulators in K-theory [CdS88], [Col82], and the nonabelian Chabauty method [Kim10a].

As in earlier chapters, we assume that $p > 2g - 1$ and C is a genus g hyperelliptic curve. For clarity, we consider C just over $K = \mathbb{Q}_p$, but the natural generalization to an unramified extension K of $\mathbb{Q}_p$ exists, as in Chapter 3.

Let ϕ be a p-power lift of Frobenius. When ω_i is said to be a basis differential, we mean that it is the differential $\omega_i = x^i \frac{dx}{2y}$.

Our methods for computing iterated integrals are similar in spirit to those detailed in Chapter 3. We begin with algorithms for tiny iterated integrals, use Frobenius equivariance to write down a linear system yielding the values of integrals between points in different residue disks, and, if needed, use basic properties of integration to correct endpoints.

5.2 Iterated path integrals

We follow the convention of Kim [Kim10a] and define our integrals as follows:

$$\int_P^Q \omega_{i_1}\omega_{i_2}\cdots\omega_{i_{n-1}}\omega_{i_n} := \int_P^Q \omega_{i_1}(R_1)\int_P^{R_1}\omega_{i_2}(R_2)\cdots\int_P^{R_{n-2}}\omega_{i_{n-1}}(R_{n-1})\int_P^{R_{n-1}}\omega_{i_n},$$

for a collection of dummy parameters $R_1, \ldots, R_{n-1}$.

We begin by recalling some key formal properties satisfied by iterated path integrals [Che71], which we shall use throughout this chapter:

Proposition 5.2.1. *Let $\omega_{i_1}, \ldots, \omega_{i_n}$ be 1-forms, holomorphic at points P, Q on C. Then the following are true:*

1. $\int_P^P \omega_{i_1}\omega_{i_2}\cdots\omega_{i_n} = 0,$
2. $\sum_{\text{all permutations }\sigma}\int_P^Q \omega_{\sigma(i_1)}\omega_{\sigma(i_2)}\cdots\omega_{\sigma(i_n)} = \prod_{j=1}^n \int_P^Q \omega_{i_j},$
3. $\int_P^Q \omega_{i_1}\cdots\omega_{i_n} = (-1)^n\int_Q^P \omega_{i_n}\cdots\omega_{i_1}.$

As an easy corollary of Proposition 5.2.1(2), we have

Corollary 5.2.2. *For a 1-form ω_i and points P, Q as before,*

$$\int_P^Q \omega_i\omega_i\cdots\omega_i = \frac{1}{n!}\left(\int_P^Q \omega_i\right)^n.$$

When possible, we will use this to write an iterated integral in terms of a single integral.

As in Chapter 3, we will use Kedlaya's algorithm to rewrite an odd differential

$$\omega = g(x,y)\frac{dx}{2y} \in A^\dagger\frac{dx}{2y}$$

as

$$\omega = df + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1} \tag{5.2.1}$$

with $f \in A^\dagger$, $c_i \in K$, and $\omega_i = \frac{x^i\,dx}{2y}$ $(i = 0, \ldots, 2g-1)$. This then reduces the problem of integrating ω to the integration of the ω_i.

Recall that we refer to Coleman integrals between two points in the same residue disk as a tiny integral. Naturally, then, by a *tiny iterated integral* we mean an iterated integral between points in the same residue disk. As we would also like to consider iterated integrals that are not necessarily tiny, we will need to employ the analogue of "additivity in endpoints" to link integrals between different residue disks:

First, let us consider the case where we are breaking up the path by one point.

Lemma 5.2.3. *Let P, P', Q be points on C such that a path is to be taken from P to Q via P'. Let $\omega_1, \ldots, \omega_n$ be a collection of 1-forms holomorphic at the points P, P', Q.*

Then the following statement holds:

$$\int_P^Q \omega_1 \cdots \omega_n = \sum_{i=0}^{n} \int_{P'}^{Q} \omega_1 \cdots \omega_i \int_P^{P'} \omega_{i+1} \cdots \omega_n.$$

Proof. We proceed by induction. The case $n = 1$ is clear. Let us suppose the statement holds for $n = k$. Then we have that

$$\begin{aligned}
\int_P^Q \omega_1 \cdots \omega_{k+1} &= \left(\int_P^Q \omega_1 \cdots \omega_k\right) (R) \int_P^R \omega_{k+1} \\
&= \left(\sum_{i=0}^{k} \int_{P'}^{Q} \omega_1 \cdots \omega_i \int_P^{P'} \omega_{i+1} \cdots \omega_k\right) (R) \int_P^R \omega_{k+1} \\
&= \left(\int_P^{P'} \omega_1 \cdots \omega_k\right) (R) \int_P^R \omega_{k+1} && (5.2.2) \\
&\quad + \left(\int_{P'}^{Q} \omega_1\right) \left(\int_P^{P'} \omega_2 \cdots \omega_k\right) (R) \int_P^R \omega_{k+1} && (5.2.3) \\
&\quad \cdots + \left(\int_{P'}^{Q} \omega_1 \cdots \omega_{k-1} \int_P^{P'} \omega_k\right) (R) \int_P^R \omega_{k+1} && (5.2.4) \\
&\quad + \left(\int_{P'}^{Q} \omega_1 \cdots \omega_k\right) (R) \int_P^R \omega_{k+1}. && (5.2.5)
\end{aligned}$$

Observe that this last iterated integral (5.2.5) can be rewritten as

$$\left(\int_{P'}^{Q} \omega_1 \cdots \omega_k\right) (R) \left(\int_P^{P'} \omega_{k+1} + \int_{P'}^{R} \omega_{k+1}\right),$$

and that further, the terms from (5.2.2) through (5.2.4) give us

$$\sum_{i=0}^{k-1} \int_{P'}^{Q} \omega_1 \cdots \omega_i \int_P^{P'} \omega_{i+1} \cdots \omega_{k+1},$$

Thus we have

$$\begin{aligned}
\int_P^Q \omega_1 \cdots \omega_{k+1} &= \sum_{i=0}^{k-1} \int_{P'}^{Q} \omega_1 \cdots \omega_i \int_P^{P'} \omega_{i+1} \cdots \omega_{k+1} \\
&\quad + \left(\int_{P'}^{Q} \omega_1 \cdots \omega_k\right) \left(\int_P^{P'} \omega_{k+1}\right) + \int_{P'}^{Q} \omega_1 \cdots \omega_{k+1} \\
&= \sum_{i=0}^{k+1} \int_{P'}^{Q} \omega_1 \cdots \omega_i \int_P^{P'} \omega_{i+1} \cdots \omega_{k+1},
\end{aligned}$$

as desired. □

Applying Lemma 5.2.3 twice, we obtain the following, which will be used to link integrals between different residue disks:

Lemma 5.2.4 (Link lemma). *Let points P, P', Q', Q be on C such that a path is to be taken from P to P' to Q' to Q. Let $\omega_1, \ldots, \omega_n$ be a collection of 1-forms holomorphic at the points P, P', Q, Q'. Then we have*

$$\int_P^Q \omega_1 \cdots \omega_n = \sum_{i=0}^{n} \int_{Q'}^{Q} \omega_1 \cdots \omega_i \left(\sum_{j=i}^{n} \int_{P'}^{Q'} \omega_{i+1} \cdots \omega_j \int_P^{P'} \omega_{j+1} \cdots \omega_n \right).$$

Below we record some specific cases of the link lemma, which we shall use throughout this chapter.

Example 5.2.5 (Link lemma for double integrals). Suppose we have two differentials ω_0, ω_1. Then we have

$$\int_P^Q \omega_0\omega_1 = \int_P^{P'} \omega_0\omega_1 + \int_{P'}^{Q'} \omega_0\omega_1 + \int_{Q'}^{Q} \omega_0\omega_1 + \int_P^{P'} \omega_1 \int_{P'}^{Q} \omega_0 + \int_{P'}^{Q'} \omega_1 \int_{Q'}^{Q} \omega_0.$$

Example 5.2.6 (Link lemma for triple integrals). Suppose we have three differentials $\omega_0, \omega_1, \omega_2$. Then we have

$$\begin{aligned}\int_P^Q \omega_0\omega_1\omega_2 &= \int_P^{P'} \omega_0\omega_1\omega_2 + \int_{P'}^{Q'} \omega_0\omega_1\omega_2 + \int_{Q'}^{Q} \omega_0\omega_1\omega_2 \\ &\quad + \int_P^{Q'} \omega_2 \int_{Q'}^{Q} \omega_0\omega_1 + \int_P^{P'} \omega_2 \int_{P'}^{Q'} \omega_0\omega_1 + \int_{P'}^{Q'} \omega_1\omega_2 \int_{Q'}^{Q} \omega_0 + \int_P^{P'} \omega_1\omega_2 \int_{P'}^{Q'} \omega_0 \\ &\quad + \int_P^{P'} \omega_2 \int_{P'}^{Q'} \omega_1 \int_{Q'}^{Q} \omega_0.\end{aligned}$$

For a numerical verification of this identity, see Example 5.3.4.

5.3 Tiny iterated integrals

We begin with an algorithm to compute tiny iterated integrals.

Algorithm 5.3.1 (Tiny iterated integrals).
Input: Points $P, Q \in C(\mathbb{Q}_p)$ in the same residue disk (neither equal to the point at infinity) and differentials $\xi_1, \ldots, \xi_n$ without poles in the disk of P.
Output: The integral $\int_P^Q \xi_1\xi_2 \cdots \xi_n$.

1. Compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t.

2. For each k, write $\xi_k(x, y)$ in terms of t: $\xi_k(t) := \xi_k(x(t), y(t)) = \frac{(x(t))^k x'(t)dt}{2y(t)}$.

3. Let $I_{n+1}(t) := 1$.

4. Compute, for $k = n, \ldots, 2$, in descending order,

$$\begin{aligned} I_k(t) &= \int_P^{R_n} \xi_k I_{k+1} \\ &= \int_0^{t(R_n)} \xi_k(u) I_{k+1}(u), \end{aligned}$$

   with R_k in the disc of P.

5. Upon computing $I_2(t)$, we arrive at the desired integral:

$$\int_P^Q \xi_1\xi_2\cdots\xi_n = I_1(t) = \int_0^{t(Q)} \xi_1(u) I_2(u).$$

5.3.1 Examples

Here we provide some numerical examples. See also §5.5.1 for more detail regarding the first example.

Example 5.3.2 (Tiny double integrals). Take C to be the elliptic curve

$$y^2 = x(x-1)(x+9),$$

let $p = 7$, and consider the points $P = (9, 36)$ and $P' = \phi(P)$. Let $\omega_0 = \frac{dx}{2y}, \omega_1 = \frac{xdx}{2y}$, and we compute

$$\begin{aligned} \int_P^{P'} \omega_0\omega_0 &= 2\cdot 7^2 + 4\cdot 7^3 + 5\cdot 7^4 + 4\cdot 7^5 + 6\cdot 7^6 + O(7^7) = \int_{P'}^{P} \omega_0\omega_0 \\ \int_P^{P'} \omega_0\omega_1 &= 4\cdot 7^2 + 5\cdot 7^3 + 2\cdot 7^5 + 4\cdot 7^6 + O(7^7) = \int_{P'}^{P} \omega_1\omega_0 \\ \int_P^{P'} \omega_1\omega_0 &= 4\cdot 7^2 + 5\cdot 7^5 + 6\cdot 7^6 + O(7^7) = \int_{P'}^{P} \omega_0\omega_1 \\ \int_P^{P'} \omega_1\omega_1 &= 7^2 + 2\cdot 7^3 + 2\cdot 7^4 + 5\cdot 7^5 + 2\cdot 7^6 + O(7^7) = \int_{P'}^{P} \omega_1\omega_1. \end{aligned}$$

Moreover, given that

$$\begin{aligned} \int_P^{P'} \omega_0 &= 5\cdot 7 + 4\cdot 7^2 + 7^3 + 6\cdot 7^4 + 7^5 + O(7^6) \\ \int_P^{P'} \omega_1 &= 3\cdot 7 + 4\cdot 7^2 + 7^3 + 7^4 + 6\cdot 7^5 + O(7^6), \end{aligned}$$

we can verify that

$$\begin{aligned}\int_P^{P'} \omega_0\omega_0 &= \frac{1}{2}\left(\int_P^{P'} \omega_0\right)^2\\ \int_P^{P'} \omega_1\omega_1 &= \frac{1}{2}\left(\int_P^{P'} \omega_1\right)^2,\end{aligned}$$

as well as that

$$\int_P^{P'} \omega_0 w_1 + \int_P^{P'} \omega_1\omega_0 = 7^2 + 6\cdot 7^3 + 4\cdot 7^6 + O(7^7) = \left(\int_P^{P'} \omega_0\right)\left(\int_P^{P'} \omega_1\right).$$

Example 5.3.3 (Tiny triple integrals and some identities). Let E be the elliptic curve $y^2 = x^3 - 16x + 16$ and take $p = 5$. Consider the following points on E:

$$\begin{aligned}P &= \left(0, 4 + O(5^{10}))\right)\\ P' &= \left(5 + O(5^{11}), 4 + 3\cdot 5 + 5^2 + 4\cdot 5^4 + 3\cdot 5^5 + 5^6 + 3\cdot 5^7 + 2\cdot 5^9 + O(5^{10})\right).\end{aligned}$$

Let $\omega_0 = \frac{dx}{2y}, \omega_1 = x\frac{dx}{2y}$; we compute the following integrals:

$$\begin{aligned}\int_P^{P'} \omega_0\omega_0\omega_0 &= 3\cdot 5^3 + 2\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 3\cdot 5^7 + O(5^9)\\ \int_P^{P'} \omega_0\omega_0\omega_1 &= 5^4 + 2\cdot 5^5 + 4\cdot 5^6 + 2\cdot 5^7 + 3\cdot 5^8 + 3\cdot 5^9 + O(5^{10})\\ \int_P^{P'} \omega_0\omega_1\omega_0 &= 5^4 + 4\cdot 5^5 + 5^6 + 4\cdot 5^7 + 5^9 + O(5^{10})\\ \int_P^{P'} \omega_0\omega_1\omega_1 &= 5^4 + 5^5 + 4\cdot 5^6 + 4\cdot 5^7 + 5^8 + 5^9 + O(5^{10})\\ \int_P^{P'} \omega_1\omega_0\omega_0 &= 5^5 + 5^6 + 5^7 + 2\cdot 5^8 + 4\cdot 5^9 + O(5^{10})\\ \int_P^{P'} \omega_1\omega_0\omega_1 &= 3\cdot 5^4 + 5^5 + 4\cdot 5^7 + 2\cdot 5^8 + 3\cdot 5^9 + O(5^{10})\\ \int_P^{P'} \omega_1\omega_1\omega_0 &= 5^4 + 3\cdot 5^5 + 4\cdot 5^6 + 2\cdot 5^7 + 3\cdot 5^8 + 3\cdot 5^9 + O(5^{10})\\ \int_P^{P'} \omega_1\omega_1\omega_1 &= 5^6 + 5^7 + 4\cdot 5^{10} + 2\cdot 5^{11} + O(5^{12}).\end{aligned}$$

We also have

$$\int_P^{P'} \omega_0 = 2 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + 4 \cdot 5^5 + 4 \cdot 5^6 + O(5^7)$$
$$\int_P^{P'} \omega_1 = 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 + 5^6 + 5^7 + O(5^8).$$

So we see that

$$\begin{aligned}\int_P^{P'} \omega_0\omega_0\omega_0 &= \frac{1}{6}\left(\int_P^{P'} \omega_0\right)^3 \\ &= 3 \cdot 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 + O(5^9),\end{aligned}$$

as well as that

$$\begin{aligned}\int_P^{P'} \omega_0\omega_0\omega_1 + \int_P^{P'} \omega_0\omega_1\omega_0 + \int_P^{P'} \omega_1\omega_0\omega_0 &= \frac{1}{2}\left(\int_P^{P'} \omega_0\right)^2 \left(\int_P^{P'} \omega_1\right) \\ &= 2 \cdot 5^4 + 2 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 + 5^8 + 4 \cdot 5^9 + O(5^{10}),\end{aligned}$$

and

$$\begin{aligned}\int_P^{P'} \omega_1\omega_1\omega_0 + \int_P^{P'} \omega_1\omega_0\omega_1 + \int_P^{P'} \omega_0\omega_1\omega_1 &= \frac{1}{2}\left(\int_P^{P'} \omega_0\right) \left(\int_P^{P'} \omega_1\right)^2 \\ &= 5^5 + 4 \cdot 5^6 + 5^7 + 3 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}),\end{aligned}$$

and finally, that

$$\begin{aligned}\int_P^{P'} \omega_1\omega_1\omega_1 &= \frac{1}{6}\left(\int_P^{P'} \omega_1\right)^3 \\ &= 5^6 + 5^7 + 4 \cdot 5^{10} + 2 \cdot 5^{11} + O(5^{12}).\end{aligned}$$

Example 5.3.4 (Triple link lemma). Continuing with the previous example, further set

$$\begin{aligned}Q &= (2 \cdot 5 + O(5^{11}), 4 + 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 5^6 + 3 \cdot 5^7 + 3 \cdot 5^8 + 5^9 + O(5^{10})), \\ Q' &= (3 \cdot 5 + O(5^{11}), 4 + 4 \cdot 5 + 5^2 + 2 \cdot 5^3 + 4 \cdot 5^4 + 3 \cdot 5^5 + 5^7 + 2 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10})),\end{aligned}$$

so that P, P', Q', Q all lie in the same residue disk. Let $\omega_0 = \frac{dx}{y}, \omega_1 = x\,\frac{dx}{2y}, \omega_2 = x^2\,\frac{dx}{2y}$.

Directly computing the triple integral between P and Q yields

$$\int_P^{Q} \omega_0\omega_1\omega_2 = 4 \cdot 5^5 + 2 \cdot 5^6 + 4 \cdot 5^9 + O(5^{10}).$$

We would like to provide a numerical verification of the identity present in the link lemma for triple integrals. So we begin by computing

$$\begin{aligned}
\int_P^{P'} \omega_2 &= 4 \cdot 5^3 + 5^5 + 2 \cdot 5^6 + 2 \cdot 5^8 + 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_2 &= 4 \cdot 5^3 + 3 \cdot 5^4 + 3 \cdot 5^5 + 4 \cdot 5^6 + 5^7 + 2 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}) \\
\int_{Q'}^{Q} \omega_0 &= 3 \cdot 5 + 4 \cdot 5^3 + 5^4 + 3 \cdot 5^5 + 4 \cdot 5^7 + 4 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_0 &= 4 \cdot 5 + 2 \cdot 5^2 + 5^3 + 5^4 + 2 \cdot 5^5 + 3 \cdot 5^6 + 2 \cdot 5^7 + 2 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_1 &= 3 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 4 \cdot 5^5 + 3 \cdot 5^6 + 3 \cdot 5^7 + 3 \cdot 5^8 + O(5^{10})
\end{aligned}$$

as well as that

$$\begin{aligned}
\int_P^{P'} \omega_1\omega_2 &= 3 \cdot 5^4 + 4 \cdot 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_0\omega_1 &= 4 \cdot 5^4 + 3 \cdot 5^5 + 4 \cdot 5^7 + 5^9 + O(5^{10}) \\
\int_P^{P'} \omega_1\omega_2 &= 3 \cdot 5^4 + 4 \cdot 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_1\omega_2 &= 5^4 + 3 \cdot 5^5 + 5^7 + 2 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}) \\
\int_{Q'}^{Q} \omega_0\omega_1 &= 2 \cdot 5^3 + 3 \cdot 5^5 + 5^6 + 2 \cdot 5^7 + 2 \cdot 5^8 + 4 \cdot 5^9 + O(5^{10}) \\
\int_P^{P'} \omega_0\omega_1\omega_2 &= 5^5 + 5^6 + 5^7 + 3 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}) \\
\int_{Q'}^{Q} \omega_0\omega_1\omega_2 &= 3 \cdot 5^5 + 2 \cdot 5^6 + 2 \cdot 5^7 + 2 \cdot 5^8 + 3 \cdot 5^9 + O(5^{10}) \\
\int_{P'}^{Q'} \omega_0\omega_1\omega_2 &= 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 + 5^8 + 4 \cdot 5^9 + O(5^{10}),
\end{aligned}$$

from which we see that

$$\begin{aligned}
&\int_P^{P'} \omega_0\omega_1\omega_2 + \int_{P'}^{Q'} \omega_0\omega_1\omega_2 + \int_{Q'}^{Q} \omega_0\omega_1\omega_2 \\
&+ \int_P^{Q'} \omega_2 \int_{Q'}^{Q} \omega_0\omega_1 + \int_P^{P'} \omega_2 \int_{P'}^{Q'} \omega_0\omega_1 + \int_{P'}^{Q'} \omega_1\omega_2 \int_{Q'}^{Q} \omega_0 + \int_P^{P'} \omega_1\omega_2 \int_{P'}^{Q'} \omega_0 \\
&+ \int_P^{P'} \omega_2 \int_{P'}^{Q'} \omega_1 \int_{Q'}^{Q} \omega_0 \\
&= 4\cdot 5^5 + 2\cdot 5^6 + 4\cdot 5^9 + O(5^{10}).
\end{aligned}$$

5.4 Iterated integrals: linear system

As with single integrals, to compute general Coleman integrals, we use Dwork's principle of analytic continuation along Frobenius, in the form of Kedlaya's algorithm (Algorithm 2.2.4) for calculating the action of Frobenius on de Rham cohomology. This gives us a linear system that allows us to solve for all $(2g)^n$ n-fold iterated integrals on basis differentials.

Theorem 5.4.1. *Let P, Q be non-Weierstrass points on a hyperelliptic curve C and $\omega_0, \ldots, \omega_{2g-1}$ basis differentials. For constants $c_{i_0,\ldots,i_{2g-1}}$ computable in terms of $(2g-1)$-fold iterated integrals and $2g$-fold tiny iterated integrals, the $2g$-fold iterated Coleman integrals on basis differentials between P, Q can be computed via a linear system of the form*

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_{i_0}\cdots\omega_{i_{2g-1}} \\ \vdots \end{pmatrix} = (I_{(2g)^n} - B^{\otimes n}) \begin{pmatrix} \vdots \\ c_{i_0\cdots i_{2g-1}} \\ \vdots \end{pmatrix},$$

where $B = M^t$ is the transpose of the matrix of Frobenius M.

Proof. By the Link lemma (Lemma 5.2.4), we can reduce to the case where both P and Q are Teichmüller. Then we have

$$\begin{aligned}
\int_P^Q \omega_{i_i}\cdots\omega_{i_n} &= \int_{\phi(P)}^{\phi(Q)} \omega_{i_i}\cdots\omega_{i_n} \\
&= \int_P^Q \phi^*(\omega_{i_i}\cdots\omega_{i_n}) \\
&= \int_P^Q \phi^*(\omega_{i_i})\cdots\phi^*(\omega_{i_n}). \qquad (5.4.1)
\end{aligned}$$

Recall that given $\omega_0, \ldots, \omega_{2g-1}$ a basis for $H^1_{dR}(C)$, we have

$$\phi^*\omega_{i_\ell} = df_{i_\ell} + \sum_{j=0}^{2g-1} M_{i_\ell j}\omega_j.$$

Substituting this expression in for each factor of (5.4.1) and expanding yields the linear system. □

To illustrate our methods, in the next section, we present a more explicit version of this theorem, accompanied by algorithms, in the case of double integrals. We shall use these in our applications to Kim's nonabelian Chabauty method in Chapter 7.

5.5 Explicit double integrals

5.5.1 Tiny double integrals

We revisit Example 5.3.2 and show how we carry out Algorithm 5.3.1 for double integrals for an elliptic curve:

Example 5.5.1. Take C to be the elliptic curve $y^2 = x(x-1)(x+9)$, let $p = 7$, and consider the points $P = (9, 36), Q = \mathrm{Frob}(P)$, and $R = (a + x(P), \sqrt{f(a + x(P))})$ so that R is in the same disk as P and Q. Furthermore, let $\omega_0 = \frac{dx}{2y}, \omega_1 = \frac{xdx}{2y}$.

We compute the local coordinates at P:

$$\begin{aligned} x(t) &= 9 + t + O(t^{20}) \\ y(t) &= 36 + \frac{21}{4}t + \frac{119}{1152}t^2 - \frac{65}{55296}t^3 + \frac{2219}{95551488}t^4 - \frac{7}{509607936}t^5 + O(t^6). \end{aligned}$$

Then setting $I_2 := \int x\frac{dx}{2y}$, and making it a definite integral, we have

$$\begin{aligned} I_2|_P^R &= \int_P^R x\frac{dx}{2y} \\ &= \int_0^a x(t)\frac{dx(t)}{2y(t)} \\ &= \frac{1}{8}a - \frac{5}{2304}a^2 + \frac{91}{995328}a^3 - \frac{1121}{191102976}a^4 \\ &\quad + \frac{22129}{45864714240}a^5 - \frac{360185}{7925422620672}a^6 + O(a^7), \end{aligned}$$

from which we arrive at

$$\begin{aligned} I &= \int_0^{x(Q)-x(P)} I_2(a)\frac{dx(R(a))}{2y(R(a))} \\ &= 4 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 4 \cdot 7^5 + O(7^6). \end{aligned}$$

5.5.2 The linear system for double integrals between Teichmüller points

Let M be the matrix of Frobenius, and let P, Q be Teichmüller points.

In this subsection, we make explicit one aspect of Theorem 5.4.1: we give an algorithm to compute double integrals between Teichmüller points.

Algorithm 5.5.2 (Double Coleman integration between Teichmüller points).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, Teichmüller points $P, Q \in C(\mathbb{Q}_p)$ in non-Weierstrass residue disks.
Output: The double integrals $\left(\int_P^Q \omega_i\omega_j\right)_{i,j=0}^{2g-1}$.

1. Calculate the action of Frobenius on each basis element
$$(\phi)^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j. \tag{5.5.1}$$

2. Use Algorithm 3.2.3 to compute single Coleman integrals on all basis differentials: $\int_P^Q \omega_j, j = 0, \ldots, 2g-1$.

3. Use Algorithm 3.2.8 to compute other single Coleman integrals: $\int_P^Q df_i f_k, \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j f_k$ for each i, k.

4. Use the results of the above two steps to write down, for each i, k, the constant
$$c_{ik} = \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) + \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)(f_k(R) - f_k(P))$$
$$+ f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)).$$

5. Recover the double integrals (see Remark 5.5.3 below) via the linear system
$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1}\omega_{2g-1} \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} c_{00} \\ c_{01} \\ \vdots \\ c_{2g-1,2g-1} \end{pmatrix}.$$

Remark 5.5.3. We obtain the linear system in the following manner. Since P, Q are Teichmüller, we have
$$\int_P^Q \omega_i\omega_k = \int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k = \int_P^Q \phi^*(\omega_i\omega_k). \tag{5.5.2}$$

We begin by expanding the right side of (5.5.2).

Recall that given $\omega_0, \ldots, \omega_{2g-1}$ a basis for $H^1_{dR}(C)$, we have

$$\phi^*\omega_i = df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j.$$

Thus we have

$$\begin{aligned}
\int_P^Q \phi^*(\omega_i\omega_k) &= \int_P^Q \phi^*(\omega_i)\phi^*(\omega_k)\\
&= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}\omega_j)(df_k + \sum_{j=0}^{2g-1} M_{kj}\omega_j)\\
&= \int_P^Q df_i df_k + (\sum_{j=0}^{2g-1} M_{ij}\omega_j)df_k + df_i(\sum_{j=0}^{2g-1} M_{kj}\omega_j) + (\sum_{j=0}^{2g-1} M_{ij}\omega_j)(\sum_{j=0}^{2g-1} M_{kj}\omega_j)
\end{aligned}$$

We expand the first three quantities separately. First, we have

$$\begin{aligned}
\int_P^Q df_i df_k &= \int_P^Q df_i(R)\int_P^R df_k\\
&= \int_P^Q df_i(R)(f_k(R) - f_k(P))\\
&= \int_P^Q df_i(R)(f_k(R)) - f_k(P)\int_P^Q df_i(R)\\
&= \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)).
\end{aligned}$$

Next, we have

$$\begin{aligned}
\int_P^Q (\sum_{j=0}^{2g-1} M_{ij}\omega_j)df_k &= \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)\int_P^R df_k\\
&= \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)(f_k(R) - f_k(P)).
\end{aligned}$$

The third term (via integration by parts) is

$$\begin{aligned}\int_P^Q df_i(\sum_{j=0}^{2g-1} M_{kj}\omega_j) &= \int_P^Q df_i(R)\int_P^R (\sum_{j=0}^{2g-1} M_{kj}\omega_j)\\ &= \left(f_i(R)\int_P^R (\sum_{j=0}^{2g-1} M_{kj}\omega_j)\right)|_{R=P}^{R=Q} - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R))\\ &= f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)).\end{aligned}$$

Denote the sum of these terms by c_{ik}; in other words,

$$\begin{aligned}c_{ik} = \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) + \int_P^Q \sum_{j=0}^{2g-1} M_{ij}\omega_j(R)(f_k(R) - f_k(P))\\ + f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}\omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}\omega_j(R)).\end{aligned}$$

Then rearranging terms, our linear system reads

$$\begin{pmatrix} \int_P^Q \omega_0\omega_0 \\ \int_P^Q \omega_0\omega_1 \\ \vdots \\ \int_P^Q \omega_{2g-1}\omega_{2g-1} \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} c_{00} \\ c_{01} \\ \vdots \\ c_{2g-1,2g-1} \end{pmatrix}.$$

5.5.3 Linking double integrals

Let P' and Q' be in the disks of P and Q, respectively. Using the Link lemma for double integrals (Example 5.2.5), we may link double integrals between different residue disks:

$$\int_P^Q \omega_i\omega_k = \int_P^{P'} \omega_i\omega_k + \int_{P'}^{Q'} \omega_i\omega_k + \int_{Q'}^{Q} \omega_i\omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i. \quad (5.5.3)$$

Algorithm 5.5.4 (Double Coleman integration via Teichmüller points).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in C(\mathbb{C}_p)$ in non-Weierstrass residue disks.
Output: The double integrals $\left(\int_P^Q \omega_i\omega_j\right)_{i,j=0}^{2g-1}$.

1. Compute Teichmüller points P', Q' in the disks of P, Q, respectively.

2. Use Algorithm 3.2.3 to compute the single integrals $\int_P^Q \omega_i, \int_{P'}^{P} \omega_i, \int_Q^{Q'} \omega_i$ for all i.

3. Use Algorithm 5.3.1 to compute the tiny double integrals $\int_{P'}^{P} \omega_i\omega_k, \int_{Q'}^{Q} \omega_i\omega_k$

4. Use Algorithm 5.5.2 to compute the double integrals $\{\int_{P'}^{Q'} \omega_i\omega_j\}_{i,j=0}^{2g-1}$.

5. Correct endpoints using

$$\int_P^Q \omega_i\omega_k = \int_P^{P'} \omega_i\omega_k + \int_{P'}^{Q'} \omega_i\omega_k + \int_{Q'}^{Q} \omega_i\omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i .$$

5.5.4 Without Teichmüller points

Alternatively, instead of finding Teichmüller points and correcting endpoints, we can directly compute double integrals using a slightly different linear system. Indeed, using the Link lemma for double integrals, we take $\phi(P)$ and $\phi(Q)$ to be the points in the disks of P and Q, respectively, which gives

$$\int_P^Q \omega_i\omega_k = \int_P^{\phi(P)} \omega_i\omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k + \int_{\phi(Q)}^{Q} \omega_i\omega_k + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^{Q} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^{Q} \omega_i \tag{5.5.4}$$

To write down a linear system without Teichmüller points, we begin as before, with

$$\int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k = \int_P^Q \phi^*(\omega_i\omega_k) = c_{ik} + \int_P^Q \left(\sum_{j=0}^{2g-1} A_{ij}\omega_j\right)\left(\sum_{j=0}^{2g-1} A_{kj}\omega_j\right). \tag{5.5.5}$$

Putting together (5.5.4) and (5.5.5), we get

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^{P} \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^{P} \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^{Q} \omega_i\omega_k \\ \vdots \end{pmatrix}. \tag{5.5.6}$$

This gives us the following alternative to Algorithm 5.5.2:

Algorithm 5.5.5 (Double Coleman integration).
Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P, Q \in C(\mathbb{Q}_p)$ in non-Weierstrass residue disks or in Weierstrass disks in the region of convergence.
Output: The double integrals $\left(\int_P^Q \omega_i\omega_j\right)_{i,j=0}^{2g-1}$.

1. Use Algorithm 3.2.3 to compute the single integrals $\int_P^Q \omega_i, \int_{\phi(P)}^{\phi(Q)} \omega_i$ for all i.

2. Use Algorithm 5.3.1 to compute $\int_{\phi(P)}^{P} \omega_i\omega_k, \int_{\phi(Q)}^{Q} \omega_i\omega_k$ for all i, k

3. As in Step 4 of Algorithm 5.5.2, compute the constants c_{ik} for all i, k.

4. Recover the double integrals using the linear system

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^P \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^Q \omega_i\omega_k \\ \vdots \end{pmatrix}$$

Example 5.5.6. Let C be the genus 2 curve $y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$ and let $P = (1, -1), Q = (-1, -1)$ and $p = 7$. We compute double integrals on basis differentials:

$$\int_P^Q \omega_0\omega_0 = 2 \cdot 7^2 + 7^3 + 4 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_0\omega_1 = 7^2 + 5 \cdot 7^3 + 3 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_0\omega_2 = 4 \cdot 7 + 5 \cdot 7^2 + 7^3 + O(7^4)$$

$$\int_P^Q \omega_0\omega_3 = 7 + 5 \cdot 7^2 + 3 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_1\omega_0 = 7^2 + 6 \cdot 7^3 + 5 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_1\omega_1 = 4 \cdot 7^2 + 3 \cdot 7^3 + O(7^5)$$

$$\int_P^Q \omega_1\omega_2 = 5 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 4 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_1\omega_3 = 2 + 3 \cdot 7 + 7^2 + 4 \cdot 7^3 + O(7^4)$$

$$\int_P^Q \omega_2\omega_0 = 7^2 + 4 \cdot 7^3 + O(7^4)$$

$$\int_P^Q \omega_2\omega_1 = 4 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3 + 5 \cdot 7^4 + O(7^5)$$

$$\int_P^Q \omega_2\omega_2 = 2 + 5 \cdot 7 + 3 \cdot 7^2 + O(7^3)$$

$$\int_P^Q \omega_2\omega_3 = 5 + 2 \cdot 7 + 3 \cdot 7^2 + O(7^3)$$

$$\begin{aligned}\int_P^Q \omega_3\omega_0 &= 3\cdot 7+2\cdot 7^2+5\cdot 7^3+5\cdot 7^4+O(7^5)\\ \int_P^Q \omega_3\omega_1 &= 5+5\cdot 7+7^2+6\cdot 7^3+O(7^4)\\ \int_P^Q \omega_3\omega_2 &= 6+7+5\cdot 7^2+O(7^3)\\ \int_P^Q \omega_3\omega_3 &= 2+6\cdot 7+5\cdot 7^2+O(7^3)\end{aligned}$$

Example 5.5.7. Using the previous example, we verify the Fubini identity

$$\int_P^Q \omega_j\omega_i+\int_P^Q \omega_i\omega_j=\left(\int_P^Q \omega_i\right)\left(\int_P^Q \omega_j\right).$$

We have

$$\begin{aligned}\int_P^Q \omega_0 &= 5\cdot 7+2\cdot 7^2+5\cdot 7^3+7^4+4\cdot 7^5+O(7^6)\\ \int_P^Q \omega_1 &= 6\cdot 7+6\cdot 7^2+2\cdot 7^3+4\cdot 7^4+3\cdot 7^5+O(7^6)\\ \int_P^Q \omega_2 &= 5+5\cdot 7^3+6\cdot 7^4+2\cdot 7^5+O(7^6)\\ \int_P^Q \omega_3 &= 5+3\cdot 7+4\cdot 7^2+3\cdot 7^3+6\cdot 7^4+2\cdot 7^5+O(7^6).\end{aligned}$$

We see, for example,

$$\begin{aligned}\int_P^Q \omega_0\omega_1+\int_P^Q \omega_1\omega_0 &= 2\cdot 7^2+4\cdot 7^3+2\cdot 7^4+O(7^5)=\left(\int_P^Q \omega_0\right)\left(\int_P^Q \omega_1\right)\\ \int_P^Q \omega_2\omega_3+\int_P^Q \omega_3\omega_2 &= 4+4\cdot 7+7^2+O(7^3)=\left(\int_P^Q \omega_2\right)\left(\int_P^Q \omega_3\right).\end{aligned}$$

5.5.5 Weierstrass points

Suppose one of P or Q is a Weierstrass point. Then directly using the linear system as above fails, since the f_i have essential singularities at Weierstrass points. We remedy this by following the approach in Algorithm 4.3.6.

Proposition 5.5.8. *Let Q be a non-Weierstrass point, P a finite Weierstrass point, and S be a point in the residue disk of P, near the boundary. Then the integral from P to Q can be computed as a sum of integrals:*

$$\int_P^Q \omega_i\omega_k=\int_P^S \omega_i\omega_k+\int_S^Q \omega_i\omega_k+\int_P^S \omega_k\int_S^Q \omega_i.$$

Proof. Take $Q' = Q, P' = S$ in

$$\int_P^Q \omega_i\omega_k = \int_P^{P'} \omega_i\omega_k + \int_{P'}^{Q'} \omega_i\omega_k + \int_{Q'}^{Q} \omega_i\omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i.$$

This gives

$$\begin{aligned}\int_P^Q \omega_i\omega_k &= \int_P^{S} \omega_i\omega_k + \int_{S}^{Q} \omega_i\omega_k + \int_P^{S} \omega_k \int_{S}^{Q} \omega_i + \int_{P'}^{Q} \omega_k \int_{Q}^{Q} \omega_i \\ &= \int_P^{S} \omega_i\omega_k + \int_{S}^{Q} \omega_i\omega_k + \int_P^{S} \omega_k \int_{S}^{Q} \omega_i. \qquad (5.5.7)\end{aligned}$$

Now the first integral on the right hand side of (5.5.7) is a tiny double integral from a Weierstrass point (see Algorithm 5.5.9), the second double can be computed via the linear system (see Algorithm 5.5.5), and the product is of two single integrals. □

To compute tiny iterated integrals in a Weierstrass disk, we slightly modify Algorithm 5.3.1:

Algorithm 5.5.9 (Tiny iterated integral in a Weierstrass disk).
Input: P a Weierstrass point, d the degree of totally ramified extension, ω_i, ω_j basis differentials
Output: The integral

$$\int_P^S \omega_i\omega_j = \int_P^S \omega_i(R) \int_P^R \omega_j = \int_{t=0}^{t=1} \omega_i(R) \int_{u=0}^{u=t} \omega_j.$$

1. Compute local coordinates $(x(u), u)$ at P.

2. Let $a = p^{1/d}$. Rescale coordinates so that $y := au, x := x(au)$.

3. Compute $I_2(u) = \int x^j \frac{dx}{2y}$ as a power series in u.

4. Compute the appropriate definite integral using the step above:

$$\int_R^S x^j \frac{dx}{2y} = \int_0^t x(au)\frac{adu}{u} = I_2(t)$$

(where $R = (x(t), t)$). Call this definite integral (now a power series in t) I_2.

5. Now since $R = (x(t), t)$, we have $\int_P^S w_i w_j = \int_0^1 x(t)^i I_2 \frac{dx(t)}{2t}$.

Suppose P is a finite Weierstrass point. While one could compute the integral $\int_P^Q \omega_i\omega_j$ directly using Algorithm 5.5.5 for all of the tiny double integrals (and Algorithm 5.5.9 for the other double integrals), in practice, that approach is expensive, as it requires the computation of several intermediate integrals with Frobenius of points that are defined over extensions. This, in turn, makes the requisite degree d extension for convergence quite large. For instance, in a few numerical experiments we performed, computing double integrals directly for an elliptic curve required d to be 200. Instead, we use the following two algorithms to make a few shortcuts using the Weierstrass point and some properties of double integrals, thereby lowering the necessary d for convergence (in that same example, these modifications cut down d to 30).

The key idea is to compute a local parametrization at the finite Weierstrass point P and to use this to compute the indefinite integral $\int_P^* \omega_i$. Then to compute integrals involving "boundary points," one can simply evaluate this indefinite integral at the appropriate points, instead of directly computing parametrizations, and thus integrals, over a totally ramified extension of $\mathbb{Q}_p$. This idea is also used to evaluate double integrals involving boundary points.

Algorithm 5.5.10 (Intermediary integral computations for double integrals with a Weierstrass endpoint).
Input: P finite Weierstrass point, Q non-Weierstrass point, d the degree of totally ramified extension, n the precision of $\mathbb{Q}_p$, basis differentials ω_i, ω_j.
Output: Necessary things for the eventual computation of $\int_P^Q \omega_i\omega_j$.

1. Compute $(x(t), t)$ local coordinates at P to precision nd.

2. Let $S = (x(a), a)$, where $a = p^{1/d}$.

3. Compute as a power series in t, $I_2(t) = \int x(t)^i \frac{dx(t)}{y(t)}$.

4. Compute the definite integral $\int_P^S \omega_i = I_2(1)$.

5. Compute the definite integral $\int_P^S \omega_0\omega_1$ via Algorithm 5.3.1. Keep the intermediary indefinite integral.

6. Use the fact that $\int_P^S \omega_1\omega_0 = -\int_P^S \omega_0\omega_1 + \int_P^S \omega_0 \int_P^S \omega_1$ (same for rest of lower-diagonal entries) to compute $\int_P^S \omega_1\omega_0$ (instead of directly computing it as a double integral).

7. Compute $\int_S^{\phi(S)} \omega_i = \int_P^{\phi(S)} \omega_i - \int_P^S \omega_i$ by the indefinite integral in Step 3.

8. Use the indefinite integral in Step 5 to get $\int_S^{\phi(S)} \omega_0\omega_1$.

9. Repeat the trick in Step 6 to get $\int_S^{\phi(S)} \omega_1\omega_0$.

10. Compute $\int_Q^{\phi(Q)} \omega_i$.

11. Compute $\int_Q^{\phi(Q)} \omega_0\omega_1$.

12. Repeat the trick in Step 6 to get $\int_Q^{\phi(Q)} \omega_1\omega_0$.

13. Use $\int_S^Q \omega_i = \int_P^Q \omega_i - \int_P^S \omega_i$ to get $\int_S^Q \omega_i$.

Algorithm 5.5.11 (Double integrals from a Weierstrass endpoint).
Input: P finite Weierstrass point, Q non-Weierstrass point, ω_i, ω_j basis differentials.
Output: The double integrals $\int_P^Q \omega_i\omega_j$.

1. Compute all of the integrals as in Algorithm 5.5.10.
2. Use additivity to recover the double integrals $\int_P^Q \omega_i\omega_j = \int_P^S \omega_i\omega_j + \int_S^Q \omega_i\omega_j + \int_P^S \omega_i \int_S^Q \omega_j$.

As consistency checks for our algorithms, one may use the following corollaries of Proposition 5.5.8.

Corollary 5.5.12. *For P, Q Weierstrass points and S a third point, we have additivity in endpoints: $\int_P^Q \omega_i\omega_j + \int_Q^S \omega_i\omega_j = \int_P^S \omega_i\omega_j$.*

Corollary 5.5.13. *For P, Q Weierstrass points, we have*

$$\int_P^Q \omega_i\omega_j + \int_P^Q \omega_j\omega_i = 0.$$

It is worth noting that in general, unlike in the case of a single Coleman integral, for P and Q both Weierstrass points, unless $i = k$, the double Coleman integral $\int_P^Q \omega_i\omega_k$ is not necessarily 0. However, in the case of $i = k$, the integral can be computed as $\int_P^Q \omega_i\omega_i = \frac{1}{2}\left(\int_P^Q \omega_i\right)^2 = 0$.

Example 5.5.14. Consider the curve $y^2 = x(x-1)(x+9)$, over $\mathbb{Q}_7$, and the points $P_1 = (1,0)$, $P_2 = (0,0)$, and $Q = (-1,4)$.

We have

$$\begin{pmatrix} \int_{P_1}^Q \omega_0\omega_0 \\ \int_{P_1}^Q \omega_0\omega_1 \\ \int_{P_1}^Q \omega_1\omega_0 \\ \int_{P_1}^Q \omega_1\omega_1 \end{pmatrix} = \begin{pmatrix} 2\cdot 7^2 + 5\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + O(7^6) \\ 6\cdot 7 + 5\cdot 7^2 + 4\cdot 7^3 + 6\cdot 7^4 + O(7^6) \\ 2\cdot 7^2 + 3\cdot 7^3 + 3\cdot 7^4 + 7^5 + O(7^6) \\ 1 + 5\cdot 7 + 5\cdot 7^3 + 4\cdot 7^4 + 4\cdot 7^5 + O(7^6) \end{pmatrix}$$

and

$$\begin{pmatrix} \int_{P_2}^Q \omega_0\omega_0 \\ \int_{P_2}^Q \omega_0\omega_1 \\ \int_{P_2}^Q \omega_1\omega_0 \\ \int_{P_2}^Q \omega_1\omega_1 \end{pmatrix} = \begin{pmatrix} 2\cdot 7^2 + 5\cdot 7^3 + 4\cdot 7^4 + 3\cdot 7^5 + O(7^6) \\ 2\cdot 7^2 + 7^3 + 6\cdot 7^4 + 5\cdot 7^5 + O(7^6) \\ 6\cdot 7 + 5\cdot 7^2 + 6\cdot 7^3 + 3\cdot 7^4 + 3\cdot 7^5 + O(7^6) \\ 1 + 5\cdot 7 + 5\cdot 7^3 + 4\cdot 7^4 + 4\cdot 7^5 + O(7^6) \end{pmatrix},$$

from which we see that $\int_{P_1}^{P_2} \omega_0\omega_1 \neq 0$ and likewise $\int_{P_1}^{P_2} \omega_1\omega_0 \neq 0$.

5.6 Future work

We present some yet unresolved questions arising from our work.

5.6.1 Tangential basepoint at infinity

We originally began working with double integrals to provide examples of Kim's nonabelian Chabauty method (see Chapter 7) for elliptic curves. Our algorithms can produce examples when the curve has a rational finite Weierstrass point. However, we would also like to produce examples when the curve does not; in this case, one would have to compute with the tangential basepoint at infinity. How do we modify our algorithms to do this? It would be of great interest to yield algorithms to compute double (and further iterated) integrals from infinity, as this would provide a wealth of further examples.

5.6.2 The fundamental linear system

The linear system we alluded to in Theorem 5.4.1 for computing general iterated integrals has a dizzying number of terms. Is there a recursion we could write down that would allow us to go from $(n-1)$-fold integrals to n-fold integrals in a manageable way?

5.6.3 The region of convergence in a Weierstrass disk

While we have performed computations with double integrals in finite Weierstrass disks, the minimal degree d of the totally ramified extension necessary to ensure convergence still remains mysterious. Explicitly computing this d as a function of p, g, and the precision n of the base ring would be essential to formulating error bounds and calculating precision of integrals with an endpoint in a Weierstrass disk.

Chapter 6

Explicit computations with the Chabauty method

In this chapter, we give a quick summary of the method of Chabauty and Coleman, following the exposition in [MP07] and provide numerical examples showing how our algorithms can be used to find rational points on hyperelliptic curves.

6.1 Introduction

Let C be a curve over $\mathbb{Q}$. Finding the set of $\mathbb{Q}$-rational points $C(\mathbb{Q})$ is a difficult question that has led to many new techniques in arithmetic geometry. For example, suppose that C is a curve of genus greater than 1. By work of Faltings [Fal83], we know that $C(\mathbb{Q})$ is finite. However, his proof is not effective: it does not yield an algorithm to compute $C(\mathbb{Q})$. Nevertheless, by work of Chabauty and Coleman, in the case when the Jacobian of the curve over $\mathbb{Q}$ has rank less than the genus of the curve, explicit functions can be written down in terms of p-adic integrals and solved to give information about $C(\mathbb{Q})$.

Let us fix some notation. Let J be the Jacobian of C, and suppose that we know a point $O \in C(\mathbb{Q})$. Then we can identify the curve with a subvariety of its Jacobian via the embedding

$$\begin{aligned} C &\to J \\ P &\mapsto [P - O], \end{aligned}$$

where $[D]$ is the class of a divisor D. Suppose that we have already computed $J(\mathbb{Q})$ as a free abelian group, and that in particular, we know its rank r. In general, obtaining such information about $J(\mathbb{Q})$ is a difficult global problem (in contrast to the methods we describe below, which are local), but nevertheless, let us suppose that we have this information.

Let $J_{\mathbb{Q}_p}$ denote the base change of J to $\mathbb{Q}_p$. Let $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ denote the g-dimensional $\mathbb{Q}_p$-vector space of holomorphic 1-forms on $J_{\mathbb{Q}_p}$. We have a bilinear pairing

$$J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) \to \mathbb{Q}_p \tag{6.1.1}$$

$$P \quad , \quad \omega_J \mapsto \int_0^P \omega_J. \tag{6.1.2}$$

For a holomorphic differential ω_J, let η_J be the map $\eta_J \colon J(\mathbb{Q}_p) \to \mathbb{Q}_p$ sending $P \mapsto \int_0^P \omega_J$. Let T be the vector space dual of $H^0(J_{\mathbb{Q}_p}, \Omega^1)$. Then we may rewrite (6.1.1) as a homomorphism

$$\log : J(\mathbb{Q}_p) \to T.$$

The closure $\overline{J(\mathbb{Q})}$ of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ with its p-adic topology is a subgroup of $J(\mathbb{Q}_p)$. Its dimension as a p-adic manifold is of interest.

