Author: Bommel, R. van
Title: Models of curves : the birch and Swinnerton-Dyer conjecture & ordinary reduction
Issue Date: 2018-10-31

Models of curves

The Birch and Swinnerton-Dyer conjecture & ordinary reduction

Proefschrift

ter verkrijging van
de graad Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 31 oktober 2018
klokke 12.30 uur

door

Raymond van Bommel

geboren te Haarlem

in 1991

Promotor	prof. dr. S. J. Edixhoven	Universiteit Leiden
Copromotor	dr. D. S. T. Holmes	Universiteit Leiden
Copromotor	prof. dr. F. M. Pazuki	Københavns Universitet

Doctorate Committee

Chair	prof. dr. A. W. van der Vaart	Universiteit Leiden
Secretary	prof. dr. B. de Smit	Universiteit Leiden
Member	prof. dr. T. Dokchitser	University of Bristol
Member	prof. dr. M. Stoll	Universität Bayreuth

Contents

Preface **iii**

1 Numerical verification of BSD for hyperelliptic curves of higher genus over $\mathbb{Q}$ **1**

1.1 Introduction 1

1.2 Results 4

1.3 Period 6

1.4 Torsion subgroup and rank 15

1.5 L-function 17

1.6 Regulator 20

1.7 Tamagawa numbers 24

1.8 Tate-Shafarevich group 25

2 The BSD conjecture for an elliptic curve over $\mathbb{Q}\big(\sqrt[4]{5}\,\big)$ **27**

2.1 Introduction 27

2.2 Verification for an elliptic curve over $\mathbb{Q}\big(\sqrt[4]{5}\,\big)$ 29

2.3 Methodology 33

3 Inverse Galois problem for ordinary curves **37**

3.1 Introduction 37

3.2 Ordinarity of semi-stable curves 38

3.3 Quotients of curves and their associated graphs 39

3.4 Proof of the main theorem 43

3.5 Examples of ordinary curves 46

4 Primes of ordinary reduction for hyperelliptic curves 51

4.1 Introduction . . . 51

4.2 Generalisation of Yui's criterion . . . 52

4.3 Counting ordinary polynomials over $\mathbb{F}_q$ . . . 53

4.4 Density in Specmax $\mathcal{O}_K$ . . . 54

4.5 Density in $\mathcal{O}^N$ . . . 55

4.6 Density of hyperelliptic curves with ordinary primes . . . 56

Bibliography 59

Samenvatting 65

Acknowledgements 67

Curriculum vitae 69

Preface

In the first half of the 1960s Bryan Birch and Peter Swinnerton-Dyer conceived a conjecture on certain arithmetic and geometric invariants of elliptic curves, which is now known as the Birch and Swinnerton-Dyer conjecture (BSD).

Conjecture ([BiSw65])**.** *Let $E/\mathbb{Q}$ be an elliptic curve of algebraic rank r. Let $L(E,s)$ be its L-function, R_E its regulator, $Ш(E)$ its Tate-Shafarevich group and Ω_E its real period. For each prime p, let c_p be the Tamagawa number of E at p. Then $L(E,s)$ has an analytic continuation, $Ш(E)$ is finite, $L(E,s)$ has a zero of order r at $s=1$, and*

$$\lim_{s\to 1}(s-1)^{-r}L(E,s) = \frac{R_E\cdot\Omega_E\cdot|Ш(E)|\cdot\prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

The conjecture, which has been the result of many computations with elliptic curves, has been generalised later to abelian varieties over general number fields by Tate ([Tate66]).

Due to work of Holmes ([Holm12]) and Müller ([Müll14]), it became possible to compute the regulator for Jacobians of hyperelliptic curves over $\mathbb{Q}$ of higher genus. Due to work of Dokchitser ([Dokc04]), it became possible to evaluate the L-function for the same Jacobians. The computation of Ш was still difficult, even for elliptic curves. This lead us to the following question.

Question. Is it possible to numerically verify, except for the computation of Ш, the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves over $\mathbb{Q}$?

In [FLSSSW01], Flynn, Leprévost, Schaefer, Stein, Stoll and Wetherell already showed that this is possible for some curves of genus 2, but they relied on modular methods to do so.

In chapter 1, we describe the implementation and results of an algorithm in `Magma` to do this verification without using modular methods, and also for hyperelliptic curves of genus greater than 2. The main contribution of the author is an implementation of an algorithm to compute the Tamagawa numbers, and a better theoretical understanding of the different sheaves of differentials on the regular model of the curve, resulting in an algorithm to compute the real period.

It has already been known due to Tate ([Tate66]) and Milne ([Mil72]) that the Birch and Swinnerton-Dyer conjecture is compatible with isogenies and Weil restrictions. The

Jacobian of an elliptic curve over a quadratic number field is an abelian surface over $\mathbb{Q}$, and most abelian surfaces are Jacobians. So we asked ourselves the following question.

Question. Is it possible to numerically verify, except for Ш, the Birch and Swinnerton-Dyer conjecture for an elliptic curve over a quadratic number field, using the methods for genus 2 curves over $\mathbb{Q}$?

Unfortunately, this turned out to be more difficult than expected, but we did manage to find an example of an elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$ for which we could verify the Birch and Swinnerton-Dyer conjecture, using the methods for genus 2 curves over $\mathbb{Q}$. In chapter 2, we prove the results and explain the methods used to find this example.

The last two chapters of this thesis treat ordinary reduction for curves. While proving that for all positive integers M and g and any number field K, a proportion of 100% of hyperelliptic curves of genus g over K, ordered by height, have at least M primes of ordinary good reduction (see chapter 4), we found that the hardest part was to actually prove that there exist ordinary hyperelliptic curves of genus g in each characteristic.

For hyperelliptic curves, this matter has been resolved by Glass and Pries in [GlPr05]. Instead of hyperelliptic curves, which are $\mathbb{Z}/2\mathbb{Z}$-covers of $\mathbb{P}^1$, one could also look at Galois covers of $\mathbb{P}^1$ with fixed Galois group G, and ask the following question, for which the methods of Glass and Pries do not give an easy answer.

Question. Are there Galois covers $C \to \mathbb{P}^1$ with Galois group G in characterstic p, such that C is ordinary?

The inverse Galois problem has already been studied extensively for $\mathbb{P}^1$, but the methods used for this, mainly based on rigid geometry, does not seem to give any information on whether the curves obtained are ordinary or not.

In chapter 3, we show how one can partially answer the question for ordinary curves. We construct Galois covers of ordinary semi-stable curves, and use deformation theory to deform them into Galois covers of ordinary smooth curves. We provide several classes of examples for which this construction gives a positive answer to the question. The content of this chapter has appeared, in a shortened form, in the International Journal of Number Theory, see [vB18].

In chapter 4, we will apply the results of chapter 3 to prove the aforementioned result on the proportion of hyperelliptic curves having at least M primes of ordinary good reduction.

The reader is advised that the chapters of this thesis are written to be independent. The author intends to also publish the first two chapters separately, in shortened form, as articles. The content of each chapter is supposed to be self-contained. It could happen that notations between the different chapters differ slightly.

Chapter 1

Numerical verification of BSD for hyperelliptic curves of higher genus over $\mathbb{Q}$

Abstract. The Birch and Swinnerton-Dyer conjecture has been numerically verified for the Jacobians of 32 modular hyperelliptic curves of genus 2 by Flynn, Leprévost, Schaefer, Stein, Stoll and Wetherell, using modular methods. In the calculation of the real period, there is a slight inaccuracy, which might give problems for curves with non-reduced components in the special fibre of their Néron model. In this chapter we explain how the real period can be computed, and how the verification has been extended to many more hyperelliptic curves, some of genus 3, 4 and 5, without using modular methods.

1.1 Introduction

In [BiSw65], Birch and Swinnerton-Dyer first stated their famous conjecture, based on computations with elliptic curves. Later, in [Tate66], Tate generalised the conjecture to abelian varieties of higher dimension.

Conjecture 1.1.1 (BSD over $\mathbb{Q}$, [HiSi00, Conj. F.4.1.6, p. 462]). *Let $A/\mathbb{Q}$ be an abelian variety of dimension d and algebraic rank r. Let $L(A,s)$ be its L-function, $A^\vee$ its dual, R_A its regulator, $\text{Ш}(A)$ its Tate-Shafarevich group and P_A its period. For each prime p, let c_p be the Tamagawa number of A at p. Then $L(A,s)$ has a zero of order r at $s=1$ and*

$$\lim_{s\to 1}(s-1)^{-r}L(A,s) = \frac{P_A R_A \cdot |\text{Ш}(A)| \cdot \prod_p c_p}{|A(\mathbb{Q})_{\text{tors}}| \cdot |A^\vee(\mathbb{Q})_{\text{tors}}|}.$$

In fact, Tate stated the conjecture for abelian varieties over general number fields.

Conjecture 1.1.2 (BSD over number fields, [Tate66])**.** *Let K be a number field of degree n over $\mathbb{Q}$ and discriminant D_K. Let A/K be an abelian variety of dimension d and algebraic rank r. Let $L(A,s)$ be its L-function, $A^\vee$ its dual, R_A its regulator, $Ш(A)$ its Tate-Shafarevich group and P_A its period. For each prime p of $\mathcal{O}_K$, let c_p be the Tamagawa number of A at p. Then $L(A,s)$ has a zero of order r at $s=1$ and*

$$\lim_{s\to 1}(s-1)^{-r}L(A,s) = \frac{P_A R_A \cdot |Ш(A)| \cdot \prod_p c_p}{\sqrt{|D_K|^d} \cdot |A(K)_{\mathrm{tors}}| \cdot |A^\vee(K)_{\mathrm{tors}}|}.$$

Remark 1.1.3. In Tate's original version, [Tate66], the period, Tamagawa numbers and discriminant are put in the normalisation of the L-function.