Lemma 6.1.1 ([MP07, Lemma 4.2]). *Let r' be the dimension of $\overline{J(\mathbb{Q})}$. Then $r' \leq r$.*

Proof. We have $r' = \dim \overline{J(\mathbb{Q})} = \dim \log(\overline{J(\mathbb{Q})})$, as log is a local diffeomorphism. Since log is continuous and $\overline{J(\mathbb{Q})}$ is compact, $\log(\overline{J(\mathbb{Q})}) = \overline{\log J(\mathbb{Q})}$. But the closure of any subgroup in $\mathbb{Q}_p^{\oplus g}$ is its $\mathbb{Z}_p$-span. So

$$r' = \operatorname{rank}_{\mathbb{Z}_p}(\log J(\mathbb{Q})) \leq \operatorname{rank}_{\mathbb{Z}} \log J(\mathbb{Q}) \leq \operatorname{rank}_{\mathbb{Z}} J(\mathbb{Q}) = r.$$

□

Sitting inside $J(\mathbb{Q}_p)$ is $C(\mathbb{Q}_p)$, a submanifold of dimension 1. Suppose $r' < g$. Then the dimensions suggest that the intersection $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ should be at most $0-$dimensional, and in particular, as a discrete subset of a compact space $J(\mathbb{Q}_p)$, the intersection would be finite. This would then imply that $C(\mathbb{Q})$ is finite. This is what Chabauty proved.

Theorem 6.1.2 ([Cha41]). *With hypotheses as before, suppose $r' < g$. Then $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$ is finite. In particular, $C(\mathbb{Q})$ is finite.*

The problem now is to describe the set $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$. Coleman's approach, which we describe below, is to find functions on $J(\mathbb{Q}_p)$ that vanish on $\overline{J(\mathbb{Q})}$ and restrict them to a parametrization of $C(\mathbb{Q}_p)$. These functions are given in terms of Coleman integrals.

Now suppose that C has good reduction at p. Then J has good reduction at p as well, and the embedding $C \to J$ induces an embedding of the special fibre of C into the reduction of J. The restriction map $H^0(J_{\mathbb{Q}_p}, \Omega^1) \to H^0(C_{\mathbb{Q}_p}, \Omega^1)$ induced by $C \to J$ is an isomorphism of $\mathbb{Q}_p$-vector spaces. Suppose that ω_J restricts to the differential ω. Then for $P, P' \in \mathbb{C}(\mathbb{Q}_p)$, we define

$$\int_P^{P'} \omega := \int_0^{[P'-P]} \omega_J.$$

By the properties of integration on J, we see

1. If $P_i, P_i' \in C(\mathbb{Q}_p)$ are such that $\sum(P_i' - P_i)$ is the divisor of a rational function, or more generally, $[\sum(P_i' - P_i)]$ is a torsion element of $J(\mathbb{Q}_p)$, then $\sum \int_{P_i}^{P_i'} \omega = 0$.
2. If $P, P' \in C(\mathbb{Q}_p)$ have the same reduction in $C(\mathbb{F}_p)$, then recall Algorithm 4.3.1: $\int_P^{P'} \omega$ can be calculated by expanding in power series in a local parameter t on the curve C.

The restriction $\eta := \eta_J|_{C(\mathbb{Q}_p)}$ is the function

$$\begin{aligned} \eta : C(\mathbb{Q}_p) &\to \mathbb{Q}_p \\ P &\mapsto \int_O^P \omega. \end{aligned}$$

The proof of the lemma shows that $\log \overline{J(\mathbb{Q})}$ is a $\mathbb{Z}_p$-module of rank r' contained in $T \simeq \mathbb{Q}_p^{\oplus g}$. Suppose that $r' < g$. Then there is a nonzero $\mathbb{Q}_p$-linear functional $\lambda : T \mapsto \mathbb{Q}_p$ that vanishes on $\log \overline{J(\mathbb{Q})}$. By the duality between T and $H^0(J_{\mathbb{Q}_p}, \Omega^1)$, the functional λ corresponds to a particular nonzero $\omega_J \in H^0(J_{\mathbb{Q}_p}, \Omega^1)$, which in turn gives rise to ω_J, ω, η as above. By definition of log, the map η_J equals the composition

$$J(\mathbb{Q}_p) \to T \twoheadrightarrow \mathbb{Q}_p,$$

where the first map is log and the second λ. Hence η_J vanishes on $\overline{J(\mathbb{Q})}$. It follows that our particular ω satisfies the following:

3. If $P_i, P_i' \in C(\mathbb{Q}_p)$ are such that $[\sum(P_i' - P_i)] \in \overline{J(\mathbb{Q})}$, then $\sum \int_{P_i}^{P_i'} \omega = 0$.

So η vanishes on $C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}$, and the goal is to bound the zeros of η.

Coleman did precisely this, using p-adic integrals to interpret Chabauty's theorem:

Theorem 6.1.3. *Let C, J, p, r' be as before. Suppose that p is a prime of good reduction for C.*

1. *Let ω be a nonzero 1-form in $H^0(\mathbb{C}_{\mathbb{Q}_p}, \Omega^1)$ satisfying conditions (1) - (3). Scale ω by an element of $\mathbb{Q}_p^\times$ so that it reduces to a nonzero 1-form $\tilde{\omega} \in H^0(C_{\mathbb{F}_p}, \Omega^1)$. Suppose $\tilde{P} \in C(\mathbb{F}_p)$. Let $m = \operatorname{ord}_{\tilde{Q}} \tilde{\omega}$. If $m < p - 2$, then the number of points in $C(\mathbb{Q})$ reducing to $\tilde{Q}$ is at most $m + 1$.*
2. *If $p > 2g$, then $\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + 2g - 2$.*

6.2 Explicit integrals to a parameter

Explicitly computing the map η, then, has the potential to yield valuable information about the set of rational points on the curve. Let us now assume that the curve C is hyperelliptic, given by a model of the form $y^2 = f(x)$, where f is monic and nonsingular. We may modify our algorithms in Chapters 3 and 4 to compute integrals to a parameter z. Having these integrals will allow us to experiment with the Chabauty method.

Indeed, in the single integral case (we consider the double integral case in the next chapter), for a Weierstrass basepoint P and a holomorphic basis differential ω_i, we write

$$f_Q(z) = \int_P^{Q_z} \omega_i = (M-I)^{-1}\left(-f_i(Q_z) - \int_{\phi(Q_z)}^{Q_z} \omega_i\right),$$

where $x(Q_z) = z + x(Q)$ is a parameter in the residue disk of a choice of non-Weierstrass point Q and M is the matrix of Frobenius, as before. Each Coleman integral $f_Q(z)$ converges only within a single residue disk (the residue disk of Q).

Algorithm 6.2.1 (Single Coleman integrals on basis elements from a Weierstrass point to a parameter z).
Input: P Weierstrass basepoint, Q a non-Weierstrass point (within whose disk the computations will occur), holomorphic basis differential ω_i.
Output: A power series $f_Q(z) = \int_P^{Q_z} w_i$, where $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ is taken so that Q_z is in the disk of Q.

1. Compute $Q_z = (x(Q) + z, \sqrt{f(x(Q)+z)})$, choosing the right square root so that Q_z is in the same disk as Q.

2. Compute $\phi(Q_z)$, choosing the right square root.

3. Compute the local coordinate at Q_z: $x(t) = t + z + x(Q), y(t) = \sqrt{f(x(t))}$.

4. This gives us $\int_{\phi(Q_z)}^{Q_z} \omega_i = \int_{x(\phi(Q))-x(Q)}^{0} x(t)^i \frac{dx(t)}{2y(t)} dt$.

5. Using the fundamental linear system, compute $f_Q(z) = \int_P^{Q_z} \omega_i = (M-I)^{-1}(-f_i(Q_z) - \int_{\phi(Q_z)}^{Q_z} \omega_i$.

Remark 6.2.2. If one would like to take as the basepoint a non-Weierstrass point P', it suffices to perform the above algorithm and then correct endpoints by computing the integral $\int_{P'}^{P} \omega_i$.

6.3 Example: odd model

Example 6.3.1. We give an example arising from the Chabauty method, taken from [MP07, § 8.1]. Let C be the curve

$$y^2 = x(x-1)(x-2)(x-5)(x-6),$$

whose Jacobian has Mordell-Weil rank 1. The curve C has good reduction at 7, and

$$X(\mathbb{F}_7) = \{(0,0), (1,0), (2,0), (5,0), (6,0), (3,6), (3,-6), \infty\}.$$

By Theorem 6.1.3(2), we know $|C(\mathbb{Q})| \leq 10$. However, we can find 10 rational points on C: the six rational Weierstrass points, and the points $(3, \pm 6), (10, \pm 120)$. Hence $|C(\mathbb{Q})| = 10$.

Since the Chabauty condition holds, there must exist a holomorphic differential ω for which $\int_\infty^Q \omega = 0$ for all $Q \in C(\mathbb{Q})$. We can find such a differential by taking Q to be one of the rational non-Weierstrass points, then computing $a := \int_\infty^Q \omega_0, b := \int_\infty^Q \omega_1$ and setting $\omega = b\omega_0 - a\omega_1$. For $Q = (3, 6)$, we obtain

$$\begin{aligned} a &= 6 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^5 + O(7^6) \\ b &= 4 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 4 \cdot 7^5 + O(7^6). \end{aligned}$$

We then verify that $\int_Q^R \omega$ vanishes for each of the other rational points R.

Remark 6.3.2. It is worth pointing out some facts not exposed by Example 6.3.1. For instance, since ω is already determined by a single rational non-torsion point, we could have used it instead of a brute-force search to find other rational points. However, in other examples, the integral ω may vanish at a point defined over a number field which has a rational multiple in the Jacobian. Such points may be difficult to find by brute-force search; it may be easier to reconstruct them from p-adic approximations, obtained by writing $\int_\infty^* \omega$ as a function of a linear parameter of a residue disk using Algorithm 6.2.1, then finding the zeroes of that function. More seriously, as noted in [MP07, §7], even if $\#\left(C(\mathbb{Q}_p) \cap \overline{J(\mathbb{Q})}\right)$ is known, the true value of $\#C(\mathbb{Q})$ could be smaller; some of the intersection points could be irrational points in $C(\mathbb{Q}_p)$. In this case, while the upper bound on $\#C(\mathbb{Q})$ is not sharp, the method can contribute more information by restricting the possible integer combinations of generators of $J(\mathbb{Q})$ that could lie on C. This would give good lower bounds on the height of any unknown points in $C(\mathbb{Q})$, which would provide strong evidence that no further points exist.

6.4 Future work

The following question was originally asked by Michael Stoll:

Question 6.4.1. Let C be a curve of genus g over $\mathbb{Q}$ whose Mordell-Weil rank is at most $g - 2$. Then for all but finitely many p, do the power series produced by the method of Chabauty only have rational zeros? If not, is there a meaningful interpretation of the "extra" zeros?

We sketch how our algorithms can be used to produce data for a concrete example. We have also learned that this question is being investigated in the Ph.D. thesis of Tzanko Matev.

Example 6.4.2. Let

$$C : y^2 = (x^4 - 2x^2 - 8x + 1)(x^3 + x + 1)$$

over $\mathbb{Q}$ (from [Wet97, §1.9]). This is a genus 3 curve with Mordell-Weil rank 1. The curve has bad reduction at the primes 2 and 31, and one can show that $C(\mathbb{Q}) = \{\infty, (0,1), (0,-1)\}$.

One could carry out the following process:

1. Let p be a prime of good reduction, and fix the points $P = \infty, Q = (0, -1)$. (The divisor class $[Q - P]$ is not torsion.)

2. Using Algorithm 3.2.3, compute the single p-adic integrals

$$a := \int_P^Q \omega_0,$$
$$b := \int_P^Q \omega_1,$$
$$c := \int_P^Q \omega_2.$$

3. Set $\alpha := b\omega_0 - a\omega_1, \beta := c\omega_0 - a\omega_2$. These are differentials whose integrals vanish on the rational points of C.

4. Let S denote the set $C(\mathbb{F}_p)$. For each $\mathbb{F}_p$-point $R \in S$, do the following:

   - Lift R to a $\mathbb{Q}_p$-point R' on C.
   - Using Algorithm 6.2.1, compute the following integrals to a parameter z: $I_0(z) = \int_P^{R'_z} \omega_0, I_1(z) = \int_P^{R'_z} \omega_1, I_2 = \int_P^{R'_z} \omega_2$.
   - Check if $\alpha(z) = bI_0(z) - aI_1(z), \beta(z) = cI_0(z) - aI_2(z)$ have a common zero in the residue disk of R'.

It would indeed be interesting to investigate Stoll's question numerically.

Chapter 7

Kim's nonabelian Chabauty method

Portions of this chapter appeared in joint work of the author with Kedlaya and Kim in the Appendix and Erratum to [Kim10a].

7.1 Introduction: the method

In a recent series of papers [Kim05, Kim09, Kim10a], Kim has pioneered methods for producing finiteness theorems in Diophantine geometry. The key idea, motivated by Grothendieck's philosophy of anabelian geometry, is to study nonabelian analogues of Selmer groups as a way to control rational points. Indeed, in [Kim05], using p-adic analysis (as well as nonabelian Hodge theory and étale cohomology) on these so-called *Selmer varieties*, Kim furnished a new proof of Siegel's theorem on the finiteness of integral points on the projective line over $\mathbb{Q}$ minus three points.

Kim's idea is to carry out a nonabelian analogue of the method of Chabauty where the Jacobian of a curve is replaced by a certain group scheme, the unipotent de Rham fundamental group. As we briefly discussed in the previous chapter, the classical Chabauty-Coleman approach constructs a certain p-adic function on the Jacobian of C, which is then pulled back to the curve to yield information about its rational points. Kim defines an Albanese map from the $\mathbb{Q}_p$-points of the curve to $\mathbb{Q}_p$-points of this group scheme. Pulling back the images of integral points under this map back to $C(\mathbb{Q}_p)$ gives certain finiteness conditions and explicit local conditions analogous to those found by Chabauty and Coleman. It is in this way that certain p-adic functions are constructed whose zeros yield information about the integral points on the curve.

7.1.1 Elliptic curves

In the case of a rank 1 elliptic curve minus a point (currently subject to some other technical assumptions), Kim [Kim10a] gives explicit functions (in terms of double Coleman integrals) that cut out the set of integral points. In this chapter, we give algorithms to carry out this approach for elliptic curves and produce the first numerical examples of the nonabelian Chabauty method.

7.2 A few more explicit double integrals

We begin by giving algorithms to compute with a few more types of explicit double integrals, which will serve as the analogue of those power series present in the usual Chabauty method.

7.2.1 Integrals to a parameter z

First, let us reformulate Coleman integrals from a fixed Weierstrass basepoint to a parameter z. Although we gave one method to do this in Chapter 6, here we provide an alternate algorithm, which generalizes to double integrals in a more effective way.

Algorithm 7.2.1 (Coleman integrals from a Weierstrass point to a parameter z using a near-boundary point S).
Input: Finite Weierstrass point P, non-Weierstrass point Q, basis differential ω_i.
Output: A power series $f_Q(z) = \int_P^{Q_z} \omega_i$, where $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ is taken so that Q_z is in the disk of Q.

1. Compute local coordinates at P.

2. Use Algorithm 4.3.5 to find a near-boundary point S.

3. Compute $\int_P^S \omega_i$.

4. Compute $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ and $\phi(Q_z)$, choosing the correct square roots.

5. Compute local coordinates at Q_z.

6. Compute $\int_{\phi(Q_z)}^{Q_z} \omega_i = \int_{x(\phi(Q_z))-x(Q)}^{0} \omega_i$.

7. Compute $\int_S^{\phi(S)} \omega_i$.

8. Compute $\int_S^{Q_z} \omega_i$ using the fundamental linear system.

9. Recover $\int_P^{Q_z} \omega_i$ by additivity : $\int_P^S \omega_i + \int_S^{Q_z} \omega_i$.

7.2.2 Double integrals to a parameter z

To compute double integrals from a finite Weierstrass point to a parameter z, we generalize Algorithm 5.5.10 to compute intermediate objects that will give us a speed-up in the overall double integration algorithm. These algorithms can be used to produce the power series that cut out integral points on a hyperbolic curve in Kim's nonabelian Chabauty method.

Algorithm 7.2.2 (Double integrals from a finite Weierstrass P to z: intermediate terms).
Input: Finite Weierstrass point P, non-Weierstrass point Q, two differentials ω_0, ω_1, base ring precision n, degree of totally ramified extension d.
Output: Necessary things for the eventual computation of $\int_P^{Q_z} \omega_0\omega_1$, with $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ in the disk of Q.

1. Compute $(x(t), t)$ local coordinates at P to precision nd.

2. Let $S = (x(a), a)$, where $a = p^{1/d}$.

3. Compute as a power series in t, $I_2(t) = \int x(t) \frac{dx(t)}{2y(t)} dt$.

4. Compute the definite integral $\int_P^S \omega_i = I_2(1)$.

5. Compute the definite integral $\int_P^S \omega_0\omega_1$ via Algorithm 5.5.9. Keep the intermediary indefinite integral.

6. Use $\int_P^S \omega_1\omega_0 = -\int_P^S \omega_0\omega_1 + \int_P^S \omega_0 \int_P^S \omega_1$ (same for rest of lower-diagonal entries) to compute $\int_P^S \omega_1\omega_0$.

7. Compute $\int_S^{\phi(S)} \omega_i = \int_P^{\phi(S)} \omega_i - \int_P^S \omega_i$ by the indefinite integral in Step 3.

8. Use the indefinite integral in Step 5 to get $\int_S^{\phi(S)} \omega_0\omega_1$.

9. Repeat the trick in Step 6 to get $\int_S^{\phi(S)} \omega_1\omega_0$.

10. Compute $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ and $\phi(Q_z)$.

11. Compute local coordinates at Q_z.

12. Using the local coordinates above, compute $I_2(t) = \int \omega_i$ as a power series in t with coefficients in $\mathbb{Q}_p[[z]]$.

13. Compute the definite integral $\int_{Q_z}^{\phi(Q_z)} \omega_i = \int_0^{x(\phi(Q_z))-x(Q)} \omega_i$.

14. Now use the indefinite integral in Step 12 to write
$$\int_{Q_z}^{\phi(Q_z)} \omega_0(R) \int_R^{\phi(Q_z)} \omega_1 = \int_z^{x(\phi(Q_z))-x(Q)} \omega_0(R) \int_{t-z}^{x(\phi(Q_z))-x(Q)} \omega_1.$$

15. Use $\int \omega_1\omega_0 = \int \omega_0\omega_1 - \int \omega_0 \int \omega_1$ to calculate the other double integral.

16. Compute $\int_P^{Q_z} \omega_i$ by Algorithm 6.2.1 or Algorithm 7.2.1.

17. Recover $\int_S^{Q_z} \omega_i$ by taking $\int_P^{Q_z} \omega_i - \int_P^S \omega_i$.

18. Compute $\int_{\phi(S')}^{\phi(Q_z)} \omega_i$ via $\int_S^{Q_z} \omega_i - \int_S^{\phi(S)} \omega_i + \int_{Q_z}^{\phi(Q_z)} \omega_i$.

Algorithm 7.2.3 (Double integrals from a finite Weierstrass point to z).
Input: Finite Weierstrass point P, non-Weierstrass point Q, differentials ω_i, ω_j, precision of base ring n, degree of totally ramified extension d.
Output: The double integrals $\int_P^{Q_z} \omega_i\omega_j$, with $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ in the disk of Q.

1. Use Algorithm 5.5.11 but with $Q_z = (z + x(Q), \sqrt{f(z + x(Q))})$ instead of Q.

2. Use Algorithm 7.2.2 to get the major inputs.

3. Use the analogue of additivity in endpoints (Algorithm 5.5.11) to produce the desired double integrals.

7.3 Carrying out the nonabelian Chabauty method

We are now prepared to carry out the nonabelian Chabauty method for elliptic curves. Following the notation in [Kim10a], let $\mathcal{C}/\mathbb{Z}$ be the minimal regular model of an elliptic curve $C/\mathbb{Q}$ of analytic rank 1 with Tamagawa numbers all 1. Let $\mathcal{X} = \mathcal{C} - \{\infty\}$ and $\omega_0 = \frac{dx}{2y}, \omega_1 = \frac{xdx}{2y}$. Taking a tangential base point b at ∞, we have the analytic functions

$$\log_{\omega_0}(z) = \int_b^z \omega_0, \quad \log_{\omega_1}(z) = \int_b^z \omega_1, \quad D_2(z) = \int_b^z \omega_0\omega_1.$$

With this setup, we have

Theorem 7.3.1 ([Kim10a]). *Suppose y is a point of infinite order in $\mathcal{C}(\mathbb{Z})$. Then $\mathcal{X}(\mathbb{Z}) \subset \mathcal{C}(\mathbb{Z}_p)$ is in the zero set of*

$$f(z) := (\log_{\omega_0}(y))^2 D_2(z) - (\log_{\omega_0}(z))^2 D_2(y).$$

As a consequence, given the same hypotheses, we have the following result:

Corollary 7.3.2. *The expression*

$$\frac{D_2(y)}{(\log_{\omega_0}(y))^2} \tag{7.3.1}$$

is independent of the point y of infinite order in $\mathcal{C}(\mathbb{Z})$.

We discuss some related Chabauty-style formulas and computations demonstrating these results.

First recall (5.5.8), adapted to our situation:

$$\int_b^y \omega_0\omega_1 = \int_b^x \omega_0\omega_1 + \int_x^y \omega_0\omega_1 + \int_b^x \omega_1 \int_x^y \omega_0. \tag{7.3.2}$$

Since we know

$$\frac{\int_b^x \omega_0\omega_1}{\left(\int_b^x \omega_0\right)^2} = \frac{\int_b^y \omega_0\omega_1}{\left(\int_b^y \omega_0\right)^2}, \tag{7.3.3}$$

we use this to rewrite (7.3.2):

$$\int_b^y \omega_0\omega_1 = \left(\int_b^y \omega_0\omega_1\right)\frac{\left(\int_b^x \omega_0\right)^2}{\left(\int_b^y \omega_0\right)^2} + \int_x^y \omega_0\omega_1 + \int_b^x \omega_1 \int_x^y \omega_0,$$

from which we get

$$\frac{\int_b^y \omega_0\omega_1}{\left(\int_b^y \omega_0\right)^2} = \frac{\int_x^y \omega_0\omega_1 + \int_b^x \omega_1 \int_x^y \omega_0}{\left(\int_b^y \omega_0\right)^2 - \left(\int_b^x \omega_0\right)^2}, \tag{7.3.4}$$

with the additional assumption that $\left(\int_b^y \omega_0\right)^2 \neq \left(\int_b^x \omega_0\right)^2$.

Remark 7.3.3. While this identity is not as simple as the original (7.3.3), it has the benefit that the right hand side involves no iterated integrals from Weierstrass points. One can show that the expression is symmetric in x and y.

It remains to discuss evaluation of the single integral $\int_b^x \omega_1$, which requires a tangential basepoint.

When b is a 2−torsion point, recall that Lemma 3.2.9 allows us to compute integrals from b to a non-Weierstrass point solely in terms of the non-Weierstrass point. Indeed, an analogous result holds when b is a tangential basepoint at infinity and $\omega = \beta$; i.e., the regularization of the tangential basepoint results in the same expression of the integral in terms of the non-Weierstrass point.

Proposition 7.3.4. *Let b be a tangential basepoint at infinity. Then*

$$\int_b^Q \omega_1 = \frac{1}{2}\int_{\iota(Q)}^Q \omega_1.$$

Proof. See [Kim10a, §1, Ex. 3]. □

7.3.1 An example with 65A

Example 7.3.5. Let E be the elliptic curve $y^2 = x^3 - 1323x + 3942$, with minimal model

$$\mathcal{E} : y^2 + xy = x^3 - x$$

(Cremona [Cre] label "65a1"). Let $b = (3,0), P = (39,108), Q = (-33,-108), R = (147,1728), S = (103,980), T = (-6,-108)$ be points on E, which arise from points on $\mathcal{E}$ in the following manner:

$$\begin{aligned}
\mathcal{E} &\longrightarrow E \\
(0,0) &\mapsto (3,0) \\
(1,0) &\mapsto (39,108) \\
(-1,0) &\mapsto (-33,-108) \\
(4,6) &\mapsto (147,1728) \\
\left(\frac{25}{9},\frac{85}{27}\right) &\mapsto (103,980) \\
\left(-\frac{1}{4},-\frac{3}{8}\right) &\mapsto (-6,-108).
\end{aligned}$$

Note that $p=11$ is a prime of good reduction for E.

By a direct computation of iterated integrals from the two-torsion point b, we found

$$\frac{D_2(P)}{\left(\int_b^P \omega_0\right)^2} = \frac{D_2(Q)}{\left(\int_b^Q \omega_0\right)^2} = \frac{D_2(R)}{\left(\int_b^R \omega_0\right)^2} = 3{\cdot}11^{-1}{+}6{+}2{\cdot}11{+}10{\cdot}11^2{+}3{\cdot}11^3{+}5{\cdot}11^4{+}O(11^5).$$

We wish to try the second form of the quotient, which requires a pair of integral points. Let b_1 denote the tangential basepoint at infinity. First note that the pair P, Q does not work, as

$$\left(\int_{b_1}^P \omega_0\right)^2 = \left(\int_{b_1}^Q \omega_0\right)^2 = 5{\cdot}11^2{+}2{\cdot}11^3{+}5{\cdot}11^4{+}7{\cdot}11^5{+}11^6{+}9{\cdot}11^7{+}2{\cdot}11^8{+}9{\cdot}11^9{+}O(11^{10}).$$

However, R is compatible with either P or Q, as

$$\left(\int_{b_1}^R \alpha\right)^2 = 9\cdot 11^2 + 9\cdot 11^3 + 9\cdot 11^4 + 7\cdot 11^5 + 6\cdot 11^6 + 3\cdot 11^7 + 4\cdot 11^9 + O(11^{10}).$$

Thus taking $x=P, y=R$ as well as $x=Q, y=R$, we compute

$$\frac{\int_x^y \omega_0\omega_1 + \int_{b_1}^x \omega_1 \int_x^y \omega_0}{\left(\int_{b_1}^y \omega_0\right)^2 - \left(\int_{b_1}^x \omega_0\right)^2} = 3{\cdot}11^{-1}{+}6{+}2{\cdot}11{+}10{\cdot}11^2{+}3{\cdot}11^3{+}5{\cdot}11^4{+}9{\cdot}11^5{+}2{\cdot}11^6{+}O(11^7).$$

7.3.2 An example with 37A

Furthermore, we can derive another formula starting from the identity

$$\int_b^z \omega_0\omega_1 = \int_y^z \omega_0\omega_1 + \int_y^z \omega_0 \int_b^y \omega_1 + \int_b^y \omega_0\omega_1.$$

Suppose x, y are integral on the minimal model. Then we may write the last integral without a double integral from the tangential basepoint using our previous formula:

$$\int_b^z \omega_0\omega_1 = \int_y^z \omega_0\omega_1 + \int_y^z \omega_0 \int_b^y \omega_1 + \left(\int_b^y \omega_0\right)^2 \frac{\int_x^y \omega_0\omega_1 + \int_x^y \omega_0 \int_b^x \omega_1}{(\int_b^y \omega_0)^2 - (\int_b^x \omega_0)^2},$$

giving us that

$$\frac{D_2(z)}{(\log_{\omega_0}(z))^2} = \frac{\int_y^z \omega_0\omega_1}{(\log_{\omega_0}(z))^2} + \frac{\int_y^z \omega_0 \int_b^y \omega_1}{(\log_{\omega_0}(z))^2} + \frac{(\log_{\omega_0}(y))^2}{(\log_{\omega_0}(z))^2} \frac{\int_x^y \omega_0\omega_1 + \int_x^y \omega_0 \int_b^x \omega_1}{(\log_{\omega_0}(y))^2 - (\log_{\omega_0}(x))^2}. \tag{7.3.5}$$

We will use Equation 7.3.5 to compute the iterated quotient when z is not integral on the minimal model. Note that (7.3.5) is independent of the choice of x, y as long as x, y are integral on the minimal model, so it's our best workaround for computing directly with the tangential basepoint in this case.

We can now verify the identity on quotients for curves that do not have integral two-torsion.

Example 7.3.6. We compute the quotient using (7.3.4) when the curve does not have integral 2-torsion. Consider the curve $E : y^2 = x^3 - 16x + 16$, with minimal model given by

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

(Cremona label "37a1"). Let $P = (0,4), Q = 2P = (4,4), R = 3P = (-4,-4), S = 4P = (8,-20), T = 5P = (1,-1), U = 6P = (24,116)$ be points on E, which arise from points on $\mathcal{E}$ in the following manner:

$$\begin{aligned} \mathcal{E} &\longrightarrow E \\ (0,0) &\mapsto (0,4) \\ (1,0) &\mapsto (4,4) \\ (-1,-1) &\mapsto (-4,-4) \\ (2,-3) &\mapsto (8,-20) \\ \left(\frac{1}{4}, -\frac{5}{8}\right) &\mapsto (1,-1) \\ (6,14) &\mapsto (24,116). \end{aligned}$$

Note that $p = 7$ is a prime of good reduction. We compute the quotient (7.3.4) via b_1 the tangential basepoint at infinity. For each of the ten (unordered) pairs (x, y), where $x \neq y, x, y \in \{P, Q, R, S, U\}$, we see

$$\frac{D_2(y)}{(\log_{\omega_0}(y))^2} = \frac{\int_x^y \omega_0\omega_1 + \int_{b_1}^x \omega_1 \int_x^y \omega_0}{\left(\int_{b_1}^y \omega_0\right)^2 - \left(\int_{b_1}^x \omega_0\right)^2} = 7^{-1} + 1 + 3 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^4 + O(7^5).$$

However, we have, using (7.3.5):

$$\begin{aligned}
\frac{D_2(5P)}{\log^2_{\omega_0}(5P)} &= 2\cdot 7^{-1} + 5 + 3\cdot 7 + 6\cdot 7^2 + 3\cdot 7^3 + 5\cdot 7^4 + 4\cdot 7^5 + 2\cdot 7^6 + O(7^7)\\
\frac{D_2(7P)}{\log^2_{\omega_0}(7P)} &= 5\cdot 7^{-3} + 3\cdot 7^{-1} + 1 + 4\cdot 7 + 3\cdot 7^2 + 7^3 + 6\cdot 7^4 + O(7^5)\\
\frac{D_2(8P)}{\log^2_{\omega_0}(8P)} &= 6\cdot 7^{-1} + 4 + 7 + 7^2 + 5\cdot 7^3 + 4\cdot 7^4 + 2\cdot 7^5 + 5\cdot 7^6 + O(7^7)\\
\frac{D_2(10P)}{\log^2_{\omega_0}(10P)} &= 5\cdot 7^{-1} + 6 + 6\cdot 7 + 2\cdot 7^2 + 2\cdot 7^3 + 5\cdot 7^4 + 5\cdot 7^5 + 4\cdot 7^6 + O(7^7).
\end{aligned}$$

By the theorem, all ratios involving integral points are equal; the second set of ratios differed because the points were merely rational. Perhaps more similar to the original Chabauty method: given two integral points x, y of infinite order, a third point z occurs in the zero set of the function

$$\left(\left(\int_b^z \omega_0\right)^2 - \left(\int_b^x \omega_0\right)^2\right) \frac{\int_x^y \omega_0\omega_1 + \int_x^y \omega_0 \int_b^x \omega_1}{(\int_b^y \omega_0)^2 - (\int_b^x \omega_0)^2} - \left(\int_x^z \omega_0\omega_1 + \int_x^z \omega_0 \int_b^x \omega_1\right).$$

Indeed, fixing $x = (0,4), y = (4,4)$ on E, we may recover $z = (-4,-4). (8. -20), (24, 116)$.

7.4 Connection to p-adic heights

As originally observed by Kim [Kim10b], there is a striking connection between the invariant ratio (7.3.1) and the cyclotomic p-adic height: the double integral present in the numerator of the invariant ratio is essentially the logarithm of the p-adic sigma function of Mazur and Tate.

Recall ([MST06, Theorem 1.3]) that one interpretation of the p-adic sigma function is the following: it is the unique odd function

$$\sigma(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$$

(along with a unique constant $c \in \mathbb{Z}_p$) satisfying the differential equation

$$x(t) + c = -\frac{d}{\omega_0}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega_0}\right).$$

With this definition, one can see that the double integral is essentially the p-adic height of the point in the rank 1 case. Indeed, recall ([MST06]) that the global p-adic height of a point P on an elliptic curve, given in terms of the sigma function is as follows:

$$h_p(P) = \frac{1}{p}\log_p\left(\frac{\sigma(P)}{d(P)}\right),$$

where $d(P)$ is the denominator of P. When the point is integral, the height is indeed (up to constant) the logarithm of the sigma function. However, when the point is merely rational, this is not the case.

Here are some computations illustrating the constant ratio between the double integral and the height of the point:

Example 7.4.1. Let E be the elliptic curve "37a1" and P the point $(0,0)$. Let I_P be the value of the double integral $\int_b^P \omega_0\omega_1$ from a finite Weierstrass point to P.

We have

$$\begin{aligned}\frac{h(P)}{I_P/7} &= \frac{h(2P)}{I_{2P}/7}\\ &= \frac{h(3P)}{I_{3P}/7}\\ &= 2\cdot 7 + 5\cdot 7^2 + 6\cdot 7^4 + 6\cdot 7^6 + 7^8 + O(7^9).\end{aligned}$$

7.5 Future work

7.5.1 Tangential basepoint

As discussed in Chapter 5, we would ultimately like to formulate techniques for explicitly computing with tangential basepoints, as this would provide a wealth of examples.

7.5.2 Tamagawa number hypothesis

With some work, one could remove the hypothesis that the Tamagawa numbers of the elliptic curve must all be 1. This would also produce several more examples.

Chapter 8

p-adic heights on Jacobians of hyperelliptic curves

This material originally appeared in joint work of the author with Besser [BB].

Our main result in this chapter is the following

Theorem 8.0.1. *Let D_1, D_2 be divisors on a hyperelliptic curve C with disjoint support over $\mathbb{Q}_p$. There exists an explicit algorithm which computes the local height pairing at p, $h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$, for an appropriately constructed differential ω_{D_1} associated to the divisor D_1.*

8.1 Introduction

For an elliptic curve over $\mathbb{Q}$, the classical Birch and Swinnerton-Dyer (BSD) conjecture predicts that a special value of its L-function can be given in terms of certain arithmetic invariants of the curve, one of which involves the canonical height pairing matrix of a basis of rational points. The p-adic analogue [MTT86] of the BSD conjecture makes a similar prediction, with the canonical height pairing replaced by a p-adic one [MT83]. These conjectures have natural generalizations to abelian varieties.

The p-adic height pairing was first defined by Schneider [Sch82] for abelian varieties and was extended to motives by Nekovář [Nek93]. For Jacobians of curves there is a third definition, due to Coleman and Gross [CG89], relying on Coleman's theory of p-adic integration [Col82, Col85, CdS88, Bes02a]. This third definition of the height pairing is known to be equivalent to the previous ones [Bes04].

For the purpose of numerically verifying p-adic BSD type conjectures, it is important to have an effective algorithm for the computation of the p-adic height pairing. By the work of Kedlaya [Ked01] and Mazur, Stein, and Tate [MST06], we can easily compute p-adic heights on elliptic curves. Our work deals with the next logical step, p-adic height pairings on Jacobians of hyperelliptic curves.

The reason for treating Jacobians is that we have available the Coleman-Gross definition of the height pairing, which is much more concrete than previous definitions. The restriction to hyperelliptic curves is made primarily so that we may apply the recent algorithm [BBK10] for the computation of Coleman integrals on such curves, relying in turn on Kedlaya's work on the computation of the matrix of Frobenius on hyperelliptic curves [Ked01]. We note that generalizations of Kedlaya's work to other types of curves can be applied to generalize the results to these curves as well.

Coleman and Gross give a decomposition of the global p-adic height pairing as a sum of local height pairings at each prime. The local heights away from the prime p behave in much the same way as local archimedean heights, so the main interest lies in the primes above p, where Coleman integration is used. It is this last type of local height pairing which we aim to compute.

To fix ideas, consider a hyperelliptic curve C over $\mathbb{Q}_p$ with p a prime of good reduction. Then, for D_1, D_2 in the group $\mathrm{Div}^0(C)$ of degree 0 divisors on C, with disjoint support, the Coleman-Gross p-adic height pairing at the prime p is given in terms of the Coleman integral

$$h_p(D_1, D_2) = \int_{D_2} \omega_{D_1},$$

for an appropriately constructed differential ω_{D_1} associated to the divisor D_1. This last association is not straightforward and relies again on Coleman integration.

We say next to nothing in this work about the computation of local height pairings away from p. As mentioned above, this is not a p-adic problem and is shared with the computation of archimedean height pairings. In [Bes07], Besser suggested a method for treating this problem, which needed in particular some refined estimates of Kausz [Kau99]. In the meantime, we have learned that this problem is treated in the recent Ph.D. thesis of Müller [Mül10].

The structure of the chapter is as follows: in Section 8.2, we review the work of Coleman and Gross [CG89]. After restricting our focus to hyperelliptic curves in Section 8.3 we describe, in Section 8.4, a new construction that allows us to compute a broader class of Coleman integrals that the heights necessitate. We describe the algorithm for computing the local height pairings in Section 8.5. In Section 8.6, we discuss our implementation of the algorithm in Sage along with error bounds on our results. We follow this in Section 8.7 with numerical examples illustrating our methods. We conclude in Section 8.8 by posing some questions arising from our work.

8.2 The p-adic height pairing

In this section we review the definition of the Coleman-Gross height pairing. As explained in the introduction, there are two required ingredients for making this definition: the theory of Coleman integration and a certain choice of a canonical form. These will be discussed in detail in a later section.

Suppose X/K is a curve defined over a number field K, with good reduction at primes above p. To define the height pairing

$$h : \mathrm{Div}^0(X) \times \mathrm{Div}^0(X) \to \mathbb{Q}_p \ ,$$

one needs the following data:

- A "global log"- a continuous idele class character

$$\ell : \mathbb{A}_K^*/K^* \to \mathbb{Q}_p \, .$$

- For each $v|p$ a choice of a subspace $W_v \subset H^1_{\mathrm{dR}}(X \otimes K_v/K_v)$ complementary to the space of holomorphic forms.

For the definition of the Coleman-Gross height we must insist that the local characters ℓ_v induced by ℓ, for $v|p$, are ramified in the sense that they do not vanish on the units in K_v.

From ℓ one deduces the following data:

- For any place $v \nmid p$ we have $\ell_v(\mathcal{O}^*_{K_v}) = 0$ for continuity reasons, which implies that ℓ_v is completely determined by the number $\ell_v(\pi_v)$, where π_v is any uniformizer in K_v.

- For any place $v|p$ we can decompose

$$\begin{tikzcd} \mathcal{O}^*_{K_v} \arrow[rr, "\ell_v"] \arrow[dr, "\log_v"'] & & \mathbb{Q}_p \\ & K_v \arrow[ur, "t_v"'] & \end{tikzcd} \tag{8.2.1}$$

where t_v is a $\mathbb{Q}_p$-linear map. Since we assume that ℓ_v is ramified it is then possible to extend $\log_v$ to

$$\log_v : K_v^* \to K_v \tag{8.2.2}$$

in such a way that the diagram remains commutative.

Let us now describe the height pairing $h(D_1, D_2)$ for a pair of degree zero divisors D_1 and D_2 with disjoint support. The height pairing is a sum of local terms

$$h(D_1, D_2) = \sum_v h_v(D_1, D_2)$$

over all finite places v. The local terms depend only on the completion at v of K. Thus, let k be a local field of characteristic 0, with valuation ring $\mathcal{O}$, uniformizer π and let $F = \mathcal{O}/\pi\mathcal{O}$ be the residue field, with order q. Let C denote the curve X over the local field k. We shall assume that C has a k-rational point and that C has good reduction at π.

Let $\chi : k^* \to \mathbb{Q}_p$ be a continuous homomorphism, which is the local component of ℓ.

Proposition 8.2.1. *If* $\mathrm{char}\, F \neq p$, *there exists a unique function* $\langle D_1, D_2 \rangle$ *defined for all* $D_1, D_2 \in \mathrm{Div}^0(C)$ *of disjoint support that is continuous, symmetric, bi-additive,taking values in* $\mathbb{Q}_p$, *and satisfying*

$$\langle (f), D_2 \rangle = \chi(f(D_2)) \tag{8.2.3}$$

for $f \in k(C)^*$.

Proof. See [CG89, Prop 1.2]. In fact, one has [CG89, (1.3)]

$$h_v(D_1, D_2) = \ell_v(\pi_v) \cdot (D_1, D_2)\ . \tag{8.2.4}$$

Here, (D_1, D_2) denotes intersection multiplicity on a regular model of C over $\mathcal{O}$ of extensions of D_1 and D_2 to this model. To make this have the required properties one of these extensions has to have zero intersection with all components of the special fibre. □

We now describe the local contribution at a place $v|p$. Let us first recall the following standard terminology.

Definition 8.2.2. A meromorphic differential on C over k is said to be of the *first kind* if it is holomorphic, of the *second kind* if it has residue 0 at every point, and of the *third kind* if it has a simple pole with residue in $\mathbb{Z}$ (at every point it is not holomorphic), respectively.

Recall that the differentials of the second kind, modulo exact differentials, i.e., differentials of rational functions, form a finite dimensional k-vector space of dimension $2g$. It is canonically isomorphic to the first algebraic de Rham cohomology of C/k, $H^1_{\mathrm{dR}}(C/k)$, which is the hypercohomology group of the de Rham complex

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \Omega^1_{C/k} \longrightarrow 0$$

on C. We have a short exact sequence

$$0 \longrightarrow H^0(C, \Omega^1_{C/k}) \longrightarrow H^1_{\mathrm{dR}}(C/k) \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow 0, \tag{8.2.5}$$

where, relying on the description of de Rham cohomology in terms of forms of the second kind we have

- $H^0(C, \Omega^1_{C/k})$, the space of differentials of the first kind, is identified with its image. It has dimension g, and we will denote it $H^{1,0}_{\mathrm{dR}}(C/k)$.
- $H^1(C, \mathcal{O}_C)$ also has dimension g and may be canonically identified with the tangent space at the origin of the Jacobian of C, $J = \mathrm{Pic}^0(C)$.
- $H^1_{\mathrm{dR}}(C/k)$ has a canonical non-degenerate alternating form given by the algebraic cup product pairing

$$\begin{aligned} H^1_{\mathrm{dR}}(C/k) \times H^1_{\mathrm{dR}}(C/k) &\longrightarrow k \\ ([\mu_1], [\mu_2]) \qquad &\mapsto [\mu_1] \cup [\mu_2], \end{aligned}$$

  which can be described by the formula

$$[\mu_1] \cup [\mu_2] = \sum_P \mathrm{Res}_P(\mu_2 \int \mu_1), \tag{8.2.6}$$

where μ_1, μ_2 are differentials of the second kind, with classes $[\mu_1]$ and $[\mu_2]$, respectively, in $H^1_{\mathrm{dR}}(C/k)$ and the sum is over all points in C. The residue does not depend on the choice of a particular local integral for μ_1 because μ_2 is of the second kind and has no residue at any point.

We will also need the theory of *Coleman integration*, as in Chapter 3. For forms that have residues, the Coleman integral depends on the choice of a branch of the p-adic logarithm function. We fix this choice for the computation of the local height pairing to be the one determined in (8.2.2).

Let $T(k)$ denote the subgroup of differentials on C of the third kind. We have a *residue divisor homomorphism*

$$\mathrm{Res} : T(k) \to \mathrm{Div}^0(C), \qquad \mathrm{Res}(\omega) = \sum_P \mathrm{Res}_P\, \omega$$

where the sum ranges over all closed points of C. That the image is contained in $\mathrm{Div}^0(C)$ is just the Residue Theorem. By the residue divisor homomorphism, $T(k)$ fits into the following exact sequence:

$$0 \longrightarrow \Omega^1(C/k) \longrightarrow T(k) \xrightarrow{\mathrm{Res}} \mathrm{Div}^0(C) \longrightarrow 0. \tag{8.2.7}$$

We are interested in a particular subgroup of $T(k)$ whose elements are the logarithmic differentials, i.e., those of the form $\frac{df}{f}$ for $f \in k(C)^*$. We denote this subgroup as $T_l(k)$. Since $T_l(k) \cap H^{1,0}_{\mathrm{dR}}(C/k) = \{0\}$ and $\mathrm{Res}(\frac{df}{f}) = (f)$, we deduce from the sequence (8.2.7) the short exact sequence

$$0 \longrightarrow H^{1,0}_{\mathrm{dR}}(C/k) \longrightarrow T(k)/T_l(k) \longrightarrow J(k) \longrightarrow 0.$$

This sequence has a natural identification with the k-rational points of an exact sequence of commutative algebraic groups over k:

$$0 \longrightarrow H^{1,0}_{\mathrm{dR}}(C/k) \longrightarrow E \longrightarrow J \longrightarrow 0,$$

where E is the universal extension of J by a vector group and $H^{1,0}_{\mathrm{dR}}(C/k) \cong \mathbb{G}_a^g$. Since the Lie algebra of E is canonically isomorphic to $H^1_{\mathrm{dR}}(C/k)$, the exact sequence (8.2.5) is the resulting exact sequence of Lie algebras over k.

Now as k is p-adic, we will make use of the fact that we have a logarithmic homomorphism defined on an open subgroup of the points of any commutative p-adic Lie group, G, to the points of its Lie algebra $\mathrm{Lie}(G)$. When $G = E$ or J, the open subgroup on which the logarithm converges has finite index, so the homomorphism can be uniquely extended to the entire group. We denote this extension as $\log_E$ or $\log_J$, respectively. Since the logarithm is functorial and equal to the identity on $H^{1,0}_{\mathrm{dR}}(C/k)$, we obtain the following:

Proposition 8.2.3. *There is a canonical homomorphism*

$$\Psi : T(k)/T_l(k) \longrightarrow H^1_{\mathrm{dR}}(C/k)$$

which is the identity on differentials of the first kind and makes the following diagram commute:

$$\begin{tikzcd}
0 \arrow[r] & H^{1,0}_{\mathrm{dR}}(C/k) \arrow[r] \arrow[d, equal] & E(k) \arrow[r] \arrow[d, "\Psi=\log_E"] & J(k) \arrow[r] \arrow[d, "\log_J"] & 0 \\
0 \arrow[r] & H^{1,0}_{\mathrm{dR}}(C/k) \arrow[r] & H^1_{\mathrm{dR}}(C/k) \arrow[r] & H^1(C, \mathcal{O}_{C/k}) \arrow[r] & 0.
\end{tikzcd}$$

Note that the map Ψ takes a differential of the third kind on C to a differential of the second kind modulo exact differentials, sending log differentials to 0. It can be extended to a linear map from the k-vector space of all differentials on C/k to $H^1_{\mathrm{dR}}(C/k)$ by writing an arbitrary differential ν as a linear combination $\nu = \sum \alpha_i \mu_i + \gamma$, where μ_i is of the third kind, $\alpha_i \in \overline{k}$, and γ is of the second kind on C. We then define $\Psi(\nu) = \sum \alpha_i \Psi(\mu_i) + [\gamma]$.

The definition of the log map Ψ is not very useful for computations. An equivalent alternative definition has been given in [Bes00]. It is based on the notions of local and global symbols or indices, also discussed there. A simplified version, sufficient for our purposes is given as follows.

Definition 8.2.4. For ω a meromorphic form and ρ a form of the second kind, we define the *global symbol* $\langle \omega, \rho \rangle$ as follows. Fix a point Z. Then, the global symbol is a sum of *local symbols* $\langle \omega, \rho \rangle_A$,

$$\langle \omega, \rho \rangle = \sum_A \langle \omega, \rho \rangle_A,$$

where

$$\langle \omega, \rho \rangle_A = \mathrm{Res}_A \left(\omega \int \rho \right), \tag{8.2.8}$$

where $\int \rho$ is the function $Q \to \int_Z^Q \rho$. The sum is taken over all points A where either ρ or ω has a singularity.

To compute the local symbol $\langle \omega, \rho \rangle_A$ one needs to compute a local expansion of ρ around A, integrate it term by term, fixing the constant of integration to be the Coleman integral $\int_Z^A \rho$, and then multiplying by ω and computing the residue at A. If ρ is singular at A one should instead fix the constant of integration so that the value of the integral at a nearby point A' matches $\int_Z^{A'} \rho$. However, if ω is not also singular at A, then the choice of constant of integration does not matter.

The following result [Bes00] reduces the computation of Ψ to the computation of global symbols.

Proposition 8.2.5. *Let ω be a meromorphic form and ρ a form of the second kind. Then $\langle \omega, \rho \rangle = \Psi(\omega) \cup [\rho]$.*

Proof. See [Bes00, Prop 4.10]. □

Remark 8.2.6. For the actual computation of p-adic height pairings we will need a more general version of Coleman integrals and local indices, see below subsections 8.4.1 and 8.4.2.

Now recall that we have at our disposal the complementary subspace $W = W_v$. It allows us to isolate a canonical form ω_D with residue divisor D as follows.

Definition 8.2.7. For any divisor D of degree 0 on C we let ω_D be the unique form of the third kind satisfying

$$\text{res}(\omega_D) = D, \quad \Psi(\omega_D) \in W.$$

It is easy to see from the properties of Ψ that this indeed uniquely defines the form ω_D.

Definition 8.2.8. The local height pairing is defined by

$$h_v(D_1, D_2) := t_v \left(\int_{D_2} \omega_{D_1} \right)$$

(recalling that the supports of D_1 and D_2 are disjoint), where t_v is the trace map determined by the decomposition of ℓ_v (see (8.2.1)).

Remark 8.2.9. In certain cases, there is a canonical complement W to $H^{1,0}_{\text{dR}}(C/k)$ in $H^1_{\text{dR}}(C/k)$. Namely, when C has good ordinary reduction, we may take W to be the unit root subspace for the action of Frobenius.

Some properties of the local height pairing are as follows:

Proposition 8.2.10. *The local height pairing $h_v(D_1, D_2)$ is continuous and bi-additive. It is symmetric if and only if the subspace W of $H^1_{\text{dR}}(C/k)$ is isotropic with respect to the cup product pairing. Finally, the formula* (8.2.3) *continues to hold.*

Proof. See [CG89, Prop 5.2]. □

8.3 Hyperelliptic curves

Let us now suppose that C is a hyperelliptic curve. The curve C is singular only at infinity (and non-singular when $g = 1$). To describe the neighborhood of infinity we normalize the curve there and obtain the *equation at infinity*

$$t^2 = sf^{\text{rev}}(s) \text{ with } x = \frac{1}{s}, \quad y = \frac{t}{s^{g+1}}, \tag{8.3.1}$$

where $f^{\text{rev}}(s) = s^{2g+1}f(1/s)$ is the reversed polynomial. As is well-known, the first de Rham cohomology of C has a basis consisting of the forms of the second kind

$$\omega_i := \frac{x^i dx}{2y} \text{ for } i = 0, \ldots, 2g - 1.$$

We will denote this basis as

$$\mathcal{B} = \left\{ \frac{dx}{2y}, \frac{xdx}{2y}, \ldots, \frac{x^{2g-1}dx}{2y} \right\}. \tag{8.3.2}$$

If we make the change of coordinates (8.3.1) we see that these are transformed as follows:

$$\frac{x^i dx}{2y} \mapsto -s^{g-1-i}\frac{ds}{2t}.$$

Since s has a double zero at the point at infinity one sees that these forms are holomorphic for $i = 0, \ldots, g-1$ and meromorphic otherwise. We finally recall the *hyperelliptic involution* w defined by $w(x, y) = (x, -y)$.

8.4 Coleman integrals

Here we review the relevant background on Coleman integrals and describe new techniques to compute Coleman integrals of meromorphic differentials with poles in "non-Weierstrass" residue discs. This gives us the necessary tools to present our algorithm to compute local heights.

8.4.1 Generalities on Coleman integrals and symbols

We begin with a result that is needed to formulate our algorithms on annuli:

Theorem 8.4.1. *For a fixed P and for Q restricted to a single residue disc contained in U, the Coleman integral $\int_P^Q \mu$ is analytic and its differential is the restriction of μ to that residue disc. The same is true on an annulus around one of the D_i's, contained in U, provided that the residue around this annulus is 0.*

Proof. See [CdS88] for the general theory. □

Here we present a new method to compute Coleman integrals of meromorphic differentials with poles in non-Weierstrass residue disks. This gives us the necessary tools to present our algorithm to compute local heights.

Suppose now that $k = \mathbb{Q}_p$, and throughout, let ϕ denote a p-power lift of Frobenius.

Definition 8.4.2. The Weierstrass residue discs in C are the residue discs of the Weierstrass points on the reduction.

We will consider a wide open space U_{nw} obtained by throwing away from C, within each Weierstrass residue disc, a disc of sufficiently large radius smaller than 1.

8.4.2 Integration of forms with poles outside Weierstrass discs

The above approach does not work for a meromorphic differential with poles in non-Weierstrass residue discs. We provide a new approach for dealing with this case (again we describe things only over $\mathbb{Q}_p$ but things work in general). Let ω be such a differential. As before, if R, S are points in the same non-Weierstrass residue disc (different from those discs containing the poles of ω), then $\int_S^R \omega$ is just a tiny integral, which can be computed as in Algorithm 4.3.1. Let us now suppose that R, S are in distinct non-Weierstrass residue discs.

To explain the algorithm, we need to extend the theory of local and global symbols in several directions, and in particular to the more general setup of rigid forms on wide open spaces. For the (essentially) full story we refer to [Bes00]. First of all, we can extend Definition 8.2.4 to any two meromorphic forms ω and ρ provided that there are no points where both have non-trivial residues. This is done by setting, when $\mathrm{Res}_A \omega = 0$,

$$\langle \omega, \rho \rangle_A = -\mathrm{Res}_A \left(\rho \int \omega \right) . \tag{8.4.1}$$

This is consistent with the previous definition when also $\mathrm{Res}_A \rho = 0$. The above reference deals also with the case where both forms can have non-trivial residues at a point, but this is not required for the present work.

Next, we consider the extension to wide open spaces. Suppose that the wide open space U is obtained from C by removing discs D_i. One can then define the residue at D_i to be the residue on a small annulus around D_i with respect to a parameter that maps D_i to some disc around 0. We can say that a differential form ρ on U is of the second kind if the residues around each D_i is 0 (It is possible, however, that ρ will have singularities inside D_i with residues, but that their sum is 0). This implies, by property 8.4.1 of Coleman integration, that on an annulus around D_i the form ρ will have an integral which is a Laurent series in the local parameter. Then, for an arbitrary form ω on U the notion of a local symbol from Definition 8.2.4 and (8.4.1) continues to make sense, provided we replace residues along points by residues around the D_i.

Algorithm 8.4.3 (Coleman integration: differential with poles in non-Weierstrass discs).
Input:

- The differential ω with residue divisor $(P) - (Q)$, with non-Weierstrass points $P, Q \in C(\mathbb{Q}_p)$.
- Points $R, S \in C(\mathbb{Q}_p)$ in distinct non-Weierstrass residue discs, not equal to P and Q.

Output: The integral $\int_S^R \omega$.
The algorithm:

1. Let $\alpha = \phi^*(\omega) - p\omega$. Using the methods of Section 8.5.2, compute $\Psi(\omega)$. Using this, set $\Psi(\alpha)$ as $\phi^*(\Psi(\omega)) - p\Psi(\omega)$.
2. Let β be a form with residue divisor $(R) - (S)$. Compute $\Psi(\beta)$.
3. Compute the cup product $\Psi(\alpha) \cup \Psi(\beta)$ (see Section 8.5.1 for more details).

4. Evaluate the tiny integrals $\int_{\phi(S)}^{S} \omega$ and $\int_{R}^{\phi(R)} \omega$.

5. Let $\mathcal{S}$ be the set of points and discs which are either poles of α on U_{nw} or the discs in the complement of U_{nw}. For each $A \in \mathcal{S}$ compute the residue $\mathrm{Res}_A(\alpha \int \beta)$ and compute the sum
$$\sum_{A \in \mathcal{S}} \mathrm{Res}_A(\alpha \int \beta).$$
Here, when A is a pole of α, even though the integral $\int \beta$ is required only locally at A one needs to compute it as a convergent power series on a residue disc, so that for all points A in the same residue disc the same integral is used.

6. We obtain the desired integral using the formula (see Remark 8.4.4)
$$\int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in \mathcal{S}} \mathrm{Res}_A\left(\alpha \int \beta\right) - \int_{\phi(S)}^{S} \omega - \int_{R}^{\phi(R)} \omega\right). \tag{8.4.2}$$

Remark 8.4.4. We obtain (8.4.2) as follows:
$$\begin{aligned}\int_S^R \alpha &= \int_S^R \phi^* \omega - p \int_S^R \omega \\ &= \int_{\phi(S)}^{\phi(R)} \omega - p \int_S^R \omega \\ &= (1-p) \int_S^R \omega + \left(\int_{\phi(S)}^{S} \omega + \int_{R}^{\phi(R)} \omega\right).\end{aligned} \tag{8.4.3}$$

At this point we need to use the full strength of the theory of local symbols [Bes00]. It tells us that Ψ extends to rigid forms on wide open spaces, and that with this extension we have indeed $\Psi(\alpha) = \phi^*(\Psi(\omega)) - p\Psi(\omega)$. It furthermore gives us the formula
$$\Psi(\alpha) \cup \Psi(\beta) = \sum_A \langle \alpha, \beta \rangle .$$

The last sum separates into two sums. The first is over $A \in \mathcal{S}$. Here we can take, according to (8.4.1),
$$\langle \alpha, \beta \rangle = -\,\mathrm{Res}_A\left(\alpha \int \beta\right).$$

The second sum is over the two singular points R and S of β. This sum reads as
$$\mathrm{Res}_R(\beta \int \alpha) + \mathrm{Res}_S(\beta \int \alpha) = \int_S^R \alpha .$$

Thus, we obtain

$$\Psi(\alpha) \cup \Psi(\beta) = \int_S^R \alpha - \sum_{A \in \mathcal{S}} \mathrm{Res}_A \left(\alpha \int \beta \right) .$$

From this and (8.4.3), formula (8.4.2) is easily derived. We just need to note that the form α is "essentially" of the second kind, in that its residue around each annulus surrounding a residue disc is 0 (because ϕ^* multiplies residues by p). This means that for the discs A in the sum over $\mathcal{S}$ we can indeed compute the local symbol as stated, and that instead of using a Coleman integral for β we may just pick any integral, consistently on each residue disc, as it will differ from the Coleman integral by a constant on that disc and the sum over the disc will be modified by the product of this constant with the sum of the residues of α on the residue disc, which is 0. Another remark is that the above fails if ω has a singularity at $\phi(R)$ or $\phi(S)$ (even though the integral is actually defined). The simplest solution to this problem is to move R or S within their residue disc, recompute and complement with tiny integrals.

Remark 8.4.5. In practice, the computation in Step 5 of Algorithm 8.4.3 is the slowest part of the algorithm, as it involves high-precision local calculations over all poles of α. In particular, Frobenius introduces essential singularities at Weierstrass points, and the computations in Weierstrass discs are done in annuli with Laurent series with an essential singularity. However, since $\sum_{T \in U} \mathrm{Res}_T(\alpha) = 0$ in each residue disc U, for the Weierstrass discs, we do not need a constant of integration. For the non-Weierstrass poles of α, we may choose one constant of integration within each residue disc. More precisely, if P and Q are in separate residue discs, we compute

$$\sum_{A \in U_P} \mathrm{Res}_A \left(\alpha \int \beta \right) = \mathrm{tr}_{k(x(P_1))/k} \left(\mathrm{Res}_{P_1} \left(\alpha \int_P^{P_1} \beta \right) \right) = \mathrm{tr}_{k(x(P_1))/k} \left(\int_P^{P_1} \beta \right),$$

$$\sum_{A \in U_Q} \mathrm{Res}_A \left(\alpha \int \beta \right) = \mathrm{tr}_{k(x(Q_1))/k} \left(\mathrm{Res}_{Q_1} \left(\alpha \int_Q^{Q_1} \beta \right) \right) = \mathrm{tr}_{k(x(Q_1))/k} \left(- \int_Q^{Q_1} \beta \right),$$

where U_P (resp, U_Q) is the residue disc of P (resp, Q) and $x(P_1)$ (resp. $x(Q_1)$) is a root of $x^p - x(P)$ (resp, $x^p - x(Q)$) such that P_1 (resp, Q_1) is in the residue disc of P (resp Q).

8.5 The local height pairing at primes above p

In this section we will explain the algorithm that computes the local height pairing at a prime above p for degree zero divisors on the hyperelliptic curve C. Recall that we have as additional data the complementary subspace W and the character χ from which we deduce a branch of the logarithm to be used in Coleman integration and the trace map t_v (we keep the subscript v at some places for clarity, even though it now serves no purpose).

Let D_1 and D_2 be two divisors of degree 0 on C. Our main algorithm computes the local height pairing $h_v(D_1, D_2)$. It may be described in two steps

- Compute the height pairing in the case where D_1 and D_2 are anti-symmetric with respect to the hyperelliptic involution (Algorithm 8.5.8)
- Compute the height pairing in the general case using the first case (Algorithm 8.5.7).

Before discussing either algorithm, we begin with some general notes about the representation of divisors on hyperelliptic curves (see [Kob98, App §5-6]).

Recall that a divisor of degree 0 on C may be written in the form

$$D = \sum m_i P_i - \left(\sum m_i\right)(\infty).$$

Definition 8.5.1. A divisor D as above is called *semi-reduced* if the following conditions are satisfied:

- $m_i \geq 0$
- If P_i is in the support of D, then $w(P_i)$ is not, unless $w(P_i) = P_i$ in which case $m_i = 1$.

A semi-reduced divisor is called *reduced* if in addition

- $\sum m_i \leq g$.

One may represent a semi-reduced divisor D by a pair of polynomials $a(x), b(x)$ with $\deg(b) < \deg(a)$ such that

- The projection of $\sum m_i P_i$ on $\mathbb{P}^1$ is the zero divisor of $a(x)$.
- $b(x)$ is an interpolation polynomial with the property that for $P_i = (x_i, y_i)$ we have $b(x_i) = y_i$.

The condition that D is reduced is equivalent to having $\deg(a) \leq g$.

Remark 8.5.2. One can associate b uniquely to the divisor by insisting that $a(x) | (b(x)^2 - f(x))$. This would be less important for us and there are cases we may not achieve this.

Definition 8.5.3. Let us denote by (a, b) the semi-reduced divisor determined by the pair of polynomials a and b and call (a, b) the standard representation of the divisor.

It is known that any degree zero divisor D on C is equivalent to a unique reduced divisor. Furthermore, the reduction is effective. More precisely, passing from an arbitrary divisor to a semi-reduced one is just a question of adding or subtracting divisors of functions pulled back from $\mathbb{P}^1$. Passing from a semi-reduced divisor to a reduced divisor has an effective algorithm described in [Kob98, App, Alg 2 and Thm 7.2]. Since we know our height pairing satisfies (8.2.3) by Proposition 8.2.10, which easily allows to pass from a divisor to an equivalent divisor in the pairing there is no harm in assuming that our divisors are reduced.

Unfortunately for us, reduced divisors are not sufficient. The reason is that since they always have a component at infinity, two such divisors cannot have disjoint support unless one of them is trivial. For this reason we will work with the difference of two reduced divisors.

Definition 8.5.4. The divisor denoted $(a, b) - (c, d)$, where a and c are polynomials of the same degree $\leq g$, stands for the difference of the reduced divisors defined by (a, b) and (c, d).

We always assume that the two divisors defined by (a, b) and (c, d) have no common components other than at ∞. If there are common components they can be cancelled out.

We will mostly work with anti-symmetric divisors. Given any zero divisor D, the divisor $D - w^*D$ is anti-symmetric. Conversely, any anti-symmetric divisor is obtained in this way. It follows easily that any anti-symmetric divisor is equivalent to $D - w^*D$ for a reduced divisor D. There may be several representations in this form for a given divisor, however, there is just one containing no points P_i with $P_i = w(P_i)$. In the representation (a, b) for D this is equivalent to having the polynomial a prime to f.

Definition 8.5.5. An anti-symmetric divisor in standard representation is a divisor of the form

$$[a, b] := D - w^*D$$

with D a reduced divisor given in the form (a, b). Such a divisor is in *minimal* standard representation if a is prime to f.

As noted before, any anti-symmetric divisor is linearly equivalent to one in standard representation. For height pairings of anti-symmetric divisors we do not need to consider differences of such divisors because they do not generically have components at infinity. Thus, $[a_1, b_1]$ and $[a_2, b_2]$ have disjoint support if and only if a_1 and a_2 are relatively prime and of the same degree.

We now describe Algorithm 8.5.7. For any divisor D we have a decomposition, with rational coefficients

$$D = \frac{1}{2}D^+ + \frac{1}{2}D^-, \qquad D^+ = D + w^*(D)\ ,\ D^- = D - w^*(D). \tag{8.5.1}$$

Lemma 8.5.6. *Suppose D is given by the representation $(a, b) - (c, d)$. Then, the divisor D^- is just $[a \cdot c, e]$ in terms of Definition 8.5.5, where e is obtained by solving a Chinese Remainder Theorem problem to be congruent to b modulo a and to $-d$ modulo c.*

Proof. If a is prime to c this is clear. In general, suppose $(x - \alpha)$ has multiplicity m in a and n in c. We may assume $m \geq n$. Since we are assuming (a, b) and (c, d) have no common components, it follows that $D - w^*(D)$ is going to have the two summands $(m+n)[(\alpha, b(\alpha)) - (\alpha, -b(\alpha)]$, and $m+n$ is indeed the multiplicity of ac in α (it seems though that we can only solve the Chinese remainder problem modulo the least common multiple of a and c). □

On the other hand, D^+ is nothing but the divisor of the rational function $\frac{a(x)}{c(x)}$ considered as a rational function on C. It follows from the fact that (8.2.3) is satisfied by Proposition 8.2.10 that for any $E \in \mathrm{Div}^0(C)$ we have

$$h_v(D^+, E) = h_v(E, D^+) = \chi\left(\frac{a}{c}(E)\right), \tag{8.5.2}$$

where $\frac{a}{c}(E)$ means as usual the product of the values of $\frac{a}{c}$ on the x-coordinates of the points making up E with the appropriate multiplicities. An easy consequence of this formula is that

$$h_v(D^+, E) = h_v(E, D^+) = 0 \quad \text{if } E \text{ is anti-symmetric.} \tag{8.5.3}$$

Consider now two divisors D_1 and D_2 in $\mathrm{Div}^0(C)$. Decomposing into plus and minus parts it follows from (8.5.3) that

$$h_v(D_1, D_2) = \frac{1}{4}h_v(D_1^+, D_2^+) + \frac{1}{4}h_v(D_1^-, D_2^-). \tag{8.5.4}$$

The first term can be computed using (8.5.2), while the second term is a height pairing between anti-symmetric divisors. This immediately gives the following algorithm.

Algorithm 8.5.7 (p-adic height pairing for general divisors).
Input:

- The subspace W, branch of logarithm and trace map t.
- Divisors D_1 and D_2 with disjoint support given as

$$D_1 = (a_1, b_1) - (c_1, d_1)$$
$$D_2 = (a_2, b_2) - (c_2, d_2).$$

Output: The local height pairing $h_v(D_1, D_2)$.
The algorithm:

1. Compute expressions for the divisors D_1^- and D_2^- using Lemma 8.5.6.
2. Compute using (8.5.2),
$$h_v(D_1^+, D_2^+) = \chi((a_1/c_1)(D_2^+)).$$
3. Compute, using Algorithm 8.5.8, the local height pairing for anti-symmetric divisors $h_v(D_1^-, D_2^-)$.
4. Substitute in (8.5.4) to obtain $h_v(D_1, D_2)$.

We next turn to Algorithm 8.5.8 for the case of anti-symmetric divisors D_1 and D_2. First of all, we have to introduce yet another decomposition. The algorithm behaves differently with respect to parts that reduce to the Weierstrass points (Weierstrass divisors) and those which do not. We can decompose a divisor D into the sum of its Weierstrass part D^{w} (the part consisting of all the points reducing to a Weierstrass point) and its non-Weierstrass part D^{nw}. Then, in a similar way to (8.5.4) we have the decomposition

$$h_v(D_1, D_2) = h_v(D_1, D_2^{\mathrm{w}}) + h_v(D_1^{\mathrm{w}}, D_2^{\mathrm{nw}}) + h_v(D_1^{\mathrm{nw}}, D_2^{\mathrm{nw}}). \tag{8.5.5}$$

We may now outline the algorithm:

Algorithm 8.5.8 (p-adic height pairing for anti-symmetric divisors).
Input:

- The subspace W, branch of logarithm and trace map t.
- Anti-symmetric divisors D_1 and D_2 given in standard representation (a_1, b_1), (a_2, b_2).

Output: The local height pairing $h_v(D_1, D_2)$.
The algorithm:

1. Compute the cup product matrix for a basis of $H^1_{\mathrm{dR}}(C/k)$.
2. Compute D_1^{w} and D_1^{nw}.
3. Write down forms ν_1^{w} and ν_1^{nw} with residue divisors D_1^{w} and D_1^{nw}, respectively.
4. Compute the form $\omega_{D_1^{\mathrm{w}}} \in W$ and a holomorphic form η_1 such that
$$\omega_{D_1^{\mathrm{nw}}} = \nu_1^{\mathrm{nw}} - \eta_1 \in W.$$
5. Compute the tiny Coleman integral $h_v(D_1, D_2^{\mathrm{w}}) = t(\int_{D_2^{\mathrm{w}}} (\omega_{D_1^{\mathrm{w}}} + \nu_1^{\mathrm{nw}} - \eta_1))$.
6. Compute the Coleman integral $h_v(D_1^{\mathrm{w}}, D_2^{\mathrm{nw}}) = t(\int_{D_2^{\mathrm{nw}}} \omega_{D_1^{\mathrm{w}}})$.
7. Compute the Coleman integral $h_v(D_1^{\mathrm{nw}}, D_2^{\mathrm{nw}}) = t(\int_{D_2^{\mathrm{nw}}} \nu_1^{\mathrm{nw}} - \int_{D_2^{\mathrm{nw}}} \eta_1)$.
8. Compute $h_v(D_1, D_2)$ using (8.5.5).

Remark 8.5.9. Note that it is also possible to directly compute the heights without these decompositions. In this case, we have the following algorithm:

Algorithm 8.5.10 (Coleman-Gross local height for hyperelliptic curves (alternate algorithm)).
Input:

- Hyperelliptic curve C of genus g over $k = \mathbb{Q}_p$ of the form $y^2 = f(x)$, with $\deg f(x) = 2g+1$, such that p is a prime of good ordinary reduction for C and all finite Weierstrass points of C are $\mathbb{Q}_p$-rational,
- Divisors[1] $D_1, D_2 \in \operatorname{Div}^0(C)$ of the form $D_1 = (P) - (Q)$ and $D_2 = (R) - (S)$, where $P, Q \notin U_R, U_S$ and none of P, Q, R, S Weierstrass.

Output:

- The p-component of the p-adic height pairing $h_p(D_1, D_2) = \int_{D_2} \omega_{D_1}$.

Algorithm:

1. **From D_1 to ω.** Choose ω a differential of the third kind with $\operatorname{Res}(\omega) = D_1$.
2. **The map Ψ.** Compute $\log(\omega) = \Psi(\omega)$ for ω a meromorphic differential.
3. **From ω to ω_{D_1} and η.** Via the decomposition

$$H^1_{dR}(C/k) \simeq H^{1,0}_{dR}(C/k) \oplus W,$$

write

$$\log(\omega) = \eta + \log(\omega_{D_1}),$$

where η is holomorphic, and $\log(\omega_{D_1}) \in W$. This gives $\omega_{D_1} = \omega - \eta$.

4. **Coleman integration: holomorphic differential.** Compute $\int_{D_2} \eta$.
5. **Coleman integration: meromorphic differential.** Let ϕ be a p-power lift of Frobenius and set $\alpha := \phi^*\omega - p\omega$. Then for β a differential with residue divisor $D_2 = (R) - (S)$, we compute

$$\int_{D_2} \omega = \int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum \operatorname{Res}\left(\alpha \int \beta\right) - \int_{\phi(S)}^S \omega - \int_R^{\phi(R)} \omega\right). \tag{8.5.6}$$

6. **Height pairing**. Subtract the integrals to recover the pairing:

$$h_p(D_1, D_2) = \int_S^R \omega_{(P)-(Q)} = \int_S^R \omega - \int_S^R \eta.$$

We now add some further details on each of the quantities appearing in our algorithms.

[1] For ease of presentation, D_1 and D_2 will be chosen in this manner, though the algorithm applies to any $D_1, D_2 \in \operatorname{Div}^0(C)$ with the integrals computed accordingly.

8.5.1 Computing cup products

We first compute the cup product between any two elements of the standard basis (8.3.2) for $H^1_{\mathrm{dR}}(X/k)$. This is easily done using the formula (8.2.6).

We can be a bit more precise as follows.

Definition 8.5.11. The *cup product matrix* associated to C with respect to $\mathcal{B}$ is the $2g \times 2g$ matrix with entry $a_{i,j}$ given by the cup product of differentials $[\omega_{i-1}] \cup [\omega_{j-1}]$, normalized so that $[\omega_{i-1}] \cup [\omega_{j-1}] = \mathrm{Res}(\omega_{j-1} \int \omega_{i-1})$.

By computing in the local coordinates at infinity, we may record the following:

Lemma 8.5.12. *The cup product matrix for C with respect to $\mathcal{B}$ satisfies the following properties:*

1. *Anti-diagonal elements are given by the sequence*

$$\left\{\frac{1}{2g-1}, \frac{1}{2g-3}, \dots, \frac{1}{3}, 1, -1, -\frac{1}{3}, \dots, -\frac{1}{2g-1}\right\}.$$

2. *Entries above the anti-diagonal are 0.*

3. *Diagonal elements are 0.*

Example 8.5.13. The cup product matrix with respect to $\mathcal{B}$ for an elliptic curve is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Note that the subspace spanned by $\frac{xdx}{2y}$ is isotropic. In particular, for genus 1, we may take $H^{1,0}_{\mathrm{dR}}(C/k)$ spanned by ω_0 and W spanned by ω_1, and we need not require p to be a prime of ordinary reduction for the pairing to be symmetric.

8.5.2 The map Ψ

We compute Ψ of a differential ω by writing

$$\Psi(\omega) = c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1},$$

and solving for the coefficients c_i. This is done by considering a linear system involving global symbols and cup products:

$$\langle \omega, \omega_j \rangle = \Psi(\omega) \cup [\omega_j] = \sum_{i=0}^{2g-1} c_i([\omega_i] \cup [\omega_j]).$$

Recall that as in Definition 8.2.4, we calculate the global symbol as a sum of local symbols, each of which involves a Coleman integral and a calculation in local coordinates. This computation is actually much simpler:

Proposition 8.5.14. *Suppose ω is a form of the third kind with residue divisor D which does not contain ∞. Then we have*

$$\langle \omega, \omega_i \rangle = \int_D \omega_i + \mathrm{Res}_\infty \left(\omega \int \omega_i \right),$$

where the residue at ∞ is computed by taking any anti-derivative of ω_i.

Proof. The sum of local symbols is over all points where either ω or ω_i has a singularity. These are the points in the support of D and possibly the point ∞. Since ω has a simple pole at each point P in the support of D, the local symbol is simply the multiplicity of D at P times $\int_Z^P \omega_i$ (where Z is a fixed point throughout the global symbol calculation). Summing over all points gives $\int_D \omega_i$. On the other hand, since we are assuming that ω is holomorphic at ∞, the choice of the constant of integration for ω_i at ∞ does not matter. □

Now letting N denote the cup product matrix, we have

$$\Psi(\omega) = N^{-1} \begin{pmatrix} \langle \omega, \omega_0 \rangle \\ \vdots \\ \langle \omega, \omega_{2g-1} \rangle \end{pmatrix}.$$

8.5.3 Decomposing a divisor D into D^{w} and D^{nw}

This is very easy to do. When the divisor is given in standard form $[a, b]$ one just reduces a modulo the prime π, picks up the part that reduces to Weierstrass points by taking the greatest common divisor with the reduction of f, and then applies a Hensel lift to get the factor a^{w} of a corresponding to the points reducing to Weierstrass. Then we have $a^{\mathrm{nw}} = a/a^{\mathrm{w}}$, from which one may deduce the divisor decomposition.

8.5.4 A form with the required residue divisor

This is an easy task with the following.

Proposition 8.5.15. *Let D be an anti-symmetric divisor in standard representation $[a, b]$. The differential form*

$$\omega = \frac{a'(x)b(x)dx}{a(x)y}$$

has simple poles and its residue divisor is D.

Proof. Suppose that $(a, b) = \sum m_i P_i - \left(\sum m_i\right)(\infty)$. We can write $\omega = (b/y)da/a$. The form da/a has simple poles at $\pm P_i$ with residue m_i while b/y has value 1 at P_i and value -1 at ιP_i. On the other hand we can also write $\omega = (a'b/a)(\frac{dx}{2y})$ and since $\frac{dx}{2y}$ is holomorphic, it follows that ω has no poles where a does not vanish. Finally, it is easy to see that ω does not have a pole at infinity. □

8.5.5 Finding ω_D for a Weierstrass divisor D

Suppose we have already written down a form whose residue divisor is D. Since the singularities of the form are contained in the Weierstrass residue discs, it is amenable to the reduction algorithm done in Kedlaya's algorithm [Ked01]. This means that we may compute a representation of ω as a linear combination of the basis $\mathcal{B}$ plus an exact differential dg. Since it follows that $\Psi(\omega)$ is just the above combination of basis elements, we need only subtract the appropriate combination of holomorphic basis elements to make it reside in W.

8.5.6 Finding ω_D for a non-Weierstrass divisor D

We start with a form ω whose residue divisor is D. We compute $\Psi(\omega)$ as in Subsection 8.5.2. All that is left to do is to let η be the projection of $\Psi(\omega)$ on $H^{1,0}_{\mathrm{dR}}$ along W.

8.5.7 Integration when D_2 reduces to Weierstrass points

Suppose that the points of D_2 reduce to the Weierstrass points. Since D_2 is anti-symmetric, this means that in computing the integral we need to take the sum of differences over pairs of points $\pm P$ which reduce to the same point. This is a sum of tiny integrals.

8.5.8 Computation when D_1 is Weierstrass and D_2 is not

In this case, we are given, by the previous reduction, the form ω_{D_1} as a combination $\sum \alpha_i \omega_i + dg$. Thus $\int_{D_2} \omega_{D_1} = \sum \alpha_i \int_{D_2} \omega_i + g(D_2)$. Since the points of D_2 are in the domain where the integrals of the ω_i may be computed, this is a standard computation.

8.5.9 Computation when both divisors are non-Weierstrass

In this case, ω_{D_1} is given in the form $\nu_1 - \eta_1$, where ν_1 is a form with residue divisor D_1 and η_1 is holomorphic. The integral of η_1 poses no problems while that of ν_1 is discussed in Subsection 8.4.2.

8.6 Implementation notes

In this section, we discuss the choices made in our Sage [S$^+$11] implementation and give error estimates on the precision of our results. We work over $\mathbb{Q}_p$ with a precision of n digits; note that if one desires an answer with n digits of precision, one has to start with a larger working precision, as seen below.

We only discuss the computation for anti-symmetric divisors, as the extension to general divisors is trivial, as discussed in Section 8.5. Furthermore, our implementation assumes that the divisors are of the form $(P) - (-P)$ for a $\mathbb{Q}_p$-rational point P, as it is then quite easy to consider cases when the divisor is a sum of such expressions. Finally, all computations are done with respect to a particular choice of the complementary subspace W, which we describe below.

8.6.1 Auxiliary choices

Our algorithm relies on the splitting

$$H^1_{\mathrm{dR}}(C/k) \simeq H^{1,0}_{\mathrm{dR}}(C/k) \oplus W,$$

which allows us to write

$$\Psi(\nu_1) = \eta_1 + \Psi(\omega_{D_1}),$$

where η_1 is holomorphic, and $\Psi(\omega_{D_1}) \in W$.

As noted in Example 8.5.13, when $g = 1$, we may simply take $H^{1,0}_{\mathrm{dR}}(C/k)$ spanned by ω_0 and W spanned by ω_1. Note that for genus $g > 1$ it does not suffice to take W spanned by $\omega_g, \omega_{g+1}, \ldots, \omega_{2g-1}$, as the resulting subspace is not necessarily isotropic. While the local height is independent of basis, it is not independent of the choice of W. For the local height to be symmetric, it is necessary that W be an isotropic subspace. For $g > 1$, we thus further require that p be a prime of *ordinary* reduction, so that W can be chosen to be the unit root subspace. Suppose $p > g$ so that the standard basis is crystalline. Generalizing [MST06], we compute a basis for W as follows:

Proposition 8.6.1. *Suppose $p > 2g-1$ (so that the matrix of Frobenius is p-integral). Let n be the working precision in the underlying base ring $\mathbb{Z}_p$, so that all computations are done modulo p^n. Let* Frob *denote the matrix of a p-power lift of Frobenius, as acting on the standard basis $\mathcal{B}$ of $H^1_{\mathrm{dR}}(C/k)$. Then $\{\mathrm{Frob}^n\, \omega_g, \mathrm{Frob}^n\, \omega_{g+1}, \ldots, \mathrm{Frob}^n\, \omega_{2g-1}\}$ is a basis for W.*

Proof. With the integral structure provided by crystalline cohomology, it is well known that Frob maps the holomorphic forms to p times the integral structure. Thus, with W the unit root part decomposing a vector v into $\omega + \eta$ with $\omega \in W$ and η holomorphic it is easy to see that $\mathrm{Frob}^n v$ is in $W + p^n$ times the integral structure. In other words, up to the prescribed precision, $\mathrm{Frob}^n v$ lies in W. On the other hand, Frob is invertible so starting with g independent vectors modulo the holomorphic differentials one gets g independent vectors in W. □

8.6.2 Precision

Broadly speaking, the p-adic precision of a local height depends on two types of calculation:

1. Coleman integrals of basis differentials (or otherwise "nice" differentials – e.g., holomorphic in the discs corresponding to the limits of integration) and

2. expansion of local coordinates at a point.

Each key step of the algorithm in Section 8.4.3 can be categorized as depending on one or both of these:

- $\Psi(\nu_1)$ needs the cup product matrix (local coordinates) and local symbols (Coleman integrals of basis differentials)
- $\int \eta_1$ is a sum of Coleman integrals of basis differentials
- $\int \nu_1$ is defined in terms of
  - tiny integrals (Coleman integrals of a "nice" differential),
  - sums of residues of Laurent series (local coordinates), and
  - $\Psi(\alpha)$, $\Psi(\beta)$ (as above).

Precision of Coleman integrals

We will now carefully review the precision of each of the objects we computed, as an expansion of the overview in §3.3.1. Let ν_P be a differential with residue divisor

$$D_P = (P) - (-P)$$

and β a differential with residue divisor

$$D_Q = (Q) - (-Q).$$

The precision of $\Psi(\nu_P)$ (and $\Psi(\beta)$) just depends on the Coleman integral involved, as the residue can just be read off of the differential.

After computing $\Psi(\nu_P)$ with respect to the standard basis of $H^1_{\mathrm{dR}}(C)$, we fix a splitting of $H^1_{\mathrm{dR}}(C/k)$ into $H^{1,0}_{\mathrm{dR}}(C/k) \oplus W$, which gives η_P and $\omega_{D_P} = \nu_P - \eta_P$. Since the height pairing is given by $\int \omega_{D_P}$, we need to compute the integrals $\int \nu_P$ and $\int \eta_P$.

The integral $\int \eta_P$ is just a linear combination of the integrals of holomorphic basis differentials. On the other hand, the integral of ν_P requires the computation of $\Psi(\alpha)$, $\Psi(\beta)$, $\sum \mathrm{Res}(\alpha \int \beta)$, and the tiny integral $\int_Q^{\phi(-Q)} \nu_P$. As before, the tiny integral is computed with precision as in Proposition 3.3.1.

Since $\alpha = \phi^*\nu_P - p\nu_P$, we may write $\Psi(\alpha)$ in terms of things we have already computed, namely $\Psi(\alpha) = \mathrm{Frob}(\Psi(\nu_P)) - p\Psi(\nu_P)$. So we need not do more work here. However, the precision of $\sum \mathrm{Res}(\alpha \int \beta)$ merits further discussion, as we must consider its representation in local coordinates.

Precision: local coordinates

Computing with local coordinates is crucial to the algorithm. More precisely, for any point P, we must construct power series $x(t), y(t)$ for a local parameter t such that $P = (x(0), y(0))$. To explicitly compute with power series, we need to know where (t-adically) it is acceptable to truncate them.

Precision: Cup product matrix.

The first instance this problem arises is in the computation of the cup product matrix, as ω_j must be written in terms of the local coordinates $x(t), y(t)$ at infinity. Let v_t denote the t-adic valuation. Since $v_t(\omega_j) = 2(g-j)-2$, which is minimal for $j = 2g-1$, we have $\min v_t(\omega_j) = -2g$. Thus it suffices to compute each basis differential ω_k to a precision of t^{2g}. Consequently, we compute $x(t)$ to a precision of $t^{2(2g-1)}$ and $y(t)$ to a precision of t^{2g-1}.

Precision: $\sum \mathrm{Res}(\alpha \int \beta)$.

Now we consider $\sum_A \mathrm{Res}_A(\alpha \int \beta)$, where the sum is taken over all points A that are poles of α. We begin by looking at the expansion for $\alpha = \phi^*\nu_P - p\nu_P$.

As noted earlier, for the non-Weierstrass poles of α, we may choose one constant of integration within each residue disc. More precisely, if P and Q are in separate residue discs, we compute

$$\sum_{A\in U_P} \mathrm{Res}_A\left(\alpha \int \beta\right) = \mathrm{tr}_{k(x(P_1))/k}\left(\mathrm{Res}_{P_1}\left(\alpha \int_P^{P_1} \beta\right)\right) = \mathrm{tr}_{k(x(P_1))/k}\left(\int_P^{P_1} \beta\right),$$

$$\sum_{A\in U_Q} \mathrm{Res}_A\left(\alpha \int \beta\right) = \mathrm{tr}_{k(x(Q_1))/k}\left(\mathrm{Res}_{Q_1}\left(\alpha \int_Q^{Q_1} \beta\right)\right) = \mathrm{tr}_{k(x(Q_1))/k}\left(-\int_Q^{Q_1} \beta\right).$$

where U_P (resp, U_Q) is the residue disc of P (resp, Q) and $x(P_1)$ (resp, $x(Q_1)$) is a root of $x^p - x(P)$ (resp, $x^p - x(Q)$) such that P_1 (resp, Q_1) is in the residue disc of P (resp Q).

For these computations, we have to compute Coleman integrals and local coordinates, so we must study the precision of both, as given by the following corollary of Proposition 3.3.1:

Corollary 8.6.2. *Let A be non-Weierstrass, defined over a degree d extension k' of $\mathbb{Q}_p$. Let U_A denote the residue disc of A, and let B be a non-Weierstrass point in U_A defined over $\mathbb{Q}_p$. Suppose a working precision of n p-adic digits (so that A has precision dn in a uniformizer π of k'). Let β be written in terms of the local coordinate $(x(t), y(t))$ at B, so that $\beta = h(t)dt$ with $h(t)$ truncated modulo t^{dm}. Then the residue $\sum_{S\in U_A} \mathrm{Res}(\alpha \int \beta)$ has $\min\{n, dm + 1 - \lfloor \log_p(dm+1) \rfloor\}$ digits of precision.*

Proof. Suppose we are working in the residue disc of P and that A is defined over a degree d extension of $\mathbb{Q}_p$. Note that we must compute the local coordinates $(x(t), y(t))$ at P with a precision of at least t^{dm}. As the interpolation from P to A is linear, we merely make a linear substitution

$$\begin{aligned} x(t) &:= x((x(A) - x(P))t) \\ y(t) &:= y((x(A) - x(P))t). \end{aligned}$$

This new $(x(t), y(t))$ is used to compute the tiny integral of β from P to A, the result of which has precision $\min\{n, dm + 1 - \lfloor \log_p(dm+1) \rfloor\}$. Taking the trace from K to

$\mathbb{Q}_p$ accounts for the other poles of α in the disc of P. □

Finally, in the case where A is a finite Weierstrass point, we have to compute in the local coordinates of A. (Note that we need not compute the residue at $(0,0)$ if on the curve or at infinity.)

Proposition 8.6.3. *Let α be above and let A be a finite Weierstrass point not equal to $(0,0)$. Let $(x(t), y(t))$ represent the local coordinates at A. Then to compute $\operatorname{Res}(\alpha \int \beta)$ with n digits of p-adic precision, we compute $(x(t), y(t))$ to $t^{2pn-p-3}$.*

Proof. We have

$$\begin{aligned}\alpha &= \phi^* \nu_P - p\nu_P \\ &= \frac{y(P)px^{p-1}dx}{\phi(y)(x^p - x(P))} - \frac{py(P)dx}{y(x - x(P))},\end{aligned}$$

where

$$\frac{1}{\phi(y)} = y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(f(x^p) - f(x)^p)^i}{f(x)^{pi}}.$$

For $\operatorname{Res}(\alpha \int \beta)$ to have n digits of p-adic precision, we must compute n terms of the binomial expansion of $\frac{1}{\phi(y)}$.

Recall that for a finite Weierstrass point $(a, 0)$, we have

$$\begin{aligned}x(t) &= a + \frac{1}{g(a)} t^2 + O(t^4) \\ y(t) &= t,\end{aligned}$$

where $g(x) = \frac{f(x)}{x-a}$. Note that by hypothesis, $a \neq 0$. We compute the t-adic valuation of α:

$$\begin{aligned}v_t(\alpha) &= v_t(\phi^* \nu_P) \quad \text{since } \nu_P \text{ only contributes higher-order terms} \\ &= v_t\left(\frac{y(P)px^{p-1}dx}{\phi(y)(x^p - x(P))}\right) \\ &= 1 + v_t\left(\frac{1}{\phi(y)}\right) \quad (x^p \neq x(P)) \\ &= 1 - pv_t(y) + (n-1)v_t\left(\frac{f(x^p) - f(x)^p}{f(x)^p}\right) \\ &= 1 - p + (n-1)\begin{cases} (2-2p), & \text{if } v_t(f(x^p) - f(x)^p) > 0 \\ -2p, & \text{else} \end{cases}\end{aligned}$$

Thus we have

$$v_t(\alpha) = \begin{cases} p - 2pn + 2n - 1, & \text{if } v_t(f(x^p) - f(x)^p) > 0 \\ p - 2pn + 1, & \text{else.} \end{cases}$$

As $p - 2pn + 2n - 1 \geq p - 2pn + 1$ for $n \geq 1$, we have $v_t(\alpha) \geq p - 2pn + 1$. Set $m = 2pn - p - 1$. Since we want $\operatorname{Res}(\alpha \int \beta)$, we need $v_t(\alpha \int \beta) \geq -1$, so we must compute β to at least t^{m-2}. To get this precision, we must in turn compute with $x(t), y(t)$ to this precision. □

8.7 Examples

Here we provide some examples of our algorithms.

8.7.1 Local heights: genus 2, general divisors

Let C be the genus 2 hyperelliptic curve

$$y^2 = x^5 - 23x^3 + 18x^2 + 40x = (x-4)(x-2)x(x+1)(x+5)$$

over $\mathbb{Q}_{11}$, and let

$$\begin{aligned} D_1 &= (P) - (Q) \\ D_2 &= (R) - (S), \end{aligned}$$

where $P = (-4, 24), Q = (1, 6), R = (5, 30), S = (-2, 12)$. We describe how to use Algorithm 8.5.7 to compute the local contribution at $p = 11$.

We see that

$$\begin{aligned} D_1^+ &= \operatorname{div}\left(\frac{x - x(P)}{x - x(Q)}\right), \quad D_1^- = [(P) - (-P)] + [(-Q) - (Q)], \\ D_2^+ &= \operatorname{div}\left(\frac{x - x(R)}{x - x(S)}\right), \quad D_2^- = [(R) - (-R)] + [(-S) - (S)]. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} \frac{1}{4}h_{11}(D_1^+, D_2^+) &= \frac{1}{4}\log\left(\frac{x - x(P)}{x - x(Q)}(D_2^+)\right) \\ &= \frac{1}{2}\log\left(\left(\frac{x(R) - x(P)}{x(R) - x(Q)}\right)\left(\frac{x(S) - x(P)}{x(S) - x(Q)}\right)^{-1}\right) \\ &= 2 \cdot 11 + 9 \cdot 11^2 + 7 \cdot 11^3 + 2 \cdot 11^4 + O(11^5). \end{aligned}$$

Now we compute, using Algorithm 8.5.8, the contributions from anti-symmetric heights (details of which are in Subsection 8.7.2):

$$\begin{aligned} h_{11}((P) - (-P), (-S) - (S)) &= 9 \cdot 11^{-1} + 5 + 6 \cdot 11 + 8 \cdot 11^2 + 9 \cdot 11^3 + 3 \cdot 11^4 + O(11^5) \\ h_{11}((P) - (-P), (R) - (-R)) &= 6 \cdot 11^{-1} + 10 + 7 \cdot 11 + 6 \cdot 11^2 + 3 \cdot 11^3 + 7 \cdot 11^4 + O(11^5) \\ h_{11}((-Q) - (Q), (R) - (-R)) &= 8 \cdot 11^{-1} + 5 + 7 \cdot 11 + 10 \cdot 11^2 + 3 \cdot 11^3 + 7 \cdot 11^4 + O(11^5) \\ h_{11}((-Q) - (-Q), (-S) - (S)) &= 11^{-1} + 8 + 7 \cdot 11 + 2 \cdot 11^2 + 7 \cdot 11^3 + 8 \cdot 11^4 + O(11^5), \end{aligned}$$

which gives

$$\begin{aligned}\frac{1}{4}h_{11}(D_1^-, D_2^-) = \frac{1}{4}(&h_{11}((P)-(-P),(-S)-(S))+\\ &h_{11}((P)-(-P),(R)-(-R))+\\ &h_{11}((-Q)-(Q),(R)-(-R))+\\ &h_{11}((-Q)-(-Q),(-S)-(S)))\\ =6\cdot 11^{-1}+7+4\cdot 11&+4\cdot 11^2+3\cdot 11^3+11^4+O(11^5).\end{aligned}$$

Finally, we have

$$\begin{aligned}h_{11}(D_1, D_2) &= \frac{1}{4}h_{11}(D_1^+, D_2^+) + \frac{1}{4}h_{11}(D_1^-, D_2^-)\\ &= 6\cdot 11^{-1}+7+6\cdot 11+2\cdot 11^2+4\cdot 11^4+O(11^5).\end{aligned}$$

8.7.2 Local heights: genus 2, anti-symmetric divisors

Keeping notation as in Subsection 8.7.1, we describe in more detail how to use Algorithm 8.5.8 to compute the local contribution for one of the anti-symmetric divisors:

$$h_{11}((P)-(-P),(R)-(-R)).$$

For ease of notation, let us call these divisors

$$D_P = (P)-(-P), \quad D_R = (R)-(-R).$$

With respect to the standard basis $\mathcal{B}$, the cup product matrix is

$$N = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & -\frac{23}{3} \\ -\frac{1}{3} & 0 & \frac{23}{3} & 0 \end{pmatrix}.$$

Let ν_P be a differential with residue divisor D_P: we can take $\nu_P = \frac{24dx}{y(x+4)}$. We compute $\Psi(\nu_P)$ with respect to the basis $\{\omega_0, \omega_1, \mathrm{Frob}^n\,\omega_2, \mathrm{Frob}^n\,\omega_3\}$:

$$\Psi(\nu_P) = \begin{pmatrix} 8\cdot 11^{-1}+9+6\cdot 11+3\cdot 11^2+7\cdot 11^3+11^4+O(11^5) \\ 7\cdot 11^{-1}+1+4\cdot 11^2+2\cdot 11^3+8\cdot 11^4+O(11^5) \\ 7+9\cdot 11+7\cdot 11^2+4\cdot 11^4+8\cdot 11^5+O(11^6) \\ 2+2\cdot 11+8\cdot 11^2+6\cdot 11^3+7\cdot 11^4+2\cdot 11^5+O(11^6) \end{pmatrix}.$$

Let η_P denote the holomorphic component of ν_P. The computation above implies that

$$\begin{aligned}\int_{D_R}\eta_P &= (8\cdot 11^{-1}+9+6\cdot 11+3\cdot 11^2+7\cdot 11^3+11^4+O(11^5))\int_{D_R}\omega_0 + \\ &\quad (7\cdot 11^{-1}+1+4\cdot 11^2+2\cdot 11^3+8\cdot 11^4+O(11^5))\int_{D_R}\omega_1 \\ &= 5\cdot 11^{-1}+6+3\cdot 11+11^3+7\cdot 11^4+O(11^5).\end{aligned}$$

To integrate ν_P, we compute several quantities. Noting that $\alpha = \phi^*\nu_P - p\nu_P$ and that the Ψ map is Frobenius equivariant, we have

$$\Psi(\alpha) = \Psi(\phi^*\nu_P - p\nu_P) = \phi^*(\Psi(\nu_P)) - p\Psi(\nu_P).$$

In particular, this makes the computation of $\phi^*(\Psi(\nu_P))$ rather easy, as we have already computed $\Psi(\nu_P)$, and all that is left to do is multiply by the matrix of Frobenius. We find that

$$\Psi(\alpha) = \begin{pmatrix} 6\cdot 11+5\cdot 11^2+2\cdot 11^4+9\cdot 11^5+O(11^6) \\ 2\cdot 11+10\cdot 11^2+8\cdot 11^3+6\cdot 11^4+2\cdot 11^5+O(11^6) \\ 4\cdot 11+6\cdot 11^2+2\cdot 11^3+11^4+9\cdot 11^5+O(11^6) \\ 3\cdot 11+2\cdot 11^2+8\cdot 11^3+2\cdot 11^4+4\cdot 11^5+O(11^6) \end{pmatrix}.$$

We wish β to have residue divisor D_R, so let $\beta = \frac{30dx}{y(x-5)}$. Then

$$\Psi(\alpha)\cup\Psi(\beta) = 6+11^2+9\cdot 11^4+5\cdot 11^5+O(11^6).$$

To compute $\sum \mathrm{Res}(\alpha\int\beta)$, we must sum over all Weierstrass point and poles of α. Recall that within a single residue disc, $\sum_A \mathrm{Res}_A(\alpha) = 0$. Now computing the action of Ψ on this differential is slightly more complicated, since instead of just two non-Weierstrass poles, we have $2p = 2\cdot 11$ non-Weierstrass poles: those points in the residue discs of P and $-P$ with x-coordinate $\zeta_{11}^j(-4)^{1/11}$ (where $j = 0,\ldots,10$). This means we must work over the splitting field $L_{-4} = \mathbb{Q}_{11}(\zeta_{11},(-4)^{1/11})$ of $x^{11}+4$ over $\mathbb{Q}_{11}$ to compute the local symbols. Since each set of pth roots is Galois conjugate, working over L_{-4} yields

$$\sum_j \langle \nu_P,\omega_i\rangle_{P_j} = \mathrm{tr}_{L_{-4}/\mathbb{Q}_{11}}(\langle \nu_P,\omega_i\rangle_{P_1}),$$

where P_j is the point in the residue disc of P with x-coordinate $\zeta_{11}^j(-4)^{1/11}$. We have the following contribution from the disc of P:

$$10\cdot 11+9\cdot 11^2+4\cdot 11^3+3\cdot 11^4+4\cdot 11^5+O(11^6),$$

and the total contribution from non-Weierstrass points is twice this, or

$$9\cdot 11+8\cdot 11^2+9\cdot 11^3+6\cdot 11^4+8\cdot 11^5+O(11^6).$$

Meanwhile, the sum of contributions from all Weierstrass discs is the following:

$$11 + 4 \cdot 11^3 + 6 \cdot 11^4 + 11^5 + O(11^6).$$

We compute the tiny integral

$$\int_R^{\phi(R)} \nu_P = 8 \cdot 11 + 11^2 + 8 \cdot 11^3 + 2 \cdot 11^5 + O(11^6).$$

Putting all of this together, we have

$$h_{11}(D_P, D_R) = 6 \cdot 11^{-1} + 10 + 7 \cdot 11 + 6 \cdot 11^2 + 3 \cdot 11^3 + 7 \cdot 11^4 + O(11^5).$$

As a consistency check, we also compute $h_{11}(D_R, D_P)$. Here we have

$$\int_{D_P} \nu_R = 2 + 11^3 + 10 \cdot 11^4 + 4 \cdot 11^5 + O(11^6)$$

and

$$\int_{D_P} \eta_R = 5 \cdot 11^{-1} + 2 + 3 \cdot 11 + 4 \cdot 11^2 + 8 \cdot 11^3 + 2 \cdot 11^4 + O(11^5),$$

which gives

$$h_{11}(D_R, D_P) = 6 \cdot 11^{-1} + 10 + 7 \cdot 11 + 6 \cdot 11^2 + 3 \cdot 11^3 + 7 \cdot 11^4 + O(11^5),$$

illustrating symmetry of the local height pairing.