In [Tate66], Tate proved that the conjecture is compatible with products and isogenies. In [Mil72], Milne proved that the conjecture is compatible with Weil restriction, so BSD holds for all abelian varieties over all number fields if and only if it holds for all abelian varieties over $\mathbb{Q}$.

Due to work of Kolyvagin ([Koly89], [Koly91]) and others, a weak version of BSD has been proven for elliptic curves over $\mathbb{Q}$ with analytic rank at most 1. More precisely, we know that in these cases the algebraic rank equals the analytic rank and that $Ш$ is finite. On the other hand, on the numerical side, in [FLSSSW01] Flynn et al. numerically verified BSD for the Jacobians of 32 hyperelliptic curves of genus 2 with small conductor, using modular methods for their calculations.

There is, however, a slight inaccuracy in [FLSSSW01]. In the calculation of the real period, calculations seem to be done inside the sheaf of relative differentials, while they should be done inside the canonical sheaf. For curves whose Néron model has non-reduced fibres, this could cause a problem. For the curves considered, it did not seem to invalidate the final results.

The goal of this chapter is twofold. On the one hand, we will give a more explicit algorithm to compute the real period, or more specifically, a Néron differential, along with the theoretical foundations that are needed for this. On the other hand, we will present how we extended the numerical verification of BSD to many more hyperelliptic curves of genus 2, 3, 4 and 5 without using modular methods. As far as the author is aware, this is the first time BSD has been numerically verified for curves of genus 3, 4 and 5.

We did not compute, however, the order of $Ш(A)$. Moreover, the verification is only provable up to squares. That is, all terms but $|Ш(A)|$ are computed, of which some are only provably correct up to squares. Then it is verified that the conjectural order of $Ш(A)$, as predicted by the conjecture, up to a certain high precision, is a rational square or two times a rational square, in accordance with the criteria described in [PoSt99].

1.1.1 Chapter outline

The structure of this chapter is as follows. First we present our verification results. Then we discuss the computation of the real period and the theoretical background needed. Then we discuss the other terms in the BSD formula, including some background material which is already known.

Throughout this chapter, except for section 1.3, we will use the following notation.

Notation 1.1.4. We define $H/\mathbb{Q}$ to be a hyperelliptic curve of genus g. When a prime p is introduced, $\mathcal{H}/\mathbb{Z}_{(p)}$ is a regular model of H over $\mathbb{Z}_{(p)}$. The Jacobian of H is denoted by J, and the Néron model of J over $\mathbb{Z}$ is called $\mathcal{J}$.

Unless stated otherwise, as for example in Example 1.1.5, we will assume that H is given by a model of the form $y^2 = f(x)$, where the input polynomial $f(x)$ has odd degree (and hence H has a rational Weierstraß point).

Moreover, the following examples will be used to illustrate the computations.

Example 1.1.5. Let H_1 be the hyperelliptic curve over $\mathbb{Q}$ defined by

$$y^2 + (x^3 + x + 1)y = x^6 + 5x^5 + 12x^4 + 12x^3 + 6x^2 - 3x - 4.$$

It is curve 125,B from [FLSSSW01]. Its discriminant is 5^{16} and its conductor is 125. We will numerically verify BSD for J_1, the Jacobian of H_1, and check that the results agree with those from [FLSSSW01].

Example 1.1.6. Let H_2 be the hyperelliptic curve over $\mathbb{Q}$ defined by

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

having discriminant $62720 = 2^8 \cdot 5 \cdot 7^2$ and conductor 7840 (label $7840.a.62720.1$ from [LMFDB]). We will numerically verify BSD for J_2, the Jacobian of H_2, which has algebraic rank equal to 1.

Example 1.1.7. Let H_3 be the hyperelliptic curve over $\mathbb{Q}$ defined by

$$y^2 = x^7 - x^6 + 3x^5 - x^4 + 2x^3 + x^2 + 1,$$

having discriminant $-1523712 = -2^{14} \cdot 3 \cdot 31$. We will numerically verify BSD for J_3, the Jacobian of H_3, which has algebraic rank 1.

1.1.2 Acknowledgements

The author wishes to thank his supervisors David Holmes and Fabien Pazuki. Moreover, Tim Dokchitser and Steffen Müller are thanked for their advise and insight, Carlo Pagano is thanked for helping with the proof of a lemma, and an anonymous referee, who refereed an article submitted on which this chapter is based, is thanked for the comments they provided to improve this chapter.

1.2 Results

For the Jacobians of the curves listed below, we numerically verified BSD in the following sense. We numerically determined the algebraic and analytic rank, the special value of the L-function, the regulator (provably only up to squares), the real period, the Tamagawa numbers, and the size of the torsion subgroup of the Jacobian, assuming some conjectures mentioned below. Then the BSD formula was used to calculate a conjectural order for Ш, and it was verified that it is a rational square (which it should be according to the criteria in [PoSt99]).

In practice this meant that the conjectural order for Ш was less than 10^{-9} away from an integer. Moreover, for all but one of the curves of genus 2, this conjectural order was actually equal to 1.000000000.

The conjectural results that we assume to hold for the verification include the analytic continuation, and the correctness of the functional equation of the L-function (see [HiSi00, Conj. F.4.1.5, p. 461]). When we computed the analytic rank, we did this by numerically checking whether the L-function and its derivatives up to certain order, vanish at 1. Even though this does not prove that these functions vanish, we do assume this to be true. Moreover, we assume the correctness of Ogg's formula for the computation of the 2-part of the conductor (for more details, see Remark 1.5.8). In a certain sense, one could say that our verification also provides evidence for these conjectures.

List of curves:

- All elliptic curves of the form $y^2 = x^3 + ax + b$ with $a, b \in \{-15, \dots, 15\}$, and compared it with the outcomes of already existing algorithms in `Magma`.
- All hyperelliptic curves from [FLSSSW01], comparing it with the outcomes given in that article.
- All 300 hyperelliptic curves C of genus 2, of the form

  $$y^2 = x^5 + ax^4 + bx^3 + cx^2 + dx + e,$$

  up to isomorphism, with $a, b, c, d, e \in \{-10, \dots, 10\}$ and $\Delta(C) \le 10^5$. About one third of them have rank 1, the rest are of rank 0. They are all contained in the LMFDB, cf. [BSSVY16].
- All 6 hyperelliptic curves of genus 3, of the form

  $$y^2 = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + fx + g,$$

  with $a, b, c, d, e, f, g \in \{-3, \dots, 3\}$ and $\Delta(C) \le 10^6$, i.e., we checked BSD, up to squares, for

  - H_4: $(a, b, c, d, e, f, g) = (1, -3, 2, 2, -3, 0, 1, 0)$,
  - H_5: $(a, b, c, d, e, f, g) = (1, -2, -1, 2, 2, -1, -1, 0)$,
  - H_6: $(a, b, c, d, e, f, g) = (1, 0, -3, -2, 2, 3, 1, 0)$,

- $H_7\colon (a,b,c,d,e,f,g) = (1,0,-1,0,-2,3,-1,0)$,
- $H_8\colon (a,b,c,d,e,f,g) = (1,1,-2,-2,1,2,-1,0)$,
- $H_9\colon (a,b,c,d,e,f,g) = (1,-3,2,0,1,0,-1,0)$,

and, in order to have an example of rank 1, the curve

- $H_{10}\colon (a,b,c,d,e,f,g) = (1,-3,1,3,-2,0,1,0)$.

As far as we are aware these are the first examples of curves of genus 3 for which BSD has been numerically verified. These were the invariants we found:

	r	$\lim_{s\to 1}\dots$	P_A	R_A	c_p	$\lvert A(\mathbb{Q})_{\text{tors}}\rvert$	$\lvert Ш\rvert_{\text{an}}$
H_4	0	0.8006061	51.23879	1	$c_2 = c_5 = c_{23} = 1$	8	1.000000
H_5	0	0.7636550	48.87392	1	$c_2 = c_5 = c_{23} = 1$	8	1.000000
H_6	0	0.9275079	59.36050	1	$c_2 = c_5 = c_{23} = 1$	8	1.000000
H_7	0	0.8087909	51.76262	1	$c_2 = c_5 = c_{31} = 1$	8	1.000000
H_8	0	0.9784790	62.62265	1	$c_2 = c_5 = c_{23} = 1$	8	1.000000
H_9	0	0.4310775	55.17793	1	$c_2 = 2, c_5 = c_{23} = 1$	16	1.000000
H_{10}	1	1.953631	50.85263	0.6146799	$c_2 = c_5 = c_{11} = 1$	4	1.000000

For the torsion and regulator, points were searched up to a certain height on the Jacobian. This maximum search height is considerably smaller than the height given by the various height bounds in the literature. It is possible that the size of the torsion subgroups and the regulator is incorrect, but this would only cause a rational square error factor for the value of $\lvert Ш\rvert_{\text{an}}$.

- The curve

$$y^2 + (x^5 + x^2)y = x^8 + x^7 + x^6 + 4x^5 + 3x^4 + 2x^3 + 4x^2 + 2x$$

of genus 4, with discriminant -1,064,000, which was found by Harrison ([Harr18]). It has Mordell-Weil rank 0. We found $L(A,1) \approx 0.09889146$, $P_A \approx 178.0046$, $c_2 = 2$, $c_p = 1$ for all other p, and $\lvert A(\mathbb{Q})_{\text{tors}}\rvert = 60$, yielding $\lvert Ш\rvert_{\text{an}} = 1.0000000$. Again the torsion is not computed in a provable way. However by reducing modulo 3, we found that the torsion is a divisor of 180. As far as we are aware this is the first example of a curve of genus 4 for which BSD has been numerically verified.

- The curve

$$y^2 + (x^6 + x^4 + 1)y = x^4 + x^2$$

of genus 5, with discriminant 116,985,856, found in the aforementioned list. It has Mordell-Weil rank 0. We found $L(A,1) \approx 0.1002872$, $P_A \approx 579.2589$, $c_p = 1$ for all p, and $\lvert A(\mathbb{Q})_{\text{tors}}\rvert = 76$, yielding $\lvert Ш\rvert_{\text{an}} = 1.0000000$. As this curve does not have a rational Weierstaß point (which we actually do assume for most of the chapter), the search for torsion points was much more cumbersome, due to the Mumford representation not behaving well in this case. Again it is not provable; the best upper bound for the torsion that we found is 304. As far as we are aware this is the first example of a curve of genus 5 for which BSD has been numerically verified.

Remark 1.2.1. It could be the case that some of these curves have isomorphic (or isogenous) Jacobians. Then we actually verified BSD two times for the same abelian variety. In the verification process, we did not check for this.

Remark 1.2.2. Even though for all our curves the verification went well, it should be remarked that problems are to be expected when trying to verify BSD for curves with higher discriminant (or rather, higher conductor). The computation of the L-function takes much longer in these cases. Also the computation of the regulator will be harder, as the heights of the points involved might increase, in particular in case the Mordell-Weil rank is higher.

It should be feasible to carry out the verification for more of the small examples from Harrison's list, [Harr18] of genus 4, as long as the maximum bad prime is small enough. We also tried the verification for some more examples of genus 5, but in these cases the computation of the special value of the L-function was taking hours and the computation of the regular model sometimes did not seem to finish in reasonable time.

1.3 Period

Let C/K be a smooth, geometrically irreducible, projective curve of genus g over K. Let J/K be its Jacobian. The goal of this section is to define the period of J, and to describe a way to compute it in the case C is hyperelliptic. We will be following the algorithm described in [FLSSSW01, sect. 3.5].

First we will discuss the theoretical considerations that are needed for this algorithm. Throughout the section p will be a prime of the ring of integers $\mathcal{O}_K$ of K, and S will be the scheme $\operatorname{Spec}(\mathcal{O}_{K,p})$. The generic point of S is called η and the special point is called s.

1.3.1 Preliminaries

First, for completeness, we will recall the following definition.

Definition 1.3.1 ([BLR90, p. 166])**.** A *(relative) curve* $\mathcal{C}$ over S is a normal, proper, flat S-scheme, such that for all $t \in S$, the scheme $\mathcal{C}_t = \mathcal{C} \times_S k(t)$ is of pure dimension 1. A *model of C over S* is a relative curve $\mathcal{C}$ over S together with an isomorphism $\mathcal{C}_\eta \cong C$. Models are called *regular* when the relative curve $\mathcal{C}$ is regular.

Remark 1.3.2. Without the normality assumption, the special fibre of a curve over S could have embedded components. For example, $\operatorname{Spec}(R)$ for $R = \mathbb{Z}_{(2)}[x,y]/(x^2, 2x, xy)$, without the normality assumption, is a curve over $\mathbb{Z}_{(2)}$. But, in the special fibre, the associated prime $\operatorname{Ann}(\bar{x}) = (\bar{x}, \bar{y})$ gives rise to an embedded component. In order to be able to use the results from [BLR90], which have been partially derived from [Rayn70], it is necessary to assume that our curves do not have embedded components.

1.3.2 Generalities about the Picard functor and regular model

In this subsection, we will consider two objects: the identity component of the Néron model of the Jacobian of C, and the Picard scheme of componentwise degree zero divisors on a regular model of C. Under some mild assumptions, we will prove that these objects exist and that they are isomorphic.

Let $\overline{s} : \operatorname{Spec}(\overline{\mathbb{F}_p}) \to S$ be a geometric point lying above s. Let $\mathcal{C}/S$ be a regular model of C. Let $C_1, \ldots, C_n$ be the irreducible components of the special fibre $\mathcal{C}_s$ of $\mathcal{C}$ with generic points $\eta_1, \ldots, \eta_n \in \mathcal{C}$.

For $i = 1, \ldots, n$ let δ_i be the geometric multiplicities of the irreducible component C_i inside the special fibre of $\mathcal{C}$, i.e. the length of the local Artinian ring $\mathcal{O}_{\mathcal{C}_{\overline{s}},\overline{\eta_i}}$, where $\overline{\eta_i} \in \mathcal{C}_{\overline{s}}$ is a point lying above η_i. For the remainder of this chapter, we shall assume that the greatest common divisor of the δ_i equals 1. This is, for example, the case when C has a K-rational point.

On the one hand, J has a Néron model J_{N} over S by [BLR90, Prop. 9.5.6, p. 268], and this Néron model has a fibrewise connected component $\mathcal{J}$ containing the identity. On the other hand, we have the functor $\operatorname{Pic}^0_{\mathcal{C}/S}$ of componentwise degree zero divisors on $\mathcal{C}$. The following theorem will prove that these two things are the same.

Theorem 1.3.3 ([BLR90, Thm. 4(b), sect. 9.5, p. 267]). *Let $\mathcal{C}$ be a curve over S whose generic fibre is geometrically irreducible. Assume that, in addition, $\mathcal{C}$ is regular, and that the greatest common divisor of the δ_i is 1. Then $\operatorname{Pic}^0_{\mathcal{C}/S}$ is a separated scheme and $\operatorname{Pic}^0_{\mathcal{C}/S}$ coincides with the identity component of the Néron model of J.*

Let $f : \mathcal{C} \to S$ be the structure morphism. From [Rayn70, Prop. 5.2, p. 46], it now follows that f is cohomologically flat, i.e. for every sheaf $\mathcal{F}$ of $\mathcal{O}_{\mathcal{C}}$-modules and every $T \to S$ the sheaves of $\mathcal{O}_T$-modules $(f_*\mathcal{F})_T$ and $f_*(\mathcal{F}_{\mathcal{C}_T})$ are naturally isomorphic, which we will need for the next part.

1.3.3 Differentials of Jacobian and regular model

A classical theorem (see for example [Mil86, Prop. 2.2, p. 172]) relates the differentials on the Jacobian of a smooth curve over a field with the differentials on the curve itself. We will generalise this to $\mathcal{J}$ and $\mathcal{C}$.

Definition 1.3.4 ([Liu02, Def. 4.7, sect. 6.4.2, p. 239]). Let Y/T be a quasi-projective locally noetherian scheme. Let $i : Y \to Z$ be an immersion into a smooth scheme Z/T. Then the *canonical sheaf of Y/T* is defined to be the $\mathcal{O}_Y$-module

$$\omega_{Y/T} := \det(i^*(\mathcal{I}/\mathcal{I}^2))^\vee \otimes_{\mathcal{O}_T} i^*(\det \Omega^1_{Z/T}),$$

where $\mathcal{I}$ is the sheaf of ideals defining Y in an open $Z' \subset Z$ containing Y as closed subset. This is independent of the choice of Z and i, see *loc. cit.*

The following lemma generalises the aforementioned theorem.

Lemma 1.3.5. *There are canonical isomorphisms of $\mathcal{O}_S$-modules*

$$\begin{tikzcd}
\Omega^1_{\mathcal{J}/S}(\mathcal{J}) \arrow[d, "\sim"] & & \omega_{\mathcal{C}/S}(\mathcal{C}) \arrow[d, "\sim"', "GD"] \\
\mathit{Hom}_{\mathcal{O}_S}(\mathrm{Lie}(\mathcal{J}), \mathcal{O}_S) \arrow[rr, "\alpha", "\sim"'] & & \mathit{Hom}_{\mathcal{O}_S}(R^1 f_*(\mathcal{O}_{\mathcal{C}}), \mathcal{O}_S)
\end{tikzcd}$$

Proof. The right hand isomorphism is given by Grothendieck duality, see [Liu02, Sect. 6.4.3, p. 243]. The bottom isomorphism, α, is from [BLR90, Thm. 8.4.1, p. 231] (here we use that $\mathcal{C}/S$ is cohomologically flat). Getting the left hand isomorpism is a little bit more involved.

First note that global differentials on an abelian variety are translation invariant. As the image of J is dense in $\mathcal{J}$, also the differentials in $\Omega^1_{\mathcal{J}/S}(\mathcal{J})$ are translation invariant. Combining this with [BLR90, Prop. 4.2.1, p. 100], we get

$$\Omega^1_{\mathcal{J}/S}(\mathcal{J}) = \Omega^1_{\mathcal{J}/S}(\mathcal{J})^{\mathrm{inv}} = (e^*\Omega^1_{\mathcal{J}/S})(S), \tag{1.1}$$

where $e : S \to \mathcal{J}$ is the unit section. Now, by [Liu02, Prop. 6.1.24, p. 217], we get an exact sequence of $\mathcal{O}_S$-modules

$$\mathfrak{m}/\mathfrak{m}^2 \to e^*\Omega^1_{\mathcal{J}/S} \to \Omega^1_{S/S} = 0,$$

where $\mathfrak{m}$ is the ideal of the schematic image of e inside $\mathcal{J}$. As both $\mathfrak{m}/\mathfrak{m}^2$ and $\Omega^1_{\mathcal{J}/S}$, and hence $e^*\Omega^1_{\mathcal{J}/S}$ are locally free of rank g (as $\mathcal{J}$ is regular), we get that the kernel of $\mathfrak{m}/\mathfrak{m}^2 \to e^*\Omega^1_{\mathcal{J}/S}$ is torsion. As $\mathcal{O}_S$ is torsion-free in our case, and hence the locally free module $\mathfrak{m}/\mathfrak{m}^2$ is torsion-free, we find a canonical isomorphism of $\mathcal{O}_S$-modules

$$e^*\Omega^1_{\mathcal{J}/S} = \mathfrak{m}/\mathfrak{m}^2 = \mathscr{H}\!om_{\mathcal{O}_S}(\mathrm{Lie}(\mathcal{J}), \mathcal{O}_S),$$

which gives, by taking global sections and composing with eqn. (1.1), the construction of the left hand isomorphism in the diagram. □

Remark 1.3.6. Under the usual natural identifications $\Omega^1_{\mathcal{J}/S}(\mathcal{J}) \otimes_{\mathcal{O}_{K,p}} K = \Omega^1_{J/K}(J)$ and $\omega_{\mathcal{C}/S}(\mathcal{C}) \otimes_{\mathcal{O}_{K,p}} K = \Omega^1_{C/K}(C)$, the isomorphism $\Omega^1_{\mathcal{J}/S}(\mathcal{J}) \cong \omega_{\mathcal{C}/S}(\mathcal{C})$ in the lemma above is compatible with the aforementioned classical isomorphism $\Omega^1_{J/K}(J) \cong \Omega^1_{C/K}(C)$.