8.7.3 Global heights: genus 1

We give an example of our implementation in genus 1, which allows for comparison of global heights via the algorithm of Mazur-Stein-Tate.

Let C be the elliptic curve

$$y^2 = x^3 - 5x,$$

with $Q = (-1, 2), R = (5, 10)$, so that

$$(Q) - (-Q) = (R) - (-R) = \left(\frac{9}{4}, -\frac{3}{8}\right) =: P.$$

We compute the 13-adic height of P:

- Above 13, the local height $h_{13}((Q) - (-Q), (R) - (-R))$ is

$$2 \cdot 13 + 6 \cdot 13^2 + 13^3 + 5 \cdot 13^4 + O(13^5).$$

- Away from 13, the only nontrivial contribution is at 3, which is $2 \log 3$ (by work of Müller).
- So the global 13-adic height is $12 \cdot 13 + 4 \cdot 13^2 + 10 \cdot 13^3 + 9 \cdot 13^4 + O(13^5)$.

We compare this to Harvey's implementation [Har08] of the Mazur-Stein-Tate algorithm in Sage:

```
sage: C = EllipticCurve([-5,0])
sage: f = C.padic_height(13)
sage: f(C(9/4,-3/8)) + O(13^5)
12*13 + 4*13^2 + 10*13^3 + 9*13^4 + O(13^5)
```

8.7.4 Global heights: genus 2

We give an example of a pairing of torsion points on the Jacobian of a curve of genus 2.

Let

$$C : y^2 = x^5 + \frac{33}{16}x^4 + \frac{3}{4}x^3 + \frac{3}{8}x^2 - \frac{1}{4}x + \frac{1}{16}$$

be the example due to Leprévost [Lep95] (as in Example 3.3.4). The divisor $(P)-(Q)$, where $P = (-1,1)$, $Q = (0, \frac{1}{4})$ is torsion of order 29. The curve C has good reduction at $p = 11$, and we compute

$$h_{11}((P)-(Q),(-Q)-(-P)) = 9\cdot 11 + 7\cdot 11^2 + 5\cdot 11^3 + 8\cdot 11^4 + 5\cdot 11^5 + 7\cdot 11^6 + 11^7 + O(11^8).$$

Steffen Müller has computed that the contribution away from $p = 11$ is merely at 2, and the height at 2 is given by

$$\begin{aligned} h_2((P)-(Q),(-Q)-(-P)) &= -\frac{16}{29}\log_{11}(2) \\ &= 2\cdot 11 + 3\cdot 11^2 + 5\cdot 11^3 + 2\cdot 11^4 \\ &\quad + 5\cdot 11^5 + 3\cdot 11^6 + 9\cdot 11^7 + O(11^8). \end{aligned}$$

Indeed, we see that the global 11-adic height is

$$\begin{aligned} \langle (P)-(Q),(-Q)-(-P)\rangle_{11} &= h_2((P)-(Q),(-Q)-(-P)) \\ &\quad + h_{11}((P)-(Q),(-Q)-(-P)) \\ &= O(11^8). \end{aligned}$$

8.8 Future work

Below we discuss some natural questions arising from our work.

8.8.1 Global height pairings

Ultimately, we would like to compute the global height pairing. To do so, we would again require C to be a curve over a number field K with good reduction at each place v dividing p. We would also need a continuous idèle class character $\ell : \mathbb{A}_K^*/K^* \longrightarrow$

$\mathbb{Q}_p$ and a splitting $H^1_{\mathrm{dR}}(C/K_v) = H^{1,0}(C/K_v) \oplus W_v$ for each place v dividing p. Computing the local heights at those primes v away from p and those above p, the global height would then be the sum of all local heights. When $K = \mathbb{Q}$, the recent Ph.D. thesis of Müller [Mül10] addresses these local heights away from p, and putting together our results, we are able to compute global heights, as shown in Section 8.7. It would be quite interesting to extend these computations to number fields.

8.8.2 Optimizations

In another direction, it is also of interest to optimize the present algorithm. Currently, the most expensive step is in computing the Laurent series expansion of α in the various Weierstrass local coordinates to reasonably high precision. As we are just interested in the residue of $\alpha \int \beta$, is there a way to make this faster?

8.8.3 Comparison with the work of Mazur-Stein-Tate

When the curve is elliptic, we are able to compare our computations for the global height pairing with those of [MST06], as in Section 8.7. But it should be interesting to compare the algorithms themselves. We note that we compute the height pairing for divisors with disjoint support. It is obviously possible to compute without this assumption by replacing one divisor by a linearly equivalent one with this property. But it is also possible to extend the method described in [Gro86, §5]. This extended method can be compared directly with the method of [MST06], as the height is just the height pairing of a divisor with itself.

Chapter 9

A p-adic Birch and Swinnerton-Dyer conjecture

In this chapter, we use the algorithms in the previous chapter, coupled with joint work with William Stein to compute p-adic L-series and results of Müller on local p-adic heights (away from p) to produce data for a p-adic Birch and Swinnerton-Dyer conjecture for certain Jacobians of hyperelliptic curves. This conjecture is essentially a higher-dimensional analogue of the Mazur-Tate-Teitelbaum conjecture [MTT86].

We begin by fixing notation. For an abelian variety A over $\mathbb{Q}$, let L be the L-series associated to A, r the analytic rank, $Ш(A)$ the Shafarevich-Tate group, $\Omega(A)$ the real period, $\operatorname{Reg}(A)$ the regulator, c_p the Tamagawa number at p, $A(\mathbb{Q})_{\mathrm{tors}}$ the torsion subgroup of the Mordell-Weil group of rational points $A(\mathbb{Q})$, and $A^\vee$ its dual. Let $J_0(N)$ denote the Jacobian of $X_0(N)$, the modular curve of level N. Throughout, we assume that p is a prime of good ordinary reduction for A and that p is not an anomalous prime.

9.1 Introduction

The Birch and Swinnerton-Dyer (BSD) conjecture gives a precise relationship between several arithmetic invariants of an abelian variety $A/\mathbb{Q}$. As formulated by Tate [Tat95], the conjecture states the following:

Conjecture 9.1.1 (BSD conjecture for abelian varieties). *Let A be an abelian variety over $\mathbb{Q}$. Then*

$$\lim_{s\to 1}(s-1)^{-r}L(A,s) = \frac{\Omega(A)\cdot|Ш(A)|\cdot \operatorname{Reg}(A)\cdot\prod_{p|N} c_p}{|A(\mathbb{Q})_{\mathrm{tors}}||A^\vee(\mathbb{Q})_{\mathrm{tors}}|}.$$

This conjecture relies on two assumptions: that the Shafarevich-Tate group Ш is finite and that the L-series can be analytically continued to $s = 1$. An analytic continuation is known to exist for *modular abelian varieties* over $\mathbb{Q}$, where an abelian variety is said to be modular if it is a quotient of $J_0(N)$ for some level N. We shall thus assume that all abelian varieties discussed here are modular. Moreover, it is often advantageous to consider *optimal quotients*, those quotients of $J_0(N)$ for which the kernel of the quotient map is connected.

In particular, for an elliptic curve $E/\mathbb{Q}$ of rank r, the refined BSD conjecture predicts

Conjecture 9.1.2 (BSD conjecture for elliptic curves). *Let E be an elliptic curve over $\mathbb{Q}$. Then*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E)\cdot|\text{Ш}(E)|\cdot \operatorname{Reg}(E)\cdot\prod_{p|N} c_p}{|E(\mathbb{Q})_{\text{tors}}|^2}.$$

Furthermore, in the case of elliptic curves, Mazur, Tate, and Teitelbaum [MTT86] give a p-adic analogue of this conjecture:

Conjecture 9.1.3 (p-adic BSD conjecture for elliptic curves). *Let E be an elliptic curve over $\mathbb{Q}$ and p a prime of good ordinary reduction. Let $\mathcal{L}_p(E,T)$ be the p-adic L-series associated to E. Then the rank r of E equals* $\operatorname{ord}_T(\mathcal{L}_p(E,T))$ *and*

$$\mathcal{L}_p^*(E,0) = (1-\alpha^{-1})^2\frac{|\text{Ш}(E)|\cdot\operatorname{Reg}_p(E)\cdot\prod_{\ell|N} c_\ell}{|E(\mathbb{Q})_{\text{tors}}|^2(\log(1+p))^r}, \qquad (9.1.1)$$

where $\mathcal{L}_p^*(E,0)$ is the leading coefficient of $\mathcal{L}_p(E,T)$, α is the unit root of $h(x) := x^2 - a_px+p$ (with a_p the Hecke eigenvalue), $(\log(1+p))^r$ *is a normalization factor present for the choice of topological generator for* $1+p\mathbb{Z}_p$, *and* Reg_p *is the p-adic regulator, the determinant of the matrix of p-adic height pairings for a basis of* $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$.

We note in the case of elliptic curves, Conjecture 9.1.2 shares many of the same arithmetic quantities with Conjecture 9.1.3; the main difference is that the regulator and L-series are replaced with their p-adic analogues. Similarly, one might expect that a statement like Conjecture 9.1.1 could be formulated and studied for modular abelian varieties. To look at this from a computational perspective, one would need to give algorithms to compute the analogues of the p-adic regulator and p-adic L-series for modular abelian varieties.

Indeed, it appears that these computations are now feasible in some cases (for example, Jacobians of hyperelliptic curves), and we describe them in greater detail below. Using data produced by these algorithms, we conjecture that an analogue of the p-adic BSD conjecture for modular abelian varieties attached to newforms would be of the following form:

Conjecture 9.1.4. *Let A_f be a modular abelian variety of dimension 2 attached to a newform f and p a prime of good ordinary reduction for A_f. Let K_f be the real quadratic field containing the Hecke eigenvalue a_p. The Mordell-Weil rank of A_f equals* $\operatorname{ord}_T(\mathcal{L}_p(A_f,T))$.

If p is inert in $\mathcal{O}_{K_f}$, then

$$\mathcal{L}_p^*(A_f,0) \doteq (1-\alpha^{-1})^2\cdot(1-\overline{\alpha}^{-1})^2\cdot\frac{|\text{Ш}(A_f)|\cdot\operatorname{Reg}_p(A_f)\cdot\prod_{\ell|N} c_\ell}{|A_f(\mathbb{Q})_{\text{tors}}||A_f^\vee(\mathbb{Q})_{\text{tors}}|(\log(1+p))^r}, \qquad (9.1.2)$$

where $\mathcal{L}_p^*(A_f, 0)$ *is the leading coefficient of the p-adic L-series* $\mathcal{L}_p(A_f, T)$, α *is the unit root,* $\overline{\alpha}$ *its conjugate, and* $\doteq$ *is an equality up to a sign* $c = \pm 1$.

If p splits in $\mathcal{O}_{K_f}$, *then*

$$\mathcal{L}_p^*(A_f, 0) = \mathcal{L}_{\mathfrak{p}_1}^*(A_f, 0)\mathcal{L}_{\mathfrak{p}_2}^*(A_f, 0) \doteq (1-\alpha_1^{-1})^2\cdot(1-\alpha_2{}^{-1})^2\cdot\frac{|\text{Ш}(A_f)|\cdot \mathrm{Reg}_p(A_f)\cdot\prod_{\ell|N} c_\ell}{|A_f(\mathbb{Q})_{\mathrm{tors}}||A_f^\vee(\mathbb{Q})_{\mathrm{tors}}|(\log(1+p))^r},$$

where $p\mathcal{O}_{K_f} = \mathfrak{p}_1\mathfrak{p}_2$, *the* α_i *correspond to the two embeddings of* K_f *into* $\mathbb{Q}_p$, *and* $\doteq$ *is an equality up to a sign* $c = \pm 1$.

9.2 p-adic height pairings and regulators

We take as our list of candidate A_f those appearing in [FpS+01] of rank 2, as these have nontrivial p-adic regulator. Let us recall what is known about computing the quantities appearing on the right side of Equation 9.1.2. As described in [FpS+01], the order of the torsion subgroups and Tamagawa numbers c_p are computable. While no general techniques exist to compute the Shafarevich-Tate group Ш(A_f), for each of the abelian varieties in [FpS+01], the conjectural order of the group is given. conditional on the usual BSD conjecture. It thus remains to compute the p-adic regulator, $\mathrm{Reg}_p(A_f)$.

In Chapter 8, we gave algorithms to compute the local height at p. These results, combined with those of Müller [Mül10], give the first algorithm to compute p-adic regulators of Jacobians of hyperelliptic curves. The strategy is to compute each relevant p-adic height pairing as a sum of local height pairings, which we compute by Coleman integration (at the prime above p) and intersection theory (at primes away from p). We will treat Müller's work as a black box from which we can obtain the relevant local heights as needed.

Definition 9.2.1. Let $D_1, \ldots, D_r$ be a set of generators of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$. The *p-adic regulator* is the determinant of the matrix M whose entries m_{ij} are the global p-adic height pairings

$$m_{ij} := \langle D_i, D_j\rangle_p = \sum_l h_l(D_i, D_j).$$

Remark 9.2.2. There are a few normalizations of p-adic heights throughout the literature. Here is what we have chosen: the local and global heights computed by our algorithms agree with the global heights for elliptic curves computed by Harvey [Har08]. However, to obtain agreement with the Birch and Swinnerton-Dyer conjecture, the p-adic regulator must then be computed as $2^r \det(M)$, where M is the matrix of global p-adic height pairings $\langle D_i, D_j\rangle_p$.

Algorithm 9.2.3 (p-adic regulator of a rank 2 Jacobian J of a hyperelliptic curve C).

Input: Non-Weierstrass points $P, Q, R, S \in C(\mathbb{Q}_p)$ arising from rational points on an integral model of C such that $\{(P)-(Q), (R)-(S)\}$ give a basis for $J(\mathbb{Q})/J(\mathbb{Q})_{tors}$,

p a prime of good ordinary reduction.
Output: The p-adic regulator of J.

1. Using Algorithm 8.5.10, compute the following p-adic local heights at p:
$h_p((P)-(Q),(-Q)-(-P))$, $h_p((R)-(S),(-S)-(-R))$,
$h_p((P)-(Q),(R)-(S)), h_p((R)-(S),(P)-(Q)) = h_p((P)-(Q),(R)-(S))$.

2. Using the methods of [Mül10], compute the sum of p-adic local heights away from p for the pairings of divisors above.

3. Compute the global p-adic heights $\langle\cdot,\cdot\rangle_p = \sum_l h_l(\cdot,\cdot)$ for each of the divisors in Step 2.

4. Take the determinant of the 2×2 matrix whose entries are the global heights in Step 3. For normalization purposes, multiply this determinant by 4. This is the p-adic regulator.

9.3 p-adic L-series

The left side of Equation 9.1.2 concerns the appropriate generalization of p-adic L-series associated to modular abelian varieties attached to newforms. We take as our starting point the algorithm to compute p-adic L-series associated to elliptic curves, as in [SW11]. Suppose A_f is an abelian variety as in [FpS$^+$01]. The key difference is that the modular symbol map now takes values in a real quadratic field K_f instead of just in the field of rational numbers. The p-adic L-series then has coefficients in the completion of K_f at a prime above p.

More precisely, let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be the newform associated to A_f, with coefficients a_i in a real quadratic field K_f. The *plus modular symbol map* is the map

$$\begin{aligned}[] [\,] &: \mathbb{Q} \to K_f \\ r &\mapsto [r] = \frac{2\pi i}{\Omega}\left(\int_r^{i\infty} f(z)dz + \int_{-r}^{i\infty} f(z)dz\right),\end{aligned}$$

up to scaling.

Now consider the polynomial

$$h(x) := x^2 - a_p x + p \in K_f[x]$$

and let $\mathfrak{p} = p\mathcal{O}_{K_f}$. This is where our algorithm diverges from the original: at this point, there are two separate cases to consider, depending on the factorization of $\mathfrak{p}$ into primes.

9.3.1 Inert case

If $\mathfrak{p}$ is inert, let $F = (K_f)_{\mathfrak{p}}$, and consider $h(x) \in F[x]$. Let $\alpha \in F$ be the unit root of h, i.e., the root with $|\alpha|_p = 1$.

Using the plus modular symbol map $[\,]$, define a measure μ on $\mathbb{Z}_p^*$ by

$$\mu(a+p^n\mathbb{Z}_p) = \frac{1}{\alpha^n}\left[\frac{a}{p^n}\right] - \frac{1}{\alpha^{n+1}}\left[\frac{a}{p^{n-1}}\right].$$

Now we can define the p-adic L-function as a function on characters $\chi \in \mathrm{Hom}_{\mathrm{conts}}(\mathbb{Z}_p^*, \mathbb{C}_p^*)$. For a character χ, we have

$$L_p(A_f, \chi) = \int_{\mathbb{Z}_p^*} \chi\, d\mu. \tag{9.3.1}$$

To obtain a Taylor series associated to L_p, we view L_p as a p-adic analytic function on the open unit disk

$$D = \{u \in \mathbb{C}_p : |u-1|_p < 1\},$$

as follows:

- let $\gamma = 1 + p$
- for $u \in D$, let $\psi_u : 1 + p\mathbb{Z}_p \to \mathbb{C}_p^*$ be the continuous character given by sending γ to u
- extend ψ_u to a character $\chi_u : \mathbb{Z}_p^* \to \mathbb{C}_p^*$ by letting $\chi_u(x) = \psi_u\left(\frac{x}{\tau(x)}\right)$, where $\tau(x)$ is the Teichmüller lift of x
- let $L_p(A_f, u) := L_p(A_f, \chi_u)$.

Theorem 9.3.1. *The function $L_p(A_f, u)$ is a p-adic analytic function on D with Taylor series about $u = 1$ in the variable T*

$$\mathcal{L}_p(A_f, T) := L_p(A_f, T+1) \in F[[T]]$$

that converges on $\{z \in \mathbb{C}_p : |z|_p < 1\}$.

Proof. This is a straightforward generalization of [Ste07, Theorem 1.15]. □

To compute the integral (9.3.1), we rewrite it as a "Riemann sum" by summing over residue classes mod p^n. More precisely, for each integer $n \geq 1$, let

$$P_n(T) = \sum_{a=1}^{p-1}\left(\sum_{j=0}^{p^{n-1}-1} \mu\left(\tau(a)(1+p)^j + p^n\mathbb{Z}_p\right)\cdot(1+T)^j\right) \in F[T].$$

Proposition 9.3.2. *We have that the p-adic limit of these polynomials is the p-adic L-series:*

$$\lim_{n\to\infty} P_n(T) = \mathcal{L}_p(A_f, T).$$

This convergence is coefficient-by-coefficient, in the sense that if $P_n(T) = \sum_j a_{n,j}T^j$ and $\mathcal{L}_p(A_f, T) = \sum_j a_j T^j$, then

$$\lim_{n\to\infty} a_{n,j} = a_j.$$

Proof. This is a straightforward generalization of [SW11, Proposition 3.1]. □

9.3.2 Split case

If $\mathfrak{p} = \mathfrak{p}_1\mathfrak{p}_2$ splits, let $F_1 = (K_f)_{\mathfrak{p}_1} \simeq \mathbb{Q}_p, F_2 = (K_f)_{\mathfrak{p}_2} \simeq \mathbb{Q}_p$ be the completions at each prime. Consider $h(x) \in F_1[x]$, and let $\alpha_1 \in F_1$ be the unit root; likewise, find the unit root $\alpha_2 \in F_2$.

Now for each unit root α_i, we define a measure μ_i on $\mathbb{Z}_p^*$ by

$$\mu_i(a + p^n\mathbb{Z}_p) = \frac{1}{\alpha_i^n}\left[\frac{a}{p^n}\right] - \frac{1}{\alpha_i^{n+1}}\left[\frac{a}{p^{n-1}}\right].$$

For each integer $n \geq 1$, let

$$P_{i,n}(T) = \sum_{a=1}^{p-1}\left(\sum_{j=0}^{p^{n-1}-1} \mu_i\left(\tau(a)(1+p)^j + p^n\mathbb{Z}_p\right) \cdot (1+T)^j\right) \in F[[T]],$$

where $\tau(a)$ here is the lift of $\tau(a)$ modulo p^n.

Proposition 9.3.3. *We have that the p-adic limit of these polynomials is the p-adic L-series at $\mathfrak{p}_i$:*

$$\lim_{n\to\infty} P_{i,n}(T) = \mathcal{L}_{\mathfrak{p}_i}(A_f, T).$$

The p-adic L-series associated to A_f is then the product

$$\mathcal{L}_{\mathfrak{p}_1}(A_f, T)\mathcal{L}_{\mathfrak{p}_2}(A_f, T).$$

To summarize:

Algorithm 9.3.4 (p-adic L-series).
Input: Good ordinary prime p, A_f modular abelian variety attached to newform f, precision n.
Output: p-adic L-series $\mathcal{L}_p(A_f, T)$.

1. Let $\mathfrak{p} = p\mathcal{O}_K$. If p is inert, let $F := (K_f)_{\mathfrak{p}}$. If p is split, we consider the two copies of $\mathbb{Q}_p$ corresponding to the two primes: $(K_f)_{\mathfrak{p}_1}$ and $(K_f)_{\mathfrak{p}_2}$.

2. If p is inert, compute the unit root $\alpha \in F$; if p is split, compute the two unit roots $\alpha_1, \alpha_2 \in \mathbb{Q}_p$. Note that if p is inert, α is defined over F, where $[F : \mathbb{Q}_p] = 2$. If p is split, we have α_1, α_2 corresponding to the two embeddings of $(K_f)_{\mathfrak{p}_i}$ into $\mathbb{Q}_p$.

3. Define measure(s) $\mu(a \bmod \mathfrak{p}^n)$ or $\mu_i(a \bmod \mathfrak{p}^n), i = 1, 2$.

4. Compute $\mathcal{L}_p(T) := P_n(T)$ as a Riemann sum, using the measure(s) computed in Step 3. If the prime $\mathfrak{p}$ is split, $\mathcal{L}_p$ is a product of two L-functions: $\mathcal{L}_p = \mathcal{L}_{\mathfrak{p}_1}\mathcal{L}_{\mathfrak{p}_2}$.

Remark 9.3.5. Note that this algorithm is exponential in p; see §9.4.3 for a possible enhancement.

9.4 Data for rank 2 Jacobians of genus 2 curves

As we now have algorithms to compute the p-adic regulator and p-adic L-series, we proceed to verify Conjecture 9.1.4 for specific abelian varieties, using BSD data from [FpS+01, Table 2] and local intersection data from [Mül11].

9.4.1 Auxiliary data

Here is a table of the curves and levels. Note that for each curve, the associated abelian variety has Mordell-Weil rank 2.

N	Equation
67	$y^2 + (x^3 + x + 1)y = x^5 - x$
73	$y^2 + (x^3 + x^2 + 1)y = -x^5 - 2x^3 + x$
85	$y^2 + (x^3 + x^2 + x)y = x^4 + x^3 + 3x^2 - 2x + 1$
93	$y^2 + (x^3 + x^2 + 1)y = -2x^5 + x^4 + x^3$
103	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4$
107	$y^2 + (x^3 + x^2 + 1)y = x^4 - x^2 - x - 1$
115	$y^2 + (x^3 + x^+1)y = 2x^3 + x^2 + x$
125,A	$y^2 + (x^3 + x + 1)y = x^5 + 2x^4 + 2x^3 + x^2 - x - 1$
133,B	$y^2 + (x^3 + x^2 + 1)y = -x^5 + x^4 - 2x^3 + 2x^2 - 2x$
147	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + x^3 + x^2 + 1$
161	$y^2 + (x^3 + x + 1)y = x^3 + 4x^2 + 4x + 1$
165	$y^2 + (x^3 + x^2 + x)y = x^5 + 2x^4 + 3x^3 + x^2 - 3x$
167	$y^2 + (x^3 + x + 1)y = -x^5 - x^3 - x^2 - 1$
177	$y^2 + (x^3 + x^2 + 1)y = x^5 + x^4 + x^3$
188	$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$
191	$y^2 + (x^3 + x + 1)y = -x^3 + x^2 + x$

Table 9.4.1: Levels and integral models (Table 1, [FpS+01])

For our algorithms, we take the curves in Table 9.4.1 and do a change of coordinates to obtain the corresponding curves of the form $y^2 = f(x)$. We record these models in Table 9.4.2.

We will also need the following Birch and Swinnerton-Dyer data:

The table below (computed by Müller [Mül11]) provides the data necessary to compute the local heights away from p. The global generators for $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ are given by the pair of points $[[P, Q], [R, S]]$. The intersections list has three entries, namely the intersections needed to compute the global height pairing $([P - Q], [R - S])_p$, those for $([P - Q], [(-Q) - (-P)])_p$ and for $([R - S], [(-S) - (-R)])_p$. The intersections of two divisors D and E are returned as a list of pairs $[l, -i(D, E))_l]$, where l is a prime and $i(D, E)_l$ is the intersection of D and E at l.

Remark 9.4.1. The generators given for $N = 125, A$ are actually generators for an index 2 subgroup of $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$. (An actual set of generators for the full group

N	Equation
67	$y^2 = x^6 + 4x^5 + 2x^4 + 2x^3 + x^2 - 2x + 1$
73	$y^2 = x^6 - 2x^5 + x^4 - 6x^3 + 2x^2 + 4x + 1$
85	$y^2 = x^6 + 2x^5 + 7x^4 + 6x^3 + 13x^2 - 8x + 4$
93	$y^2 = x^6 - 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
103	$y^2 = x^6 + 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$
107	$y^2 = x^6 + 2x^5 + 5x^4 + 2x^3 - 2x^2 - 4x - 3$
115	$y^2 = x^6 + 2x^4 + 10x^3 + 5x^2 + 6x + 1$
125,A	$y^2 = x^6 + 4x^5 + 10x^4 + 10x^3 + 5x^2 - 2x - 3$
133,B	$y^2 = x^6 - 2x^5 + 5x^4 - 6x^3 + 10x^2 - 8x + 1$
147	$y^2 = x^6 + 6x^5 + 11x^4 + 6x^3 + 5x^2 + 4$
161	$y^2 = x^6 + 2x^4 + 6x^3 + 17x^2 + 18x + 5$
165	$y^2 = x^5 + 5x^4 - 168x^3 + 1584x^2 - 10368x + 20736$
167	$y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$
177	$y^2 = x^6 + 6x^5 + 5x^4 + 6x^3 + 2x^2 + 1$
188	$y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$
191	$y^2 = x^6 + 2x^4 - 2x^3 + 5x^2 + 6x + 1$

Table 9.4.2: Levels and $y^2 = f(x)$ models

N	c_p's	$\mid J(\mathbb{Q})_{\text{tors}} \mid$	Ш ?
67	1	1	1
73	1	1	1
85	4,2	2	1
93	4,1	1	1
103	1	1	1
107	1	1	1
115	4,1	1	1
125,A	1	1	1
133,B	1,1	1	1
147	2,2	2	1
161	4,1	1	1
165	4,2,2	4	1
167	1	1	1
177	1,1	1	1
188	9,1	1	1
191	1	1	1

Table 9.4.3: BSD data for rank 2 Jacobians of genus 2 curves (Table 2, [FpS$^+$01])

$J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$ whose support solely consisted of non-Weierstrass points was not readily available.)

N	global generators for $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$	intersections $[[p, i_p]]$
67	$[[-1,0,1],[1,-1,0]],[[0,-1,1],[1,0,0]]$	$[],[],[]$
73	$[[-1,-2,1],[1,-1,0]],[[0,-1,1],[1,0,0]]$	$[],[[3,1]],[]$
85	$[[-1,-2,1],[1,-1,0]],[[1,-4,1],[1,0,0]]$	$[[2,-1]],[[5,\frac{1}{2}]],[[5,\frac{1}{2}]]$
93	$[[-1,-2,1],[1,-1,0]],[[1,-3,1],[1,0,0]]$	$[],[[3,\frac{1}{2}]],[[3,\frac{1}{2}]]$
103	$[[-1,-1,1],[1,-1,0]],[[0,-1,1],[1,0,0]]$	$[],[],[]$
107	$[[-1,-1,1],[1,-1,0]],[[1,-2,1],[1,0,0]]$	$[],[],[]$
115	$[[1,-4,1],[1,-1,0]],[[-2,2,1],[1,0,0]]$	$[[3,-1]],[[5,\frac{1}{2}]],[[5,\frac{1}{2}]]$
125,A	$[[-1,0,1],[1,-1,0]],[[1,-4,1],[1,0,0]]$	$[[2,-1]],[],[[5,1]]$
133,B	$[[0,-1,1],[1,-1,0]],[[1,-2,1],[1,0,0]]$	$[],[],[]$
147	$[[-1,-1,1],[1,-1,0]],[[-3,7,1],[1,0,0]]$	$[[2,-1]],[[3,\frac{1}{2}]],[[7,\frac{1}{2}]]$
161	$[[1,-5,1],[1,-1,0]],[[1,-24,2],[1,0,0]]$	$[],[[7,\frac{1}{2}]],[[5,1],[7,\frac{1}{2}]]$
165	$[[-8,-528,1],[0,-144,1]],[[8,80,1],[0,144,1]]$	$[[2,2],[3,-\frac{1}{2}]],$ $[[2,-2],[11,\frac{1}{2}],[3,\frac{3}{2}]],$ $[[2,-2],[5,\frac{1}{2}],[3,\frac{1}{2}]]$
167	No data (no generators supported on $\mathbb{Q}$)	
177	$[[0,0,1],[1,-1,0]],[[-2,-7,3],[1,0,0]]$	$[[3,1]],[],[[3,-2],[17,1]]$
188	$[[0,1,1],[1,-1,1]],[[-1,-1,1],[2,5,1]]$	$[[1,2]],[[\frac{2}{3},2]],[[\frac{2}{3},2],[1,5]]$
191	$[[0,-1,1],[1,-1,0]],[[-2,10,1],[1,0,0]]$	$[],[],[[11,1]]$

Table 9.4.4: Global generators and intersection data (computed by Steffen Müller)

9.4.2 Evidence for Conjecture 9.1.4

Theorem 9.4.2. *Conjecture 9.1.4 is satisfied for all N in Table 9.4.1 at all good ordinary $p < 100$ satisfying the hypotheses of our algorithms.*

The tables below show the specific primes p and precision $O(p^n)$ for each level N at which Conjecture 9.1.4 is satisfied.

Remark 9.4.3. A note on our models and choices of primes. Since our p-adic heights algorithm requires that the curve be given by an odd degree model, for each curve $y^2 = g(x)$ above, we consider those good ordinary primes p for which $g(x)$ has a $\mathbb{Q}_p$-rational zero and do another change of coordinates to obtain the odd model $y^2 = f(x), f(x) \in \mathbb{Q}_p[x]$. We compute the p-adic regulators and p-adic L-values for these primes.

To clarify Remark 9.4.3, for example, for $N = 67, p = 7$, we work with the model

$$\begin{aligned} y^2 = {} & \left(1 + O(7^{10})\right) x^5 \\ & + \left(2 + 2\cdot 7 + 6\cdot 7^2 + 7^3 + 3\cdot 7^4 + 6\cdot 7^5 + 3\cdot 7^7 + 5\cdot 7^8 + 7^9 + O(7^{10})\right) x^4 \\ & + \left(6 + 7 + 2\cdot 7^2 + 6\cdot 7^3 + 2\cdot 7^4 + 3\cdot 7^5 + 7^6 + 4\cdot 7^7 + 3\cdot 7^8 + 2\cdot 7^9 + O(7^{10})\right) x^3 \\ & + \left(4\cdot 7 + 4\cdot 7^2 + 6\cdot 7^3 + 6\cdot 7^4 + 6\cdot 7^5 + 7^6 + 7^7 + 2\cdot 7^8 + 3\cdot 7^9 + O(7^{10})\right) x^2 \\ & + \left(6\cdot 7 + 3\cdot 7^2 + 6\cdot 7^3 + 5\cdot 7^4 + 5\cdot 7^5 + 7^6 + 4\cdot 7^7 + 4\cdot 7^8 + 3\cdot 7^9 + O(7^{11})\right) x \\ & + 1 + 3\cdot 7 + 5\cdot 7^2 + 6\cdot 7^3 + 3\cdot 7^5 + 7^6 + 4\cdot 7^7 + 2\cdot 7^8 + O(7^{10}) \end{aligned}$$

and the points

$$\begin{aligned}
P &= (O(7^{10}), 1 + 5 \cdot 7 + 5 \cdot 7^3 + 6 \cdot 7^4 + 2 \cdot 7^5 + 7^6 + 5 \cdot 7^7 + 5 \cdot 7^8 + 5 \cdot 7^9 + O(7^{10})), \\
Q &= (3 + 6 \cdot 7 + 4 \cdot 7^2 + 7^3 + 2 \cdot 7^5 + 7^6 + 7^7 + 6 \cdot 7^8 + 5 \cdot 7^9 + O(7^{10}), \\
&\quad 1 + 3 \cdot 7 + 2 \cdot 7^2 + 5 \cdot 7^3 + 3 \cdot 7^4 + 5 \cdot 7^6 + 6 \cdot 7^7 + 7^9 + O(7^{10})) \\
R &= (O(7^{10}), 6 + 7 + 6 \cdot 7^2 + 7^3 + 4 \cdot 7^5 + 5 \cdot 7^6 + 7^7 + 7^8 + 7^9 + O(7^{10}) \\
S &= (2 + 5 \cdot 7 + 2 \cdot 7^2 + 5 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + 5 \cdot 7^6 + 2 \cdot 7^7 + 7^8 + 3 \cdot 7^9 + O(7^{10}), \\
&\quad 6 + 4 \cdot 7^3 + 4 \cdot 7^4 + 3 \cdot 7^5 + 4 \cdot 7^7 + 5 \cdot 7^8 + 5 \cdot 7^9 + O(7^{10}))
\end{aligned}$$

As these models and points are cumbersome, we omit them for the remaining primes. For each N, p for which we have data, we provide the corresponding α and $\epsilon = (1 - \alpha^{-1})^2$ factors in Appendix A.

$N = 67$

For $N = 67, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
7	$6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^4 + 5 \cdot 7^5 + 2 \cdot 7^6 + 4 \cdot 7^7 + O(7^8)$
13	$7 \cdot 13^2 + 7 \cdot 13^3 + 3 \cdot 13^4 + 4 \cdot 13^5 + 10 \cdot 13^6 + 2 \cdot 13^7 + O(13^8)$
17	$10 \cdot 17^2 + 2 \cdot 17^3 + 9 \cdot 17^4 + 9 \cdot 17^5 + 8 \cdot 17^6 + 11 \cdot 17^7 + O(17^8)$
19	$14 \cdot 19^2 + 13 \cdot 19^3 + 17 \cdot 19^4 + 4 \cdot 19^5 + 14 \cdot 19^6 + 8 \cdot 19^7 + O(19^8)$
37	$13 \cdot 37^2 + 35 \cdot 37^3 + 22 \cdot 37^4 + 28 \cdot 37^5 + 17 \cdot 37^6 + 14 \cdot 37^7 + 7 \cdot 37^8 + O(37^9)$
41	$27 \cdot 41^2 + 41^3 + 2 \cdot 41^4 + 15 \cdot 41^5 + 17 \cdot 41^6 + 27 \cdot 41^7 + 18 \cdot 41^8 + O(41^9)$
43	$20 \cdot 43^2 + 33 \cdot 43^3 + 16 \cdot 43^4 + 16 \cdot 43^5 + 27 \cdot 43^6 + 13 \cdot 43^7 + 36 \cdot 43^8 + O(43^9)$
47	$46 \cdot 47^2 + 44 \cdot 47^3 + 45 \cdot 47^4 + 18 \cdot 47^5 + 34 \cdot 47^6 + 18 \cdot 47^7 + 43 \cdot 47^8 + O(47^9)$
59	$24 \cdot 59^2 + 19 \cdot 59^3 + 44 \cdot 59^4 + 22 \cdot 59^5 + 52 \cdot 59^6 + 37 \cdot 59^7 + 21 \cdot 59^8 + O(59^9)$
61	$55 \cdot 61^2 + 10 \cdot 61^3 + 3 \cdot 61^4 + 52 \cdot 61^5 + 46 \cdot 61^6 + 12 \cdot 61^7 + 4 \cdot 61^8 + O(61^9)$
73	$20 \cdot 73^2 + 27 \cdot 73^3 + 24 \cdot 73^4 + 2 \cdot 73^5 + 49 \cdot 73^6 + 18 \cdot 73^7 + 45 \cdot 73^8 + O(73^9)$
79	$8 \cdot 79^2 + 25 \cdot 79^3 + 79^4 + 41 \cdot 79^5 + 57 \cdot 79^6 + 36 \cdot 79^7 + 24 \cdot 79^8 + O(79^9)$
83	$82 \cdot 83^2 + 3 \cdot 83^3 + 80 \cdot 83^4 + 43 \cdot 83^5 + 7 \cdot 83^6 + 7 \cdot 83^7 + 31 \cdot 83^8 + O(83^9)$

Table 9.4.5: p-adic regulators, $N = 67$

Here are values of the special value of the p-adic L-series for various p:

p	p-adic special value
7	$5 + 5 \cdot 7 + 6 \cdot 7^3 + O(7^4)$
13	$8 + 10 \cdot 13^2 + 10 \cdot 13^3 + O(13^4)$
17	$14 + 17 + 13 \cdot 17^2 + 3 \cdot 17^3 + O(17^4)$
19	$14 + 12 \cdot 19 + 19^2 + 7 \cdot 19^3 + O(19^4)$
37	$35 + 30 \cdot 37 + 9 \cdot 37^2 + O(37^3)$
41	$19 + 4 \cdot 41 + 13 \cdot 41^2 + O(41^3)$
43	$32 + 32 \cdot 43 + 5 \cdot 43^2 + O(43^3)$
47	$38 + 40 \cdot 47 + 16 \cdot 47^2 + O(47^3)$
59	$52 + 45 \cdot 59 + O(59^2)$
61	$43 + 58 \cdot 61 + O(61^2)$
73	$34 + 25 \cdot 73 + O(73^2)$
79	$73 + 74 \cdot 79 + O(79^2)$
83	$35 + 57 \cdot 83 + O(83^2)$

Table 9.4.6: p-adic special values, $N = 67$

$N = 73$

For $N = 73, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
11	$11^2 + 5 \cdot 11^3 + 6 \cdot 11^4 + 7 \cdot 11^5 + 6 \cdot 11^6 + O(11^8)$
13	$8 \cdot 13^2 + 13^3 + 4 \cdot 13^4 + 3 \cdot 13^5 + 10 \cdot 13^6 + 4 \cdot 13^7 + O(13^8)$
23	$7 \cdot 23^2 + 9 \cdot 23^3 + 13 \cdot 23^4 + 17 \cdot 23^5 + 2 \cdot 23^6 + 14 \cdot 23^7 + O(23^8)$
31	$4 \cdot 31^3 + 21 \cdot 31^4 + 22 \cdot 31^5 + 13 \cdot 31^6 + 18 \cdot 31^7 + O(31^8)$
41	$31 \cdot 41^2 + 10 \cdot 41^3 + 32 \cdot 41^4 + 30 \cdot 41^5 + 14 \cdot 41^6 + 29 \cdot 41^7 + O(41^8)$
59	$12 \cdot 59^2 + 58 \cdot 59^3 + 59^4 + 19 \cdot 59^5 + 21 \cdot 59^6 + 2 \cdot 59^7 + O(59^8)$
61	$15 \cdot 61^2 + 32 \cdot 61^3 + 50 \cdot 61^4 + 30 \cdot 61^5 + 52 \cdot 61^6 + 28 \cdot 61^7 + O(61^8)$
71	$2 \cdot 71^2 + 26 \cdot 71^3 + 68 \cdot 71^4 + 44 \cdot 71^5 + 50 \cdot 71^6 + 48 \cdot 71^7 + O(71^8)$
83	$42 \cdot 83^2 + 10 \cdot 83^3 + 77 \cdot 83^5 + 71 \cdot 83^6 + 3 \cdot 83^7 + O(83^8)$
97	$57 \cdot 97^2 + 43 \cdot 97^3 + 45 \cdot 97^4 + 15 \cdot 97^5 + 13 \cdot 97^6 + 44 \cdot 97^7 + O(97^8)$

Table 9.4.7: p-adic regulators, $N = 73$

Here are values of the special value of the L-series for various p:

p	p-adic special value
11	$3 + 6 \cdot 11 + 8 \cdot 11^2 + 10 \cdot 11^3 + 7 \cdot 11^4 + O(11^5)$
13	$8 + 12 \cdot 13^2 + 12 \cdot 13^3 + O(13^4)$
23	$10 + 5 \cdot 23 + 10 \cdot 23^2 + 19 \cdot 23^3 + O(23^4)$
31	$25 \cdot 31 + 19 \cdot 31^2 + O(31^3)$
41	$33 + 38 \cdot 41 + 10 \cdot 41^2 + O(41^3)$
59	$9 + 20 \cdot 59 + O(59^2)$
61	$9 + 36 \cdot 61 + O(61^2)$
71	$16 + 16 \cdot 71 + O(71^2)$
83	$56 + 53 \cdot 83 + O(83^2)$
97	$78 + 16 \cdot 97 + O(97^2)$

Table 9.4.8: p-adic special values, $N = 73$

$N = 85$

For $N = 85, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
37	$15 \cdot 37^2 + 14 \cdot 37^3 + 35 \cdot 37^4 + 18 \cdot 37^5 + 28 \cdot 37^6 + 5 \cdot 37^7 + O(37^8)$
41	$28 \cdot 41^2 + 40 \cdot 41^3 + 31 \cdot 41^4 + 35 \cdot 41^5 + 2 \cdot 41^6 + 17 \cdot 41^7 + O(41^8)$
53	$42 \cdot 53^2 + 41 \cdot 53^3 + 26 \cdot 53^4 + 26 \cdot 53^5 + 27 \cdot 53^6 + 30 \cdot 53^7 + O(53^8)$
61	$8 \cdot 61^2 + 42 \cdot 61^3 + 20 \cdot 61^4 + 23 \cdot 61^5 + O(61^6)$
73	$7 \cdot 73^2 + 20 \cdot 73^3 + 42 \cdot 73^4 + 27 \cdot 73^5 + 17 \cdot 73^6 + 43 \cdot 73^7 + O(73^8)$
89	$15 \cdot 89^2 + 27 \cdot 89^3 + 5 \cdot 89^4 + 8 \cdot 89^5 + 58 \cdot 89^6 + 86 \cdot 89^7 + O(89^8)$
97	$57 \cdot 97^2 + 21 \cdot 97^3 + 13 \cdot 97^4 + 22 \cdot 97^5 + 81 \cdot 97^6 + 60 \cdot 97^7 + O(97^8)$

Table 9.4.9: p-adic regulators, $N = 85$

Here are values of the special value of the L-series for various p:

p	p-adic special value
13	$8 + 11 \cdot 13 + 5 \cdot 13^2 + 9 \cdot 13^3 + O(13^4)$
29	$11 + 18 \cdot 29^2 + O(29^3)$
37	$33 + 17 \cdot 37 + 37^2 + O(37^3)$
41	$17 + 14 \cdot 41 + 22 \cdot 41^2 + O(41^3)$
53	$32 + 16 \cdot 53 + O(53^2)$
61	$47 + 10 \cdot 61 + O(61^2)$
73	$10 + 9 \cdot 73 + O(73^2)$
89	$58 + 42 \cdot 89 + O(89^2)$
97	$45 + 70 \cdot 97 + O(97^2)$

Table 9.4.10: p-adic special values, $N = 85$

$N = 93$

For $N = 93$, $c = -1$.