1.3.4 Periods for abelian varieties

For this subsection, let us consider a general abelian variety A/K of dimension g over a number field. Let $\mathcal{A}/\mathcal{O}_K$ be a Néron model of A. The $\mathcal{O}_K$-module $\Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})^{\mathrm{inv}}$ of translation invariant 1-forms is finite locally free of rank g, and it satisfies

$$\Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})^{\mathrm{inv}} \otimes_{\mathcal{O}_K} K = \Omega^1_{A/K}(A)^{\mathrm{inv}}.$$

Let $\underline{\omega} = (\omega_1, \ldots, \omega_g)$ be a K-basis of $\Omega^1_{A/K}(A)^{\mathrm{inv}}$. Then the element $\omega_1 \wedge \ldots \wedge \omega_g$ generates the linear space $\bigwedge^g \Omega^1_{A/K}(A)^{\mathrm{inv}}$, inside which there is the finite locally free $\mathcal{O}_K$-module $\bigwedge^g \Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})^{\mathrm{inv}}$ of rank 1. Then let $I_{\underline{\omega}}$ be the fractional ideal such that

$$\bigwedge^g \Omega^1_{\mathcal{A}/\mathcal{O}_K}(\mathcal{A})^{\mathrm{inv}} = I_{\underline{\omega}} \cdot (\omega_1 \wedge \ldots \wedge \omega_g).$$

Remark 1.3.7. Over $\mathbb{Q}$, the situation is much easier. As $\mathbb{Q}$ has class number 1, the ideal $I_{\underline{\omega}}$ is always principal, and $\bigwedge^g \Omega^1_{\mathcal{A}/\mathbb{Z}}(\mathcal{A})^{\mathrm{inv}}$ is generated by a differential, which is also called a *Néron differential* of A. Over general number fields, such a differential does not need to exist.

Let v be a complex place of K and let $\sigma_v : K \hookrightarrow \mathbb{C}$ be an embedding of K corresponding to v. Then $A_{\mathbb{C},\sigma_v}$ is isomorphic to $\mathbb{C}^g/\Lambda_v$, where Λ_v is a full-rank lattice inside $\mathbb{C}^g$. This lattice Λ_v is not unique, but we can use our chosen basis $\underline{\omega}$ to find a specific lattice Λ_v. The local period at v is to be thought of as the covolume of this lattice.

Definition 1.3.8 (Local complex period)**.** Let v be a complex place of K, and let $K_v \cong \mathbb{C}$ be the completion of K at v. Let $(\gamma_1, \ldots, \gamma_{2g})$ be a basis of $H^1(A(K_v), \mathbb{Z})$. Then the *local period of A at v with respect to $\underline{\omega}$* is

$$\Omega_{A/K_v,\underline{\omega}} = \left| \det \left(\int_{\gamma_i} \omega_j , \overline{\int_{\gamma_i} \omega_j} \right)_{i,j=1}^{i=2g,j=g} \right| .$$

For a real place v of K, let $\sigma_v : K \hookrightarrow \mathbb{R} \subset \mathbb{C}$ be an embedding corresponding to v. Again we get a lattice Λ_v inside $\mathbb{C}^g$, but this time, we are interested in $\Lambda'_v := \Lambda_v \cap \mathbb{R}^g$. The lattice Λ_v is closed under complex conjugation and Λ'_v is a lattice of full rank inside $\mathbb{R}^g$. The local period at v is to be thought of as the covolume of this lattice Λ'_v multiplied by the number of connected components of $A_{\mathbb{R},\sigma_v}$.

Definition 1.3.9 (Local real period)**.** Let v be a real place of K, and let $K_v \cong \mathbb{R}$ be the completion of K at v. Let $(\gamma_1, \ldots, \gamma_g)$ be a basis of $H^1(A(\overline{K_v}), \mathbb{Z})^{\mathrm{Gal}(\overline{K_v}/K_v)}$ and let m_v be the number of connected components of $A(K_v)$. Then the *local period of A at v with respect to $\underline{\omega}$* is

$$\Omega_{A/K_v,\underline{\omega}} = m_v \cdot \left| \det \left(\int_{\gamma_i} \omega_j \right)_{i,j=1}^{g} \right| .$$

Remark 1.3.10. For a real place v, we have the following characterisation of connected components of $A(K_v)$. In $\mathbb{C}^g$, we can consider g-dimensional affine spaces ν parallel to $\mathbb{R}^g$. Each such ν is of the form $\{x \in \mathbb{C}^g : \mathrm{Re}(x) = c\}$, for some $c \in \mathbb{R}^g$. The space ν gives rise to a real component if and only if $c \in \frac{1}{2}\Lambda'_v$ (because, this is equivalent to the condition $x - \overline{x} \in \Lambda'_v$ for all $x \in \nu$), and two of them give rise to the same component if one of them is a translate of the other one by an element in Λ_v. In other words, the connected components correspond to $\frac{1}{2}\Lambda'_v/\pi(\Lambda_v)$, where $\pi : \mathbb{C}^g \to \mathbb{R}^g$ is the projection on the real coordinates. Hence, we have $m_v := [\Lambda'_v : 2\pi(\Lambda_v)]$.

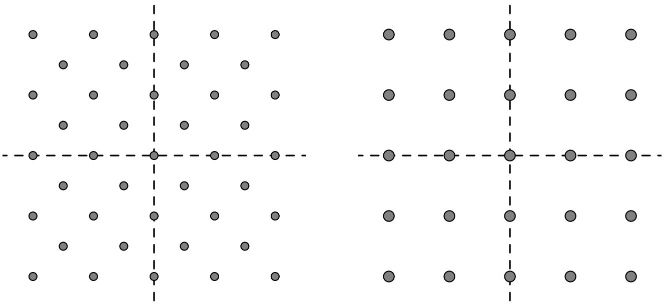


Figure: *Examples of lattices in $\mathbb{C}$ with one (left) and two (right) real components.*

Observe that $2\pi(\Lambda_v) = \{\lambda + \overline{\lambda} : \lambda \in \Lambda_v\}$. Let $(\gamma_1', \dots, \gamma_{2g}')$ be a basis of $H^1(A(\overline{K_v}), \mathbb{Z})$. Then, combining all these observations, we find that the vectors

$$s_i := \left(\int_{\gamma_i'} \omega_j \right)_{j=1}^{g} + \left(\overline{\int_{\gamma_i'} \omega_j} \right)_{j=1}^{g}, \quad \text{for } i = 1, \dots, 2g,$$

generate the lattice $2\pi(\Lambda_v)$ inside $\mathbb{R}^g$, which has covolume $\Omega_{A/K_v, \underline{\omega}}$. We will use this later to calculate the local period in practice.

Now we will define the period of A as the product of the local periods. However, we do have to compensate with some factors depending on $\underline{\omega}$ to make sure that the definition does not depend on the choice of $\underline{\omega}$.

Definition 1.3.11 (Period)**.** The *period of A* is defined as

$$\Omega_{A/K} = N_{K/\mathbb{Q}}(I_{\underline{\omega}}) \cdot \prod_{v | \infty} \Omega_{A/K_v, \underline{\omega}}.$$

Proposition 1.3.12. *The period of A does not depend on the choice of $\underline{\omega}$.*

Proof. We can reduce the proposition to the following specific case. Suppose that $\underline{\omega}_1$ and $\underline{\omega}_2$ are bases, such that $\mathcal{O}_K$-module generated by $\underline{\omega}_1$ is contained in the $\mathcal{O}_K$-module generated by $\underline{\omega}_2$, and has index N. Then, on the one hand,

$$\Omega_{A/K_v, \underline{\omega}_2} = N^{[K_v:\mathbb{R}]} \cdot \Omega_{A/K_v, \underline{\omega}_1},$$

On the other hand

$$N_{K/\mathbb{Q}}(I_{\underline{\omega}_1}) = N^{[K:\mathbb{Q}]} \cdot N_{K/\mathbb{Q}}(I_{\underline{\omega}_2}).$$

Hence, taking the product, we see that these factors cancel and that the definition indeed does not depend on the choice of $\underline{\omega}$. □

Remark 1.3.13. If A is the Jacobian of a curve C over K, then it is also possible to find a basis of differentials in $\Omega^1_{C/K}$ and integrate them along a symplectic basis of $H^1(C, \mathbb{Z})$. As these integrals are the pull-backs of the corresponding integrals on the Jacobian along the Abel-Jacobi map, this gives the same result.

1.3.5 Algorithm for the real period

We will return to the situation where C is a hyperelliptic curve, $\mathcal{C}$ a regular model, J its Jacobian with Néron model $\mathcal{J}$. From now on we will assume that $K = \mathbb{Q}$.