We obtain the following p-adic regulators:

p	p-adic regulator
11	$6 + 2 \cdot 11 + 11^2 + 6 \cdot 11^3 + 2 \cdot 11^4 + 4 \cdot 11^5 + 11^6 + 5 \cdot 11^7 + O(11^8)$
13	$12 \cdot 13^2 + 4 \cdot 13^3 + 4 \cdot 13^4 + 11 \cdot 13^6 + 12 \cdot 13^7 + O(13^8)$
23	$20 \cdot 23^2 + 4 \cdot 23^3 + 13 \cdot 23^4 + 18 \cdot 23^5 + 12 \cdot 23^6 + 5 \cdot 23^7 + O(23^8)$
29	$17 \cdot 29^2 + 5 \cdot 29^3 + 3 \cdot 29^4 + 23 \cdot 29^5 + 2 \cdot 29^6 + 20 \cdot 29^7 + O(29^8)$
37	$25 \cdot 37^2 + 13 \cdot 37^3 + 23 \cdot 37^4 + 6 \cdot 37^5 + 27 \cdot 37^6 + 33 \cdot 37^7 + O(37^8)$
43	$24 \cdot 43^2 + 42 \cdot 43^3 + 18 \cdot 43^4 + 40 \cdot 43^5 + 14 \cdot 43^6 + 35 \cdot 43^7 + O(43^8)$
47	$25 \cdot 47^2 + 44 \cdot 47^3 + 11 \cdot 47^4 + 11 \cdot 47^5 + 39 \cdot 47^6 + 38 \cdot 47^7 + O(47^8)$
53	$19 \cdot 53^2 + 30 \cdot 53^3 + 9 \cdot 53^4 + 15 \cdot 53^5 + 47 \cdot 53^6 + 16 \cdot 53^7 + O(53^8)$
61	$60 \cdot 61^2 + 25 \cdot 61^3 + 12 \cdot 61^4 + 52 \cdot 61^5 + 5 \cdot 61^6 + 60 \cdot 61^7 + O(61^8)$
67	$66 \cdot 67^2 + 49 \cdot 67^3 + 19 \cdot 67^4 + 27 \cdot 67^5 + 23 \cdot 67^6 + 50 \cdot 67^7 + O(67^8)$
73	$38 \cdot 73^2 + 11 \cdot 73^3 + 6 \cdot 73^4 + 3 \cdot 73^5 + 55 \cdot 73^6 + 9 \cdot 73^7 + O(73^8)$
79	$52 \cdot 79^2 + 48 \cdot 79^3 + 8 \cdot 79^4 + 13 \cdot 79^5 + 29 \cdot 79^6 + 51 \cdot 79^7 + O(79^8)$
83	$7 \cdot 83^2 + 58 \cdot 83^3 + 45 \cdot 83^4 + 32 \cdot 83^5 + 42 \cdot 83^6 + 79 \cdot 83^7 + O(83^8)$
89	$61 \cdot 89^2 + 57 \cdot 89^3 + 19 \cdot 89^4 + 74 \cdot 89^5 + 72 \cdot 89^6 + 8 \cdot 89^7 + O(89^8)$

Table 9.4.11: p-adic regulators, $N = 93$

Here are values of the special value of the L-series for various p:

p	p-adic special value
11	$5 + 3 \cdot 11^2 + 8 \cdot 11^3 + O(11^4)$
13	$10 + 5 \cdot 13 + 13^2 + 13^3 + O(13^4)$
23	$13 + 20 \cdot 23^2 + 11 \cdot 23^3 + O(23^4)$
29	$17 + 19 \cdot 29 + 28 \cdot 29^2 + O(29^3)$
37	$34 + 26 \cdot 37 + 29 \cdot 37^2 + O(37^3)$
43	$3 + 7 \cdot 43^2 + O(43^3)$
47	$11 + 23 \cdot 47 + 15 \cdot 47^2 + O(47^3)$
53	$30 + 28 \cdot 53 + 11 \cdot 53^2 + O(53^3)$
61	$3 + 58 \cdot 61 + O(61^2)$
67	$49 + 15 \cdot 67 + O(67^2)$
73	$18 + 46 \cdot 73 + O(73^2)$
79	$7 + 14 \cdot 79 + O(79^2)$
83	$2 + 34 \cdot 83 + O(83^2)$
89	$62 + 43 \cdot 89 + O(89^2)$

Table 9.4.12: p-adic special values, $N = 93$

$N = 103$

For $N = 103$, $c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
11	$4 \cdot 11^2 + 4 \cdot 11^3 + 4 \cdot 11^4 + 8 \cdot 11^5 + 2 \cdot 11^6 + 8 \cdot 11^7 + O(11^8)$
13	$3 \cdot 13^2 + 13^3 + 2 \cdot 13^4 + 5 \cdot 13^5 + 2 \cdot 13^6 + 5 \cdot 13^7 + O(13^8)$
19	$8 \cdot 19^2 + 13 \cdot 19^3 + 3 \cdot 19^4 + 14 \cdot 19^5 + 11 \cdot 19^7 + O(19^8)$
23	$14 \cdot 23^2 + 12 \cdot 23^3 + 21 \cdot 23^4 + 4 \cdot 23^5 + 18 \cdot 23^6 + 8 \cdot 23^7 + O(23^8)$
29	$22 \cdot 29^2 + 5 \cdot 29^3 + 22 \cdot 29^4 + 3 \cdot 29^5 + 7 \cdot 29^6 + 29^7 + O(29^8)$
41	$7 \cdot 41^2 + 34 \cdot 41^3 + 17 \cdot 41^4 + 17 \cdot 41^5 + 26 \cdot 41^6 + 16 \cdot 41^7 + O(41^8)$
47	$7 \cdot 47^2 + 16 \cdot 47^3 + 47^4 + 12 \cdot 47^5 + 13 \cdot 47^6 + 44 \cdot 47^7 + O(47^8)$
53	$16 \cdot 53^2 + 15 \cdot 53^3 + 50 \cdot 53^4 + 22 \cdot 53^5 + 9 \cdot 53^6 + 32 \cdot 53^7 + O(53^8)$
59	$8 \cdot 59^2 + 4 \cdot 59^3 + 33 \cdot 59^4 + 27 \cdot 59^5 + 39 \cdot 59^6 + 30 \cdot 59^7 + O(59^8)$
61	$14 \cdot 61^3 + 18 \cdot 61^4 + 2 \cdot 61^5 + 47 \cdot 61^7 + O(61^8)$
71	$12 \cdot 71^2 + 45 \cdot 71^3 + 18 \cdot 71^4 + 34 \cdot 71^5 + 3 \cdot 71^6 + 63 \cdot 71^7 + O(71^8)$
73	$66 \cdot 73^2 + 48 \cdot 73^3 + 22 \cdot 73^4 + 49 \cdot 73^5 + 68 \cdot 73^6 + 16 \cdot 73^7 + O(73^8)$
79	$72 \cdot 79^2 + 49 \cdot 79^3 + 63 \cdot 79^4 + 14 \cdot 79^5 + 16 \cdot 79^6 + 59 \cdot 79^7 + O(79^8)$
83	$74 \cdot 83^2 + 32 \cdot 83^3 + 35 \cdot 83^4 + 55 \cdot 83^5 + 82 \cdot 83^6 + 75 \cdot 83^7 + O(83^8)$
89	$30 \cdot 89^2 + 62 \cdot 89^3 + 31 \cdot 89^4 + 88 \cdot 89^5 + 20 \cdot 89^6 + 42 \cdot 89^7 + O(89^8)$
97	$95 \cdot 97^2 + 51 \cdot 97^3 + 28 \cdot 97^4 + 12 \cdot 97^5 + 78 \cdot 97^6 + 62 \cdot 97^7 + O(97^8)$

Table 9.4.13: p-adic regulators, $N = 103$

Here are values of the special value of the L-series for various p:

p	p-adic special value
11	$1 + 10 \cdot 11 + 3 \cdot 11^2 + 6 \cdot 11^3 + O(11^5)$
13	$12 + 11 \cdot 13 + 5 \cdot 13^2 + 5 \cdot 13^3 + O(13^4)$
19	$13 + 9 \cdot 19 + 18 \cdot 19^2 + 10 \cdot 19^4 + O(19^5)$
23	$7 + 19 \cdot 23 + 13 \cdot 23^2 + 13 \cdot 23^3 + O(23^4)$
29	$25 + 5 \cdot 29 + 24 \cdot 29^2 + O(29^3)$
41	$26 + 10 \cdot 41 + 31 \cdot 41^2 + O(41^3)$
47	$18 + 31 \cdot 47 + O(47^2)$
53	$47 + 36 \cdot 53 + O(53^2)$
59	$44 + 48 \cdot 59 + O(59^2)$
61	$13 \cdot 61 + O(61^2)$
71	$36 + 13 \cdot 71 + O(71^2)$
73	$30 + 39 \cdot 73 + O(73^2)$
79	$20 + 57 \cdot 79 + O(79^2)$
83	$8 + 80 \cdot 83 + O(83^2)$
89	$35 + 5 \cdot 89 + O(89^2)$
97	$70 + 50 \cdot 97 + O(97^2)$

Table 9.4.14: p-adic special values, $N = 103$

$N = 107$

For $N = 107$, $c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
13	$2 \cdot 13^2 + 4 \cdot 13^3 + 9 \cdot 13^4 + 11 \cdot 13^5 + 4 \cdot 13^6 + 6 \cdot 13^7 + O(13^8)$
17	$17^2 + 9 \cdot 17^3 + 4 \cdot 17^4 + 15 \cdot 17^5 + 5 \cdot 17^6 + 16 \cdot 17^7 + O(17^8)$
19	$3 \cdot 19^2 + 17 \cdot 19^3 + 7 \cdot 19^4 + 13 \cdot 19^5 + 2 \cdot 19^6 + 3 \cdot 19^7 + O(19^8)$
37	$14 \cdot 37^2 + 17 \cdot 37^3 + 5 \cdot 37^4 + 19 \cdot 37^5 + 3 \cdot 37^6 + 20 \cdot 37^7 + O(37^8)$
41	$17 \cdot 41^2 + 24 \cdot 41^3 + 14 \cdot 41^4 + 39 \cdot 41^5 + 35 \cdot 41^7 + O(41^8)$
43	$20 \cdot 43^2 + 14 \cdot 43^4 + 22 \cdot 43^5 + 9 \cdot 43^6 + 29 \cdot 43^7 + O(43^8)$
47	$4 \cdot 47^2 + 25 \cdot 47^3 + 23 \cdot 47^4 + 21 \cdot 47^5 + 43 \cdot 47^6 + 25 \cdot 47^7 + O(47^8)$
59	$59^2 + 41 \cdot 59^3 + 56 \cdot 59^4 + 58 \cdot 59^5 + 59^6 + 48 \cdot 59^7 + O(59^8)$
61	$20 \cdot 61^2 + 36 \cdot 61^3 + 50 \cdot 61^4 + 40 \cdot 61^5 + 41 \cdot 61^6 + 32 \cdot 61^7 + O(61^8)$
67	$49 \cdot 67^2 + 62 \cdot 67^3 + 66 \cdot 67^4 + 4 \cdot 67^5 + 21 \cdot 67^6 + 8 \cdot 67^7 + O(67^8)$
71	$43 \cdot 71^2 + 61 \cdot 71^3 + 34 \cdot 71^4 + 60 \cdot 71^5 + 55 \cdot 71^6 + 32 \cdot 71^7 + O(71^8)$
79	$11 \cdot 79^2 + 46 \cdot 79^3 + 32 \cdot 79^4 + 32 \cdot 79^5 + 51 \cdot 79^6 + 55 \cdot 79^7 + O(79^8)$
83	$64 \cdot 83^2 + 47 \cdot 83^3 + 11 \cdot 83^4 + 57 \cdot 83^5 + 35 \cdot 83^6 + 59 \cdot 83^7 + O(83^8)$

Table 9.4.15: p-adic regulators, $N = 107$

Here are values of the special value of the L-series for various p:

p	p-adic special value
13	$2 + 8 \cdot 13 + 6 \cdot 13^2 + 4 \cdot 13^3 + O(13^4)$
17	$8 + 8 \cdot 17 + 16 \cdot 17^2 + 7 \cdot 17^3 + O(17^4)$
19	$12 + 18 \cdot 19 + 17 \cdot 19^2 + 4 \cdot 19^3 + O(19^4)$
37	$29 + 8 \cdot 37 + O(37^2)$
41	$28 + 34 \cdot 41 + O(41^2)$
43	$39 + 39 \cdot 43 + O(43^2)$
47	$17 + 18 \cdot 47 + O(47^2)$
59	$16 + 44 \cdot 59 + O(59^2)$
61	$45 + 44 \cdot 61 + O(61^2)$
67	$6 + 30 \cdot 67 + O(67^2)$
71	$20 + 57 \cdot 71 + O(71^2)$
79	$11 + 50 \cdot 79 + O(79^2)$
83	$29 + 18 \cdot 83 + O(83^2)$

Table 9.4.16: p-adic special values, $N = 107$

$N = 115$

For $N = 115, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
11	$9 \cdot 11^3 + 7 \cdot 11^4 + 8 \cdot 11^5 + 11^6 + 9 \cdot 11^7 + O(11^8)$
17	$14 \cdot 17^2 + 3 \cdot 17^3 + 14 \cdot 17^4 + 16 \cdot 17^5 + 2 \cdot 17^6 + 8 \cdot 17^7 + O(17^8)$
37	$3 \cdot 37^2 + 11 \cdot 37^3 + 10 \cdot 37^4 + 26 \cdot 37^5 + 24 \cdot 37^6 + 18 \cdot 37^7 + O(37^8)$
43	$38 \cdot 43^2 + 16 \cdot 43^3 + 15 \cdot 43^4 + 21 \cdot 43^5 + 26 \cdot 43^6 + 25 \cdot 43^7 + O(43^8)$
53	$44 \cdot 53^2 + 2 \cdot 53^3 + 46 \cdot 53^4 + 7 \cdot 53^5 + 17 \cdot 53^6 + 35 \cdot 53^7 + O(53^8)$
59	$42 \cdot 59^2 + 47 \cdot 59^3 + 8 \cdot 59^4 + 2 \cdot 59^5 + 37 \cdot 59^6 + 51 \cdot 59^7 + O(59^8)$
61	$38 \cdot 61^2 + 59 \cdot 61^3 + 57 \cdot 61^4 + 29 \cdot 61^5 + 4 \cdot 61^6 + 27 \cdot 61^7 + O(61^8)$
67	$55 \cdot 67^2 + 9 \cdot 67^3 + 18 \cdot 67^4 + 13 \cdot 67^5 + 26 \cdot 67^6 + 10 \cdot 67^7 + O(67^8)$
79	$66 \cdot 79^2 + 56 \cdot 79^3 + 14 \cdot 79^4 + 78 \cdot 79^5 + 77 \cdot 79^6 + 7 \cdot 79^7 + O(79^8)$
83	$64 \cdot 83^2 + 20 \cdot 83^3 + 82 \cdot 83^4 + 26 \cdot 83^5 + 18 \cdot 83^6 + 34 \cdot 83^7 + O(83^8)$
89	$9 \cdot 89^2 + 9 \cdot 89^3 + 28 \cdot 89^4 + 67 \cdot 89^5 + 75 \cdot 89^6 + 65 \cdot 89^7 + O(89^8)$
97	$17 \cdot 97^2 + 54 \cdot 97^3 + 95 \cdot 97^4 + 80 \cdot 97^5 + 66 \cdot 97^6 + 16 \cdot 97^7 + O(97^8)]$

Table 9.4.17: p-adic regulators, $N = 115$

Here are values of the special value of the L-series for various p:

p	p-adic special value
11	$5 \cdot 11 + 11^2 + 4 \cdot 11^3 + 4 \cdot 11^4 + O(11^5)$
17	$10 + 9 \cdot 17 + 15 \cdot 17^2 + 11 \cdot 17^3 + 13 \cdot 17^4 + O(17^5)$
19	$12 + 18 \cdot 19 + 14 \cdot 19^2 + 18 \cdot 19^3 + 13 \cdot 19^4 + O(19^5)$
37	$28 + 23 \cdot 37 + 6 \cdot 37^2 + O(37^3)$
43	$6 + 41 \cdot 43 + O(43^2)$
53	$29 + 6 \cdot 53 + 37 \cdot 53^2 + O(53^3)$
59	$40 + 5 \cdot 59 + O(59^2)$
61	$37 + 53 \cdot 61 + O(61^2)$
67	$37 + 36 \cdot 67 + O(67^2)$
79	$41 + 44 \cdot 79 + O(79^2)$
83	$38 + 4 \cdot 83 + O(83^2)$
89	$10 + 59 \cdot 89 + O(89^2)$
97	$21 + 61 \cdot 97 + O(97^2)$

Table 9.4.18: p-adic special values, $N = 115$

$N = 125, A$

For $N = 125$, we have $c = 1$.

p	p-adic regulator
13	$2 \cdot 13^2 + 6 \cdot 13^4 + 5 \cdot 13^5 + 6 \cdot 13^7 + O(13^8)$
19	$5 \cdot 19^2 + 8 \cdot 19^3 + 14 \cdot 19^4 + 13 \cdot 19^5 + 11 \cdot 19^7 + O(19^8)$
23	$4 \cdot 23^2 + 11 \cdot 23^3 + 5 \cdot 23^4 + 3 \cdot 23^5 + 18 \cdot 23^6 + 10 \cdot 23^7 + O(23^8)$
37	$4 \cdot 37^2 + 35 \cdot 37^3 + 24 \cdot 37^4 + 19 \cdot 37^5 + 31 \cdot 37^6 + 30 \cdot 37^7 + O(37^8)$
47	$45 \cdot 47^2 + 37 \cdot 47^3 + 34 \cdot 47^4 + 16 \cdot 47^5 + 46 \cdot 47^7 + O(47^8)$
53	$24 \cdot 53^2 + 52 \cdot 53^3 + 35 \cdot 53^4 + 28 \cdot 53^5 + 12 \cdot 53^6 + 43 \cdot 53^7 + O(53^8)$
59	$43 \cdot 59^2 + 7 \cdot 59^4 + 34 \cdot 59^5 + 29 \cdot 59^6 + 59^7 + O(59^8)$
61	$15 \cdot 61^2 + 3 \cdot 61^3 + 11 \cdot 61^4 + 8 \cdot 61^5 + 51 \cdot 61^6 + 59 \cdot 61^7 + O(61^8)$
67	$30 \cdot 67^2 + 44 \cdot 67^3 + 16 \cdot 67^4 + 18 \cdot 67^5 + 31 \cdot 67^6 + 26 \cdot 67^7 + O(67^8)$
73	$48 \cdot 73^2 + 45 \cdot 73^3 + 23 \cdot 73^4 + 55 \cdot 73^5 + 10 \cdot 73^6 + 33 \cdot 73^7 + O(73^8)$
83	$68 \cdot 83^2 + 76 \cdot 83^3 + 49 \cdot 83^4 + 39 \cdot 83^5 + 24 \cdot 83^6 + 51 \cdot 83^7 + O(83^8)$
89	$58 \cdot 89^2 + 87 \cdot 89^3 + 26 \cdot 89^4 + 51 \cdot 89^5 + 70 \cdot 89^6 + 77 \cdot 89^7 + O(89^8)$
97	$59 \cdot 97^2 + 48 \cdot 97^3 + 89 \cdot 97^4 + 92 \cdot 97^5 + 33 \cdot 97^6 + 92 \cdot 97^7 + O(97^8)$

Table 9.4.19: p-adic regulators, $N = 125, A$

Here are values of the special value of the L-series for various p:

p	p-adic special value
13	$8 + 9 \cdot 13 + 10 \cdot 13^2 + 6 \cdot 13^3 + O(13^4)$
19	$9 + 6 \cdot 19 + 16 \cdot 19^3 + O(19^4)$
23	$12 + 22 \cdot 23 + 13 \cdot 23^2 + 13 \cdot 23^3 + O(23^4)$
37	$34 + 37 + O(37^2)$
47	$11 + 40 \cdot 47 + O(47^2)$
53	$40 + 13 \cdot 53 + O(53^2)$
59	$54 + 47 \cdot 59 + O(59^2)$
61	$13 + 55 \cdot 61 + O(61^2)$
67	$20 + 21 \cdot 67 + O(67^2)$
73	$4 + 37 \cdot 73 + O(73^2)$
83	$44 + 40 \cdot 83 + O(83^2)$
89	$59 + 58 \cdot 89 + O(89^2)$
97	$63 + 60 \cdot 97 + O(97^2)$

Table 9.4.20: p-adic special values, $N = 125, A$

$N = 133, B$

For $N = 133, c = -1$.

We obtain the following p-adic regulators:

p	p-adic regulator
17	$4 \cdot 17^2 + 17^3 + 8 \cdot 17^4 + 13 \cdot 17^5 + 6 \cdot 17^6 + 10 \cdot 17^7 + O(17^8)$
29	$27 + 5 \cdot 29 + 7 \cdot 29^2 + 16 \cdot 29^3 + 3 \cdot 29^4 + 7 \cdot 29^5 + O(29^6)$
31	$5 \cdot 31^2 + 6 \cdot 31^3 + 3 \cdot 31^4 + 19 \cdot 31^5 + 14 \cdot 31^6 + 10 \cdot 31^7 + O(31^8)$
41	$17 \cdot 41^2 + 4 \cdot 41^3 + 31 \cdot 41^4 + 21 \cdot 41^5 + 38 \cdot 41^6 + 17 \cdot 41^7 + O(41^8)$
43	$12 \cdot 43^2 + 10 \cdot 43^3 + 17 \cdot 43^4 + 37 \cdot 43^5 + 4 \cdot 43^6 + 8 \cdot 43^7 + O(43^8)$
53	$4 \cdot 53^2 + 20 \cdot 53^3 + 51 \cdot 53^4 + 11 \cdot 53^5 + 42 \cdot 53^6 + 30 \cdot 53^7 + O(53^8)$
67	$6 \cdot 67^2 + 19 \cdot 67^3 + 3 \cdot 67^4 + 32 \cdot 67^5 + 18 \cdot 67^6 + 55 \cdot 67^7 + O(67^8)$
73	$22 \cdot 73^2 + 49 \cdot 73^3 + 16 \cdot 73^4 + 36 \cdot 73^5 + 67 \cdot 73^6 + 64 \cdot 73^7 + O(73^8)$
79	$8 \cdot 79^2 + 54 \cdot 79^3 + 21 \cdot 79^4 + 68 \cdot 79^6 + 49 \cdot 79^7 + O(79^8)$
83	$21 \cdot 83^2 + 81 \cdot 83^3 + 32 \cdot 83^4 + 8 \cdot 83^5 + 57 \cdot 83^6 + 49 \cdot 83^7 + O(83^8)$
89	$18 \cdot 89^2 + 36 \cdot 89^3 + 81 \cdot 89^4 + 18 \cdot 89^5 + 89^6 + 79 \cdot 89^7 + O(89^8)$

Table 9.4.21: p-adic regulators, $N = 133, B$

Here are values of the special value of the L-series for various p:

p	p-adic special value
17	$8 + 10 \cdot 17 + 13 \cdot 17^2 + 4 \cdot 17^3 + O(17^4)$
29	$11 + 23 \cdot 29 + 24 \cdot 29^2 + O(29^3)$
31	$21 + 20 \cdot 31 + 20 \cdot 31^2 + O(31^3)$
41	$24 + 14 \cdot 41 + 12 \cdot 41^2 + O(41^3)$
43	$36 + 22 \cdot 43 + 40 \cdot 43^2 + O(43^3)$
53	$28 + 51 \cdot 53 + O(53^2)$
67	$2 + 62 \cdot 67 + O(67^2)$
73	$60 + 27 \cdot 73 + O(73^2)$
79	$47 + 56 \cdot 79 + O(79^2)$
83	$14 + 72 \cdot 83 + O(83^2)$
89	$16 + 50 \cdot 89 + O(89^2)$

Table 9.4.22: p-adic special values, $N = 133, B$

$N = 147$

For $N = 147, c = -1$.

We obtain the following p-adic regulators:

p	p-adic regulator
13	$13^2 + 6 \cdot 13^3 + 8 \cdot 13^4 + 10 \cdot 13^5 + 8 \cdot 13^6 + 13^7 + O(13^8)$
19	$8 \cdot 19^2 + 8 \cdot 19^3 + 19^4 + 7 \cdot 19^5 + 15 \cdot 19^6 + 13 \cdot 19^7 + O(19^8)$
23	$15 + 9 \cdot 23 + 6 \cdot 23^3 + 11 \cdot 23^4 + 12 \cdot 23^5 + O(23^6)$
31	$7 \cdot 31^2 + 23 \cdot 31^3 + 26 \cdot 31^5 + 31^6 + 25 \cdot 31^7 + O(31^8)$
37	$6 \cdot 37^2 + 14 \cdot 37^3 + 32 \cdot 37^4 + 15 \cdot 37^5 + 33 \cdot 37^6 + 15 \cdot 37^7 + O(37^8)$
43	$9 \cdot 43^2 + 17 \cdot 43^3 + 30 \cdot 43^4 + 26 \cdot 43^5 + 24 \cdot 43^6 + 43^7 + O(43^8)$
53	$46 \cdot 53^2 + 47 \cdot 53^3 + 43 \cdot 53^4 + 12 \cdot 53^5 + 51 \cdot 53^6 + 20 \cdot 53^7 + O(53^8)$
61	$20 \cdot 61^2 + 37 \cdot 61^3 + 41 \cdot 61^4 + 50 \cdot 61^5 + 20 \cdot 61^6 + 12 \cdot 61^7 + O(61^8)$
67	$43 \cdot 67^2 + 61 \cdot 67^3 + 39 \cdot 67^4 + 40 \cdot 67^5 + 41 \cdot 67^6 + 32 \cdot 67^7 + O(67^8)$
71	$33 \cdot 71^2 + 61 \cdot 71^3 + 43 \cdot 71^4 + 50 \cdot 71^5 + 51 \cdot 71^6 + 69 \cdot 71^7 + O(71^8)$
73	$53 + 18 \cdot 73 + 6 \cdot 73^2 + 6 \cdot 73^3 + 42 \cdot 73^4 + 14 \cdot 73^5 + 13 \cdot 73^6 + 33 \cdot 73^7 + O(73^8)$
79	$32 \cdot 79^2 + 27 \cdot 79^3 + 4 \cdot 79^4 + 57 \cdot 79^5 + 75 \cdot 79^6 + 57 \cdot 79^7 + O(79^8)$
97	$85 \cdot 97^2 + 2 \cdot 97^3 + 90 \cdot 97^4 + 54 \cdot 97^5 + 54 \cdot 97^6 + 17 \cdot 97^7 + O(97^8)$

Table 9.4.23: p-adic regulators, $N = 147$

Here are values of the special value of the L-series for various p:

p	p-adic special value
13	$4 + 3 \cdot 13 + 6 \cdot 13^2 + 2 \cdot 13^4 + O(13^5)$
19	$1 + 8 \cdot 19 + 13 \cdot 19^2 + 9 \cdot 19^3 + O(19^4)$
23	$8 + 21 \cdot 23 + 15 \cdot 23^2 + 21 \cdot 23^3 + O(23^4)$
31	$12 + 10 \cdot 31 + 31^2 + O(31^3)$
37	$29 + 7 \cdot 37 + O(37^3)$
43	$33 + 26 \cdot 43 + O(43^2)$
53	$52 + 6 \cdot 53 + O(53^2)$
61	$1 + O(61^2)$
67	$22 + 13 \cdot 67 + O(67^2)$
71	$2 + 61 \cdot 71 + O(71^2)$
73	$20 + 41 \cdot 73 + O(73^2)$
79	$28 + 28 \cdot 79 + O(79^2)$
97	$70 + 25 \cdot 97 + O(97^2)$

Table 9.4.24: p-adic special values, $N = 147$

$N = 161$

For $N = 161, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
11	$7 \cdot 11^2 + 3 \cdot 11^4 + 2 \cdot 11^5 + 3 \cdot 11^6 + 2 \cdot 11^7 + O(11^8)$
19	$12 \cdot 19^2 + 13 \cdot 19^3 + 8 \cdot 19^4 + 16 \cdot 19^5 + 11 \cdot 19^6 + 17 \cdot 19^7 + O(19^8)$
37	$35 \cdot 37^2 + 30 \cdot 37^3 + 18 \cdot 37^4 + 32 \cdot 37^5 + 15 \cdot 37^6 + 15 \cdot 37^7 + O(37^8)$
43	$22 \cdot 43^2 + 3 \cdot 43^3 + 38 \cdot 43^4 + 29 \cdot 43^5 + 26 \cdot 43^6 + 27 \cdot 43^7 + O(43^8)$
53	$51 \cdot 53^2 + 25 \cdot 53^3 + 11 \cdot 53^4 + 27 \cdot 53^5 + 26 \cdot 53^6 + 6 \cdot 53^7 + O(53^8)$
59	$2 \cdot 59^2 + 37 \cdot 59^3 + 21 \cdot 59^4 + 10 \cdot 59^5 + 31 \cdot 59^6 + 54 \cdot 59^7 + O(59^8)$
61	$24 \cdot 61^2 + 57 \cdot 61^3 + 19 \cdot 61^4 + 48 \cdot 61^5 + 15 \cdot 61^6 + 61^7 + O(61^8)$
67	$40 \cdot 67^2 + 62 \cdot 67^3 + 4 \cdot 67^4 + 2 \cdot 67^5 + 53 \cdot 67^6 + 61 \cdot 67^7 + O(67^8)$
79	$79^2 + 68 \cdot 79^3 + 55 \cdot 79^4 + 37 \cdot 79^5 + 50 \cdot 79^6 + 77 \cdot 79^7 + O(79^8)$
83	$26 \cdot 83^2 + 48 \cdot 83^3 + 16 \cdot 83^4 + 53 \cdot 83^5 + 58 \cdot 83^6 + 19 \cdot 83^7 + O(83^8)$
89	$86 \cdot 89^2 + 67 \cdot 89^3 + 77 \cdot 89^4 + 12 \cdot 89^5 + 81 \cdot 89^6 + 9 \cdot 89^7 + O(89^8)$
97	$66 \cdot 97^2 + 58 \cdot 97^3 + 17 \cdot 97^4 + 71 \cdot 97^5 + 28 \cdot 97^6 + 26 \cdot 97^7 + O(97^8)$

Table 9.4.25: p-adic regulators, $N = 161$

Here are values of the special value of the L-series for various p:

p	p-adic special value
11	$8 + 2 \cdot 11 + 2 \cdot 11^2 + 2 \cdot 11^3 + O(11^4)$
19	$15 + 11 \cdot 19 + 4 \cdot 19^2 + 7 \cdot 19^3 + O(19^4)$
37	$19 + 31 \cdot 37 + O(37^2)$
43	$8 + 9 \cdot 43 + O(43^2)$
53	$23 + 22 \cdot 53 + O(53^2)$
59	$6 + 56 \cdot 59 + O(59^2)$
61	$8 + 31 \cdot 61 + O(61^2)$
67	$56 + 21 \cdot 67 + O(67^2)$
79	$42 + 34 \cdot 79 + O(79^2)$
83	$4 + 76 \cdot 83 + O(83^2)$
89	$61 + 52 \cdot 89 + O(89^2)$
97	$33 + 86 \cdot 97 + O(97^2)$

Table 9.4.26: p-adic special values, $N = 161$

$N = 165$

For $N = 165, c = 1$. We obtain the following p-adic regulators:

p	p-adic regulator
7	$5 \cdot 7^2 + 2 \cdot 7^3 + 6 \cdot 7^4 + 7^5 + 5 \cdot 7^7 + 7^8 + O(7^9)$
13	$13^2 + 2 \cdot 13^3 + 6 \cdot 13^4 + 8 \cdot 13^5 + 2 \cdot 13^7 + 11 \cdot 13^8 + O(13^9)$
17	$6 + 7 \cdot 17 + 12 \cdot 17^2 + 7 \cdot 17^3 + 13 \cdot 17^4 + O(17^5)$
19	$18 \cdot 19^2 + 17 \cdot 19^3 + 2 \cdot 19^4 + 2 \cdot 19^5 + 18 \cdot 19^6 + 13 \cdot 19^7 + 17 \cdot 19^8 + O(19^9)$
23	$6 \cdot 23^2 + 23^3 + 16 \cdot 23^4 + 18 \cdot 23^5 + 19 \cdot 23^6 + 3 \cdot 23^7 + 15 \cdot 23^8 + O(23^9)$
29	$21 \cdot 29^2 + 18 \cdot 29^3 + 25 \cdot 29^4 + 11 \cdot 29^5 + 11 \cdot 29^6 + 13 \cdot 29^7 + 29^8 + O(29^9)$
37	$36 \cdot 37^2 + 16 \cdot 37^3 + 22 \cdot 37^4 + 37^6 + 23 \cdot 37^7 + 34 \cdot 37^8 + O(37^9)$
41	$12 \cdot 41^3 + 29 \cdot 41^4 + 19 \cdot 41^5 + 17 \cdot 41^6 + 29 \cdot 41^7 + 27 \cdot 41^8 + O(41^9)$
43	$9 \cdot 43^2 + 30 \cdot 43^3 + 14 \cdot 43^4 + 11 \cdot 43^5 + 19 \cdot 43^6 + 8 \cdot 43^7 + 26 \cdot 43^8 + O(43^9)$
47	$13 \cdot 47^2 + 39 \cdot 47^3 + 36 \cdot 47^4 + 41 \cdot 47^5 + 46 \cdot 47^6 + 16 \cdot 47^7 + O(47^9)$
53	$24 \cdot 53^2 + 3 \cdot 53^3 + 6 \cdot 53^4 + 26 \cdot 53^5 + 20 \cdot 53^6 + 51 \cdot 53^7 + 6 \cdot 53^8 + O(53^9)$
59	$40 \cdot 59^2 + 23 \cdot 59^3 + 44 \cdot 59^4 + 30 \cdot 59^5 + 8 \cdot 59^6 + 24 \cdot 59^7 + 43 \cdot 59^8 + O(59^9)$
61	$49 \cdot 61^2 + 44 \cdot 61^3 + 31 \cdot 61^4 + 6 \cdot 61^5 + 28 \cdot 61^6 + 37 \cdot 61^7 + 46 \cdot 61^8 + O(61^9)$
67	$4 \cdot 67^2 + 51 \cdot 67^3 + 18 \cdot 67^4 + 17 \cdot 67^5 + 31 \cdot 67^6 + 4 \cdot 67^7 + 63 \cdot 67^8 + O(67^9)$
71	$2 \cdot 71^2 + 10 \cdot 71^3 + 7 \cdot 71^4 + 11 \cdot 71^5 + 37 \cdot 71^6 + 10 \cdot 71^7 + 42 \cdot 71^8 + O(71^9)$
73	$41 \cdot 73^2 + 40 \cdot 73^3 + 27 \cdot 73^4 + 52 \cdot 73^5 + 47 \cdot 73^6 + 16 \cdot 73^7 + 63 \cdot 73^8 + O(73^9)$
79	$70 \cdot 79^3 + 9 \cdot 79^4 + 31 \cdot 79^5 + 3 \cdot 79^6 + 18 \cdot 79^7 + 28 \cdot 79^8 + O(79^9)$
83	$66 \cdot 83^2 + 72 \cdot 83^3 + 49 \cdot 83^4 + 39 \cdot 83^5 + 59 \cdot 83^6 + 23 \cdot 83^7 + 54 \cdot 83^8 + O(83^9)$
89	$70 \cdot 89^2 + 42 \cdot 89^3 + 51 \cdot 89^4 + 71 \cdot 89^5 + 28 \cdot 89^6 + 55 \cdot 89^7 + 69 \cdot 89^8 + O(89^9)$
97	$4 \cdot 97^2 + 50 \cdot 97^3 + 25 \cdot 97^4 + 22 \cdot 97^5 + 8 \cdot 97^6 + 35 \cdot 97^7 + 33 \cdot 97^8 + O(97^9)$

Table 9.4.27: p-adic regulators, $N = 165$

Here are values of the special value of the L-series for various p:

p	p-adic special value
7	$6 + 7 + O(7^4)$
13	$9 + 10 \cdot 13^2 + 11 \cdot 13^3 + O(13^4)$
17	$14 + 7 \cdot 17 + 8 \cdot 17^2 + 7 \cdot 17^3 + O(17^4)$
19	$13 + 10 \cdot 19 + 5 \cdot 19^2 + 12 \cdot 19^3 + O(19^4)$
23	$8 + 16 \cdot 23 + 14 \cdot 23^2 + O(23^3)$
29	$14 + 8 \cdot 29 + 26 \cdot 29^2 + O(29^3)$
37	$27 + 6 \cdot 37 + 8 \cdot 37^2 + O(37^3)$
41	$6 \cdot 41 + 38 \cdot 41^2 + O(41^3)$
43	$38 + 20 \cdot 43 + 41 \cdot 43^2 + O(43^3)$
47	$40 + 39 \cdot 47 + O(47^2)$
53	$40 + 50 \cdot 53 + O(53^2)$
59	$11 + 47 \cdot 59 + O(59^2)$
61	$12 + 28 \cdot 61 + O(61^2)$
67	$26 + 32 \cdot 67 + O(67^2)$
71	$24 + 63 \cdot 71 + O(71^2)$
73	$4 + 39 \cdot 73 + O(73^2)$
79	$35 \cdot 79 + O(79^2)$
83	$42 + 54 \cdot 83 + O(83^2)$
89	$52 + 41 \cdot 89 + O(89^2)$
97	$85 + 57 \cdot 97 + O(97^2)$

Table 9.4.28: p-adic special values, $N = 165$

$N = 177$

For $N = 177, c = 1$.

We obtain the following p-adic regulators:

p	p-adic regulator
7	$4 \cdot 7^2 + 2 \cdot 7^3 + 7^4 + 3 \cdot 7^5 + 7^6 + 5 \cdot 7^7 + O(7^8)$
19	$1 + 10 \cdot 19 + 18 \cdot 19^3 + 14 \cdot 19^4 + 15 \cdot 19^5 + O(19^6)$
23	$6 \cdot 23^2 + 20 \cdot 23^3 + 18 \cdot 23^4 + 4 \cdot 23^5 + 12 \cdot 23^6 + 9 \cdot 23^7 + O(23^8)$
29	$23 \cdot 29^2 + 9 \cdot 29^3 + 11 \cdot 29^4 + 25 \cdot 29^6 + 3 \cdot 29^7 + O(29^8)$
31	$10 \cdot 31^2 + 30 \cdot 31^3 + 13 \cdot 31^4 + 20 \cdot 31^5 + 17 \cdot 31^6 + 7 \cdot 31^7 + O(31^8)$
37	$17 \cdot 37^2 + 32 \cdot 37^3 + 9 \cdot 37^4 + 5 \cdot 37^5 + 35 \cdot 37^6 + 5 \cdot 37^7 + O(37^8)$
41	$18 \cdot 41^2 + 9 \cdot 41^3 + 23 \cdot 41^4 + 8 \cdot 41^5 + 23 \cdot 41^6 + 19 \cdot 41^7 + O(41^8)$
47	$28 \cdot 47^2 + 40 \cdot 47^3 + 27 \cdot 47^4 + 37 \cdot 47^5 + 30 \cdot 47^6 + 31 \cdot 47^7 + O(47^8)$
61	$49 \cdot 61^2 + 36 \cdot 61^3 + 22 \cdot 61^4 + 42 \cdot 61^5 + 46 \cdot 61^6 + 8 \cdot 61^7 + O(61^8)$
73	$69 \cdot 73^2 + 62 \cdot 73^3 + 43 \cdot 73^4 + 15 \cdot 73^5 + 56 \cdot 73^6 + 62 \cdot 73^7 + O(73^8)$
83	$22 \cdot 83^2 + 58 \cdot 83^3 + 36 \cdot 83^4 + 8 \cdot 83^5 + 38 \cdot 83^6 + 49 \cdot 83^7 + O(83^8)$

Table 9.4.29: p-adic regulators, $N = 177$

p	p-adic special value
7	$1 + 2 \cdot 7 + 6 \cdot 7^2 + 6 \cdot 7^3 + O(7^4)$
19	$1 + 19 + 2 \cdot 19^3 + O(19^4)$
23	$16 + 16 \cdot 23 + 10 \cdot 23^2 + O(23^3)$
29	$20 + 13 \cdot 29 + 24 \cdot 29^2 + O(29^3)$
31	$25 + 12 \cdot 31 + O(31^3)$
37	$8 + 5 \cdot 37^2 + O(37^3)$
41	$5 + 13 \cdot 41 + O(41^2)$
47	$9 + 3 \cdot 47 + O(47^2)$
61	$34 + 16 \cdot 61 + O(61^2)$
73	$67 + 58 \cdot 73 + O(73^2)$
83	$22 + 56 \cdot 83 + O(83^2)$

Table 9.4.30: p-adic special values, $N = 177$

$N = 188$

For $N = 188, c = 1$.

Here are values of the p-adic regulator for various p:

p	p-adic regulator
7	$6 \cdot 7^2 + 5 \cdot 7^3 + 7^4 + 7^5 + 2 \cdot 7^6 + 6 \cdot 7^7 + O(7^8)$
11	$3 + 8 \cdot 11^2 + 6 \cdot 11^3 + 2 \cdot 11^4 + 11^5 + 10 \cdot 11^6 + O(11^7)$
13	$2 \cdot 13^2 + 3 \cdot 13^3 + 4 \cdot 13^4 + 9 \cdot 13^5 + 5 \cdot 13^6 + 10 \cdot 13^7 + O(13^8)$
17	$2 \cdot 17^2 + 13 \cdot 17^3 + 2 \cdot 17^4 + 4 \cdot 17^5 + 11 \cdot 17^7 + O(17^8)$
19	$12 \cdot 19^2 + 5 \cdot 19^3 + 10 \cdot 19^4 + 2 \cdot 19^5 + 9 \cdot 19^6 + 7 \cdot 19^7 + O(19^8)$
23	$19 \cdot 23^2 + 14 \cdot 23^3 + 2 \cdot 23^4 + 19 \cdot 23^5 + 20 \cdot 23^6 + 13 \cdot 23^7 + O(23^8)$
37	$33 \cdot 37^2 + 8 \cdot 37^3 + 28 \cdot 37^4 + 36 \cdot 37^5 + 2 \cdot 37^6 + 15 \cdot 37^7 + O(37^8)$
41	$6 \cdot 41^2 + 15 \cdot 41^3 + 7 \cdot 41^4 + 40 \cdot 41^6 + 5 \cdot 41^7 + O(41^8)$
43	$19 \cdot 43^2 + 29 \cdot 43^4 + 9 \cdot 43^5 + 2 \cdot 43^6 + 12 \cdot 43^7 + O(43^8)$
53	$46 \cdot 53^2 + 26 \cdot 53^3 + 19 \cdot 53^4 + 33 \cdot 53^5 + 17 \cdot 53^6 + 11 \cdot 53^7 + O(53^8)$
59	$51 \cdot 59^2 + 54 \cdot 59^3 + 37 \cdot 59^4 + 5 \cdot 59^5 + 58 \cdot 59^6 + 27 \cdot 59^7 + O(59^8)$
61	$37 \cdot 61^2 + 20 \cdot 61^3 + 37 \cdot 61^4 + 56 \cdot 61^5 + 32 \cdot 61^6 + 8 \cdot 61^7 + O(61^8)$
67	$22 \cdot 67^2 + 3 \cdot 67^3 + 26 \cdot 67^4 + 23 \cdot 67^5 + 11 \cdot 67^6 + 17 \cdot 67^7 + O(67^8)$
71	$68 \cdot 71^2 + 25 \cdot 71^3 + 62 \cdot 71^4 + 36 \cdot 71^5 + 62 \cdot 71^6 + 2 \cdot 71^7 + O(71^8)$
73	$60 \cdot 73^2 + 7 \cdot 73^3 + 12 \cdot 73^4 + 22 \cdot 73^5 + 46 \cdot 73^6 + 30 \cdot 73^7 + O(73^8)$
79	$21 \cdot 79^2 + 15 \cdot 79^3 + 17 \cdot 79^4 + 78 \cdot 79^5 + 2 \cdot 79^6 + 25 \cdot 79^7 + O(79^8)$
83	$44 \cdot 83^2 + 71 \cdot 83^3 + 32 \cdot 83^4 + 54 \cdot 83^5 + 18 \cdot 83^6 + 56 \cdot 83^7 + O(83^8)$
89	$30 \cdot 89^2 + 27 \cdot 89^3 + 11 \cdot 89^4 + 43 \cdot 89^5 + 27 \cdot 89^6 + 43 \cdot 89^7 + O(89^8)$
97	$50 \cdot 97^2 + 8 \cdot 97^3 + 77 \cdot 97^4 + 73 \cdot 97^5 + 82 \cdot 97^6 + 16 \cdot 97^7 + O(97^8)$

Table 9.4.31: p-adic regulators, $N = 188$

Here are values of the special value of the L-series for various p:

p	p-adic special value
7	$3 + 5 \cdot 7 + 4 \cdot 7^2 + 2 \cdot 7^4 + O(7^4)$
11	$5 + 10 \cdot 11 + 9 \cdot 11^2 + 5 \cdot 11^3 + O(11^4)$
13	$8 + 13 + 13^2 + 6 \cdot 13^3 + O(13^4)$
17	$8 + 15 \cdot 17 + 5 \cdot 17^2 + 2 \cdot 17^3 + O(17^4)$
19	$8 + 13 \cdot 19 + 6 \cdot 19^2 + 17 \cdot 19^3 + O(19^4)$
23	$5 + 15 \cdot 23 + 2 \cdot 23^2 + 8 \cdot 23^3 + O(23^4)$
37	$33 + 13 \cdot 37 + 22 \cdot 37^2 + O(37^3)$
41	$35 + 2 \cdot 41 + 37 \cdot 41^2 + O(41^3)$
43	$26 + 15 \cdot 43 + 19 \cdot 43^2 + O(43^3)$
53	$9 + 41 \cdot 53 + 13 \cdot 53^2 + O(53^3)$
59	$46 + 41 \cdot 59 + 2 \cdot 59^2 + O(59^3)$
61	$59 + 59 \cdot 61 + O(61^2)$
67	$37 + 67 + O(67^2)$
71	$66 + 14 \cdot 71 + O(71^2)$
73	$13 + 10 \cdot 73 + O(73^2)$
79	$26 + 13 \cdot 79 + O(79^2)$
83	$40 + 43 \cdot 83 + O(83^2)$
89	$24 + 54 \cdot 89 + O(89^2)$
97	$4 + O(97^2)$

Table 9.4.32: p-adic special values, $N = 188$

$N = 191$

For $N = 191, c = 1$.

p	p-adic regulator
7	$6 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^4 + 4 \cdot 7^5 + 2 \cdot 7^6 + 6 \cdot 7^7 + O(7^8)$
23	$10 \cdot 23^2 + 15 \cdot 23^3 + 8 \cdot 23^4 + 6 \cdot 23^5 + 2 \cdot 23^6 + 5 \cdot 23^7 + O(23^8)$
31	$24 \cdot 31^2 + 12 \cdot 31^3 + 28 \cdot 31^4 + 2 \cdot 31^5 + 6 \cdot 31^6 + 9 \cdot 31^7 + O(31^8)$
43	$41 \cdot 43^2 + 24 \cdot 43^3 + 15 \cdot 43^4 + 41 \cdot 43^5 + 20 \cdot 43^6 + 29 \cdot 43^7 + O(43^8)$
47	$3 \cdot 47^2 + 27 \cdot 47^3 + 39 \cdot 47^4 + 20 \cdot 47^5 + 10 \cdot 47^6 + 29 \cdot 47^7 + O(47^8)$
53	$48 \cdot 53^2 + 46 \cdot 53^3 + 26 \cdot 53^4 + 8 \cdot 53^5 + 29 \cdot 53^6 + 14 \cdot 53^7 + O(53^8)$
71	$61 \cdot 71^3 + 34 \cdot 71^4 + 22 \cdot 71^5 + 28 \cdot 71^6 + 20 \cdot 71^7 + O(71^8)$
73	$58 \cdot 73^2 + 24 \cdot 73^3 + 3 \cdot 73^4 + 55 \cdot 73^5 + 18 \cdot 73^6 + 38 \cdot 73^7 + O(73^8)$
97	$68 \cdot 97^2 + 46 \cdot 97^3 + 75 \cdot 97^4 + 37 \cdot 97^5 + 36 \cdot 97^6 + 20 \cdot 97^7 + O(97^8)$

Table 9.4.33: p-adic regulators, $N = 191$

p	p-adic special value
7	$6 + 2 \cdot 7 + 5 \cdot 7^2 + O(7^4)$
23	$10 + 4 \cdot 23 + 20 \cdot 23^2 + 17 \cdot 23^3 + O(23^4)$
31	$3 + 19 \cdot 31 + O(31^2)$
43	$1 + 25 \cdot 43 + O(43^2)$
47	$8 + 5 \cdot 47 + O(47^2)$
53	$48 + 32 \cdot 53 + O(53^2)$
71	$41 \cdot 71 + O(71^2)$
73	$31 + 37 \cdot 73 + O(73^2)$
97	$80 + 72 \cdot 97 + O(97^2)$

Table 9.4.34: p-adic special values, $N = 191$

9.4.3 Future work

We suggest some avenues of future work below:

More data

It would be very interesting to generate more data for Conjecture 9.1.4, first starting by extending the range of primes considered, and second, using another potential list of curves [BS]. Moreover, if one were able to generalize the techniques in Chapter 8 to handle number fields, we could finish the list in [FpS$^+$01] and obtain data for $N = 167$.

The sign c

Note that Conjecture 9.1.4 is stated up to a sign c. Where does this sign come from?

Algorithm for p-adic L-series

The work of Pollack-Stevens [PS] gives a polynomial-time algorithm (in p) for computing p-adic L-series via overconvergent modular symbols. Using their algorithm instead of ours could make it possible to generate data for the conjecture for much higher precision.

Appendix A

Auxiliary p-adic BSD data

A.1 $N = 67$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
7	$(3 \cdot a + 4) + (a + 4) \cdot 7 + (2 \cdot a + 6) \cdot 7^2 + (4 \cdot a + 3) \cdot 7^3 + (5 \cdot a + 4) \cdot 7^4 + 5 \cdot a \cdot 7^5 + (5 \cdot a + 5) \cdot 7^6 + 6 \cdot 7^7 + (2 \cdot a + 5) \cdot 7^8 + O(7^9)$
13	$(10 \cdot a + 5) + (9 \cdot a + 11) \cdot 13 + (11 \cdot a + 9) \cdot 13^2 + (4 \cdot a + 1) \cdot 13^3 + (11 \cdot a + 10) \cdot 13^4 + (6 \cdot a + 6) \cdot 13^5 + 7 \cdot a \cdot 13^6 + (4 \cdot a + 3) \cdot 13^7 + (11 \cdot a + 2) \cdot 13^8 + O(13^9)$
17	$(15 \cdot a + 11) + (7 \cdot a + 16) \cdot 17 + (7 \cdot a + 5) \cdot 17^2 + (12 \cdot a + 10) \cdot 17^3 + (2 \cdot a + 16) \cdot 17^4 + (6 \cdot a + 14) \cdot 17^5 + (6 \cdot a + 10) \cdot 17^6 + (2 \cdot a + 4) \cdot 17^7 + (12 \cdot a + 15) \cdot 17^8 + O(17^9)$
19	$6 + 15 \cdot 19 + 12 \cdot 19^2 + 16 \cdot 19^3 + 12 \cdot 19^5 + 7 \cdot 19^6 + 3 \cdot 19^7 + 9 \cdot 19^8 + O(19^9)$ $14 + 10 \cdot 19 + 12 \cdot 19^2 + 2 \cdot 19^3 + 6 \cdot 19^4 + 8 \cdot 19^5 + 7 \cdot 19^6 + 8 \cdot 19^7 + 16 \cdot 19^8 + O(19^9)$
37	$(3 \cdot a + 4) + (30 \cdot a + 13) \cdot 37 + 15 \cdot a \cdot 37^2 + (34 \cdot a + 6) \cdot 37^3 + (26 \cdot a + 17) \cdot 37^4 + (15 \cdot a + 33) \cdot 37^5 + (21 \cdot a + 16) \cdot 37^6 + 16 \cdot a \cdot 37^7 + (12 \cdot a + 4) \cdot 37^8 + O(37^9)$
41	$33 + 13 \cdot 41 + 38 \cdot 41^2 + 20 \cdot 41^3 + 17 \cdot 41^4 + 2 \cdot 41^5 + 41^6 + 36 \cdot 41^7 + 33 \cdot 41^8 + O(41^9)$ $5 + 30 \cdot 41 + 20 \cdot 41^2 + 20 \cdot 41^3 + 21 \cdot 41^4 + 17 \cdot 41^5 + 3 \cdot 41^6 + 34 \cdot 41^7 + 12 \cdot 41^8 + O(41^9)$
43	$(40 \cdot a + 40) + (28 \cdot a + 14) \cdot 43 + (a + 11) \cdot 43^2 + (20 \cdot a + 34) \cdot 43^3 + (a + 39) \cdot 43^4 + (36 \cdot a + 11) \cdot 43^5 + 9 \cdot 43^6 + 30 \cdot a \cdot 43^7 + (32 \cdot a + 19) \cdot 43^8 + O(43^9)$
47	$(a + 41) + (6 \cdot a + 6) \cdot 47 + (18 \cdot a + 46) \cdot 47^2 + (3 \cdot a + 15) \cdot 47^3 + (19 \cdot a + 28) \cdot 47^4 + (44 \cdot a + 19) \cdot 47^5 + (32 \cdot a + 25) \cdot 47^6 + (28 \cdot a + 3) \cdot 47^7 + (43 \cdot a + 9) \cdot 47^8 + O(47^9)$
59	$6 + 49 \cdot 59 + 12 \cdot 59^2 + 33 \cdot 59^3 + 23 \cdot 59^4 + 33 \cdot 59^5 + 14 \cdot 59^6 + 31 \cdot 59^7 + 57 \cdot 59^8 + O(59^9)$ $6 + 49 \cdot 59 + 12 \cdot 59^2 + 33 \cdot 59^3 + 23 \cdot 59^4 + 33 \cdot 59^5 + 14 \cdot 59^6 + 31 \cdot 59^7 + 57 \cdot 59^8 + O(59^9)$
61	$32 + 32 \cdot 61 + 32 \cdot 61^2 + 14 \cdot 61^3 + 54 \cdot 61^4 + 59 \cdot 61^5 + 31 \cdot 61^6 + 14 \cdot 61^7 + 12 \cdot 61^8 + O(61^9)$ $22 + 43 \cdot 61 + 51 \cdot 61^2 + 53 \cdot 61^3 + 37 \cdot 61^4 + 4 \cdot 61^5 + 50 \cdot 61^6 + 4 \cdot 61^7 + 46 \cdot 61^8 + O(61^9)$
73	$69 + 54 \cdot 73 + 62 \cdot 73^2 + 72 \cdot 73^3 + 7 \cdot 73^4 + 56 \cdot 73^5 + 20 \cdot 73^6 + 25 \cdot 73^7 + 31 \cdot 73^8 + O(73^9)$
79	$47 + 37 \cdot 79 + 11 \cdot 79^2 + 4 \cdot 79^3 + 45 \cdot 79^4 + 30 \cdot 79^5 + 51 \cdot 79^6 + 57 \cdot 79^7 + 79^8 + O(79^9)$ $25 + 64 \cdot 79 + 17 \cdot 79^2 + 69 \cdot 79^3 + 74 \cdot 79^4 + 14 \cdot 79^5 + 37 \cdot 79^6 + 29 \cdot 79^7 + 6 \cdot 79^8 + O(79^9)$
83	$(7 \cdot a + 3) + (65 \cdot a + 13) \cdot 83 + (66 \cdot a + 69) \cdot 83^2 + (8 \cdot a + 57) \cdot 83^3 + (72 \cdot a + 51) \cdot 83^4 + (21 \cdot a + 68) \cdot 83^5 + (12 \cdot a + 3) \cdot 83^6 + (68 \cdot a + 50) \cdot 83^7 + (60 \cdot a + 11) \cdot 83^8 + O(83^9)$

Table A.1.1: α factors for $N = 67$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
7	$2 + 5 \cdot 7 + 7^2 + 5 \cdot 7^4 + 7^6 + 7^7 + 2 \cdot 7^8 + O(7^9)$
13	$3 + 5 \cdot 13 + 6 \cdot 13^2 + 2 \cdot 13^3 + 2 \cdot 13^4 + 3 \cdot 13^5 + 12 \cdot 13^6 + 13^7 + 7 \cdot 13^8 + O(13^9)$
17	$15 + 2 \cdot 17^2 + 12 \cdot 17^3 + 3 \cdot 17^4 + 2 \cdot 17^5 + 5 \cdot 17^6 + 7 \cdot 17^7 + 13 \cdot 17^8 + O(17^9)$
19	$1 + 3 \cdot 19 + 7 \cdot 19^2 + 15 \cdot 19^4 + 16 \cdot 19^5 + 9 \cdot 19^6 + 7 \cdot 19^7 + 11 \cdot 19^8 + O(19^9)$
37	$34 + 4 \cdot 37 + 35 \cdot 37^2 + 27 \cdot 37^3 + 12 \cdot 37^4 + 17 \cdot 37^5 + 21 \cdot 37^6 + 18 \cdot 37^7 + 14 \cdot 37^8 + O(37^9)$
41	$25 + 4 \cdot 41 + 23 \cdot 41^2 + 16 \cdot 41^3 + 38 \cdot 41^4 + 10 \cdot 41^5 + 4 \cdot 41^6 + 3 \cdot 41^7 + 2 \cdot 41^8 + O(41^9)$
43	$36 + 38 \cdot 43^2 + 3 \cdot 43^3 + 6 \cdot 43^4 + 14 \cdot 43^5 + 39 \cdot 43^6 + 42 \cdot 43^7 + 18 \cdot 43^8 + O(43^9)$
47	$9 + 26 \cdot 47 + 29 \cdot 47^2 + 34 \cdot 47^3 + 40 \cdot 47^4 + 34 \cdot 47^5 + 27 \cdot 47^6 + 42 \cdot 47^7 + 30 \cdot 47^8 + O(47^9)$
59	$12 + 22 \cdot 59 + 15 \cdot 59^2 + 4 \cdot 59^3 + 23 \cdot 59^4 + 51 \cdot 59^5 + 31 \cdot 59^7 + O(59^9)$
61	$3 + 13 \cdot 61 + 23 \cdot 61^2 + 11 \cdot 61^3 + 43 \cdot 61^4 + 23 \cdot 61^5 + 27 \cdot 61^6 + 42 \cdot 61^7 + 14 \cdot 61^8 + O(61^9)$
73	$9 + 53 \cdot 73 + 31 \cdot 73^2 + 66 \cdot 73^3 + 46 \cdot 73^4 + 37 \cdot 73^5 + 51 \cdot 73^6 + 41 \cdot 73^7 + 53 \cdot 73^8 + O(73^9)$
79	$19 + 69 \cdot 79 + 58 \cdot 79^2 + 28 \cdot 79^3 + 69 \cdot 79^4 + 20 \cdot 79^5 + 56 \cdot 79^6 + 41 \cdot 79^7 + 41 \cdot 79^8 + O(79^9)$
83	$48 + 3 \cdot 83 + 27 \cdot 83^2 + 27 \cdot 83^3 + 81 \cdot 83^4 + 5 \cdot 83^5 + 82 \cdot 83^6 + 5 \cdot 83^7 + 14 \cdot 83^8 + O(83^9)$

Table A.1.2: ϵ factors for $N = 67$

A.2 $N = 73$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$. Here are tables giving α,ϵ factors:

p	α or α_1, α_2
11	$6+5\cdot 11+10\cdot 11^2+5\cdot 11^3+7\cdot 11^4+10\cdot 11^5+10\cdot 11^6+10\cdot 11^7+11^8+O(11^9)$
	$2+8\cdot 11+7\cdot 11^2+10\cdot 11^3+5\cdot 11^4+9\cdot 11^5+11^6+6\cdot 11^7+7\cdot 11^8+O(11^9)$
13	$(3\cdot a+5)+(8\cdot a+2)\cdot 13+(8\cdot a+4)\cdot 13^2+(a+11)\cdot 13^3+(5\cdot a+8)\cdot 13^4+3\cdot 13^5+(12\cdot a+12)\cdot 13^6+(9\cdot a+7)\cdot 13^7+(9\cdot a+5)\cdot 13^8+O(13^9)$
23	$(a+17)+18\cdot a\cdot 23+(10\cdot a+21)\cdot 23^2+(9\cdot a+15)\cdot 23^3+(20\cdot a+9)\cdot 23^4+(5\cdot a+22)\cdot 23^5+(2\cdot a+6)\cdot 23^6+(20\cdot a+5)\cdot 23^7+(4\cdot a+1)\cdot 23^8+O(23^9)$
31	$19+5\cdot 31+8\cdot 31^2+8\cdot 31^3+30\cdot 31^4+28\cdot 31^5+6\cdot 31^6+8\cdot 31^7+7\cdot 31^8+O(31^9)$
	$14+18\cdot 31+12\cdot 31^2+24\cdot 31^3+18\cdot 31^4+6\cdot 31^5+28\cdot 31^6+4\cdot 31^7+15\cdot 31^8+O(31^9)$
41	$26+17\cdot 41+39\cdot 41^2+34\cdot 41^3+39\cdot 41^4+4\cdot 41^5+25\cdot 41^6+38\cdot 41^8+O(41^9)$
	$15+23\cdot 41+41^2+6\cdot 41^3+41^4+36\cdot 41^5+15\cdot 41^6+40\cdot 41^7+2\cdot 41^8+O(41^9)$
59	$10+16\cdot 59+6\cdot 59^2+53\cdot 59^3+38\cdot 59^4+16\cdot 59^5+17\cdot 59^6+10\cdot 59^7+20\cdot 59^8+O(59^9)$
	$37+28\cdot 59+47\cdot 59^2+55\cdot 59^3+44\cdot 59^4+56\cdot 59^5+32\cdot 59^6+51\cdot 59^7+15\cdot 59^8+O(59^9)$
61	$56+5\cdot 61+6\cdot 61^2+36\cdot 61^3+22\cdot 61^4+56\cdot 61^5+12\cdot 61^6+61^7+42\cdot 61^8+O(61^9)$
	$12+48\cdot 61+37\cdot 61^2+21\cdot 61^3+45\cdot 61^4+9\cdot 61^5+48\cdot 61^6+47\cdot 61^7+32\cdot 61^8+O(61^9)$
71	$69+60\cdot 71+10\cdot 71^2+40\cdot 71^3+17\cdot 71^4+43\cdot 71^5+7\cdot 71^6+14\cdot 71^7+65\cdot 71^8+O(71^9)$
	$52+60\cdot 71+19\cdot 71^2+17\cdot 71^3+36\cdot 71^4+28\cdot 71^5+16\cdot 71^6+36\cdot 71^7+29\cdot 71^8+O(71^9)$
83	$(80\cdot a+77)+(27\cdot a+27)\cdot 83+(52\cdot a+12)\cdot 83^2+(10\cdot a+33)\cdot 83^3+(47\cdot a+28)\cdot 83^4+(15\cdot a+49)\cdot 83^5+(41\cdot a+32)\cdot 83^6+(33\cdot a+17)\cdot 83^7+(71\cdot a+53)\cdot 83^8+O(83^9)$
97	$(94\cdot a+88)+(31\cdot a+96)\cdot 97+(82\cdot a+42)\cdot 97^2+(45\cdot a+88)\cdot 97^3+(82\cdot a+75)\cdot 97^4+(52\cdot a+60)\cdot 97^5+(2\cdot a+86)\cdot 97^6+(17\cdot a+96)\cdot 97^7+97^8+O(97^9)$

Table A.2.1: α factors for $N = 73$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2\cdot(1-\alpha_2^{-1})^2$
11	$3+10\cdot 11+9\cdot 11^2+7\cdot 11^3+10\cdot 11^4+8\cdot 11^5+9\cdot 11^6+9\cdot 11^7+10\cdot 11^8+O(11^9)$
13	$1+7\cdot 13+8\cdot 13^2+4\cdot 13^3+4\cdot 13^4+12\cdot 13^5+12\cdot 13^7+2\cdot 13^8+O(13^9)$
23	$8+15\cdot 23+10\cdot 23^2+8\cdot 23^3+12\cdot 23^4+17\cdot 23^5+3\cdot 23^6+14\cdot 23^7+21\cdot 23^8+O(23^9)$
31	$14+10\cdot 31+19\cdot 31^2+8\cdot 31^3+31^4+31^5+28\cdot 31^6+30\cdot 31^7+28\cdot 31^8+O(31^9)$
41	$9+5\cdot 41+27\cdot 41^2+2\cdot 41^3+41^4+22\cdot 41^5+26\cdot 41^6+27\cdot 41^7+26\cdot 41^8+O(41^9)$
59	$45+58\cdot 59+35\cdot 59^2+37\cdot 59^3+21\cdot 59^4+53\cdot 59^5+24\cdot 59^6+45\cdot 59^7+18\cdot 59^8+O(59^9)$
61	$25+5\cdot 61+24\cdot 61^2+15\cdot 61^3+15\cdot 61^4+37\cdot 61^5+22\cdot 61^6+25\cdot 61^7+55\cdot 61^8+O(61^9)$
71	$8+38\cdot 71+9\cdot 71^2+31\cdot 71^3+23\cdot 71^4+12\cdot 71^5+70\cdot 71^6+50\cdot 71^8+O(71^9)$
83	$29+50\cdot 83+79\cdot 83^2+5\cdot 83^3+74\cdot 83^4+19\cdot 83^5+44\cdot 83^6+26\cdot 83^7+65\cdot 83^8+O(83^9)$
97	$32+17\cdot 97+78\cdot 97^2+8\cdot 97^3+50\cdot 97^4+29\cdot 97^5+41\cdot 97^6+49\cdot 97^7+78\cdot 97^8+O(97^9)$

Table A.2.2: ϵ factors for $N = 73$

A.3 $N = 85$

The quadratic field K_f is generated by a root a of $x^2 + 2x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
13	$(11 \cdot a + 11) + (9 \cdot a + 9) \cdot 13 + (7 \cdot a + 7) \cdot 13^2 + (5 \cdot a + 5) \cdot 13^3 + (5 \cdot a + 5) \cdot 13^4 + (3 \cdot a + 3) \cdot 13^5 + (3 \cdot a + 3) \cdot 13^6 + (a + 1) \cdot 13^7 + (3 \cdot a + 3) \cdot 13^8 + O(13^9)$
29	$(27 \cdot a + 25) + (14 \cdot a + 28) \cdot 29 + (11 \cdot a + 6) \cdot 29^2 + (25 \cdot a + 28) \cdot 29^3 + (11 \cdot a + 23) \cdot 29^4 + (28 \cdot a + 21) \cdot 29^5 + (25 \cdot a + 12) \cdot 29^6 + (21 \cdot a + 25) \cdot 29^7 + (a + 20) \cdot 29^8 + O(29^9)$
37	$(6 \cdot a + 4) + (a + 26) \cdot 37 + (15 \cdot a + 11) \cdot 37^2 + (6 \cdot a + 20) \cdot 37^3 + (19 \cdot a + 24) \cdot 37^4 + (22 \cdot a + 16) \cdot 37^5 + (6 \cdot a + 3) \cdot 37^6 + (25 \cdot a + 1) \cdot 37^7 + (30 \cdot a + 10) \cdot 37^8 + O(37^9)$
41	$22 + 21 \cdot 41 + 22 \cdot 41^2 + 11 \cdot 41^3 + 11 \cdot 41^4 + 12 \cdot 41^5 + 2 \cdot 41^6 + 33 \cdot 41^7 + 39 \cdot 41^8 + O(41^9)$
	$23 + 7 \cdot 41 + 19 \cdot 41^2 + 18 \cdot 41^3 + 13 \cdot 41^4 + 3 \cdot 41^5 + 19 \cdot 41^7 + 18 \cdot 41^8 + O(41^9)$
53	$(49 \cdot a + 2) + (51 \cdot a + 24) \cdot 53 + (30 \cdot a + 38) \cdot 53^2 + (3 \cdot a + 21) \cdot 53^3 + (34 \cdot a + 17) \cdot 53^4 + (34 \cdot a + 17) \cdot 53^5 + (46 \cdot a + 22) \cdot 53^6 + (8 \cdot a + 9) \cdot 53^7 + (16 \cdot a + 40) \cdot 53^8 + O(53^9)$
61	$(4 \cdot a + 6) + (26 \cdot a + 13) \cdot 61 + (39 \cdot a + 36) \cdot 61^2 + (18 \cdot a + 60) \cdot 61^3 + (9 \cdot a + 4) \cdot 61^4 + (32 \cdot a + 43) \cdot 61^5 + (35 \cdot a + 48) \cdot 61^6 + (42 \cdot a + 9) \cdot 61^7 + (26 \cdot a + 36) \cdot 61^8 + O(61^9)$
73	$62 + 15 \cdot 73 + 67 \cdot 73^2 + 57 \cdot 73^3 + 21 \cdot 73^4 + 19 \cdot 73^5 + 10 \cdot 73^6 + 42 \cdot 73^7 + 27 \cdot 73^8 + O(73^9)$
	$7 + 56 \cdot 73 + 58 \cdot 73^2 + 45 \cdot 73^4 + 16 \cdot 73^5 + 34 \cdot 73^6 + 52 \cdot 73^7 + 53 \cdot 73^8 + O(73^9)$
89	$3 + 63 \cdot 89 + 15 \cdot 89^2 + 82 \cdot 89^3 + 80 \cdot 89^4 + 84 \cdot 89^5 + 80 \cdot 89^6 + 49 \cdot 89^7 + 15 \cdot 89^8 + O(89^9)$
89	$70 + 70 \cdot 89 + 10 \cdot 89^2 + 80 \cdot 89^3 + 70 \cdot 89^4 + 70 \cdot 89^5 + 85 \cdot 89^6 + 69 \cdot 89^7 + 75 \cdot 89^8 + O(89^9)$
97	$54 + 60 \cdot 97 + 75 \cdot 97^2 + 43 \cdot 97^3 + 54 \cdot 97^4 + 67 \cdot 97^5 + 68 \cdot 97^6 + 49 \cdot 97^7 + 16 \cdot 97^8 + O(97^9)$
97	$39 + 22 \cdot 97 + 54 \cdot 97^2 + 5 \cdot 97^3 + 84 \cdot 97^4 + 59 \cdot 97^5 + 36 \cdot 97^6 + 91 \cdot 97^7 + 3 \cdot 97^8 + O(97^9)$

Table A.3.1: α factors for $N = 85$

p	$(1 - \overline{\alpha}^{-1})^2$ or $(1 - \alpha_1^{-1})^2 \cdot (1 - \alpha_2^{-1})^2$
13	$3 + 8 \cdot 13 + 7 \cdot 13^2 + 12 \cdot 13^3 + 10 \cdot 13^4 + 6 \cdot 13^5 + 7 \cdot 13^6 + 6 \cdot 13^7 + 9 \cdot 13^8 + O(13^9)$
29	$20 + 4 \cdot 29 + 5 \cdot 29^2 + 28 \cdot 29^3 + 17 \cdot 29^4 + 4 \cdot 29^5 + 21 \cdot 29^6 + 9 \cdot 29^7 + 17 \cdot 29^8 + O(29^9)$
37	$27 + 34 \cdot 37 + 20 \cdot 37^3 + 32 \cdot 37^4 + 21 \cdot 37^5 + 20 \cdot 37^6 + 10 \cdot 37^7 + 29 \cdot 37^8 + O(37^9)$
41	$23 + 9 \cdot 41 + 38 \cdot 41^2 + 36 \cdot 41^3 + 3 \cdot 41^4 + 41^5 + 30 \cdot 41^6 + 36 \cdot 41^7 + 17 \cdot 41^8 + O(41^9)$
53	$13 + 26 \cdot 53 + 5 \cdot 53^2 + 38 \cdot 53^3 + 13 \cdot 53^4 + 2 \cdot 53^6 + 38 \cdot 53^7 + 6 \cdot 53^8 + O(53^9)$
61	$22 + 42 \cdot 61 + 41 \cdot 61^2 + 52 \cdot 61^3 + 7 \cdot 61^4 + 54 \cdot 61^5 + 55 \cdot 61^6 + 22 \cdot 61^7 + 6 \cdot 61^8 + O(61^9)$
73	$32 + 28 \cdot 73 + 58 \cdot 73^2 + 17 \cdot 73^3 + 36 \cdot 73^4 + 31 \cdot 73^5 + 69 \cdot 73^6 + 2 \cdot 73^7 + 8 \cdot 73^8 + O(73^9)$
89	$85 + 71 \cdot 89 + 36 \cdot 89^2 + 63 \cdot 89^3 + 28 \cdot 89^4 + 78 \cdot 89^5 + 41 \cdot 89^6 + 23 \cdot 89^7 + 6 \cdot 89^8 + O(89^9)$
97	$54 + 7 \cdot 97 + 33 \cdot 97^2 + 92 \cdot 97^3 + 74 \cdot 97^4 + 88 \cdot 97^5 + 80 \cdot 97^6 + 46 \cdot 97^7 + 57 \cdot 97^8 + O(97^9)$

Table A.3.2: ϵ factors for $N = 85$

A.4 $N = 93$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
11	$4 + 3 \cdot 11 + 8 \cdot 11^2 + 10 \cdot 11^4 + 3 \cdot 11^5 + 11^6 + 4 \cdot 11^7 + 10 \cdot 11^8 + O(11^9)$ $1 + 3 \cdot 11 + 2 \cdot 11^2 + 9 \cdot 11^3 + 11^4 + 4 \cdot 11^5 + 2 \cdot 11^6 + 2 \cdot 11^7 + O(11^9)$
13	$(2 \cdot a + 2) + (6 \cdot a + 12) \cdot 13 + 9 \cdot a \cdot 13^2 + (3 \cdot a + 8) \cdot 13^3 + (7 \cdot a + 12) \cdot 13^4 + (7 \cdot a + 7) \cdot 13^5 + (2 \cdot a + 9) \cdot 13^6 + (6 \cdot a + 7) \cdot 13^7 + (3 \cdot a + 12) \cdot 13^8 + O(13^9)$
23	$(21 \cdot a + 21) + 11 \cdot a \cdot 23 + (17 \cdot a + 15) \cdot 23^2 + (a + 16) \cdot 23^3 + (15 \cdot a + 1) \cdot 23^4 + (10 \cdot a + 7) \cdot 23^5 + (22 \cdot a + 17) \cdot 23^6 + (13 \cdot a + 3) \cdot 23^7 + (11 \cdot a + 3) \cdot 23^8 + O(23^9)$
29	$12 + 25 \cdot 29 + 15 \cdot 29^2 + 25 \cdot 29^3 + 7 \cdot 29^4 + 4 \cdot 29^5 + 2 \cdot 29^6 + 11 \cdot 29^7 + 18 \cdot 29^8 + O(29^9)$ $19 + 18 \cdot 29 + 13 \cdot 29^2 + 20 \cdot 29^3 + 15 \cdot 29^4 + 22 \cdot 29^5 + 11 \cdot 29^6 + 2 \cdot 29^7 + 22 \cdot 29^8 + O(29^9)$
37	$(31 \cdot a + 29) + (21 \cdot a + 11) \cdot 37 + (5 \cdot a + 3) \cdot 37^2 + (5 \cdot a + 35) \cdot 37^3 + 6 \cdot a \cdot 37^4 + (34 \cdot a + 10) \cdot 37^5 + (29 \cdot a + 12) \cdot 37^6 + (28 \cdot a + 26) \cdot 37^7 + (16 \cdot a + 14) \cdot 37^8 + O(37^9)$
43	$(37 \cdot a + 31) + (35 \cdot a + 35) \cdot 43 + (37 \cdot a + 36) \cdot 43^2 + (42 \cdot a + 11) \cdot 43^3 + (20 \cdot a + 33) \cdot 43^4 + (18 \cdot a + 18) \cdot 43^5 + (6 \cdot a + 13) \cdot 43^6 + (39 \cdot a + 31) \cdot 43^7 + (3 \cdot a + 15) \cdot 43^8 + O(43^9)$
47	$(43 \cdot a + 43) + (11 \cdot a + 23) \cdot 47 + (13 \cdot a + 15) \cdot 47^2 + (9 \cdot a + 31) \cdot 47^3 + (43 \cdot a + 36) \cdot 47^4 + (42 \cdot a + 33) \cdot 47^5 + (18 \cdot a + 16) \cdot 47^6 + (31 \cdot a + 27) \cdot 47^7 + (17 \cdot a + 46) \cdot 47^8 + O(47^9)$
53	$(8 \cdot a + 12) + (37 \cdot a + 29) \cdot 53 + (15 \cdot a + 23) \cdot 53^2 + (26 \cdot a + 39) \cdot 53^3 + (25 \cdot a + 11) \cdot 53^4 + (34 \cdot a + 25) \cdot 53^5 + (25 \cdot a + 38) \cdot 53^6 + (28 \cdot a + 42) \cdot 53^7 + (12 \cdot a + 18) \cdot 53^8 + O(53^9)$
61	$8 + 38 \cdot 61 + 40 \cdot 61^2 + 51 \cdot 61^3 + 48 \cdot 61^4 + 36 \cdot 61^5 + 41 \cdot 61^6 + 37 \cdot 61^7 + 39 \cdot 61^8 + O(61^9)$ $8 + 38 \cdot 61 + 40 \cdot 61^2 + 51 \cdot 61^3 + 48 \cdot 61^4 + 36 \cdot 61^5 + 41 \cdot 61^6 + 37 \cdot 61^7 + 39 \cdot 61^8 + O(61^9)$
67	$55 + 27 \cdot 67 + 37 \cdot 67^2 + 5 \cdot 67^4 + 25 \cdot 67^5 + 47 \cdot 67^6 + 40 \cdot 67^7 + 9 \cdot 67^8 + O(67^9)$
73	$(2 \cdot a + 4) + (36 \cdot a + 36) \cdot 73 + (54 \cdot a + 45) \cdot 73^2 + (40 \cdot a + 54) \cdot 73^3 + (36 \cdot a + 27) \cdot 73^4 + (67 \cdot a + 60) \cdot 73^5 + (9 \cdot a + 20) \cdot 73^6 + (21 \cdot a + 9) \cdot 73^7 + 2 \cdot 73^8 + O(73^9)$
79	$43 + 30 \cdot 79 + 47 \cdot 79^2 + 73 \cdot 79^3 + 43 \cdot 79^4 + 52 \cdot 79^5 + 66 \cdot 79^6 + 41 \cdot 79^7 + 9 \cdot 79^8 + O(79^9)$ $44 + 50 \cdot 79 + 79^2 + 71 \cdot 79^3 + 31 \cdot 79^4 + 31 \cdot 79^5 + 9 \cdot 79^6 + 25 \cdot 79^7 + 4 \cdot 79^8 + O(79^9)$
83	$(79 \cdot a + 65) + (7 \cdot a + 70) \cdot 83 + 46 \cdot a \cdot 83^2 + (8 \cdot a + 75) \cdot 83^3 + (65 \cdot a + 19) \cdot 83^4 + (50 \cdot a + 31) \cdot 83^5 + (16 \cdot a + 1) \cdot 83^6 + (53 \cdot a + 14) \cdot 83^7 + (35 \cdot a + 65) \cdot 83^8 + O(83^9)$
89	$74 + 29 \cdot 89 + 45 \cdot 89^2 + 77 \cdot 89^3 + 33 \cdot 89^4 + 69 \cdot 89^5 + 69 \cdot 89^6 + 75 \cdot 89^7 + 62 \cdot 89^8 + O(89^9)$ $11 + 73 \cdot 89 + 12 \cdot 89^2 + 49 \cdot 89^3 + 49 \cdot 89^4 + 76 \cdot 89^5 + 64 \cdot 89^6 + 75 \cdot 89^7 + 51 \cdot 89^8 + O(89^9)$

Table A.4.1: α factors for $N = 93$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
11	$3 \cdot 11^2 + 9 \cdot 11^3 + 6 \cdot 11^4 + 2 \cdot 11^5 + 6 \cdot 11^6 + 8 \cdot 11^8 + O(11^9)$
13	$9 + 13 + 6 \cdot 13^2 + 12 \cdot 13^3 + 7 \cdot 13^4 + 8 \cdot 13^5 + 8 \cdot 13^6 + 3 \cdot 13^7 + 6 \cdot 13^8 + O(13^9)$
23	$3 + 8 \cdot 23^2 + 19 \cdot 23^3 + 18 \cdot 23^4 + 15 \cdot 23^5 + 14 \cdot 23^7 + 7 \cdot 23^8 + O(23^9)$
29	$7 + 16 \cdot 29 + 28 \cdot 29^2 + 15 \cdot 29^3 + 22 \cdot 29^4 + 17 \cdot 29^5 + 26 \cdot 29^6 + 12 \cdot 29^7 + 21 \cdot 29^8 + O(29^9)$
37	$30 + 14 \cdot 37 + 21 \cdot 37^2 + 17 \cdot 37^3 + 24 \cdot 37^4 + 11 \cdot 37^5 + 19 \cdot 37^6 + 14 \cdot 37^7 + 32 \cdot 37^8 + O(37^9)$
43	$4 + 43 + 18 \cdot 43^3 + 2 \cdot 43^4 + 40 \cdot 43^5 + 26 \cdot 43^6 + 11 \cdot 43^7 + 11 \cdot 43^8 + O(43^9)$
47	$6 + 6 \cdot 47^2 + 9 \cdot 47^3 + 45 \cdot 47^4 + 34 \cdot 47^5 + 16 \cdot 47^6 + 16 \cdot 47^7 + 8 \cdot 47^8 + O(47^9)$
53	$1 + 4 \cdot 53 + 24 \cdot 53^2 + 39 \cdot 53^3 + 9 \cdot 53^4 + 39 \cdot 53^5 + 38 \cdot 53^6 + 19 \cdot 53^7 + 6 \cdot 53^8 + O(53^9)$
61	$16 + 33 \cdot 61 + 39 \cdot 61^2 + 3 \cdot 61^3 + 27 \cdot 61^4 + 56 \cdot 61^5 + 6 \cdot 61^6 + 39 \cdot 61^7 + 37 \cdot 61^8 + O(61^9)$
67	$29 + 51 \cdot 67 + 35 \cdot 67^2 + 62 \cdot 67^3 + 49 \cdot 67^4 + 53 \cdot 67^6 + 29 \cdot 67^7 + 44 \cdot 67^8 + O(67^9)$
73	$70 + 66 \cdot 73 + 20 \cdot 73^2 + 28 \cdot 73^3 + 28 \cdot 73^4 + 67 \cdot 73^5 + 15 \cdot 73^6 + 37 \cdot 73^7 + 6 \cdot 73^8 + O(73^9)$
79	$52 + 6 \cdot 79 + 7 \cdot 79^2 + 5 \cdot 79^3 + 21 \cdot 79^4 + 46 \cdot 79^5 + 18 \cdot 79^6 + 26 \cdot 79^7 + 45 \cdot 79^8 + O(79^9)$
83	$77 + 18 \cdot 83 + 24 \cdot 83^2 + 46 \cdot 83^3 + 24 \cdot 83^4 + 21 \cdot 83^5 + 41 \cdot 83^6 + 39 \cdot 83^7 + 6 \cdot 83^8 + O(83^9)$
89	$53 + 24 \cdot 89 + 14 \cdot 89^2 + 14 \cdot 89^3 + 74 \cdot 89^4 + 52 \cdot 89^5 + 28 \cdot 89^6 + 34 \cdot 89^7 + 53 \cdot 89^8 + O(89^9)$

Table A.4.2: ϵ factors for $N = 93$

A.5 $N = 103$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
11	$2 + 8 \cdot 11 + 7 \cdot 11^2 + 10 \cdot 11^3 + 5 \cdot 11^4 + 9 \cdot 11^5 + 11^6 + 6 \cdot 11^7 + 7 \cdot 11^8 + O(11^9)$
	$6 + 5 \cdot 11 + 10 \cdot 11^2 + 5 \cdot 11^3 + 7 \cdot 11^4 + 10 \cdot 11^5 + 10 \cdot 11^6 + 10 \cdot 11^7 + 11^8 + O(11^9)$
13	$(3 \cdot a + 3) + (4 \cdot a + 8) \cdot 13 + (2 \cdot a + 3) \cdot 13^2 + (4 \cdot a + 5) \cdot 13^3 + 10 \cdot a \cdot 13^4 + (5 \cdot a + 9) \cdot 13^5 + (6 \cdot a + 9) \cdot 13^6 + (4 \cdot a + 7) \cdot 13^7 + (a + 1) \cdot 13^8 + O(13^9)$
19	$16 + 3 \cdot 19^2 + 3 \cdot 19^3 + 8 \cdot 19^4 + 8 \cdot 19^5 + 19^6 + 11 \cdot 19^7 + O(19^8)$
	$8 + 10 \cdot 19^2 + 16 \cdot 19^3 + 4 \cdot 19^4 + 2 \cdot 19^5 + 12 \cdot 19^6 + 9 \cdot 19^7 + O(19^8)$
23	$(19 \cdot a + 17) + (13 \cdot a + 20) \cdot 23 + (7 \cdot a + 22) \cdot 23^2 + (14 \cdot a + 9) \cdot 23^3 + (21 \cdot a + 9) \cdot 23^4 + (a + 14) \cdot 23^5 + (22 \cdot a + 21) \cdot 23^6 + (14 \cdot a + 10) \cdot 23^7 + (13 \cdot a + 20) \cdot 23^8 + O(23^9)$
29	$8 + 2 \cdot 29 + 23 \cdot 29^2 + 4 \cdot 29^3 + 9 \cdot 29^4 + 13 \cdot 29^5 + 7 \cdot 29^6 + 20 \cdot 29^7 + 29^8 + O(29^9)$
	$15 + 13 \cdot 29 + 15 \cdot 29^2 + 26 \cdot 29^3 + 17 \cdot 29^4 + 7 \cdot 29^5 + 23 \cdot 29^6 + 7 \cdot 29^7 + 12 \cdot 29^8 + O(29^9)$
41	$30 + 41 + 29 \cdot 41^2 + 26 \cdot 41^3 + 38 \cdot 41^4 + 32 \cdot 41^5 + 17 \cdot 41^6 + 38 \cdot 41^7 + 16 \cdot 41^8 + O(41^9)$
	$11 + 39 \cdot 41 + 11 \cdot 41^2 + 14 \cdot 41^3 + 2 \cdot 41^4 + 8 \cdot 41^5 + 23 \cdot 41^6 + 2 \cdot 41^7 + 24 \cdot 41^8 + O(41^9)$
47	$(42 \cdot a + 38) + (17 \cdot a + 30) \cdot 47 + (21 \cdot a + 35) \cdot 47^2 + (6 \cdot a + 10) \cdot 47^3 + (5 \cdot a + 44) \cdot 47^4 + (5 \cdot a + 40) \cdot 47^5 + (38 \cdot a + 45) \cdot 47^6 + (40 \cdot a + 28) \cdot 47^7 + (14 \cdot a + 39) \cdot 47^8 + O(47^9)$
53	$(48 \cdot a + 41) + (38 \cdot a + 33) \cdot 53 + (39 \cdot a + 12) \cdot 53^2 + (6 \cdot a + 2) \cdot 53^3 + (24 \cdot a + 1) \cdot 53^4 + (33 \cdot a + 29) \cdot 53^5 + (15 \cdot a + 12) \cdot 53^6 + (42 \cdot a + 29) \cdot 53^7 + (6 \cdot a + 1) \cdot 53^8 + O(53^9)$
59	$41 + 28 \cdot 59 + 50 \cdot 59^2 + 3 \cdot 59^3 + 39 \cdot 59^4 + 17 \cdot 59^5 + 16 \cdot 59^6 + 26 \cdot 59^7 + 39 \cdot 59^8 + O(59^9)$
	$33 + 19 \cdot 59 + 38 \cdot 59^2 + 16 \cdot 59^3 + 32 \cdot 59^4 + 19 \cdot 59^5 + 48 \cdot 59^6 + 17 \cdot 59^7 + 56 \cdot 59^8 + O(59^9)$
61	$60 + 18 \cdot 61 + 27 \cdot 61^2 + 14 \cdot 61^3 + 34 \cdot 61^4 + 13 \cdot 61^5 + 6 \cdot 61^6 + 61^7 + 9 \cdot 61^8 + O(61^9)$
	$16 + 61 + 21 \cdot 61^2 + 57 \cdot 61^3 + 33 \cdot 61^4 + 46 \cdot 61^5 + 61^6 + 15 \cdot 61^7 + 13 \cdot 61^8 + O(61^9)$
71	$44 + 33 \cdot 71 + 53 \cdot 71^2 + 64 \cdot 71^3 + 38 \cdot 71^4 + 10 \cdot 71^5 + 37 \cdot 71^6 + 48 \cdot 71^7 + 28 \cdot 71^8 + O(71^9)$
	$30 + 42 \cdot 71 + 69 \cdot 71^2 + 65 \cdot 71^3 + 54 \cdot 71^4 + 62 \cdot 71^5 + 14 \cdot 71^6 + 27 \cdot 71^7 + 59 \cdot 71^8 + O(71^9)$
73	$(3 \cdot a + 70) + (39 \cdot a + 9) \cdot 73 + (37 \cdot a + 24) \cdot 73^2 + (25 \cdot a + 66) \cdot 73^3 + (25 \cdot a + 48) \cdot 73^4 + (68 \cdot a + 58) \cdot 73^5 + (7 \cdot a + 55) \cdot 73^6 + (65 \cdot a + 43) \cdot 73^7 + (40 \cdot a + 64) \cdot 73^8 + O(73^9)$
79	$32 + 41 \cdot 79 + 67 \cdot 79^2 + 74 \cdot 79^3 + 33 \cdot 79^4 + 48 \cdot 79^5 + 27 \cdot 79^6 + 21 \cdot 79^7 + 77 \cdot 79^8 + O(79^9)$
	$54 + 14 \cdot 79 + 61 \cdot 79^2 + 9 \cdot 79^3 + 4 \cdot 79^4 + 64 \cdot 79^5 + 41 \cdot 79^6 + 49 \cdot 79^7 + 72 \cdot 79^8 + O(79^9)$
83	$(7 \cdot a + 12) + (66 \cdot a + 73) \cdot 83 + (72 \cdot a + 2) \cdot 83^2 + (17 \cdot a + 37) \cdot 83^3 + (81 \cdot a + 31) \cdot 83^4 + (35 \cdot a + 2) \cdot 83^5 + (78 \cdot a + 7) \cdot 83^6 + (68 \cdot a + 6) \cdot 83^7 + (58 \cdot a + 5) \cdot 83^8 + O(83^9)$
89	$23 + 62 \cdot 89 + 36 \cdot 89^2 + 8 \cdot 89^3 + 66 \cdot 89^4 + 60 \cdot 89^5 + 61 \cdot 89^6 + 77 \cdot 89^7 + 65 \cdot 89^8 + O(89^9)$
	$48 + 71 \cdot 89 + 59 \cdot 89^2 + 84 \cdot 89^3 + 11 \cdot 89^4 + 45 \cdot 89^5 + 89^6 + 23 \cdot 89^7 + 17 \cdot 89^8 + O(89^9)$
97	$(6 \cdot a + 14) + (87 \cdot a + 58) \cdot 97 + (64 \cdot a + 92) \cdot 97^2 + (71 \cdot a + 66) \cdot 97^3 + (13 \cdot a + 43) \cdot 97^4 + (86 \cdot a + 81) \cdot 97^5 + (23 \cdot a + 54) \cdot 97^6 + (62 \cdot a + 54) \cdot 97^7 + (76 \cdot a + 52) \cdot 97^8 + O(97^9)$

Table A.5.1: α factors for $N = 103$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
11	$3 + 10 \cdot 11 + 9 \cdot 11^2 + 7 \cdot 11^3 + 10 \cdot 11^4 + 8 \cdot 11^5 + 9 \cdot 11^6 + 9 \cdot 11^7 + 10 \cdot 11^8 + O(11^9)$
13	$4 + 7 \cdot 13 + 9 \cdot 13^2 + 6 \cdot 13^3 + 6 \cdot 13^4 + 12 \cdot 13^5 + 4 \cdot 13^6 + 5 \cdot 13^7 + 8 \cdot 13^8 + O(13^9)$
19	$4 + 14 \cdot 19^2 + 3 \cdot 19^3 + 4 \cdot 19^4 + 14 \cdot 19^5 + 11 \cdot 19^6 + 13 \cdot 19^7 + 7 \cdot 19^8 + O(19^9)$
23	$12 + 18 \cdot 23 + 17 \cdot 23^2 + 13 \cdot 23^3 + 5 \cdot 23^4 + 6 \cdot 23^5 + 5 \cdot 23^6 + 13 \cdot 23^7 + 13 \cdot 23^8 + O(23^9)$
29	$13 + 29 + 22 \cdot 29^2 + 3 \cdot 29^3 + 6 \cdot 29^4 + 2 \cdot 29^5 + 21 \cdot 29^6 + 14 \cdot 29^8 + O(29^9)$
41	$33 + 30 \cdot 41 + 15 \cdot 41^2 + 15 \cdot 41^3 + 12 \cdot 41^4 + 17 \cdot 41^5 + 9 \cdot 41^6 + 27 \cdot 41^7 + 8 \cdot 41^8 + O(41^9)$
47	$16 + 12 \cdot 47 + 29 \cdot 47^2 + 2 \cdot 47^3 + 12 \cdot 47^4 + 20 \cdot 47^5 + 30 \cdot 47^6 + 3 \cdot 47^7 + 9 \cdot 47^8 + O(47^9)$
53	$46 + 15 \cdot 53 + 29 \cdot 53^2 + 6 \cdot 53^3 + 43 \cdot 53^4 + 38 \cdot 53^5 + 3 \cdot 53^6 + 40 \cdot 53^7 + 22 \cdot 53^8 + O(53^9)$
59	$35 + 12 \cdot 59 + 6 \cdot 59^2 + 24 \cdot 59^3 + 9 \cdot 59^4 + 14 \cdot 59^5 + 3 \cdot 59^6 + 54 \cdot 59^7 + 27 \cdot 59^8 + O(59^9)$
61	$14 + 52 \cdot 61 + 36 \cdot 61^2 + 9 \cdot 61^3 + 48 \cdot 61^4 + 31 \cdot 61^5 + 3 \cdot 61^6 + 29 \cdot 61^7 + 35 \cdot 61^8 + O(61^9)$
71	$3 + 46 \cdot 71 + 67 \cdot 71^2 + 35 \cdot 71^3 + 60 \cdot 71^4 + 68 \cdot 71^5 + 3 \cdot 71^6 + 35 \cdot 71^7 + 19 \cdot 71^8 + O(71^9)$
73	$27 + 10 \cdot 73 + 9 \cdot 73^2 + 39 \cdot 73^3 + 41 \cdot 73^4 + 9 \cdot 73^5 + 60 \cdot 73^6 + 7 \cdot 73^7 + 48 \cdot 73^8 + O(73^9)$
79	$31 + 69 \cdot 79 + 51 \cdot 79^3 + 63 \cdot 79^4 + 13 \cdot 79^5 + 36 \cdot 79^6 + 70 \cdot 79^7 + 56 \cdot 79^8 + O(79^9)$
83	$36 + 59 \cdot 83 + 55 \cdot 83^2 + 13 \cdot 83^3 + 9 \cdot 83^4 + 11 \cdot 83^5 + 73 \cdot 83^6 + 54 \cdot 83^7 + 80 \cdot 83^8 + O(83^9)$
89	$16 + 34 \cdot 89 + 74 \cdot 89^2 + 48 \cdot 89^3 + 33 \cdot 89^4 + 84 \cdot 89^5 + 41 \cdot 89^6 + 45 \cdot 89^7 + 16 \cdot 89^8 + O(89^9)$
97	$62 + 69 \cdot 97 + 31 \cdot 97^2 + 69 \cdot 97^3 + 68 \cdot 97^4 + 63 \cdot 97^5 + 58 \cdot 97^6 + 3 \cdot 97^7 + 47 \cdot 97^8 + O(97^9)$

Table A.5.2: ϵ factors for $N = 103$

A.6 $N = 107$

The quadratic field K_f is generated by a root a of $x^2 + x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
13	$7 + 10 \cdot 13 + 2 \cdot 13^2 + 10 \cdot 13^4 + 10 \cdot 13^5 + 2 \cdot 13^6 + 2 \cdot 13^8 + O(13^9)$
17	$(a + 16) + (a + 1) \cdot 17 + (8 \cdot a + 13) \cdot 17^2 + (8 \cdot a + 8) \cdot 17^3 + 4 \cdot a \cdot 17^4 + (9 \cdot a + 13) \cdot 17^5 + (2 \cdot a + 13) \cdot 17^6 + (4 \cdot a + 10) \cdot 17^7 + (15 \cdot a + 4) \cdot 17^8 + O(17^9)$
19	$9 + 15 \cdot 19 + 8 \cdot 19^2 + 11 \cdot 19^3 + 9 \cdot 19^4 + 17 \cdot 19^5 + 12 \cdot 19^6 + 3 \cdot 19^7 + O(19^9)$
	$12 + 16 \cdot 19 + 14 \cdot 19^2 + 9 \cdot 19^3 + 9 \cdot 19^4 + 5 \cdot 19^5 + 14 \cdot 19^6 + 13 \cdot 19^7 + 2 \cdot 19^8 + O(19^9)$
29	$(34 \cdot a + 29) + (18 \cdot a + 29) \cdot 37 + (20 \cdot a + 15) \cdot 37^2 + (24 \cdot a + 31) \cdot 37^3 + (22 \cdot a + 14) \cdot 37^4 + 22 \cdot 37^5 + (28 \cdot a + 26) \cdot 37^6 + (23 \cdot a + 36) \cdot 37^7 + (31 \cdot a + 31) \cdot 37^8 + O(37^9)$
41	$18 + 28 \cdot 41 + 20 \cdot 41^2 + 19 \cdot 41^3 + 25 \cdot 41^4 + 11 \cdot 41^5 + 6 \cdot 41^6 + 27 \cdot 41^7 + 29 \cdot 41^8 + O(41^9)$
	$33 + 32 \cdot 41 + 41^2 + 24 \cdot 41^3 + 11 \cdot 41^4 + 3 \cdot 41^5 + 36 \cdot 41^6 + 16 \cdot 41^7 + 39 \cdot 41^8 + O(41^9)$
43	$(3 \cdot a + 6) + (29 \cdot a + 14) \cdot 43 + (6 \cdot a + 17) \cdot 43^2 + (18 \cdot a + 14) \cdot 43^3 + (15 \cdot a + 32) \cdot 43^4 + (14 \cdot a + 27) \cdot 43^5 + (5 \cdot a + 1) \cdot 43^6 + (36 \cdot a + 40) \cdot 43^7 + (34 \cdot a + 41) \cdot 43^8 + O(43^9)$
47	$(2 \cdot a + 41) + (15 \cdot a + 12) \cdot 47 + (23 \cdot a + 34) \cdot 47^2 + (19 \cdot a + 11) \cdot 47^3 + (43 \cdot a + 36) \cdot 47^4 + (37 \cdot a + 20) \cdot 47^5 + (44 \cdot a + 37) \cdot 47^6 + (36 \cdot a + 14) \cdot 47^7 + (40 \cdot a + 14) \cdot 47^8 + O(47^9)$
59	$8 + 13 \cdot 59 + 48 \cdot 59^2 + 4 \cdot 59^3 + 4 \cdot 59^4 + 22 \cdot 59^5 + 51 \cdot 59^6 + 22 \cdot 59^7 + 50 \cdot 59^8 + O(59^9)$
	$54 + 20 \cdot 59 + 33 \cdot 59^3 + 46 \cdot 59^4 + 50 \cdot 59^5 + 41 \cdot 59^6 + 42 \cdot 59^7 + 35 \cdot 59^8 + O(59^9)$
61	$2 + 12 \cdot 61 + 25 \cdot 61^2 + 11 \cdot 61^3 + 7 \cdot 61^4 + 57 \cdot 61^5 + 17 \cdot 61^6 + 53 \cdot 61^7 + 44 \cdot 61^8 + O(61^9)$
	$46 + 13 \cdot 61 + 45 \cdot 61^2 + 22 \cdot 61^3 + 9 \cdot 61^4 + 30 \cdot 61^5 + 53 \cdot 61^6 + 2 \cdot 61^7 + 54 \cdot 61^8 + O(61^9)$
67	$(65 \cdot a + 61) + (19 \cdot a + 26) \cdot 67 + (64 \cdot a + 10) \cdot 67^2 + (39 \cdot a + 37) \cdot 67^3 + (20 \cdot a + 42) \cdot 67^4 + (24 \cdot a + 48) \cdot 67^5 + (66 \cdot a + 54) \cdot 67^6 + (18 \cdot a + 4) \cdot 67^7 + (16 \cdot a + 24) \cdot 67^8 + O(67^9)$
71	$64 + 47 \cdot 71 + 54 \cdot 71^2 + 32 \cdot 71^3 + 2 \cdot 71^4 + 27 \cdot 71^5 + 36 \cdot 71^6 + 51 \cdot 71^7 + 34 \cdot 71^8 + O(71^9)$
	$4 + 66 \cdot 71 + 8 \cdot 71^2 + 37 \cdot 71^3 + 51 \cdot 71^4 + 69 \cdot 71^5 + 55 \cdot 71^6 + 68 \cdot 71^7 + 20 \cdot 71^8 + O(71^9)$
79	$10 + 46 \cdot 79 + 37 \cdot 79^2 + 18 \cdot 79^3 + 46 \cdot 79^4 + 66 \cdot 79^5 + 26 \cdot 79^6 + 64 \cdot 79^7 + 58 \cdot 79^8 + O(79^9)$
	$70 + 68 \cdot 79 + 3 \cdot 79^2 + 4 \cdot 79^3 + 18 \cdot 79^4 + 70 \cdot 79^5 + 19 \cdot 79^6 + 70 \cdot 79^7 + 63 \cdot 79^8 + O(79^9)$
83	$80 \cdot a + (27 \cdot a + 28) \cdot 83 + (52 \cdot a + 9) \cdot 83^2 + (10 \cdot a + 71) \cdot 83^3 + (47 \cdot a + 65) \cdot 83^4 + (15 \cdot a + 64) \cdot 83^5 + (41 \cdot a + 49) \cdot 83^6 + (33 \cdot a + 49) \cdot 83^7 + (71 \cdot a + 6) \cdot 83^8 + O(83^9)$