Suppose that $\omega_1, \ldots, \omega_g \in \Omega^1_{C/\mathbb{Q}}(C)$ are such that, for every prime p, they form a $\mathbb{Z}_{(p)}$-basis of $\omega_{\mathcal{C}/S}(\mathcal{C})$, under the identification $\omega_{\mathcal{C}/S}(\mathcal{C}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} = \Omega^1_{C/\mathbb{Q}}(C)$. In other words, cf. Lemma 1.3.5, suppose that $\omega_1, \ldots, \omega_g$ correspond to generators of $\Omega^1_{\mathcal{J}_\mathbb{Z}/\mathbb{Z}}(\mathcal{J}_\mathbb{Z})$, where $\mathcal{J}_\mathbb{Z}/\mathbb{Z}$ is a Néron model of J over $\operatorname{Spec}\mathbb{Z}$. Moreover, let $\gamma_1, \ldots, \gamma_{2g} \in H^1(C, \mathbb{Z})$ form a symplectic basis for the homology. Then the real period is the covolume of the lattice

$$\mathbb{Z}(a_1 + \overline{a_1}) + \ldots + \mathbb{Z}(a_{2g} + \overline{a_{2g}}) \subset \mathbb{R}^g,$$

where $a_i = (\int_{\gamma_i} \omega_j)_{j=1}^g \in \mathbb{C}^g$ for $i = 1, \ldots, 2g$.

Now suppose that we are working with a hyperelliptic curve given by $y^2 = f$ for some $f \in \mathbb{Q}[x]$. Then, due to Van Wamelen there is a procedure in `Magma` to compute a symplectic basis of $H^1(C, \mathbb{Z})$ as mentioned before, and the integrals $\int_{\gamma_i} \frac{x^{j-1} \cdot dx}{y}$ for all $i = 1, \ldots, 2g$ and $j = 1, \ldots, g$.

In order to compute the real period, we only need to find a basis $\omega_1, \ldots, \omega_g$ as above in terms of the differentials $\frac{x^{j-1} \cdot dx}{y}$. For our purpose, the calculation can be done for each prime p separately. Fortunately for us, due to Donnelly, `Magma` also has an algorithm to compute explicit equations for a regular model $\mathcal{C}$ of C over S. It will represent $\mathcal{C}/S$ by giving charts, each of which is a relative complete intersection. The following lemma explicitly gives the isomorphism $\omega_{\mathcal{C}/S}(\mathcal{C}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q} \cong \Omega^1_{C/\mathbb{Q}}(C)$ that we need to compute whether a certain differential is vanishing or having a pole on one of the components of the special fibre (Step 5 and 6 in Algorithm 1.3.16).

Lemma 1.3.14. *Let $\mathcal{X} \subset \mathbb{A}^n_S = \operatorname{Spec}(\mathbb{Z}_p[x_1, \ldots, x_n])$ be regular, flat, and of relative dimension 1 over $S = \operatorname{Spec}\mathbb{Z}_{(p)}$. Suppose that $\mathcal{X}$ is a relative complete intersection inside $\mathbb{A}^n_S$, given by equations $g_1 = \ldots = g_{n-1} = 0$, with $g_i \in \mathbb{Z}_{(p)}[x_1, \ldots, x_n]$. Moreover, suppose that the generic fibre $\mathcal{X}_\eta$ is smooth over $\mathbb{Q}$.*

Then, on the one hand, after possibly reordering $x_1, \ldots, x_n$, we may and will assume that $\Omega^1_{k(\mathcal{X}_\eta)/\mathbb{Q}}$ is a $k(\mathcal{X}_\eta)$-vector space of dimension 1 generated by dx_n. This space contains $\Omega^1_{\mathcal{X}_\eta/\mathbb{Q}}(\mathcal{X}_\eta)$. On the other hand, we can define $\omega_{\mathcal{X}/S}$ using this immersion into $\mathbb{A}^n_S$ (cf. Def. 1.3.4). Then $\omega_{\mathcal{X}/S}$ is free of rank 1 and generated by an element, which we will denote by $(g_1 \wedge \ldots \wedge g_{n-1})^\vee \otimes dx_1 \wedge \ldots \wedge dx_n$. Then there is a canonical isomorphism of $\mathbb{Q}$-vector spaces

$$\Omega^1_{\mathcal{X}_\eta/\mathbb{Q}}(\mathcal{X}_\eta) \xrightarrow{\sim} \omega_{\mathcal{X}/S}(\mathcal{X}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q},$$

which is given by

$$f \cdot dx_n \mapsto f \cdot \det\left(\partial g_i / \partial x_j\right)_{i,j=1}^{n-1} \cdot (g_1 \wedge \ldots \wedge g_{n-1})^\vee \otimes dx_1 \wedge \ldots \wedge dx_n.$$

Proof. On the one hand, we can consider $\mathcal{X}_\eta \subset \mathcal{X}_\eta$, on the other hand, we have an embedding $\mathcal{X}_\eta \subset \mathbb{A}^n_\mathbb{Q}$. Both give us a way to construct $\Omega^1_{\mathcal{X}_\eta/\mathbb{Q}}$, and [Liu02, Lem. 6.4.5, p.

238] gives an explicit natural isomorphism between them. What is left to check, is that this isomorphism is exactly the one described in the statement of Lemma 1.3.14.

We will break down the proof of [Liu02, Lem. 6.4.5, p. 238] to find the map explicitly. In this lemma, we will take $X = Z_1 = \mathcal{X}_\eta$, $Y = \operatorname{Spec}\mathbb{Q}$ and $Z_2 = \mathbb{A}^n_{\mathbb{Q}}$, and we let $i_2\colon \mathcal{X}_\eta \to \mathbb{A}^n_{\mathbb{Q}}$ be the map induced by the embedding of $\mathcal{X}$ into $\mathbb{A}^n_S$. The two exact sequences, induced by [Liu02, Cor. 6.3.22, p. 233] are

$$0 \to 0 \to \mathcal{C}_{\mathcal{X}_\eta/W} \to i_2^*\,\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}} \to 0 \qquad \text{and} \qquad 0 \to \mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}} \to \mathcal{C}_{\mathcal{X}_\eta/W} \to \Omega^1_{\mathcal{X}_\eta/\mathbb{Q}} \to 0,$$

where $W = \mathcal{X}_\eta \times_{\mathbb{Q}} \mathbb{A}^n_{\mathbb{Q}}$, and the map $h\colon \mathcal{X}_\eta \to W$ is given by $(\mathrm{id}_{\mathcal{X}_\eta}, i_2)$, and $\mathcal{C}_{\mathcal{X}_\eta/W} = h^*\,\mathcal{I}_h/\mathcal{I}_h^2$ and $\mathcal{C}_{\mathcal{X}_\eta}/\mathbb{A}^n_{\mathbb{Q}} = i_2^*\,\mathcal{I}_{i_2}/\mathcal{I}_{i_2}^2$ with $\mathcal{I}_h$ and $\mathcal{I}_{i_2}$ the sheaf of ideals on W and $\mathbb{A}^n_{\mathbb{Q}}$ respectively, defining $\mathcal{X}_\eta$.

We will make the maps in these exact sequences explicit, starting with the first sequence. Let $p_1\colon W \to \mathcal{X}_\eta$ and $p_2\colon W \to \mathbb{A}^n_{\mathbb{Q}}$ be the two projections. We know that $\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$ is a free sheaf generated by n elements $dx_1, \ldots, dx_n$. Now $\Omega^1_{W/\mathcal{X}_\eta}$ is identified with $p_2^*\,\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$, and in this identification the differential dx_j is mapped to dz_j, where $z_j = p_2^*\,x_j$. By pulling back along h, we get an identification $h^*\,\Omega^1_{W/\mathcal{X}_\eta} = i_2^*\,\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$.

Now the isomorphism $\mathcal{C}_{\mathcal{X}_\eta/W} \to h^*\,\Omega^1_{W/\mathcal{X}_\eta}$ is ultimately coming from [Liu02, Prop. 6.1.8, p. 212]. The sheaf $\mathcal{I}_h/\mathcal{I}_h^2$ is generated by $z_j - y_j$, for $j = 1, \ldots, n-1$, where $y_j = p_1^*\,i_2^*\,x_j$. These are mapped to $d(z_j - y_j) = dz_j$ in $h^*\,\Omega^1_{W/\mathcal{X}_\eta}$ or to dx_j in $i_2^*\,\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$.

To understand the morphism $\mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}} \to \mathcal{C}_{\mathcal{X}_\eta/W}$ in the second sequence, we have to go back to [Liu02, Cor. 6.3.22]. The sheaf $\mathcal{I}_{i_2}/\mathcal{I}_{i_2}^2$ is generated by the functions $g_1, \ldots, g_{n-1}$. Following the proof of the aforementioned corollary, we consider the following cartesian diagram.

$$\begin{tikzcd}
\mathcal{X}_\eta \times_{\mathbb{Q}} \mathcal{X}_\eta \arrow[r, "(\pi_2{,}\pi_1^*\,i_2)"] \arrow[d, "\pi_1"'] & W \arrow[d, "p_2"] \\
\mathcal{X}_\eta \arrow[r, "i_2"] & \mathbb{A}^n_{\mathbb{Q}}
\end{tikzcd}$$

Here π_1 and π_2 are the first and second coordinate projections $\mathcal{X}_\eta \times_{\mathbb{Q}} \mathcal{X}_\eta \to \mathcal{X}_\eta$. The map $h\colon \mathcal{X}_\eta \to W$ from the bottom left to the top right, using the universal property of the product, gives rise to the diagonal section $\Delta\colon \mathcal{X}_\eta \to \mathcal{X}_\eta \times_{\mathbb{Q}} \mathcal{X}_\eta$ of π_1. Then, there is the identification

$$\mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}} = \Delta^*\,\pi_1^*\,\mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}} = \Delta^*\,\mathcal{C}_{\mathcal{X}_\eta \times_{\mathbb{Q}} \mathcal{X}_\eta/W},$$

identifying the functions g_i in $\mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}}$ with the functions $p_2^*\,g_i$ in $\Delta^*\,\mathcal{C}_{\mathcal{X}_\eta \times_{\mathbb{Q}} \mathcal{X}_\eta/W}$. In other words, if you express the g_i in terms of the variables x_j on $\mathbb{A}^n_{\mathbb{Q}}$, then you get $p_2^*\,g_i$ by replacing all the x_j's by z_j's.