Table A.6.1: α factors for $N = 107$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
13	$1 + 13 + 13^2 + 12 \cdot 13^3 + 12 \cdot 13^4 + 3 \cdot 13^5 + 7 \cdot 13^6 + 11 \cdot 13^7 + 6 \cdot 13^8 + O(13^9)$
17	$8 + 13 \cdot 17 + 3 \cdot 17^2 + 11 \cdot 17^3 + 14 \cdot 17^4 + 4 \cdot 17^5 + 16 \cdot 17^6 + 15 \cdot 17^7 + 12 \cdot 17^8 + O(17^9)$
19	$4 + 11 \cdot 19 + 6 \cdot 19^2 + 15 \cdot 19^3 + 14 \cdot 19^4 + 3 \cdot 19^5 + 3 \cdot 19^6 + 13 \cdot 19^7 + 11 \cdot 19^8 + O(19^9)$
37	$10 + 2 \cdot 37 + 14 \cdot 37^2 + 22 \cdot 37^3 + 15 \cdot 37^4 + 20 \cdot 37^5 + 9 \cdot 37^6 + 5 \cdot 37^7 + 19 \cdot 37^8 + O(37^9)$
41	$33 + 35 \cdot 41 + 29 \cdot 41^2 + 14 \cdot 41^3 + 22 \cdot 41^4 + 4 \cdot 41^5 + 34 \cdot 41^6 + 4 \cdot 41^7 + 21 \cdot 41^8 + O(41^9)$
43	$17 + 19 \cdot 43 + 33 \cdot 43^2 + 35 \cdot 43^3 + 31 \cdot 43^5 + 20 \cdot 43^6 + 5 \cdot 43^7 + 34 \cdot 43^8 + O(43^9)$
47	$16 + 41 \cdot 47 + 46 \cdot 47^2 + 26 \cdot 47^3 + 3 \cdot 47^4 + 33 \cdot 47^5 + 30 \cdot 47^6 + 7 \cdot 47^7 + 23 \cdot 47^8 + O(47^9)$
59	$16 + 21 \cdot 59 + 53 \cdot 59^2 + 43 \cdot 59^3 + 24 \cdot 59^4 + 3 \cdot 59^5 + 43 \cdot 59^6 + 26 \cdot 59^7 + 52 \cdot 59^8 + O(59^9)$
61	$48 + 47 \cdot 61 + 17 \cdot 61^2 + 35 \cdot 61^3 + 5 \cdot 61^4 + 41 \cdot 61^5 + 34 \cdot 61^6 + 47 \cdot 61^7 + 39 \cdot 61^8 + O(61^9)$
67	$22 + 53 \cdot 67 + 3 \cdot 67^2 + 45 \cdot 67^3 + 10 \cdot 67^4 + 47 \cdot 67^5 + 35 \cdot 67^6 + 49 \cdot 67^7 + 65 \cdot 67^8 + O(67^9)$
71	$50 + 25 \cdot 71 + 15 \cdot 71^2 + 12 \cdot 71^3 + 49 \cdot 71^4 + 49 \cdot 71^5 + 50 \cdot 71^6 + 32 \cdot 71^7 + 67 \cdot 71^8 + O(71^9)$
79	$1 + 64 \cdot 79 + 74 \cdot 79^2 + 22 \cdot 79^3 + 35 \cdot 79^4 + 28 \cdot 79^5 + 14 \cdot 79^6 + 33 \cdot 79^7 + 73 \cdot 79^8 + O(79^9)$
83	$64 + 61 \cdot 83 + 61 \cdot 83^2 + 26 \cdot 83^3 + 50 \cdot 83^4 + 6 \cdot 83^5 + 42 \cdot 83^6 + 4 \cdot 83^7 + 51 \cdot 83^8 + O(83^9)$

Table A.6.2: ϵ factors for $N = 107$

A.7 $N = 115$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
7	$(5 \cdot a + 3) + (3 \cdot a + 3) \cdot 7 + (5 \cdot a + 4) \cdot 7^2 + 3 \cdot 7^3 + (4 \cdot a + 5) \cdot 7^4 + (6 \cdot a + 4) \cdot 7^5 + 5 \cdot a \cdot 7^6 + (6 \cdot a + 6) \cdot 7^7 + (a + 5) \cdot 7^8 + O(7^9)$
11	$6 + 4 \cdot 11 + 7 \cdot 11^2 + 5 \cdot 11^3 + 4 \cdot 11^4 + 9 \cdot 11^5 + 7 \cdot 11^6 + 7 \cdot 11^7 + 7 \cdot 11^8 + O(11^9), 3 + 3 \cdot 11^2 + 5 \cdot 11^3 + 3 \cdot 11^4 + 10 \cdot 11^5 + 8 \cdot 11^7 + 9 \cdot 11^8 + O(11^9)$
17	$(13 \cdot a + 9) + (12 \cdot a + 12) \cdot 17 + (3 \cdot a + 16) \cdot 17^2 + (6 \cdot a + 4) \cdot 17^3 + (5 \cdot a + 8) \cdot 17^4 + (4 \cdot a + 16) \cdot 17^5 + (6 \cdot a + 13) \cdot 17^6 + (16 \cdot a + 2) \cdot 17^7 + (12 \cdot a + 5) \cdot 17^8 + O(17^9)$
19	$12 + 16 \cdot 19 + 14 \cdot 19^2 + 9 \cdot 19^3 + 9 \cdot 19^4 + 5 \cdot 19^5 + 14 \cdot 19^6 + 13 \cdot 19^7 + 2 \cdot 19^8 + O(19^9), 9 + 15 \cdot 19 + 8 \cdot 19^2 + 11 \cdot 19^3 + 9 \cdot 19^4 + 17 \cdot 19^5 + 12 \cdot 19^6 + 3 \cdot 19^7 + O(19^9)$
37	$(6 \cdot a + 6) + (6 \cdot a + 12) \cdot 37 + (31 \cdot a + 19) \cdot 37^2 + (4 \cdot a + 33) \cdot 37^3 + (20 \cdot a + 1) \cdot 37^4 + (16 \cdot a + 26) \cdot 37^5 + (11 \cdot a + 6) \cdot 37^6 + (25 \cdot a + 1) \cdot 37^7 + (26 \cdot a + 6) \cdot 37^8 + O(37^9)$
43	$(37 \cdot a + 31) + (35 \cdot a + 35) \cdot 43 + (37 \cdot a + 36) \cdot 43^2 + (42 \cdot a + 11) \cdot 43^3 + (20 \cdot a + 33) \cdot 43^4 + (18 \cdot a + 18) \cdot 43^5 + (6 \cdot a + 13) \cdot 43^6 + (39 \cdot a + 31) \cdot 43^7 + (3 \cdot a + 15) \cdot 43^8 + O(43^9)$
53	$47 + 8 \cdot 53 + 31 \cdot 53^2 + 22 \cdot 53^3 + 42 \cdot 53^4 + 30 \cdot 53^5 + 19 \cdot 53^6 + 6 \cdot 53^7 + 8 \cdot 53^8 + O(53^9)$
59	$27 + 38 \cdot 59 + 57 \cdot 59^2 + 22 \cdot 59^3 + 51 \cdot 59^4 + 24 \cdot 59^5 + 45 \cdot 59^6 + 3 \cdot 59^7 + 14 \cdot 59^8 + O(59^9)$ $32 + 20 \cdot 59 + 59^2 + 36 \cdot 59^3 + 7 \cdot 59^4 + 34 \cdot 59^5 + 13 \cdot 59^6 + 55 \cdot 59^7 + 44 \cdot 59^8 + O(59^9)$
61	$9 + 8 \cdot 61 + 16 \cdot 61^2 + 52 \cdot 61^3 + 52 \cdot 61^4 + 12 \cdot 61^5 + 45 \cdot 61^6 + 33 \cdot 61^7 + 58 \cdot 61^8 + O(61^9)$ $54 + 53 \cdot 61 + 15 \cdot 61^2 + 13 \cdot 61^3 + 32 \cdot 61^4 + 8 \cdot 61^5 + 8 \cdot 61^6 + 60 \cdot 61^7 + 40 \cdot 61^8 + O(61^9)$
67	$(61 \cdot a + 61) + (55 \cdot a + 44) \cdot 67 + (6 \cdot a + 22) \cdot 67^2 + (39 \cdot a + 53) \cdot 67^3 + (11 \cdot a + 44) \cdot 67^4 + (2 \cdot a + 32) \cdot 67^5 + (2 \cdot a + 33) \cdot 67^6 + 19 \cdot 67^7 + (60 \cdot a + 4) \cdot 67^8 + O(67^9)$
79	$70 + 53 \cdot 79 + 76 \cdot 79^2 + 45 \cdot 79^3 + 57 \cdot 79^4 + 77 \cdot 79^5 + 26 \cdot 79^6 + 43 \cdot 79^7 + 38 \cdot 79^8 + O(79^9)$ $31 + 18 \cdot 79 + 10 \cdot 79^2 + 41 \cdot 79^3 + 23 \cdot 79^4 + 32 \cdot 79^5 + 39 \cdot 79^6 + 56 \cdot 79^7 + 77 \cdot 79^8 + O(79^9)$
83	$(4 \cdot a + 4) + (62 \cdot a + 41) \cdot 83 + (7 \cdot a + 50) \cdot 83^2 + (14 \cdot a + 42) \cdot 83^3 + (52 \cdot a + 19) \cdot 83^4 + (80 \cdot a + 61) \cdot 83^5 + (19 \cdot a + 6) \cdot 83^6 + (11 \cdot a + 13) \cdot 83^7 + (76 \cdot a + 5) \cdot 83^8 + O(83^9)$
89	$24 + 2 \cdot 89 + 75 \cdot 89^2 + 26 \cdot 89^3 + 59 \cdot 89^4 + 68 \cdot 89^5 + 76 \cdot 89^6 + 66 \cdot 89^7 + 66 \cdot 89^8 + O(89^9)$ $75 + 41 \cdot 89 + 9 \cdot 89^2 + 32 \cdot 89^3 + 7 \cdot 89^4 + 2 \cdot 89^5 + 58 \cdot 89^6 + 14 \cdot 89^7 + 43 \cdot 89^8 + O(89^9)$
97	$(10 \cdot a + 20) + (29 \cdot a + 29) \cdot 97 + (74 \cdot a + 32) \cdot 97^2 + (11 \cdot a + 74) \cdot 97^3 + (50 \cdot a + 80) \cdot 97^4 + (67 \cdot a + 48) \cdot 97^5 + (18 \cdot a + 92) \cdot 97^6 + (23 \cdot a + 27) \cdot 97^7 + (93 \cdot a + 33) \cdot 97^8 + O(97^9)$

Table A.7.1: α factors for $N = 115$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
7	$4+5\cdot 7+7^2+3\cdot 7^3+4\cdot 7^4+4\cdot 7^5+7^6+7^7+6\cdot 7^8+O(7^9)$
11	$9+4\cdot 11+5\cdot 11^2+7\cdot 11^3+4\cdot 11^4+3\cdot 11^5+9\cdot 11^6+2\cdot 11^7+2\cdot 11^8+O(11^9)$
17	$2+4\cdot 17+6\cdot 17^2+8\cdot 17^3+12\cdot 17^5+6\cdot 17^7+6\cdot 17^8+O(17^9)$
19	$4+11\cdot 19+6\cdot 19^2+15\cdot 19^3+14\cdot 19^4+3\cdot 19^5+3\cdot 19^6+13\cdot 19^7+11\cdot 19^8+O(19^9)$
37	$27+14\cdot 37+30\cdot 37^2+11\cdot 37^3+30\cdot 37^4+37^5+17\cdot 37^6+5\cdot 37^7+37^8+O(37^9)$
43	$4+43+18\cdot 43^3+2\cdot 43^4+40\cdot 43^5+26\cdot 43^6+11\cdot 43^7+11\cdot 43^8+O(43^9)$
53	$36+9\cdot 53+44\cdot 53^2+27\cdot 53^3+5\cdot 53^4+31\cdot 53^5+53^6+21\cdot 53^7+43\cdot 53^8+O(53^9)$
49	$48+58\cdot 59+50\cdot 59^2+55\cdot 59^3+47\cdot 59^4+36\cdot 59^5+6\cdot 59^6+45\cdot 59^7+37\cdot 59^8+O(59^9)$
61	$48+48\cdot 61+47\cdot 61^2+29\cdot 61^3+12\cdot 61^4+34\cdot 61^5+54\cdot 61^6+45\cdot 61^7+16\cdot 61^8+O(61^9)$
67	$9+66\cdot 67+59\cdot 67^2+5\cdot 67^3+17\cdot 67^4+40\cdot 67^5+7\cdot 67^6+64\cdot 67^7+49\cdot 67^8+O(67^9)$
79	$22+8\cdot 79+18\cdot 79^2+13\cdot 79^3+57\cdot 79^4+40\cdot 79^5+47\cdot 79^6+44\cdot 79^7+60\cdot 79^8+O(79^9)$
83	$41+54\cdot 83+8\cdot 83^2+69\cdot 83^3+61\cdot 83^4+62\cdot 83^5+23\cdot 83^6+82\cdot 83^7+17\cdot 83^8+O(83^9)$
89	$25+28\cdot 89+36\cdot 89^2+24\cdot 89^3+33\cdot 89^4+5\cdot 89^5+65\cdot 89^6+32\cdot 89^7+25\cdot 89^8+O(89^9)$
97	$16+68\cdot 97+10\cdot 97^2+89\cdot 97^3+44\cdot 97^4+97^5+52\cdot 97^6+68\cdot 97^7+17\cdot 97^8+O(97^9)$

Table A.7.2: ϵ factors for $N = 115$

A.8 $N = 125, A$

The quadratic field K_f is generated by a root a of $x^2 + x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
37	$(31 \cdot a+31)+(30 \cdot a+36) \cdot 37+(5 \cdot a+30) \cdot 37^2+(32 \cdot a+23) \cdot 37^3+(16 \cdot a+35) \cdot 37^4+(20 \cdot a+29) \cdot 37^5+(25 \cdot a+20) \cdot 37^6+(11 \cdot a+24) \cdot 37^7+(10 \cdot a+26) \cdot 37^8+O(37^9)$
47	$(7 \cdot a+3)+(23 \cdot a+40) \cdot 47+(20 \cdot a+25) \cdot 47^2+(8 \cdot a+41) \cdot 47^3+(20 \cdot a+34) \cdot 47^4+(24 \cdot a+36) \cdot 47^5+(10 \cdot a+24) \cdot 47^6+(12 \cdot a+45) \cdot 47^7+(12 \cdot a+13) \cdot 47^8+O(47^9)$
53	$(52 \cdot a+3)+(23 \cdot a+43) \cdot 53+(43 \cdot a+18) \cdot 53^2+(4 \cdot a+1) \cdot 53^3+(7 \cdot a+28) \cdot 53^4+(41 \cdot a+16) \cdot 53^5+(3 \cdot a+20) \cdot 53^6+(9 \cdot a+12) \cdot 53^7+(14 \cdot a+26) \cdot 53^8+O(53^9)$
59	$49+22 \cdot 59+36 \cdot 59^2+35 \cdot 59^3+26 \cdot 59^4+43 \cdot 59^5+28 \cdot 59^6+48 \cdot 59^7+24 \cdot 59^8+O(59^9)$ $25+16 \cdot 59+28 \cdot 59^2+55 \cdot 59^3+7 \cdot 59^4+28 \cdot 59^5+8 \cdot 59^6+36 \cdot 59^7+21 \cdot 59^8+O(59^9)$
61	$26+16 \cdot 61+46 \cdot 61^2+14 \cdot 61^3+12 \cdot 61^5+29 \cdot 61^6+56 \cdot 61^7+32 \cdot 61^8+O(61^9)$ $34+42 \cdot 61+57 \cdot 61^2+31 \cdot 61^3+8 \cdot 61^4+41 \cdot 61^5+47 \cdot 61^6+31 \cdot 61^7+51 \cdot 61^8+O(61^9)$
67	$(3 \cdot a+58)+(65 \cdot a+58) \cdot 67+(28 \cdot a+61) \cdot 67^2+(54 \cdot a+58) \cdot 67^3+(32 \cdot a+22) \cdot 67^4+(28 \cdot a+7) \cdot 67^5+(7 \cdot a+62) \cdot 67^6+(37 \cdot a+49) \cdot 67^7+(25 \cdot a+3) \cdot 67^8+O(67^9)$
73	$(70 \cdot a+70)+(48 \cdot a+72) \cdot 73+(67 \cdot a+26) \cdot 73^2+(61 \cdot a+69) \cdot 73^3+(61 \cdot a+25) \cdot 73^4+(13 \cdot a+35) \cdot 73^5+(10 \cdot a+50) \cdot 73^6+(29 \cdot a+20) \cdot 73^7+(38 \cdot a+26) \cdot 73^8+O(73^9)$
83	$(79 \cdot a+77)+40 \cdot 83+(25 \cdot a+28) \cdot 83^2+(69 \cdot a+2) \cdot 83^3+(55 \cdot a+59) \cdot 83^4+(38 \cdot a+12) \cdot 83^5+(12 \cdot a+38) \cdot 83^6+(24 \cdot a+9) \cdot 83^7+(58 \cdot a+9) \cdot 83^8+O(83^9)$
89	$25+23 \cdot 89+47 \cdot 89^2+46 \cdot 89^3+56 \cdot 89^4+84 \cdot 89^5+88 \cdot 89^6+26 \cdot 89^7+8 \cdot 89^8+O(89^9)$ $64+65 \cdot 89+41 \cdot 89^2+42 \cdot 89^3+32 \cdot 89^4+4 \cdot 89^5+62 \cdot 89^7+80 \cdot 89^8+O(89^9)$
97	$(94 \cdot a+3)+(31 \cdot a+64) \cdot 97+(82 \cdot a+24) \cdot 97^2+(45 \cdot a+3) \cdot 97^3+(82 \cdot a+89) \cdot 97^4+(52 \cdot a+44) \cdot 97^5+(2 \cdot a+15) \cdot 97^6+(17 \cdot a+34) \cdot 97^7+95 \cdot 97^8+O(97^9)$

Table A.8.1: α factors for $N = 125, A$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
37	$27+14 \cdot 37+30 \cdot 37^2+11 \cdot 37^3+30 \cdot 37^4+37^5+17 \cdot 37^6+5 \cdot 37^7+37^8+O(37^9)$
47	$18+45 \cdot 47+17 \cdot 47^2+18 \cdot 47^3+16 \cdot 47^4+8 \cdot 47^5+35 \cdot 47^6+39 \cdot 47^7+23 \cdot 47^8+O(47^9)$
53	$37+13 \cdot 53+18 \cdot 53^2+3 \cdot 53^4+17 \cdot 53^5+36 \cdot 53^6+38 \cdot 53^7+20 \cdot 53^8+O(53^9)$
59	$4+19 \cdot 59+12 \cdot 59^2+17 \cdot 59^3+8 \cdot 59^4+11 \cdot 59^5+48 \cdot 59^7+26 \cdot 59^8+O(59^9)$
61	$9+9 \cdot 61+18 \cdot 61^2+59 \cdot 61^3+20 \cdot 61^4+30 \cdot 61^5+49 \cdot 61^6+42 \cdot 61^7+28 \cdot 61^8+O(61^9)$
67	$23+62 \cdot 67+47 \cdot 67^2+61 \cdot 67^3+57 \cdot 67^4+25 \cdot 67^5+9 \cdot 67^6+9 \cdot 67^7+21 \cdot 67^8+O(67^9)$
73	$67+13 \cdot 73+60 \cdot 73^2+13 \cdot 73^3+51 \cdot 73^4+64 \cdot 73^5+44 \cdot 73^6+30 \cdot 73^7+27 \cdot 73^8+O(73^9)$
83	$69+5 \cdot 83+24 \cdot 83^2+68 \cdot 83^3+77 \cdot 83^4+81 \cdot 83^5+40 \cdot 83^6+62 \cdot 83^7+77 \cdot 83^8+O(83^9)$
89	$67+66 \cdot 89+77 \cdot 89^2+77 \cdot 89^3+70 \cdot 89^4+59 \cdot 89^5+73 \cdot 89^7+72 \cdot 89^8+O(89^9)$
97	$6+69 \cdot 97+63 \cdot 97^2+61 \cdot 97^3+83 \cdot 97^4+30 \cdot 97^5+69 \cdot 97^6+81 \cdot 97^7+77 \cdot 97^8+O(97^9)$

Table A.8.2: ϵ factors for $N = 125, A$

A.9 $N = 133, B$

The quadratic field K_f is generated by a root a of $x^2 + 3x + 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
17	$(3 \cdot a + 3) + (11 \cdot a + 5) \cdot 17 + (15 \cdot a + 2) \cdot 17^2 + (4 \cdot a + 8) \cdot 17^3 + (4 \cdot a + 7) \cdot 17^4 + (2 \cdot a + 8) \cdot 17^5 + (11 \cdot a + 10) \cdot 17^6 + (12 \cdot a + 14) \cdot 17^7 + (16 \cdot a + 11) \cdot 17^8 + O(17^9)$
29	$1 + 20 \cdot 29 + 24 \cdot 29^2 + 24 \cdot 29^4 + 6 \cdot 29^5 + 14 \cdot 29^6 + 2 \cdot 29^7 + 15 \cdot 29^8 + O(29^9)$ $19 + 10 \cdot 29 + 4 \cdot 29^2 + 9 \cdot 29^3 + 6 \cdot 29^4 + 6 \cdot 29^5 + 18 \cdot 29^6 + 13 \cdot 29^7 + 13 \cdot 29^8 + O(29^9)$
31	$27 + 19 \cdot 31 + 26 \cdot 31^2 + 2 \cdot 31^3 + 12 \cdot 31^4 + 15 \cdot 31^5 + 4 \cdot 31^6 + 12 \cdot 31^7 + 3 \cdot 31^8 + O(31^9)$ $9 + 12 \cdot 31 + 18 \cdot 31^2 + 31^3 + 13 \cdot 31^4 + 13 \cdot 31^5 + 8 \cdot 31^6 + 15 \cdot 31^7 + 4 \cdot 31^8 + O(31^9)$
41	$8 + 27 \cdot 41 + 2 \cdot 41^2 + 20 \cdot 41^3 + 23 \cdot 41^4 + 38 \cdot 41^5 + 39 \cdot 41^6 + 4 \cdot 41^7 + 7 \cdot 41^8 + O(41^9)$ $36 + 10 \cdot 41 + 20 \cdot 41^2 + 20 \cdot 41^3 + 19 \cdot 41^4 + 23 \cdot 41^5 + 37 \cdot 41^6 + 6 \cdot 41^7 + 28 \cdot 41^8 + O(41^9)$
43	$41 + 21 \cdot 43 + 5 \cdot 43^2 + 8 \cdot 43^3 + 19 \cdot 43^4 + 32 \cdot 43^5 + 24 \cdot 43^6 + 42 \cdot 43^7 + 16 \cdot 43^8 + O(43^9)$
53	$(48 \cdot a + 41) + (38 \cdot a + 33) \cdot 53 + (39 \cdot a + 12) \cdot 53^2 + (6 \cdot a + 2) \cdot 53^3 + (24 \cdot a + 1) \cdot 53^4 + (33 \cdot a + 29) \cdot 53^5 + (15 \cdot a + 12) \cdot 53^6 + (42 \cdot a + 29) \cdot 53^7 + (6 \cdot a + 1) \cdot 53^8 + O(53^9)$
67	$(58 \cdot a + 50) + (39 \cdot a + 36) \cdot 67 + (58 \cdot a + 9) \cdot 67^2 + (48 \cdot a + 44) \cdot 67^3 + (39 \cdot a + 18) \cdot 67^4 + (20 \cdot a + 27) \cdot 67^5 + (51 \cdot a + 20) \cdot 67^6 + (63 \cdot a + 32) \cdot 67^7 + (6 \cdot a + 57) \cdot 67^8 + O(67^9)$
73	$(3 \cdot a + 12) + (39 \cdot a + 34) \cdot 73 + (37 \cdot a + 15) \cdot 73^2 + (25 \cdot a + 10) \cdot 73^3 + (25 \cdot a + 27) \cdot 73^4 + 68 \cdot a \cdot 73^5 + (7 \cdot a + 41) \cdot 73^6 + (65 \cdot a + 5) \cdot 73^7 + (40 \cdot a + 58) \cdot 73^8 + O(73^9)$
79	$69 + 7 \cdot 79 + 30 \cdot 79^2 + 24 \cdot 79^3 + 26 \cdot 79^4 + 21 \cdot 79^5 + 36 \cdot 79^6 + 3 \cdot 79^7 + 6 \cdot 79^8 + O(79^9)$ $69 + 7 \cdot 79 + 30 \cdot 79^2 + 24 \cdot 79^3 + 26 \cdot 79^4 + 21 \cdot 79^5 + 36 \cdot 79^6 + 3 \cdot 79^7 + 6 \cdot 79^8 + O(79^9)$
83	$3 \cdot a + (28 \cdot a + 1) \cdot 83 + (43 \cdot a + 10) \cdot 83^2 + (58 \cdot a + 81) \cdot 83^3 + (38 \cdot a + 26) \cdot 83^4 + (19 \cdot a + 38) \cdot 83^5 + (47 \cdot a + 44) \cdot 83^6 + (65 \cdot a + 44) \cdot 83^7 + (53 \cdot a + 20) \cdot 83^8 + O(83^9)$
89	$66 + 26 \cdot 89 + 52 \cdot 89^2 + 80 \cdot 89^3 + 22 \cdot 89^4 + 28 \cdot 89^5 + 27 \cdot 89^6 + 11 \cdot 89^7 + 23 \cdot 89^8 + O(89^9)$ $41 + 17 \cdot 89 + 29 \cdot 89^2 + 4 \cdot 89^3 + 77 \cdot 89^4 + 43 \cdot 89^5 + 87 \cdot 89^6 + 65 \cdot 89^7 + 71 \cdot 89^8 + O(89^9)$

Table A.9.1: α factors for $N = 133, B$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
17	$15 + 16 \cdot 17 + 16 \cdot 17^2 + 15 \cdot 17^3 + 17^4 + 7 \cdot 17^5 + 12 \cdot 17^6 + 3 \cdot 17^7 + 15 \cdot 17^8 + O(17^9)$
29	$20 \cdot 29^2 + 22 \cdot 29^3 + 21 \cdot 29^4 + 13 \cdot 29^5 + 26 \cdot 29^6 + 10 \cdot 29^7 + O(29^9)$
31	$2 + 10 \cdot 31 + 12 \cdot 31^2 + 5 \cdot 31^3 + 9 \cdot 31^4 + 22 \cdot 31^5 + 11 \cdot 31^6 + 2 \cdot 31^7 + 8 \cdot 31^8 + O(31^9)$
41	$1 + 22 \cdot 41 + 13 \cdot 41^2 + 27 \cdot 41^3 + 22 \cdot 41^4 + 6 \cdot 41^5 + 23 \cdot 41^6 + 26 \cdot 41^7 + 33 \cdot 41^8 + O(41^9)$
43	$40 + 17 \cdot 43 + 42 \cdot 43^2 + 27 \cdot 43^3 + 28 \cdot 43^4 + 36 \cdot 43^5 + 16 \cdot 43^6 + 26 \cdot 43^7 + 18 \cdot 43^8 + O(43^9)$
53	$46 + 15 \cdot 53 + 29 \cdot 53^2 + 6 \cdot 53^3 + 43 \cdot 53^4 + 38 \cdot 53^5 + 3 \cdot 53^6 + 40 \cdot 53^7 + 22 \cdot 53^8 + O(53^9)$
67	$22 + 54 \cdot 67 + 33 \cdot 67^2 + 41 \cdot 67^3 + 30 \cdot 67^4 + 60 \cdot 67^5 + 32 \cdot 67^6 + 47 \cdot 67^7 + 58 \cdot 67^8 + O(67^9)$
73	$57 + 33 \cdot 73 + 71 \cdot 73^2 + 64 \cdot 73^3 + 50 \cdot 73^4 + 21 \cdot 73^5 + 29 \cdot 73^6 + 19 \cdot 73^7 + 44 \cdot 73^8 + O(73^9)$
79	$4 + 31 \cdot 79 + 48 \cdot 79^2 + 55 \cdot 79^3 + 73 \cdot 79^4 + 26 \cdot 79^5 + 36 \cdot 79^6 + 4 \cdot 79^7 + 3 \cdot 79^8 + O(79^9)$
83	$27 + 39 \cdot 83 + 38 \cdot 83^2 + 23 \cdot 83^3 + 61 \cdot 83^4 + 71 \cdot 83^5 + 25 \cdot 83^6 + 53 \cdot 83^7 + 13 \cdot 83^8 + O(83^9)$
89	$9 + 69 \cdot 89 + 51 \cdot 89^2 + 45 \cdot 89^3 + 80 \cdot 89^4 + 2 \cdot 89^5 + 47 \cdot 89^6 + 35 \cdot 89^7 + 3 \cdot 89^8 + O(89^9)$

Table A.9.2: ϵ factors for $N = 133, B$

A.10 $N = 147$

The quadratic field K_f is generated by a root a of $x^2 + 2x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
31	$19+20\cdot 31+6\cdot 31^2+7\cdot 31^3+20\cdot 31^4+26\cdot 31^5+30\cdot 31^6+22\cdot 31^7+26\cdot 31^8+O(31^9)$
	$20+9\cdot 31+4\cdot 31^2+14\cdot 31^3+3\cdot 31^4+13\cdot 31^5+12\cdot 31^6+12\cdot 31^7+10\cdot 31^8+O(31^9)$
37	$33+27\cdot 37+37^2+10\cdot 37^3+11\cdot 37^4+33\cdot 37^5+15\cdot 37^6+17\cdot 37^7+32\cdot 37^8+O(37^9)$
43	$(4\cdot a+4)+(16\cdot a+16)\cdot 43+(27\cdot a+27)\cdot 43^2+(13\cdot a+13)\cdot 43^3+(4\cdot a+4)\cdot 43^4+$
	$(6\cdot a+6)\cdot 43^5+(28\cdot a+28)\cdot 43^6+(25\cdot a+25)\cdot 43^7+(21\cdot a+21)\cdot 43^8+O(43^9)$
53	$51+26\cdot 53+46\cdot 53^2+29\cdot 53^3+9\cdot 53^4+22\cdot 53^5+53^6+29\cdot 53^7+48\cdot 53^8+O(53^9)$
61	$(58\cdot a+50)+(48\cdot a+19)\cdot 61+(36\cdot a+28)\cdot 61^2+(35\cdot a+45)\cdot 61^3+(43\cdot a+60)\cdot 61^4+$
	$(49\cdot a+30)\cdot 61^5+(45\cdot a+24)\cdot 61^6+(19\cdot a+25)\cdot 61^7+(38\cdot a+56)\cdot 61^8+O(61^9)$
67	$(63\cdot a+63)+(41\cdot a+41)\cdot 67+(30\cdot a+30)\cdot 67^2+(8\cdot a+8)\cdot 67^3+(59\cdot a+59)\cdot 67^4+$
	$(66\cdot a+66)\cdot 67^5+(20\cdot a+20)\cdot 67^6+(47\cdot a+47)\cdot 67^7+(42\cdot a+42)\cdot 67^8+O(67^9)$
71	$23+61\cdot 71+66\cdot 71^2+36\cdot 71^3+21\cdot 71^4+17\cdot 71^5+13\cdot 71^6+51\cdot 71^7+50\cdot 71^8+O(71^9)$
	$44+25\cdot 71+44\cdot 71^2+53\cdot 71^3+36\cdot 71^4+46\cdot 71^5+55\cdot 71^6+28\cdot 71^7+65\cdot 71^8+O(71^9)$
73	$1+21\cdot 73+38\cdot 73^2+25\cdot 73^3+4\cdot 73^4+34\cdot 73^5+26\cdot 73^6+61\cdot 73^7+26\cdot 73^8+O(73^9)$
	$64+42\cdot 73+25\cdot 73^2+38\cdot 73^3+50\cdot 73^4+2\cdot 73^5+48\cdot 73^6+62\cdot 73^7+7\cdot 73^8+O(73^9)$
79	$44+61\cdot 79+41\cdot 79^2+33\cdot 79^3+74\cdot 79^4+53\cdot 79^5+18\cdot 79^6+20\cdot 79^7+71\cdot 79^8+O(79^9)$
	$51+56\cdot 79+50\cdot 79^2+8\cdot 79^3+72\cdot 79^4+15\cdot 79^5+57\cdot 79^6+55\cdot 79^7+13\cdot 79^8+O(79^9)$
97	$10+22\cdot 97+43\cdot 97^2+56\cdot 97^3+67\cdot 97^4+66\cdot 97^6+17\cdot 97^7+22\cdot 97^8+O(97^9)$
	$79+33\cdot 97+32\cdot 97^2+38\cdot 97^3+27\cdot 97^4+36\cdot 97^5+7\cdot 97^6+93\cdot 97^7+73\cdot 97^8+O(97^9)$

Table A.10.1: α factors for $N = 147$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
31	$16 + 18 \cdot 31 + 18 \cdot 31^2 + 23 \cdot 31^3 + 29 \cdot 31^4 + 22 \cdot 31^5 + 6 \cdot 31^6 + 8 \cdot 31^7 + 16 \cdot 31^8 + O(31^9)$
37	$26 + 10 \cdot 37 + 3 \cdot 37^2 + 16 \cdot 37^3 + 27 \cdot 37^4 + 20 \cdot 37^5 + 27 \cdot 37^6 + 9 \cdot 37^7 + 23 \cdot 37^8 + O(37^9)$
43	$25 + 15 \cdot 43 + 14 \cdot 43^2 + 19 \cdot 43^4 + 4 \cdot 43^5 + 14 \cdot 43^6 + 5 \cdot 43^7 + 17 \cdot 43^8 + O(43^9)$
53	$15 + 28 \cdot 53 + 49 \cdot 53^2 + 40 \cdot 53^3 + 41 \cdot 53^4 + 4 \cdot 53^5 + 12 \cdot 53^7 + 44 \cdot 53^8 + O(53^9)$
61	$3 + 28 \cdot 61 + 14 \cdot 61^2 + 6 \cdot 61^3 + 45 \cdot 61^4 + 42 \cdot 61^5 + 26 \cdot 61^6 + 40 \cdot 61^7 + 56 \cdot 61^8 + O(61^9)$
67	$40 + 27 \cdot 67 + 9 \cdot 67^2 + 53 \cdot 67^3 + 57 \cdot 67^4 + 48 \cdot 67^5 + 40 \cdot 67^6 + 2 \cdot 67^7 + 44 \cdot 67^8 + O(67^9)$
71	$15 + 9 \cdot 71 + 45 \cdot 71^2 + 38 \cdot 71^3 + 10 \cdot 71^4 + 50 \cdot 71^5 + 70 \cdot 71^6 + 49 \cdot 71^7 + 32 \cdot 71^8 + O(71^9)$
73	$73^2 + 2 \cdot 73^3 + 5 \cdot 73^4 + 30 \cdot 73^5 + 59 \cdot 73^6 + 23 \cdot 73^7 + 24 \cdot 73^8 + O(73^9)$
79	$9 + 54 \cdot 79 + 30 \cdot 79^2 + 26 \cdot 79^3 + 59 \cdot 79^4 + 39 \cdot 79^5 + 67 \cdot 79^6 + 3 \cdot 79^7 + 12 \cdot 79^8 + O(79^9)$
97	$22 + 42 \cdot 97 + 17 \cdot 97^2 + 38 \cdot 97^3 + 4 \cdot 97^4 + 4 \cdot 97^5 + 84 \cdot 97^6 + 91 \cdot 97^7 + 26 \cdot 97^8 + O(97^9)$

Table A.10.2: ϵ factors for $N = 147$

A.11 $N = 161$

The quadratic field K_f is generated by a root a of $x^2 + x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
11	$3 + 9 \cdot 11 + 5 \cdot 11^2 + 8 \cdot 11^3 + 11^4 + 9 \cdot 11^5 + 2 \cdot 11^6 + 5 \cdot 11^7 + 6 \cdot 11^8 + O(11^9)$
	$8 + 11 + 5 \cdot 11^2 + 2 \cdot 11^3 + 9 \cdot 11^4 + 11^5 + 8 \cdot 11^6 + 5 \cdot 11^7 + 4 \cdot 11^8 + O(11^9)$
19	$4 + 18 \cdot 19 + 18 \cdot 19^2 + 4 \cdot 19^3 + 6 \cdot 19^4 + 13 \cdot 19^6 + 17 \cdot 19^7 + 11 \cdot 19^8 + O(19^9)$
	$5 + 10 \cdot 19 + 10 \cdot 19^2 + 8 \cdot 19^3 + 17 \cdot 19^4 + 12 \cdot 19^5 + 14 \cdot 19^6 + 10 \cdot 19^7 + 9 \cdot 19^8 + O(19^9)$
37	$(31 \cdot a + 35) + (21 \cdot a + 26) \cdot 37 + (5 \cdot a + 34) \cdot 37^2 + (5 \cdot a + 29) \cdot 37^3 + (6 \cdot a + 31) \cdot 37^4 + (34 \cdot a + 12) \cdot 37^5 + (29 \cdot a + 19) \cdot 37^6 + (28 \cdot a + 34) \cdot 37^7 + (16 \cdot a + 34) \cdot 37^8 + O(37^9)$
43	$4 \cdot a + (32 \cdot a + 32) \cdot 43 + (14 \cdot a + 16) \cdot 43^2 + (13 \cdot a + 9) \cdot 43^3 + (7 \cdot a + 9) \cdot 43^4 + (32 \cdot a + 22) \cdot 43^5 + (6 \cdot a + 25) \cdot 43^6 + (36 \cdot a + 29) \cdot 43^7 + (42 \cdot a + 15) \cdot 43^8 + O(43^9)$
53	$(2 \cdot a + 10) + (7 \cdot a + 25) \cdot 53 + (31 \cdot a + 16) \cdot 53^2 + (3 \cdot a + 28) \cdot 53^3 + (28 \cdot a + 33) \cdot 53^4 + (51 \cdot a + 32) \cdot 53^5 + (25 \cdot a + 29) \cdot 53^6 + (27 \cdot a + 4) \cdot 53^7 + (35 \cdot a + 38) \cdot 53^8 + O(53^9)$
59	$10 + 16 \cdot 59 + 6 \cdot 59^2 + 53 \cdot 59^3 + 38 \cdot 59^4 + 16 \cdot 59^5 + 17 \cdot 59^6 + 10 \cdot 59^7 + 20 \cdot 59^8 + O(59^9)$
	$37 + 28 \cdot 59 + 47 \cdot 59^2 + 55 \cdot 59^3 + 44 \cdot 59^4 + 56 \cdot 59^5 + 32 \cdot 59^6 + 51 \cdot 59^7 + 15 \cdot 59^8 + O(59^9)$
61	$27 + 19 \cdot 61 + 22 \cdot 61^2 + 34 \cdot 61^3 + 37 \cdot 61^4 + 56 \cdot 61^5 + 40 \cdot 61^6 + 56 \cdot 61^7 + 47 \cdot 61^8 + O(61^9)$
	$34 + 41 \cdot 61 + 38 \cdot 61^2 + 26 \cdot 61^3 + 23 \cdot 61^4 + 4 \cdot 61^5 + 20 \cdot 61^6 + 4 \cdot 61^7 + 13 \cdot 61^8 + O(61^9)$
67	$(57 \cdot a + 61) + (65 \cdot a + 12) \cdot 67 + (27 \cdot a + 15) \cdot 67^2 + (27 \cdot a + 66) \cdot 67^3 + (62 \cdot a + 6) \cdot 67^4 + (35 \cdot a + 65) \cdot 67^5 + (22 \cdot a + 55) \cdot 67^6 + (42 \cdot a + 42) \cdot 67^7 + (42 \cdot a + 33) \cdot 67^8 + O(67^9)$
79	$15 + 11 \cdot 79 + 5 \cdot 79^2 + 74 \cdot 79^3 + 22 \cdot 79^4 + 45 \cdot 79^5 + 49 \cdot 79^6 + 21 \cdot 79^7 + 32 \cdot 79^8 + O(79^9)$
	$54 + 28 \cdot 79 + 38 \cdot 79^2 + 41 \cdot 79^3 + 45 \cdot 79^4 + 37 \cdot 79^5 + 56 \cdot 79^6 + 78 \cdot 79^7 + 26 \cdot 79^8 + O(79^9)$
83	$(4 \cdot a + 4) + 62 \cdot a \cdot 83 + (7 \cdot a + 48) \cdot 83^2 + (14 \cdot a + 68) \cdot 83^3 + (52 \cdot a + 1) \cdot 83^4 + (80 \cdot a + 17) \cdot 83^5 + (19 \cdot a + 33) \cdot 83^6 + (11 \cdot a + 9) \cdot 83^7 + (76 \cdot a + 64) \cdot 83^8 + O(83^9)$
89	$76 + 71 \cdot 89 + 51 \cdot 89^2 + 59 \cdot 89^3 + 50 \cdot 89^4 + 61 \cdot 89^5 + 27 \cdot 89^6 + 80 \cdot 89^7 + 53 \cdot 89^8 + O(89^9)$
	$13 + 17 \cdot 89 + 37 \cdot 89^2 + 29 \cdot 89^3 + 38 \cdot 89^4 + 27 \cdot 89^5 + 61 \cdot 89^6 + 8 \cdot 89^7 + 35 \cdot 89^8 + O(89^9)$
97	$6 \cdot a + (16 \cdot a + 16) \cdot 97 + (60 \cdot a + 82) \cdot 97^2 + (a + 48) \cdot 97^3 + (31 \cdot a + 88) \cdot 97^4 + (a + 70) \cdot 97^5 + (39 \cdot a + 88) \cdot 97^6 + (70 \cdot a + 62) \cdot 97^7 + (12 \cdot a + 88) \cdot 97^8 + O(97^9)$

Table A.11.1: α factors for $N = 161$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
11	$5 + 8 \cdot 11 + 11^2 + 4 \cdot 11^3 + 6 \cdot 11^5 + 5 \cdot 11^6 + 2 \cdot 11^7 + 9 \cdot 11^8 + O(11^9)$
19	$11 + 10 \cdot 19 + 8 \cdot 19^2 + 11 \cdot 19^3 + 15 \cdot 19^4 + 9 \cdot 19^5 + 7 \cdot 19^6 + 11 \cdot 19^7 + 14 \cdot 19^8 + O(19^9)$
37	$30 + 14 \cdot 37 + 21 \cdot 37^2 + 17 \cdot 37^3 + 24 \cdot 37^4 + 11 \cdot 37^5 + 19 \cdot 37^6 + 14 \cdot 37^7 + 32 \cdot 37^8 + O(37^9)$
43	$4 + 37 \cdot 43 + 8 \cdot 43^2 + 5 \cdot 43^3 + 37 \cdot 43^4 + 5 \cdot 43^5 + 3 \cdot 43^6 + 27 \cdot 43^7 + O(43^9)$
53	$17 + 22 \cdot 53 + 6 \cdot 53^2 + 44 \cdot 53^3 + 5 \cdot 53^4 + 4 \cdot 53^5 + 45 \cdot 53^6 + 31 \cdot 53^7 + 4 \cdot 53^8 + O(53^9)$
59	$45 + 58 \cdot 59 + 35 \cdot 59^2 + 37 \cdot 59^3 + 21 \cdot 59^4 + 53 \cdot 59^5 + 24 \cdot 59^6 + 45 \cdot 59^7 + 18 \cdot 59^8 + O(59^9)$
61	$56 + 22 \cdot 61 + 39 \cdot 61^2 + 59 \cdot 61^3 + 26 \cdot 61^4 + 10 \cdot 61^5 + 52 \cdot 61^6 + 60 \cdot 61^7 + 17 \cdot 61^8 + O(61^9)$
67	$64 + 24 \cdot 67 + 37 \cdot 67^2 + 31 \cdot 67^3 + 2 \cdot 67^4 + 2 \cdot 67^5 + 49 \cdot 67^6 + 37 \cdot 67^7 + 25 \cdot 67^8 + O(67^9)$
79	$50 + 34 \cdot 79 + 74 \cdot 79^2 + 21 \cdot 79^3 + 18 \cdot 79^4 + 17 \cdot 79^5 + 68 \cdot 79^6 + 71 \cdot 79^7 + 16 \cdot 79^8 + O(79^9)$
83	$16 + 38 \cdot 83 + 38 \cdot 83^2 + 55 \cdot 83^3 + 70 \cdot 83^4 + 53 \cdot 83^5 + 49 \cdot 83^6 + 73 \cdot 83^7 + 2 \cdot 83^8 + O(83^9)$
89	$32 + 73 \cdot 89 + 83 \cdot 89^2 + 28 \cdot 89^3 + 78 \cdot 89^4 + 12 \cdot 89^5 + 12 \cdot 89^6 + 9 \cdot 89^7 + 68 \cdot 89^8 + O(89^9)$
97	$85 + 40 \cdot 97 + 46 \cdot 97^2 + 77 \cdot 97^3 + 48 \cdot 97^4 + 20 \cdot 97^5 + 96 \cdot 97^6 + 46 \cdot 97^7 + 16 \cdot 97^8 + O(97^9)$

Table A.11.2: ϵ factors for $N = 161$

A.12 $N = 165$

The quadratic field K_f is generated by a root a of $x^2 + 2x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
7	$6 + 4 \cdot 7 + 6 \cdot 7^3 + 4 \cdot 7^4 + 3 \cdot 7^5 + 6 \cdot 7^6 + O(7^9)$ $4 + 6 \cdot 7^2 + 6 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^6 + 3 \cdot 7^7 + 5 \cdot 7^8 + O(7^9)$
13	$(4 \cdot a + 4) + (8 \cdot a + 8) \cdot 13 + (11 \cdot a + 11) \cdot 13^2 + (a + 1) \cdot 13^3 + (6 \cdot a + 6) \cdot 13^4 + (11 \cdot a + 11) \cdot 13^5 + (12 \cdot a + 12) \cdot 13^6 + (3 \cdot a + 3) \cdot 13^8 + O(13^9)$
17	$1 + 4 \cdot 17 + 8 \cdot 17^2 + 8 \cdot 17^3 + 13 \cdot 17^4 + 4 \cdot 17^5 + 8 \cdot 17^6 + 3 \cdot 17^7 + O(17^9)$ $8 + 13 \cdot 17 + 15 \cdot 17^2 + 8 \cdot 17^3 + 3 \cdot 17^5 + 10 \cdot 17^6 + 4 \cdot 17^7 + 16 \cdot 17^8 + O(17^9)$
19	$(2 \cdot a + 17) + (5 \cdot a + 14) \cdot 19 + (16 \cdot a + 17) \cdot 19^2 + (2 \cdot a + 11) \cdot 19^3 + (2 \cdot a + 11) \cdot 19^4 + (13 \cdot a + 13) \cdot 19^5 + (11 \cdot a + 14) \cdot 19^6 + (a + 4) \cdot 19^7 + (17 \cdot a + 12) \cdot 19^8 + O(19^9)$
23	$19 + 5 \cdot 23 + 3 \cdot 23^2 + 15 \cdot 23^3 + 23^4 + 16 \cdot 23^5 + 20 \cdot 23^6 + 9 \cdot 23^7 + 20 \cdot 23^8 + O(23^9)$ $19 + 5 \cdot 23 + 3 \cdot 23^2 + 15 \cdot 23^3 + 23^4 + 16 \cdot 23^5 + 20 \cdot 23^6 + 9 \cdot 23^7 + 20 \cdot 23^8 + O(23^9)$
29	$2 \cdot a + (14 \cdot a + 28) \cdot 29 + (17 \cdot a + 12) \cdot 29^2 + (3 \cdot a + 6) \cdot 29^3 + 17 \cdot a \cdot 29^4 + 23 \cdot 29^5 + (3 \cdot a + 18) \cdot 29^6 + (7 \cdot a + 10) \cdot 29^7 + (27 \cdot a + 17) \cdot 29^8 + O(29^9)$
37	$(33 \cdot a + 2) + (35 \cdot a + 16) \cdot 37 + (18 \cdot a + 20) \cdot 37^2 + (31 \cdot a + 17) \cdot 37^3 + (21 \cdot a + 24) \cdot 37^4 + (22 \cdot a + 12) \cdot 37^5 + (27 \cdot a + 29) \cdot 37^6 + (24 \cdot a + 13) \cdot 37^7 + (8 \cdot a + 24) \cdot 37^8 + O(37^9)$
41	$36 + 35 \cdot 41 + 23 \cdot 41^2 + 9 \cdot 41^3 + 21 \cdot 41^4 + 17 \cdot 41^5 + 39 \cdot 41^6 + 2 \cdot 41^7 + 29 \cdot 41^8 + O(41^9)$ $9 + 6 \cdot 41 + 29 \cdot 41^2 + 11 \cdot 41^4 + 6 \cdot 41^5 + 34 \cdot 41^6 + 6 \cdot 41^7 + 13 \cdot 41^8 + O(41^9)$
43	$(2 \cdot a + 39) + (40 \cdot a + 30) \cdot 43 + (30 \cdot a + 10) \cdot 43^2 + (34 \cdot a + 13) \cdot 43^3 + (12 \cdot a + 16) \cdot 43^4 + (32 \cdot a + 9) \cdot 43^5 + (18 \cdot a + 40) \cdot 43^6 + (a + 7) \cdot 43^7 + (9 \cdot a + 26) \cdot 43^8 + O(43^9)$
47	$43 + 11 \cdot 47 + 24 \cdot 47^2 + 15 \cdot 47^3 + 37 \cdot 47^4 + 42 \cdot 47^5 + 8 \cdot 47^6 + 23 \cdot 47^7 + 4 \cdot 47^8 + O(47^9)$ $43 + 11 \cdot 47 + 24 \cdot 47^2 + 15 \cdot 47^3 + 37 \cdot 47^4 + 42 \cdot 47^5 + 8 \cdot 47^6 + 23 \cdot 47^7 + 4 \cdot 47^8 + O(47^9)$
53	$(45 \cdot a + 43) + (23 \cdot a + 17) \cdot 53 + (21 \cdot a + 46) \cdot 53^2 + (35 \cdot a + 11) \cdot 53^3 + (31 \cdot a + 40) \cdot 53^4 + (3 \cdot a + 48) \cdot 53^5 + (32 \cdot a + 30) \cdot 53^6 + (18 \cdot a + 14) \cdot 53^7 + (24 \cdot a + 34) \cdot 53^8 + O(53^9)$
59	$55 + 14 \cdot 59 + 56 \cdot 59^2 + 7 \cdot 59^3 + 47 \cdot 59^4 + 31 \cdot 59^5 + 21 \cdot 59^6 + 51 \cdot 59^7 + 58 \cdot 59^8 + O(59^9)$
61	$(4 \cdot a + 59) + (a + 32) \cdot 61 + (24 \cdot a + 13) \cdot 61^2 + (34 \cdot a + 12) \cdot 61^3 + (55 \cdot a + 6) \cdot 61^4 + (4 \cdot a + 28) \cdot 61^5 + (30 \cdot a + 6) \cdot 61^6 + (7 \cdot a + 10) \cdot 61^7 + (33 \cdot a + 45) \cdot 61^8 + O(61^9)$
67	$(4 \cdot a + 4) + (25 \cdot a + 25) \cdot 67 + (36 \cdot a + 36) \cdot 67^2 + (58 \cdot a + 58) \cdot 67^3 + (7 \cdot a + 7) \cdot 67^4 + (46 \cdot a + 46) \cdot 67^6 + (19 \cdot a + 19) \cdot 67^7 + (24 \cdot a + 24) \cdot 67^8 + O(67^9)$
71	$56 + 66 \cdot 71 + 59 \cdot 71^2 + 16 \cdot 71^3 + 51 \cdot 71^4 + 57 \cdot 71^5 + 9 \cdot 71^6 + 9 \cdot 71^7 + 42 \cdot 71^8 + O(71^9)$ $31 + 39 \cdot 71 + 67 \cdot 71^2 + 14 \cdot 71^3 + 52 \cdot 71^4 + 48 \cdot 71^5 + 63 \cdot 71^6 + 34 \cdot 71^7 + 10 \cdot 71^8 + O(71^9)$
73	$37 + 54 \cdot 73 + 18 \cdot 73^2 + 37 \cdot 73^3 + 17 \cdot 73^5 + 14 \cdot 73^6 + 40 \cdot 73^7 + 33 \cdot 73^8 + O(73^9)$ $36 + 18 \cdot 73 + 54 \cdot 73^2 + 35 \cdot 73^3 + 72 \cdot 73^4 + 55 \cdot 73^5 + 58 \cdot 73^6 + 32 \cdot 73^7 + 39 \cdot 73^8 + O(73^9)$
79	$25 + 33 \cdot 79 + 48 \cdot 79^2 + 37 \cdot 79^3 + 31 \cdot 79^4 + 62 \cdot 79^5 + 66 \cdot 79^6 + 45 \cdot 79^7 + 49 \cdot 79^8 + O(79^9)$ $54 + 45 \cdot 79 + 30 \cdot 79^2 + 41 \cdot 79^3 + 47 \cdot 79^4 + 16 \cdot 79^5 + 12 \cdot 79^6 + 33 \cdot 79^7 + 29 \cdot 79^8 + O(79^9)$
83	$73 + 24 \cdot 83 + 29 \cdot 83^2 + 79 \cdot 83^3 + 40 \cdot 83^4 + 41 \cdot 83^5 + 56 \cdot 83^6 + 51 \cdot 83^8 + O(83^9)$
89	$76 + 43 \cdot 89 + 46 \cdot 89^2 + 58 \cdot 89^3 + 49 \cdot 89^4 + 39 \cdot 89^5 + 65 \cdot 89^6 + 53 \cdot 89^7 + 87 \cdot 89^8 + O(89^9)$ $9 + 83 \cdot 89 + 11 \cdot 89^2 + 45 \cdot 89^3 + 16 \cdot 89^4 + 3 \cdot 89^5 + 88 \cdot 89^6 + 29 \cdot 89^7 + 14 \cdot 89^8 + O(89^9)$
97	$47 + 60 \cdot 97 + 81 \cdot 97^2 + 90 \cdot 97^3 + 76 \cdot 97^4 + 16 \cdot 97^5 + 78 \cdot 97^6 + 14 \cdot 97^7 + 69 \cdot 97^8 + O(97^9)$ $62 + 33 \cdot 97 + 63 \cdot 97^2 + 82 \cdot 97^3 + 14 \cdot 97^5 + 15 \cdot 97^6 + 34 \cdot 97^7 + 28 \cdot 97^8 + O(97^9)$

Table A.12.1: α factors for $N = 165$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
7	$4 + 4 \cdot 7 + 4 \cdot 7^2 + 6 \cdot 7^3 + 5 \cdot 7^4 + 2 \cdot 7^5 + 3 \cdot 7^6 + 2 \cdot 7^7 + 2 \cdot 7^8 + O(7^9)$
13	$9 + 12 \cdot 13 + 12 \cdot 13^2 + 5 \cdot 13^3 + 6 \cdot 13^4 + 12 \cdot 13^5 + 3 \cdot 13^6 + 12 \cdot 13^8 + O(13^9)$
17	$8 \cdot 17^2 + 9 \cdot 17^3 + 11 \cdot 17^4 + 6 \cdot 17^5 + 7 \cdot 17^6 + 16 \cdot 17^7 + 14 \cdot 17^8 + O(17^9)$
19	$46 + 15 \cdot 19 + 3 \cdot 19^2 + 15 \cdot 19^3 + 18 \cdot 19^4 + 18 \cdot 19^5 + 12 \cdot 19^6 + 18 \cdot 19^7 + 4 \cdot 19^8 + O(19^9)$
23	$9 + 11 \cdot 23 + 18 \cdot 23^2 + 4 \cdot 23^3 + 17 \cdot 23^4 + 23^5 + 11 \cdot 23^6 + 9 \cdot 23^7 + 4 \cdot 23^8 + O(23^9)$
29	$20 + 4 \cdot 29 + 5 \cdot 29^2 + 28 \cdot 29^3 + 17 \cdot 29^4 + 4 \cdot 29^5 + 21 \cdot 29^6 + 9 \cdot 29^7 + 17 \cdot 29^8 + O(29^9)$
37	$10 + 5 \cdot 37 + 15 \cdot 37^2 + 20 \cdot 37^3 + 3 \cdot 37^4 + 30 \cdot 37^5 + 2 \cdot 37^6 + 20 \cdot 37^7 + 20 \cdot 37^8 + O(37^9)$
41	$21 + 30 \cdot 41 + 26 \cdot 41^2 + 18 \cdot 41^3 + 12 \cdot 41^4 + 8 \cdot 41^6 + 37 \cdot 41^7 + O(41^9)$
43	$9 + 30 \cdot 43 + 11 \cdot 43^2 + 18 \cdot 43^3 + 37 \cdot 43^4 + 13 \cdot 43^5 + 26 \cdot 43^6 + 3 \cdot 43^7 + 15 \cdot 43^8 + O(43^9)$
47	$32 + 19 \cdot 47 + 15 \cdot 47^2 + 27 \cdot 47^3 + 8 \cdot 47^4 + 27 \cdot 47^5 + 12 \cdot 47^6 + 31 \cdot 47^7 + 16 \cdot 47^8 + O(47^9)$
53	$37 + 15 \cdot 53 + 4 \cdot 53^2 + 27 \cdot 53^3 + 53^4 + 40 \cdot 53^5 + 13 \cdot 53^6 + 15 \cdot 53^7 + 21 \cdot 53^8 + O(53^9)$
59	$46 + 43 \cdot 59 + 3 \cdot 59^2 + 8 \cdot 59^3 + 4 \cdot 59^4 + 57 \cdot 59^5 + 12 \cdot 59^6 + 13 \cdot 59^7 + 4 \cdot 59^8 + O(59^9)$
61	$60 + 60 \cdot 61 + 17 \cdot 61^2 + 10 \cdot 61^3 + 35 \cdot 61^4 + 12 \cdot 61^5 + 38 \cdot 61^6 + 32 \cdot 61^7 + 34 \cdot 61^8 + O(61^9)$
67	$40 + 27 \cdot 67 + 9 \cdot 67^2 + 53 \cdot 67^3 + 57 \cdot 67^4 + 48 \cdot 67^5 + 40 \cdot 67^6 + 2 \cdot 67^7 + 44 \cdot 67^8 + O(67^9)$
71	$12 + 66 \cdot 71 + 19 \cdot 71^2 + 18 \cdot 71^3 + 12 \cdot 71^4 + 43 \cdot 71^5 + 56 \cdot 71^6 + 3 \cdot 71^7 + O(71^9)$
73	$9 + 24 \cdot 73 + 59 \cdot 73^2 + 46 \cdot 73^3 + 26 \cdot 73^4 + 43 \cdot 73^5 + 43 \cdot 73^6 + 3 \cdot 73^7 + 36 \cdot 73^8 + O(73^9)$
79	$40 + 40 \cdot 79 + 76 \cdot 79^2 + 39 \cdot 79^3 + 2 \cdot 79^4 + 77 \cdot 79^5 + 55 \cdot 79^6 + 9 \cdot 79^7 + 5 \cdot 79^8 + O(79^9)$
83	$61 + 31 \cdot 83 + 12 \cdot 83^2 + 70 \cdot 83^3 + 65 \cdot 83^4 + 40 \cdot 83^5 + 35 \cdot 83^6 + 55 \cdot 83^7 + 60 \cdot 83^8 + O(83^9)$
89	$16 + 60 \cdot 89 + 84 \cdot 89^2 + 3 \cdot 89^3 + 87 \cdot 89^4 + 45 \cdot 89^5 + 26 \cdot 89^6 + 41 \cdot 89^7 + 71 \cdot 89^8 + O(89^9)$
97	$94 + 54 \cdot 97 + 21 \cdot 97^2 + 19 \cdot 97^3 + 59 \cdot 97^4 + 62 \cdot 97^5 + 34 \cdot 97^6 + 54 \cdot 97^7 + 88 \cdot 97^8 + O(97^9)$

Table A.12.2: ϵ factors for $N = 165$

A.13 $N = 177$

The quadratic field K_f is generated by a root a of $x^2 + x - 1$.

Here are tables giving α,ϵ factors:

p	α or α_1, α_2
7	$(a+4) + 2 \cdot a \cdot 7 + (4 \cdot a + 3) \cdot 7^2 + 5 \cdot 7^3 + (a+3) \cdot 7^4 + (6 \cdot a + 5) \cdot 7^5 + (5 \cdot a + 6) \cdot 7^6 + (2 \cdot a + 2) \cdot 7^7 + 5 \cdot 7^8 + O(7^9)$
17	$3 \cdot a + (11 \cdot a + 11) \cdot 17 + (15 \cdot a + 3) \cdot 17^2 + (4 \cdot a + 3) \cdot 17^3 + (4 \cdot a + 3) \cdot 17^4 + (2 \cdot a + 6) \cdot 17^5 + (11 \cdot a + 16) \cdot 17^6 + (12 \cdot a + 1) \cdot 17^7 + (16 \cdot a + 12) \cdot 17^8 + O(17^9)$
19	$13 + 4 \cdot 19 + 10 \cdot 19^2 + 19^3 + 13 \cdot 19^4 + 11 \cdot 19^5 + 2 \cdot 19^6 + 5 \cdot 19^7 + 14 \cdot 19^8 + O(19^9)$ $1 + 10 \cdot 19 + 3 \cdot 19^2 + 14 \cdot 19^3 + 18 \cdot 19^4 + 17 \cdot 19^5 + 15 \cdot 19^7 + 6 \cdot 19^8 + O(19^9)$
23	$(22 \cdot a + 19) + (a + 16) \cdot 23 + (7 \cdot a + 19) \cdot 23^2 + (13 \cdot a + 18) \cdot 23^3 + 22 \cdot 23^4 + (7 \cdot a + 16) \cdot 23^5 + (3 \cdot a + 3) \cdot 23^6 + (5 \cdot a + 9) \cdot 23^7 + (10 \cdot a + 21) \cdot 23^8 + O(23^9)$
29	$2 + 22 \cdot 29 + 13 \cdot 29^3 + 6 \cdot 29^4 + 4 \cdot 29^5 + 17 \cdot 29^6 + 23 \cdot 29^7 + 23 \cdot 29^8 + O(29^9)$ $13 + 12 \cdot 29 + 26 \cdot 29^2 + 23 \cdot 29^3 + 4 \cdot 29^4 + 26 \cdot 29^5 + 19 \cdot 29^6 + 9 \cdot 29^7 + 19 \cdot 29^8 + O(29^9)$
31	$19 + 8 \cdot 31 + 16 \cdot 31^2 + 7 \cdot 31^3 + 11 \cdot 31^4 + 9 \cdot 31^5 + 10 \cdot 31^6 + 2 \cdot 31^7 + 4 \cdot 31^8 + O(31^9)$ $11 + 18 \cdot 31 + 16 \cdot 31^2 + 11 \cdot 31^3 + 17 \cdot 31^4 + 11 \cdot 31^5 + 18 \cdot 31^6 + 9 \cdot 31^7 + 23 \cdot 31^8 + O(31^9)$
37	$(3 \cdot a + 35) + (3 \cdot a + 4) \cdot 37 + (33 \cdot a + 11) \cdot 37^2 + (28 \cdot a + 31) \cdot 37^3 + (11 \cdot a + 14) \cdot 37^4 + (14 \cdot a + 6) \cdot 37^5 + (25 \cdot a + 20) \cdot 37^6 + (a + 26) \cdot 37^7 + (23 \cdot a + 9) \cdot 37^8 + O(37^9)$
41	$35 + 35 \cdot 41 + 9 \cdot 41^2 + 14 \cdot 41^3 + 29 \cdot 41^4 + 26 \cdot 41^5 + 10 \cdot 41^6 + 11 \cdot 41^7 + 35 \cdot 41^8 + O(41^9)$ $11 + 38 \cdot 41 + 24 \cdot 41^2 + 22 \cdot 41^3 + 25 \cdot 41^4 + 12 \cdot 41^5 + 26 \cdot 41^6 + 22 \cdot 41^7 + 30 \cdot 41^8 + O(41^9)$
47	$(44 \cdot a + 38) + (24 \cdot a + 43) \cdot 47 + (9 \cdot a + 35) \cdot 47^2 + (23 \cdot a + 19) \cdot 47^3 + (18 \cdot a + 1) \cdot 47^4 + (13 \cdot a + 27) \cdot 47^5 + (21 \cdot a + 34) \cdot 47^6 + (3 \cdot a + 43) \cdot 47^7 + (45 \cdot a + 21) \cdot 47^8 + O(47^9)$
61	$46 + 13 \cdot 61 + 45 \cdot 61^2 + 22 \cdot 61^3 + 9 \cdot 61^4 + 30 \cdot 61^5 + 53 \cdot 61^6 + 2 \cdot 61^7 + 54 \cdot 61^8 + O(61^9)$ $2 + 12 \cdot 61 + 25 \cdot 61^2 + 11 \cdot 61^3 + 7 \cdot 61^4 + 57 \cdot 61^5 + 17 \cdot 61^6 + 53 \cdot 61^7 + 44 \cdot 61^8 + O(61^9)$
73	$(3 \cdot a + 72) + (14 \cdot a + 42) \cdot 73 + (2 \cdot a + 7) \cdot 73^2 + (5 \cdot a + 44) \cdot 73^3 + (72 \cdot a + 41) \cdot 73^4 + (7 \cdot a + 51) \cdot 73^5 + (3 \cdot a + 53) \cdot 73^6 + (59 \cdot a + 63) \cdot 73^7 + (33 \cdot a + 64) \cdot 73^8 + O(73^9)$
83	$(82 \cdot a + 82) + 82 \cdot 83 + (2 \cdot a + 81) \cdot 83^2 + (10 \cdot a + 76) \cdot 83^3 + (65 \cdot a + 42) \cdot 83^4 + (61 \cdot a + 37) \cdot 83^5 + (8 \cdot a + 10) \cdot 83^6 + (8 \cdot a + 54) \cdot 83^7 + (30 \cdot a + 53) \cdot 83^8 + O(83^9)$
89	$72 + 43 \cdot 89 + 64 \cdot 89^2 + 80 \cdot 89^3 + 67 \cdot 89^4 + 37 \cdot 89^5 + 49 \cdot 89^6 + 19 \cdot 89^7 + 38 \cdot 89^8 + O(89^9)$ $14 + 85 \cdot 89 + 68 \cdot 89^2 + 32 \cdot 89^3 + 52 \cdot 89^4 + 26 \cdot 89^5 + 67 \cdot 89^6 + 11 \cdot 89^7 + 28 \cdot 89^8 + O(89^9)$

Table A.13.1: α factors for $N = 177$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
7	$2 + 6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + 7^8 + O(7^9)$
19	$19^2 + 9 \cdot 19^3 + 15 \cdot 19^4 + 9 \cdot 19^5 + 11 \cdot 19^6 + 12 \cdot 19^7 + 15 \cdot 19^8 + O(19^9)$
23	$18 + 16 \cdot 23 + 16 \cdot 23^2 + 8 \cdot 23^3 + 15 \cdot 23^4 + 13 \cdot 23^5 + 2 \cdot 23^6 + 23^7 + 14 \cdot 23^8 + O(23^9)$
29	$16 + 3 \cdot 29 + 19 \cdot 29^2 + 10 \cdot 29^3 + 6 \cdot 29^4 + 14 \cdot 29^5 + 22 \cdot 29^6 + 3 \cdot 29^7 + 12 \cdot 29^8 + O(29^9)$
31	$18 + 18 \cdot 31^2 + 12 \cdot 31^3 + 4 \cdot 31^4 + 25 \cdot 31^5 + 26 \cdot 31^6 + 18 \cdot 31^7 + 14 \cdot 31^8 + O(31^9)$
37	$7 + 21 \cdot 37 + 32 \cdot 37^2 + 15 \cdot 37^3 + 37^4 + 12 \cdot 37^5 + 28 \cdot 37^6 + 10 \cdot 37^7 + 37^8 + O(37^9)$
41	$39 + 21 \cdot 41 + 20 \cdot 41^2 + 8 \cdot 41^3 + 21 \cdot 41^4 + 6 \cdot 41^5 + 16 \cdot 41^6 + 30 \cdot 41^7 + 12 \cdot 41^8 + O(41^9)$
47	$2 + 12 \cdot 47 + 21 \cdot 47^2 + 28 \cdot 47^3 + 7 \cdot 47^4 + 26 \cdot 47^5 + 28 \cdot 47^6 + 35 \cdot 47^7 + 25 \cdot 47^8 + O(47^9)$
61	$48 + 47 \cdot 61 + 17 \cdot 61^2 + 35 \cdot 61^3 + 5 \cdot 61^4 + 41 \cdot 61^5 + 34 \cdot 61^6 + 47 \cdot 61^7 + 39 \cdot 61^8 + O(61^9)$
73	$38 + 16 \cdot 73 + 50 \cdot 73^2 + 36 \cdot 73^3 + 10 \cdot 73^4 + 41 \cdot 73^5 + 36 \cdot 73^6 + 42 \cdot 73^7 + 33 \cdot 73^8 + O(73^9)$
83	$1 + 14 \cdot 83 + 40 \cdot 83^2 + 5 \cdot 83^3 + 60 \cdot 83^4 + 64 \cdot 83^5 + 80 \cdot 83^6 + 74 \cdot 83^7 + 46 \cdot 83^8 + O(83^9)$
89	$25 + 22 \cdot 89 + 25 \cdot 89^2 + 28 \cdot 89^3 + 22 \cdot 89^4 + 6 \cdot 89^5 + 77 \cdot 89^6 + 2 \cdot 89^7 + 75 \cdot 89^8 + O(89^9)$

Table A.13.2: ϵ factors for $N = 177$

A.14 $N = 188$

The quadratic field K_f is generated by a root a of $x^2 - 3x + 1$.

p	α or α_1, α_2
7	$(a+2) + (2 \cdot a + 3) \cdot 7 + (4 \cdot a + 1) \cdot 7^2 + 4 \cdot 7^3 + (a+1) \cdot 7^4 + 6 \cdot a \cdot 7^5 + +(5 \cdot a + 2) \cdot 7^6 + (2 \cdot a + 4) \cdot 7^7 + 4 \cdot 7^8 + O(7^9)$
11	$6 + 6 \cdot 11 + 2 \cdot 11^2 + 11^3 + 3 \cdot 11^4 + 6 \cdot 11^5 + 9 \cdot 11^6 + 7 \cdot 11^7 + 7 \cdot 11^8 + O(11^9)$ $1 + 11 + 2 \cdot 11^2 + 2 \cdot 11^3 + 9 \cdot 11^4 + 9 \cdot 11^5 + 4 \cdot 11^6 + 8 \cdot 11^7 + 4 \cdot 11^8 + O(11^9)$
13	$(2 \cdot a + 4) + (8 \cdot a + 6) \cdot 13 + (2 \cdot a + 11) \cdot 13^2 + (6 \cdot a + 5) \cdot 13^3 + (7 \cdot a + 11) \cdot 13^4 + (2 \cdot a + 6) \cdot 13^5 + (a+3) \cdot 13^6 + (9 \cdot a + 9) \cdot 13^7 + (5 \cdot a + 3) \cdot 13^8 + O(13^9)$
17	$(14 \cdot a + 6) + (5 \cdot a + 11) \cdot 17 + (a + 10) \cdot 17^2 + (12 \cdot a + 6) \cdot 17^3 + (12 \cdot a + 5) \cdot 17^4 + (14 \cdot a + 15) \cdot 17^5 + (5 \cdot a + 5) \cdot 17^6 + (4 \cdot a + 6) \cdot 17^7 + 4 \cdot 17^8 + O(17^9)$
19	$10 + 3 \cdot 19 + 10 \cdot 19^2 + 7 \cdot 19^3 + 9 \cdot 19^4 + 19^5 + 6 \cdot 19^6 + 15 \cdot 19^7 + 18 \cdot 19^8 + O(19^9)$ $7 + 2 \cdot 19 + 4 \cdot 19^2 + 9 \cdot 19^3 + 9 \cdot 19^4 + 13 \cdot 19^5 + 4 \cdot 19^6 + 5 \cdot 19^7 + 16 \cdot 19^8 + O(19^9)$
23	$(21 \cdot a + 17) + (6 \cdot a + 20) \cdot 23 + (15 \cdot a + 22) \cdot 23^2 + (18 \cdot a + 9) \cdot 23^3 + (10 \cdot a + 9) \cdot 23^4 + (12 \cdot a + 14) \cdot 23^5 (22 \cdot a + 21) \cdot 23^6 + (18 \cdot a + 10) \cdot 23^7 + (6 \cdot a + 20) \cdot 23^8 + O(23^9)$
37	$(20 \cdot a + 27) + (21 \cdot a + 1) \cdot 37 + (18 \cdot a + 30) \cdot 37^2 + (15 \cdot a + 24) \cdot 37^3 + (2 \cdot a + 31) \cdot 37^4 + (35 \cdot a + 13) \cdot 37^5 + 9 \cdot 37^6 + (29 \cdot a + 16) \cdot 37^7 + (9 \cdot a + 9) \cdot 37^8 + O(37^9)$
41	$22 + 16 \cdot 41 + 5 \cdot 41^2 + 20 \cdot 41^3 + 4 \cdot 41^4 + 37 \cdot 41^5 + 8 \cdot 41^6 + 21 \cdot 41^7 + 20 \cdot 41^8 + O(41^9)$ $37 + 27 \cdot 41 + 3 \cdot 41^2 + 35 \cdot 41^3 + 13 \cdot 41^4 + 31 \cdot 41^5 + 25 \cdot 41^6 + 24 \cdot 41^7 + 10 \cdot 41^8 + O(41^9)$
43	$33 + 12 \cdot 43 + 8 \cdot 43^2 + 21 \cdot 43^3 + 18 \cdot 43^4 + 4 \cdot 43^5 + 12 \cdot 43^6 + 16 \cdot 43^7 + 22 \cdot 43^8 + O(43^9)$
53	$(5 \cdot a + 40) + (48 \cdot a + 1) \cdot 53 + (25 \cdot a + 21) \cdot 53^2 + (34 \cdot a + 25) \cdot 53^3 + 40 \cdot 53^4 + (8 \cdot a + 31) \cdot 53^5 + (5 \cdot a + 11) \cdot 53^6 + (23 \cdot a + 6) \cdot 53^7 + (37 \cdot a + 46) \cdot 53^8 + O(53^9)$
59	$34 + 31 \cdot 59 + 21 \cdot 59^2 + 58 \cdot 59^3 + 23 \cdot 59^4 + 18 \cdot 59^5 + 36 \cdot 59^6 + 26 \cdot 59^7 + 21 \cdot 59^8 + O(59^9)$ $26 + 28 \cdot 59 + 41 \cdot 59^2 + 22 \cdot 59^3 + 3 \cdot 59^4 + 45 \cdot 59^5 + 20 \cdot 59^6 + 34 \cdot 59^7 + 19 \cdot 59^8 + O(59^9)$
61	$55 + 7 \cdot 61 + 5 \cdot 61^2 + 10 \cdot 61^3 + 43 \cdot 61^4 + 24 \cdot 61^5 + 32 \cdot 61^6 + 50 \cdot 61^7 + 8 \cdot 61^8 + O(61^9)$ $11 + 54 \cdot 61 + 20 \cdot 61^2 + 55 \cdot 61^3 + 15 \cdot 61^4 + 56 \cdot 61^5 + 52 \cdot 61^6 + 16 \cdot 61^7 + 4 \cdot 61^8 + O(61^9)$
67	$(a + 63) + (32 \cdot a + 51) \cdot 67 + (21 \cdot a + 15) \cdot 67^2 + (5 \cdot a + 57) \cdot 67^3 + (41 \cdot a + 51) \cdot 67^4 + (61 \cdot a + 41) \cdot 67^5 + (63 \cdot a + 30) \cdot 67^6 + (13 \cdot a + 11) \cdot 67^7 + (27 \cdot a + 17) \cdot 67^8 + O(67^9)$
71	$36 + 14 \cdot 71 + 62 \cdot 71^2 + 21 \cdot 71^3 + 15 \cdot 71^4 + 61 \cdot 71^5 + 20 \cdot 71^6 + 6 \cdot 71^7 + 25 \cdot 71^8 + O(71^9)$ $50 + 27 \cdot 71 + 27 \cdot 71^2 + 43 \cdot 71^3 + 36 \cdot 71^4 + 64 \cdot 71^5 + 13 \cdot 71^6 + 49 \cdot 71^7 + 59 \cdot 71^8 + O(71^9)$
73	$(67 \cdot a + 67) + (60 \cdot a + 48) \cdot 73 + (35 \cdot a + 22) \cdot 73^2 + (42 \cdot a + 64) \cdot 73^3 + (35 \cdot a + 49) \cdot 73^4 + (66 \cdot a + 13) \cdot 73^5 + (27 \cdot a + 66) \cdot 73^6 + (21 \cdot a + 30) \cdot 73^7 + (59 \cdot a + 16) \cdot 73^8 + O(73^9)$
79	$65 + 41 \cdot 79 + 70 \cdot 79^2 + 60 \cdot 79^3 + 34 \cdot 79^4 + 35 \cdot 79^5 + 67 \cdot 79^6 + 4 \cdot 79^7 + 55 \cdot 79^8 + O(79^9)5+$ $38 \cdot 79 + 35 \cdot 79^2 + 6 \cdot 79^3 + 32 \cdot 79^4 + 6 \cdot 79^5 + 2 \cdot 79^6 + 53 \cdot 79^7 + 26 \cdot 79^8 + O(79^9)$
83	$(4 \cdot a + 71) + (29 \cdot a + 78) \cdot 83 + (55 \cdot a + 82) \cdot 83^2 + (21 \cdot a + 17) \cdot 83^3 + (54 \cdot a + 3) \cdot 83^4 + (66 \cdot a + 49) \cdot 83^5 + (20 \cdot a + 20) \cdot 83^6 + (69 \cdot a + 41) \cdot 83^7 + (7 \cdot a + 59) \cdot 83^8 + O(83^9)$
89	$59 + 49 \cdot 89 + 9 \cdot 89^2 + 68 \cdot 89^3 + 26 \cdot 89^4 + 54 \cdot 89^5 + 66 \cdot 89^6 + 18 \cdot 89^7 + 59 \cdot 89^8 + O(89^9)27+$ $9 \cdot 89 + 66 \cdot 89^2 + 12 \cdot 89^3 + 77 \cdot 89^4 + 52 \cdot 89^5 + 45 \cdot 89^6 + 19 \cdot 89^7 + 83 \cdot 89^8 + O(89^9)$
97	$(50 \cdot a + 82) + (73 \cdot a + 2) \cdot 97 + (63 \cdot a + 80) \cdot 97^2 + (50 \cdot a + 42) \cdot 97^3 + (66 \cdot a + 37) \cdot 97^4 + (92 \cdot a + 76) \cdot 97^5 + (74 \cdot a + 41) \cdot 97^6 + (47 \cdot a + 88) \cdot 97^7 + (78 \cdot a + 18) \cdot 97^8 + O(97^9)$

Table A.14.1: α factors for $N = 188$

p	$(1-\overline{\alpha}^{-1})^2$ or $(1-\alpha_1^{-1})^2 \cdot (1-\alpha_2^{-1})^2$
7	$2 + 6 \cdot 7 + 3 \cdot 7^2 + 2 \cdot 7^3 + 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + 7^8 + O(7^9)$
11	$11^2 + 5 \cdot 11^3 + 5 \cdot 11^4 + 9 \cdot 11^5 + 3 \cdot 11^6 + 7 \cdot 11^7 + 3 \cdot 11^8 + O(11^9)$
13	$12 + 6 \cdot 13 + 10 \cdot 13^2 + 9 \cdot 13^3 + 12 \cdot 13^4 + 6 \cdot 13^5 + 4 \cdot 13^6 + 8 \cdot 13^7 + 12 \cdot 13^8 + O(13^9)$
17	$8 + 15 \cdot 17 + 5 \cdot 17^2 + 2 \cdot 17^3 + 7 \cdot 17^4 + 3 \cdot 17^5 + 16 \cdot 17^6 + 10 \cdot 17^7 + 12 \cdot 17^8 + O(17^9)$
19	$5 + 16 \cdot 19 + 17 \cdot 19^2 + 2 \cdot 19^3 + 2 \cdot 19^4 + 15 \cdot 19^5 + 5 \cdot 19^6 + 5 \cdot 19^7 + 9 \cdot 19^8 + O(19^9)$
23	$12 + 18 \cdot 23 + 17 \cdot 23^2 + 13 \cdot 23^3 + 5 \cdot 23^4 + 6 \cdot 23^5 + 5 \cdot 23^6 + 13 \cdot 23^7 + 13 \cdot 23^8 + O(23^9)$
37	$33 + 4 \cdot 37 + 17 \cdot 37^2 + 29 \cdot 37^3 + 17 \cdot 37^4 + 16 \cdot 37^5 + 30 \cdot 37^6 + 19 \cdot 37^7 + 26 \cdot 37^8 + O(37^9)$
41	$9 + 23 \cdot 41 + 10 \cdot 41^2 + 6 \cdot 41^3 + 35 \cdot 41^4 + 17 \cdot 41^5 + 17 \cdot 41^6 + 22 \cdot 41^7 + 22 \cdot 41^8 + O(41^9)$
43	$17 + 35 \cdot 43 + 28 \cdot 43^2 + 3 \cdot 43^3 + 21 \cdot 43^4 + 25 \cdot 43^5 + 13 \cdot 43^6 + 30 \cdot 43^8 + O(43^9)$
53	$15 + 15 \cdot 53 + 41 \cdot 53^2 + 26 \cdot 53^3 + 22 \cdot 53^4 + 40 \cdot 53^5 + 10 \cdot 53^6 + 5 \cdot 53^7 + 47 \cdot 53^8 + O(53^9)$
59	$1 + 2 \cdot 59 + 15 \cdot 59^2 + 53 \cdot 59^3 + 56 \cdot 59^4 + 56 \cdot 59^5 + 31 \cdot 59^6 + 39 \cdot 59^7 + 20 \cdot 59^8 + O(59^9)$
61	$13 + 49 \cdot 61 + 23 \cdot 61^2 + 60 \cdot 61^3 + 15 \cdot 61^4 + 48 \cdot 61^5 + 39 \cdot 61^6 + 43 \cdot 61^7 + 8 \cdot 61^8 + O(61^9)$
67	$10 + 4 \cdot 67^2 + 46 \cdot 67^3 + 44 \cdot 67^4 + 41 \cdot 67^5 + 21 \cdot 67^6 + 6 \cdot 67^7 + 50 \cdot 67^8 + O(67^9)$
71	$37 + 17 \cdot 71 + 51 \cdot 71^2 + 37 \cdot 71^3 + 27 \cdot 71^4 + 70 \cdot 71^5 + 26 \cdot 71^6 + 58 \cdot 71^7 + 6 \cdot 71^8 + O(71^9)$
73	$8 + 56 \cdot 73 + 43 \cdot 73^2 + 33 \cdot 73^3 + 45 \cdot 73^4 + 59 \cdot 73^5 + 53 \cdot 73^6 + 14 \cdot 73^7 + 70 \cdot 73^8 + O(73^9)$
79	$62 + 51 \cdot 79 + 74 \cdot 79^2 + 22 \cdot 79^3 + 70 \cdot 79^4 + 43 \cdot 79^5 + 30 \cdot 79^6 + 55 \cdot 79^7 + 75 \cdot 79^8 + O(79^9)$
83	$11 + 58 \cdot 83 + 20 \cdot 83^2 + 16 \cdot 83^3 + 31 \cdot 83^4 + 2 \cdot 83^5 + 56 \cdot 83^6 + 40 \cdot 83^7 + 61 \cdot 83^8 + O(83^9)$
89	$8 + 66 \cdot 89 + 48 \cdot 89^2 + 50 \cdot 89^3 + 81 \cdot 89^4 + 78 \cdot 89^5 + 79 \cdot 89^6 + 22 \cdot 89^7 + 86 \cdot 89^8 + O(89^9)$
97	$47 + 67 \cdot 97 + 75 \cdot 97^2 + 12 \cdot 97^3 + 6 \cdot 97^4 + 77 \cdot 97^5 + 88 \cdot 97^6 + 78 \cdot 97^7 + 24 \cdot 97^8 + O(97^9)$

Table A.14.2: ϵ factors for $N = 188$

A.15 $N = 191$

The quadratic field K_f is generated by a root a of $x^2 + x - 1$ Here are tables giving α,ϵ factors:

p	α or α_1, α_2
7	$(6 \cdot a + 6) + 6 \cdot 7 + (2 \cdot a + 5) \cdot 7^2 + 3 \cdot a \cdot 7^3 + (3 \cdot a + 1) \cdot 7^4 + (2 \cdot a + 1) \cdot 7^5 + (6 \cdot a + 6) \cdot 7^6 + (2 \cdot a + 3) \cdot 7^7 + 3 \cdot 7^8 + O(7^9)$
23	$a + (22 \cdot a + 22) \cdot 23 + (20 \cdot a + 19) \cdot 23^2 + (12 \cdot a + 6) \cdot 23^3 + (3 \cdot a + 9) \cdot 23^4 + (4 \cdot a + 7) \cdot 23^5 + (13 \cdot a + 13) \cdot 23^6 + (15 \cdot a + 19) \cdot 23^7 + (16 \cdot a + 16) \cdot 23^8 + O(23^9)$
31	$28 + 19 \cdot 31 + 6 \cdot 31^2 + 26 \cdot 31^3 + 3 \cdot 31^4 + 2 \cdot 31^5 + 17 \cdot 31^6 + 3 \cdot 31^7 + 2 \cdot 31^8 + O(31^9)$ $29 + 16 \cdot 31 + 26 \cdot 31^2 + 9 \cdot 31^3 + 11 \cdot 31^4 + 31^5 + 26 \cdot 31^6 + 28 \cdot 31^7 + 5 \cdot 31^8 + O(31^9)$
43	$(39 \cdot a + 2) + 23 \cdot 43 + (15 \cdot a + 1) \cdot 43^2 + 11 \cdot a \cdot 43^3 + (15 \cdot a + 13) \cdot 43^4 + (38 \cdot a + 3) \cdot 43^5 + (31 \cdot a + 34) \cdot 43^6 + (13 \cdot a + 14) \cdot 43^7 + (39 \cdot a + 12) \cdot 43^8 + O(43^9)$
47	$(40 \cdot a + 45) + (27 \cdot a + 19) \cdot 47 + (9 \cdot a + 41) \cdot 47^2 + (35 \cdot a + 44) \cdot 47^3 + (41 \cdot a + 32) \cdot 47^4 + (41 \cdot a + 35) \cdot 47^5 + (14 \cdot a + 18) \cdot 47^6 + (17 \cdot a + 20) \cdot 47^7 + (6 \cdot a + 5) \cdot 47^8 + O(47^9)$
53	$(5 \cdot a + 3) + (46 \cdot a + 29) \cdot 53 + (15 \cdot a + 12) \cdot 53^2 + (5 \cdot a + 40) \cdot 53^3 + (24 \cdot a + 9) \cdot 53^4 + (13 \cdot a + 20) \cdot 53^5 + (22 \cdot a + 48) \cdot 53^6 + (36 \cdot a + 44) \cdot 53^7 + (50 \cdot a + 16) \cdot 53^8 + O(53^9)$
71	$44 + 33 \cdot 71 + 53 \cdot 71^2 + 64 \cdot 71^3 + 38 \cdot 71^4 + 10 \cdot 71^5 + 37 \cdot 71^6 + 48 \cdot 71^7 + 28 \cdot 71^8 + O(71^9)$ $30 + 42 \cdot 71 + 69 \cdot 71^2 + 65 \cdot 71^3 + 54 \cdot 71^4 + 62 \cdot 71^5 + 14 \cdot 71^6 + 27 \cdot 71^7 + 59 \cdot 71^8 + O(71^9)$
73	$63 + 21 \cdot 73 + 70 \cdot 73^2 + 23 \cdot 73^3 + 33 \cdot 73^4 + 15 \cdot 73^5 + 47 \cdot 73^6 + 65 \cdot 73^7 + 12 \cdot 73^8 + O(73^9)$
97	$(85 \cdot a + 87) + (18 \cdot a + 83) \cdot 97 + (2 \cdot a + 1) \cdot 97^2 + (78 \cdot a + 16) \cdot 97^3 + (76 \cdot a + 76) \cdot 97^4 + (29 \cdot a + 27) \cdot 97^5 + (44 \cdot a + 91) \cdot 97^6 + (31 \cdot a + 80) \cdot 97^7 + (15 \cdot a + 33) \cdot 97^8 + O(97^9)$

Table A.15.1: α factors for $N = 191$

p	$(1 - \overline{\alpha}^{-1})^2$ or $(1 - \alpha_1^{-1})^2 \cdot (1 - \alpha_2^{-1})^2$
7	$1 + 6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^4 + 6 \cdot 7^5 + 6 \cdot 7^6 + 7^7 + 7^8 + O(7^9)$
23	$1 + 14 \cdot 23 + 8 \cdot 23^2 + 16 \cdot 23^3 + 5 \cdot 23^4 + 12 \cdot 23^5 + 22 \cdot 23^6 + 13 \cdot 23^7 + 15 \cdot 23^8 + O(23^9)$
31	$4 + 5 \cdot 31 + 6 \cdot 31^2 + 13 \cdot 31^3 + 27 \cdot 31^4 + 20 \cdot 31^5 + 6 \cdot 31^6 + 22 \cdot 31^7 + 22 \cdot 31^8 + O(31^9)$
43	$21 + 35 \cdot 43 + 32 \cdot 43^2 + 12 \cdot 43^3 + 32 \cdot 43^4 + 16 \cdot 43^5 + 4 \cdot 43^6 + 37 \cdot 43^7 + 3 \cdot 43^8 + O(43^9)$
47	$34 + 37 \cdot 47 + 8 \cdot 47^2 + 20 \cdot 47^3 + 23 \cdot 47^4 + 24 \cdot 47^5 + 19 \cdot 47^6 + 19 \cdot 47^7 + 14 \cdot 47^8 + O(47^9)$
53	$1 + 23 \cdot 53 + 15 \cdot 53^2 + 48 \cdot 53^3 + 16 \cdot 53^4 + 33 \cdot 53^5 + 51 \cdot 53^6 + 18 \cdot 53^7 + 10 \cdot 53^8 + O(53^9)$
71	$3 + 46 \cdot 71 + 67 \cdot 71^2 + 35 \cdot 71^3 + 60 \cdot 71^4 + 68 \cdot 71^5 + 3 \cdot 71^6 + 35 \cdot 71^7 + 19 \cdot 71^8 + O(71^9)$
73	$32 + 33 \cdot 73 + 5 \cdot 73^2 + 52 \cdot 73^3 + 35 \cdot 73^4 + 69 \cdot 73^5 + 36 \cdot 73^6 + 14 \cdot 73^7 + 35 \cdot 73^8 + O(73^9)$
97	$24 + 69 \cdot 97 + 9 \cdot 97^2 + 77 \cdot 97^3 + 12 \cdot 97^4 + 10 \cdot 97^5 + 81 \cdot 97^6 + 20 \cdot 97^7 + 30 \cdot 97^8 + O(97^9)$

Table A.15.2: ϵ factors for $N = 191$

Bibliography

[AKR09] T.G. Abbott, K.S. Kedlaya, and D. Roe, *Bounding picard numbers of surfaces using p-adic cohomology*, Arithmetic, Geometry and Coding Theory (AGCT 2005), Societé Mathématique de France, 2009, pp. 125–159.

[BB] J. S. Balakrishnan and A. Besser, *Local heights on hyperelliptic curves*, preprint.

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer, 2010, pp. 16–31.

[BCD$^+$08] M. Baker, B. Conrad, S. Dasgupta, K. S. Kedlaya, and J. Teitelbaum, *p-adic geometry*, University Lecture Series, vol. 45, American Mathematical Society, Providence, RI, 2008, Lectures from the 10th Arizona Winter School held at the University of Arizona, Tucson, AZ, March 10–14, 2007, Edited by David Savitt and Dinesh S. Thakur.

[BdJ08] A. Besser and R. de Jeu, $\mathrm{Li}^{(p)}$*-service? An algorithm for computing p-adic polylogarithms*, Math. Comp. **77** (2008), no. 262, 1105–1134.

[Ber07] V. G. Berkovich, *Integration of one-forms on p-adic analytic spaces*, Annals of Mathematics Studies, vol. 162, Princeton University Press, Princeton, NJ, 2007.

[Bes00] A. Besser, *Syntomic regulators and p-adic integration. II. K_2 of curves*, Proceedings of the Conference on p-adic Aspects of the Theory of Automorphic Representations (Jerusalem, 1998), vol. 120, 2000, pp. 335–359.

[Bes02a] ———, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), no. 1, 19–48.

[Bes02b] ———, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), 19–48.

[Bes04] ———, *The p-adic height pairings of Coleman-Gross and of Nekovář*, Number Theory, CRM Proceedings & Lecture Notes, vol. 36, American Mathematical Society, 2004, pp. 13–25.

[Bes07] ———, *On the computation of p-adic height pairings on Jacobians of hyperelliptic curves*, Sage Days 5, `http://wiki.sagemath.org/days5/sched`, 2007.

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis: A systematic approach to rigid analytic geometry*, Springer-Verlag, Berlin, 1984.

[BS] J. S. Balakrishnan and W. A. Stein, *A table of curves and some BSD data, based on the tables of Gonzales* et al., `http://wstein.org/tables/modjac/curves.txt`.

[CdS88] R. F. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266.

[CDV06] W. Castryck, J. Denef, and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, IMRP Int. Math. Res. Pap. (2006), Art. ID 72017, 57.

[CF05] H. Cohen and G. Frey (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005.

[CG89] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, 1989, pp. 73–81.

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[Che71] K. T. Chen, *Algebras of iterated path integrals and fundamental groups*, Trans. Amer. Math. Soc. **156** (1971), 359–379.

[Col82] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208.

[Col85] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.

[Cre] J. E. Cremona, *Elliptic curves of conductor* $\leq$ 17000, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[DV06] J. Denef and F. Vercauteren, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2*, J. Cryptology **19** (2006), no. 1, 1–25.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[FpS$^+$01] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697 (electronic). MR 1 836 926

[FvdP04] J. Fresnel and M. van der Put, *Rigid analytic geometry and its applications*, Progress in Mathematics, vol. 218, Birkhäuser Boston Inc., Boston, MA, 2004.

[GG01] P. Gaudry and N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494.

[Gro86] B. H. Gross, *Local heights on curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 327–339.

[Har07] D. Harvey, *Kedlaya's algorithm in larger characteristic*, Int Math Res Notices **2007** (2007), no. rnm095, rnm095–29.

[Har08] ———, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59.

[Har10a] M. Harrison, *Some notes on Kedlaya's algorithm for hyperelliptic curves*, preprint (2010).

[Har10b] D. Harvey, *Counting points on projective hypersurfaces*, http://www.cims.nyu.edu/ harvey/talks/zetasurface.pdf (2010).

[Kau99] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, Compositio Math. **115** (1999), no. 1, 37–69.

[Ked01] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338, erratum *ibid.* **18** (2003), 417–418.

[Kim05] M. Kim, *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656.

[Kim09] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133.

[Kim10a] ———, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), 725–747, appendix and erratum *ibid.* J. S. Balakrishnan, K. S. Kedlaya, M. Kim **24** (2011), 281–291.

[Kim10b] ———, *Personal communication to Balakrishnan and Kedlaya.*

[Kob98] N. Koblitz, *Algebraic aspects of cryptography*, Algorithms and Computation in Mathematics, vol. 3, Springer-Verlag, Berlin, 1998, With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[Lau04] A. G. B. Lauder, *Deformation theory and the computation of zeta functions*, Proc. London Math. Soc. (3) **88** (2004), no. 3, 565–602.

[Lep95] F. Leprévost, *Jacobiennes de certaines courbes de genre 2: torsion et simplicité*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 283–306.

[MP07] W. McCallum and B. Poonen, *The method of Chabauty and Coleman*, preprint (2007).

[MST06] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic).

[MT83] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1.

[Mül10] J. S. Müller, *Canonical heights on Jacobians*, Universität Bayreuth Ph.D. thesis (2010).

[Mül11] S. Müller, *Personal communication to Balakrishnan.*

[Nek93] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202.

[PS] R. Pollack and G. Stevens, *Overconvergent modular forms and p-adic L-functions*, Annales Scientifiques de l'Ecole Normale Superieure, to appear.

[S^+11] W. A. Stein et al., *Sage Mathematics Software (Version 4.7)*, The Sage Development Team, 2011, `http://www.sagemath.org`.

[Sch82] P. Schneider, *p-adic height pairings I*, Invent. Math. **69** (1982), no. 3, 401–409.

[Ste07] W. A. Stein, *The Birch and Swinnerton-Dyer conjecture, a computational approach*, 2007.

[SW11] W. A. Stein and C. Wuthrich, *Computing Tate-Shafarevich groups of elliptic curves using Iwasawa theory*, preprint (2011).

[Tat95] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[Wet97] J. L. Wetherell, *Bounding the number of rational points on certain curves of high rank*, UC Berkeley Ph.D. thesis (1997).