The map $\mathcal{C}_{\mathcal{X}_\eta/W} \to \Omega^1_{\mathcal{X}_\eta/\mathbb{Q}}$ is constructed in an analogous way to the construction of the map $\mathcal{C}_{\mathcal{X}_\eta/W} \to i_2^*\,\Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$. It sends $z_j - y_j$ to $-dw_j$, where $w_j = i_2^*\,x_j$, on $\Omega^1_{\mathcal{X}_\eta/\mathbb{Q}}$.

Now the isomorphism

$$\begin{array}{ccccc}\det \mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}} \otimes \det \Omega^1_{\mathcal{X}_\eta/\mathbb{Q}} & \longrightarrow & \det \mathcal{C}_{\mathcal{X}_\eta/W} & \longrightarrow & \det i_2^* \, \Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}} \\ (g_1 \wedge \ldots \wedge g_{n-1}) \otimes dw_n & \longmapsto & p_2^* g_1 \wedge \ldots \wedge p_2^* g_{n-1} \wedge dw_n & \longmapsto & dg_1 \wedge \ldots \wedge dg_{n-1} \wedge dx_n\end{array}$$

is constructed cf. [Liu02, Lem. 6.4.1, p. 236–237]. Of course,

$$dg_1 \wedge \ldots \wedge dg_n \wedge dx_n = \det \left(\partial g_i/\partial x_j\right)_{i,j=1}^{n-1} \cdot dx_1 \wedge \ldots \wedge dx_n.$$

Recall that $\omega_{\mathcal{X}/S} = \det(\iota^* \, \mathcal{I}_\iota/\mathcal{I}_\iota^2)^\vee \otimes_S \iota^* \det \Omega^1_{\mathcal{X}/S}$, where $\iota\colon \mathcal{X} \to \mathbb{A}^n_S$ is the embedding, and $\mathcal{I}_\iota$ is the sheaf of ideals on $\mathcal{O}_{\mathbb{A}^n_S}$ defining $\mathcal{X}$. After base change to $\mathbb{Q}$, this becomes $(\det \mathcal{C}_{\mathcal{X}_\eta/\mathbb{A}^n_{\mathbb{Q}}})^\vee \otimes_{\mathbb{Q}} \det i_2^* \, \Omega^1_{\mathbb{A}^n_{\mathbb{Q}}/\mathbb{Q}}$. The result now follows immediately. □

There is still one small subtlety left. We want to calculate the covolume P of the lattice Λ of rank r inside $\mathbb{R}^g$ generated by the $2g$ elements $a_i + \overline{a_i}$, for $i = 1, \ldots, 2g$. For each subset $I \subset \{1, \ldots, 2g\}$ of cardinality g, we let Λ_I be the lattice generated by $\{s_i : i \in I\}$. It could happen that the lattices Λ_I are all not equal to Λ, even though they generate Λ (e.g. for $g = 1$, consider $2\mathbb{Z}$ and $3\mathbb{Z}$ inside the lattice $\mathbb{Z}$). One could however still compute the covolume of Λ, without trying to compute Λ (which would give a lot of trouble with precision) using the following idea of Pagano.

If P_I is the covolume of Λ_I (or 0 when Λ_I does not have full rank), then P_I is an integral multiple of P. In fact, because of the lemma that follows, P is the *greatest common divisor* of the P_I, i.e. the largest real number R such that P_I is an integral multiple of R for all I.

Lemma 1.3.15. *Consider the $\mathbb{F}_p$-vector spaces $\Lambda_I \otimes_{\mathbb{Z}} \mathbb{F}_p$, for subsets $I \subset \{1, \ldots, 2g\}$ of cardinality g, as subspace of $\Lambda \otimes_{\mathbb{Z}} \mathbb{F}_p$. One of them is equal to $\Lambda \otimes_{\mathbb{Z}} \mathbb{F}_p$.*

Proof. The space $\Lambda \otimes_{\mathbb{Z}} \mathbb{F}_p$ has dimension g and is generated by g of the elements $\overline{s_1}, \ldots, \overline{s_g}$, say $\overline{s_{i_1}}, \ldots, \overline{s_{i_g}}$ for certain indices $1 \leq i_1 < \cdots < i_g \leq 2g$. Then for the subset $I = \{i_1, \ldots, i_g\} \subset \{1, \ldots, 2g\}$, we have $\Lambda_I \otimes_{\mathbb{Z}} \mathbb{F}_p = \Lambda \otimes_{\mathbb{Z}} \mathbb{F}_p$. □

Now, we finish the first part of the algorithm, by using a modified version of Euclid's algorithm to compute the greatest common divisor of the P_I numerically (see also Step 3 of Algorithm 1.3.16).

Altogether, this leads to the following algorithm to compute the real period, see also [FLSSSW01, Sect. 3.5].

Algorithm 1.3.16.

Input: monic polynomial $f \in \mathbb{Z}[X]$ of degree $2g+1$ describing a hyperelliptic curve C of genus g over $\mathbb{Q}$.

Output: the period Ω of C.

Step 1: calculate the so-called big period matrix $(\int_{\gamma_i} \omega_j)_{i=1,\ldots,2g,\, j=1,\ldots g}$ of J, where the notation is as before, using the `Magma` command `BigPeriodMatrix` (due to Van Wamelen).

Step 2: for each subset $I \subset \{1,\ldots,2g\}$ with $|I| = g$, calculate the covolume $P_I := \left|\det\left(\int_{\gamma_i}\omega_j + \overline{\int_{\gamma_i}\omega_j}\right)_{i\in I,\, j=1,\ldots,g}\right|$.

Step 3: use Euclid's algorithm to find a generator P for the lattice spanned by the P_I.

Step 4: for each bad prime p, calculate a regular model $\mathcal{C}/\mathbb{Z}_{(p)}$ of C, using the `Magma` command `RegularModel`. This will give us a representation of $\mathcal{C}$ by charts which are relative complete intersections.

Step 5: for each of the differentials $\omega_1,\ldots,\omega_g$, check that if it has a pole on any of the irreducible components of the special fibre of $\mathcal{C}$. If so, adjust the basis by multiplying the differential having a pole with p to get a new basis $\underline{\omega}'$ and apply Step 5 again (until the basis is not changing anymore).

Step 6: for each $(c_j)_{j=1}^g \in \{0,\ldots,p-1\}^g \setminus \{(0,0,\ldots,0)\}$, check if $\sum_j c_j\omega_j$ vanishes on the whole special fibre of $\mathcal{C}$. If so, adjust the basis $\underline{\omega}'$ by replacing one of the ω_j such that $c_j \neq 0$ with $\frac{1}{p}\sum_j c_j\omega_j$, then apply Step 6 again (until the basis is not changing anymore).

Step 7: for each bad prime p compute p^{a-b}, where a is the number of basis adjustments done in Step 5, and b is the number of basis adjustments done in Step 6 (this is also the determinant of the change of basis matrix whose columns express $\underline{\omega}'$ in terms of $\underline{\omega}$). Then take the product W over p of these determinants, and output $W \cdot P$.

End.

1.3.6 Examples

These were the results for our distinguished examples.

Example 1.3.17. For H_1, we do all calculations for the simplified model H_1' given by

$$y^2 = 5x^6 + 20x^5 + 50x^4 + 50x^3 + 25x^2 - 10x - 15.$$

We found that $\{\frac{dx}{y}, \frac{x\cdot dx}{y}\}$ is a $\mathbb{Z}$-basis for the translation invariant differentials. The discriminant of the aforementioned lattice is approximately

$$2.605242317113923602166034611 37,$$

which is also the period of J_1.

Example 1.3.18. For H_2, the differentials $\frac{dx}{y}$ and $\frac{x \cdot dx}{y}$ vanished on all components of the special fibre of the regular model at 2, and $\{\frac{dx}{2y}, \frac{x \cdot dx}{2y}\}$ appears to be a $\mathbb{Z}$-basis for the translation invariant differentials. The discriminant of the aforementioned lattice, times $\frac{1}{4}$ as a correction factor (because of the basis change), is the period of J_2. We found this to be

$$17.2747582935939596362235598228.$$

Example 1.3.19. For H_3, the differentials $\frac{dx}{y}$, $\frac{x \cdot dx}{y}$ and $\frac{x^2 \cdot dx}{y}$ vanished on all components of the special fibre of the regular model at 2, and $\{\frac{dx}{2y}, \frac{x \cdot dx}{2y}, \frac{x^2 \cdot dx}{2y}\}$ appears to be a $\mathbb{Z}$-basis for the translation invariant differentials. The discriminant of the aforementioned lattices, times $\frac{1}{8}$ as a correction factor (because of the basis change), is the period of J_3. We found this to be

$$30.1157800322315549160620615332.$$

1.4 Torsion subgroup and rank

The Jacobian J has a rational principal polarisation, and the number of rational points on J and $J^\vee$ are equal. Hence, for the verification of the conjecture up to squares, the size of the torsion is irrelevant, but we still tried to compute it. In order to do so, and also to find the algebraic rank, we computed upper and lower bounds. For curves of genus 2, this is already implemented in `Magma` due to Stoll.

1.4.1 Lower bounds

For this purpose, we use the Mumford representation of points on J. First, we will briefly explain this way of representing points on the Jacobian.

Let $D \in J(\mathbb{Q})$ be a degree zero divisor on H. Then by Riemann-Roch the space $\mathcal{O}(D + g \cdot [O])$ is non-zero. This means that D can be written as

$$\sum_{i=n}^{n} [P_i] - n \cdot [O],$$

for some $n \leq g$ and points $P_1, \dots, P_n \in H(\overline{\mathbb{Q}})$. This representation is unique up to reordering of the points, if we require that for any i, the point $\iota(P_i)$, where $\iota \colon H \to H$ is the hyperelliptic involution, does not occur in the sum. In the case $P_i = \iota(P_i)$, this should be understood in the sense that the point P_i cannot occur twice.

Let $x_1, \dots, x_n \in \overline{\mathbb{Q}} \cup \{\infty\}$ be the x-coordinates of the P_i. Now, we define $u \in \overline{\mathbb{Q}}[x]$ to be the polynomial vanishing exactly in $x_1, \dots, x_n$ (with the right multiplicities). Moreover, if $y_1, \dots, y_n \in \overline{\mathbb{Q}} \cup \{\infty\}$, then we let $v \in \overline{\mathbb{Q}}[x]$ be the polynomial, obtained by Lagrange interpolation, by setting $v(x_i) = y_i$ for all i (again with the multiplicities taken into account).

Then u and v are actually polynomials over $\mathbb{Q}$, and they should satisfy some relation, coming from the equation defining H. By systematically looking at all polynomials, with bounded coefficients, satisfying these relations, we can enumerate the rational points on the Jacobian.

This method could then be used to obtain lower bounds for both the torsion subgroup and the algebraic rank. For the latter, it could be useful to also compute the height pairing on the Jacobian, which will be discussed in more depth in the section on regulators.

For genus 3, 4 and 5, the author implemented a simple search algorithm for points, using this Mumford representation.

1.4.2 Upper bounds

In order to calculate upper bounds for the torsion subgroup, we can use the following fact: for primes $p \in \mathbb{Z}$ of good reduction, the map

$$J(\mathbb{Q})_{\mathrm{tors},p} \to \mathcal{J}_p(\mathbb{F}_p)$$

from the coprime-to-p-torsion into the reduction of J modulo p is injective. By considering this for several primes of good reduction, we can find an upper bound for the torsion group that appears to be sharp quite often in our examples (but not always).

In order to calculate upper bounds for the algebraic rank, we can use the 2-Selmer group. This is already implemented in `Magma` by Stoll. We will not treat this in depth, but in fact refer to [Silv09, Sect. X.4, p. 331–341] for more information.

In general, it is also possible to make use of height bounds to exhaustively search for enough points that generate the Mordell-Weil group. For genus 2, this seems to still be practical, see for example [MüSt16]. For genus 3, the bounds still seem to be impractical in many cases, see for example [Stol17].

1.4.3 Examples

For our distinguished examples, we found the following.

Example 1.4.1. The torsion subgroup of J_1 is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Example 1.4.2. The torsion subgroup of J_2 is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Example 1.4.3. The best upper bound we found for the torsion is 16. The two-torsion subgroup of J_3 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. The reduction of J_3 modulo 13 has no rational points of order 4, which proves that torsion subgroup of J_3 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$.

1.5 L-function

In this section, we will discuss the definition and computation of the special value of the L-function associated to the Jacobian of a hyperelliptic curve. For more theoretical background, the reader is referred to [Ser70].

For the definition, we will consider abelian varieties in general, over number fields. Let A/K be an abelian variety of dimension g over a number field K and let $\mathcal{A}/\mathcal{O}_K$ be a Néron model of A. In this section, we will define the L-function associated to A. For this purpose, we will first define local L-functions at all finite places of K.

1.5.1 Local L-factors

Let v be a finite place of K with residue field characteristic p. First, we will define, for any prime number $\ell \neq p$, the Tate-ℓ-module of A. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K.

Definition 1.5.1. The Tate-ℓ-module of A is the G_K-module defined by

$$T_\ell(A) = \lim_{n\in\mathbb{Z}_{>0}} A[\ell^n](\overline{K}),$$

where the transition maps $A[\ell^{n+1}](\overline{K}) \to A[\ell^n](\overline{K})$ are given by multiplication by ℓ.

It is well-known that $T_\ell(A)$ as a group is non-canonically isomorphic to $\mathbb{Z}_\ell^{2g}$. Moreover, we define $V_\ell(A)$ as $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Its dual $\mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)$ has the natural structure of a G_K-module by setting $g \cdot \varphi(-) = \varphi(g^{-1} \cdot -)$ for all $\varphi : V_\ell(A) \to \mathbb{Q}_\ell$ and all $g \in G_K$. In fact, this G_K-module is isomorphic to the first ℓ-adic étale cohomology group of A.

Fix an extension to $\overline{K}$ of the prime ideal corresponding to v. Let $I_v \subset G_K$ be its inertia group, i.e. the subgroup of elements $\sigma \in G_K$, such that σ fixes this chosen extended prime, and σ acts trivially on $\overline{k_v}$, the residue field of this extended prime. In $\mathrm{Gal}(\overline{k_v}/k_v)$, there is the Frobenius element, generating the group (as profinite group). The inverse of this Frobenius automorphism can be lifted to an element $\sigma_v \in G_K$, which is unique up to the subgroup I_v. We consider the action of σ_v on $\mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)^{I_v}$, which is a finite dimensional $\mathbb{Q}_\ell$-vector space. Let

$$P_v(T) = \det(1 - \sigma_v T \mid \mathrm{Hom}(V_\ell(A), \mathbb{Q}_\ell)^{I_v})$$

be its characteristic polynomial. It is true, though not obvious, that this polynomial is defined over $\mathbb{Q}$ and does not depend on the choice of $\ell \neq p$ and the extension of the prime ideal to $\overline{K}$. Cf. [Ser70], we define the local L-function as follows.

Definition 1.5.2. With the notation as above, the local L-function of A at v is defined by

$$L_v(A, s) := P_v(|k_v|^{-s})^{-1}.$$

Remark 1.5.3. If v is a place of good reduction of A, then I_v acts trivially on $V_\ell(A)$, as the ℓ-torsion of A injects into $\mathcal{A}_v$, the reduction of $\mathcal{A}$ at v. According to [Tate66], the polynomial $P_v(T)$ has the following property. If $\alpha_{1,v}, \ldots, \alpha_{2g,v} \in \mathbb{C}$ are the roots of P_v, then $\prod_{i=1}^{2g}(1-\alpha_{i,v}^m) = |\mathcal{A}_v(k_v^m)|$, where k_v^m is the unique field extension of degree m of k_v.

Remark 1.5.4. In some sources, the determinant of the action of Frobenius on $V_\ell(A)$ is taken (instead of that of the inverse Frobenius on the dual). For primes of good reduction, this gives the same local L-factor. For primes of bad reduction, this is not necessarily the case.

For example, if you take an elliptic curve E over $\mathbb{Q}$ with split multiplicative reduction at p, then $E(\overline{\mathbb{Q}_p}) = \overline{\mathbb{Q}_p}^*/q^{\mathbb{Z}}$ for some $q \in \mathbb{Q}_p^*$ with $|q|_p = |\Delta(E)|_p < 1$. Then, the group $E[\ell^n](\overline{\mathbb{Q}_p}) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$ is generated by ζ_{ℓ^n} and $\sqrt[\ell^n]{q}^b$, where ζ_{ℓ^n} is an ℓ^n-th primitive root of unity.

As q is divisible by p, the extension $\mathbb{Q}_p \subset \mathbb{Q}_p(\sqrt[\ell^n]{q})$ is totally ramified at p. The extension $\mathbb{Q}_p \subset \mathbb{Q}_p(\zeta_{\ell^n})$ on the other hand is unramified at p. Hence, the Frobenius acts trivially on $\sqrt[\ell^n]{q}$ and sends ζ_{ℓ^n} to $\zeta_{\ell^n}^p$. The inertia group, on the other hand, only acts non-trivially on $\sqrt[\ell^n]{q}$.

Therefore, on the invariants of inertia, Frobenius acts by multiplication with p, on the coinvariants (the invariants of the dual) it acts trivially. The local L-factors would be different, and the product function would not satisfy a functional equation.

1.5.2 Global L-function

Now the global L-function is defined as follows.

Definition 1.5.5. Let M_K' be the set of finite places of K. Then the *global L-function* of A is defined by

$$L(A,s) := \prod_{v \in M_K'} L_v(A,s).$$

Remark 1.5.6. Sometimes, local factors are also defined at the infinite primes. This is done in order to make the functional equation more elegant. It is, however, this version of the L-function that is correct for the version of BSD that we formulated.

It is known that the L-function is holomorphic on $\{z \in \mathbb{C} : \mathrm{Im}(z) > \frac{3}{2}\}$. In full generality, it is not known yet that the L-function even exists at 1. However, it is conjectured that the L-function can be continued analytically to the whole of $\mathbb{C}$ and that it satisfies the following functional equation.

Conjecture 1.5.7 (functional equation, [Ser70, sect. 4] + parity conjecture)**.** *The L-function can be continued to an analytic function $\mathbb{C} \to \mathbb{C}$. Define*

$$\Lambda(A,s) = N^{s/2} \cdot ((2\pi)^{-s}\Gamma(s))^{g \cdot [K:\mathbb{Q}]} \cdot |\Delta(K)|^{g \cdot s} \cdot L(A,s),$$

where N is the conductor of A (for definition, see loc. cit.). This function is conjectured to satisfy the following functional equation:

$$\Lambda(A, 2-s) = \varepsilon \cdot \Lambda(A, s),$$

for all $s \in \mathbb{C}$, where $\varepsilon \in \{\pm 1\}$ is equal to 1 if the rank of A is even and equal to -1 if the rank of A is odd.

1.5.3 Calculation

By Remark 1.5.3, there is a natural algorithm to find the local L-factors at the good places. For this purpose, it suffices to find $|\mathcal{A}_v(k_v^m)|$ for sufficiently many $m \geq 1$. Then we can calculate the polynomial P_v and find the local L-factor $L_v(A, s)$.

In order to find the local L-factors at the bad places, we can use the functional equation. The idea is to guess, in a clever way, for the bad places v, the polynomials P_v and the conductor N in such a way that the L-function obtained satisfies the functional equation from Conjecture 1.5.7, see also [BSSVY16, sect. 5, p. 243–245].

Remark 1.5.8. To guess the 2-part of the conductor, the following naive version of Ogg's formula is used:

$$f^{\text{guess}} = v(\Delta) - n + 1.$$

Here, $v(\Delta)$ is the valuation of the (naive) minimal discriminant, n is the number of geometrically irreducible components in a minimal regular model, and f^{guess} is our guess for the 2-valuation of the conductor. The formula, in this shape, does not give the correct 2-valuation of the conductor in general. For curves of genus 2 over a henselian discrete valuation ring with algebraically closed residue field, we can deduce the formula

$$f = v(\Delta) - n + 1 - 11 \cdot c(X),$$

from [Liu94], where $c(X)$, as defined in loc. cit., is a non-negative integer. Over general discrete valuation rings, the discriminant could change after a quadratic field extension, cf. [Liu96, Prop. 4, p. 4595]. In this case, it drops by $2(2g+1)$. So, for genus 2, in case $v(\Delta) < 10$, the discriminant will apparently not change anymore, and $c(X) = 0$ must hold for the 2-valuation f of the conductor to not become negative. Hence, the naive version of Ogg's formula holds in this case.

In [Dokc04], Tim Dokchitser describes a trick with an inverse Mellin transform in order to actually evaluate the L-function. This has been implemented by him, together with Vladimir Dokchitser, in `Magma`. This is the method we used for our calculations. However, it is useful to note that the runtime increases quickly when the conductor increases and that this could probably by remedied by using the methods from [HMS16].

These are the results for our three distinguished examples, computed with the standard precision of 30 digits in `Magma`.

Example 1.5.9. For H_1 we found that

$$L(J_1, 1) \approx 2.08419385369113888173282768910.$$

This agrees with the fact the algebraic rank of J_1 is 0.

Example 1.5.10. For H_2 we found that

$$L(J_2, 1) \approx 5 \cdot 10^{-31} \text{ and } L'(J_2, 1) \approx 0.819558937768934171069200441694.$$

This agrees with the fact that the algebraic rank of J_2 is 1.

Example 1.5.11. For H_3 we found that

$$L(J_3, 1) \approx 3 \cdot 10^{-30} \text{ and } L'(J_3, 1) \approx 0.869490085404871842347716239330.$$

This agrees with the fact that the algebraic rank of J_3 is 1. Here the 2-valuation of the discriminant was big, and we had to assume the correctness of Ogg's formula.

1.6 Regulator

1.6.1 Definitions

In this section, we will define the regulator of an abelian variety over a number field. First, we need to discuss some generalities on heights. Let $X/\operatorname{Spec} K$ be smooth and projective over a number field.

Definition 1.6.1. Let $\mathbb{P}^n_K$ be the n-dimensional projective space over $\operatorname{Spec} K$. Then the *standard height on* $\mathbb{P}^n_K$ is defined by

$$h_{\mathbb{P}^n_K} : \mathbb{P}^n_K(\overline{K}) \to \mathbb{R} \colon (x_0 : \cdots : x_n) \mapsto \frac{1}{[L : K]} \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log \max_{i=0,\ldots,n} \{|x_i|_v\},$$

where L/K is a finite extension containing $x_0, \ldots, x_n$, and M_L is the set of (finite and infinite) places of L, and where for all finite places v over the prime $p \in \mathbb{Z}$ the absolute value $|\cdot|_v$ is normalised such that $|p|_v = p^{-1}$.

Definition 1.6.2. Let $\mathcal{L}$ be a very ample line bundle on X and let $\mathcal{B}$ be an ordered basis of its global sections, giving rise to an immersion $\varphi \colon X \to \mathbb{P}^n_K$. Then we can define the *naïve global height of* X *at* $\mathcal{L}$ *with respect to* $\mathcal{B}$ as

$$h^{\text{naive}}_{X,\mathcal{L},\mathcal{B}} \colon X(\overline{K}) \to \mathbb{R} \colon P \mapsto h_{\mathbb{P}^n_K}(\varphi(P)).$$

We will now try to extend this definition to work for all line bundles in A. For this purpose we will define the following space.

Definition 1.6.3. Let $\mathrm{Map}(X(\overline{K}),\mathbb{R})$ be the $\mathbb{R}$-vector space of all functions from $X(\overline{K})$ to $\mathbb{R}$. Let $\mathrm{Map}^0(X(\overline{K}),\mathbb{R})$ be the subspace of these functions that are bounded, i.e. the $f \in \mathrm{Map}(X(\overline{K}),\mathbb{R})$ for which there exists a $B \in \mathbb{R}$ such that $|f(P)| < B$ for all $P \in X(\overline{K})$. Then the *height function space* of X is

$$\mathcal{H}(X) := \mathrm{Map}(X(\overline{K}),\mathbb{R}) \,/\, \mathrm{Map}^0(X(\overline{K}),\mathbb{R}).$$

Now we can extend the definition of the global height of X to also work at line bundles $\mathcal{L}$, which are not necessarily very ample.

Lemma 1.6.4 ([Lang83, Thm. 5.1, sect. 4.5, p. 93])**.** *Let X be smooth and projective over* $\mathrm{Spec}\,K$*. Then there exists a function*

$$h_{A,\cdot}\colon \mathrm{Pic}(A) \to \mathcal{H}(X)\colon [\mathcal{L}] \mapsto h_{X,[\mathcal{L}]},$$

having the following properties:

- *for $[\mathcal{L}_1],[\mathcal{L}_2] \in \mathrm{Pic}(X)$ we have $h_{X,[\mathcal{L}_1]} + h_{X,[\mathcal{L}_2]} = h_{X,[\mathcal{L}_1\otimes\mathcal{L}_2]}$;*
- *if $\mathcal{L}$ is a very ample line bundle and $\mathcal{B}$ an ordered basis of its global sections then $h_{X,[\mathcal{L}]}$ is the class of $h^{\mathrm{naive}}_{X,\mathcal{L},\mathcal{B}}$.*

Moreover, this construction is functorial in the following sense. If $f\colon X \to Y$ is a morphism of smooth projective schemes over $\mathrm{Spec}\,K$ *and $\mathcal{L}$ is a line bundle on Y, then $h_{X,[f^*\mathcal{L}]} = h_{Y,[\mathcal{L}]} \circ f$.*

In case of abelian varieties, for such height functions, there is a canonical representative in $\mathrm{Map}(A(\overline{K}),\mathbb{R})$.

Proposition 1.6.5 ([Nér65, Thm. 5, sect. II.14, p. 300])**.** *Let $\mathcal{L}$ be a line bundle on an abelian variety A over* $\mathrm{Spec}\,K$*. Then there exist functions $\ell, q\colon A(\overline{K}) \to \mathbb{R}$, that are linear and quadratic (i.e. $q(P+Q) - q(P) - q(Q)$ is a bilinear form on $A(\overline{K}) \times A(\overline{K})$), respectively, such that $\ell + q$ is in the class $h_{A,[\mathcal{L}]}$.*

Definition 1.6.6. For a line bundle $\mathcal{L}$ on an abelian variety A with $\ell, q\colon A(\overline{K}) \to \mathbb{R}$ as above, we define the *canonical height of A at $\mathcal{L}$* as

$$\widehat{h}_{A,\mathcal{L}} = \ell + q.$$

Definition 1.6.7 ([Nér65])**.** Let A/K be an abelian variety. Let $\mathcal{P}$ be the Poincaré bundle on $A \times A^\vee$. Then the *Néron-Tate height on A* is defined as

$$h_{A\times A^\vee,\mathrm{NT}} = \widehat{h}_{A\times A^\vee,\mathcal{P}} : A(\overline{K}) \times A^\vee(\overline{K}) \to \mathbb{R}.$$

On the other hand, for Jacobians of curves, it is also very common to define a canonical height using an embedding of the Kummer variety associated to it. We will sketch how this is working and prove that the height you get, is the same as the Néron-Tate height. In [Gros86, Sect. 4], you can find a more detailed account of the construction.

For a smooth curve C over $\operatorname{Spec} K$, there is a natural map $C^{g-1} \to \operatorname{Pic}^{g-1}(C)$. Its image, W, which is sometimes called the Theta divisor, is a subscheme pure of codimension 1 in $\operatorname{Pic}^{g-1}(C)$. Now let $D \in \operatorname{Pic}^{g-1}(C)$ such that $2D = K_C$, where $K_C \in \operatorname{Pic}^{2g-2}(C)$ is the canonical divisor class. Then the translate of W with $-D$ defines a divisor Θ in $J := \operatorname{Pic}^0(C)$, which is also called the Theta divisor. It is not well-defined as it might depend on D. However, the divisor class of 2Θ is well-defined, hence the following definition will not depend on the choose of D.

Definition 1.6.8. Let C be as above. Then the *canonical Kummer height* on J, the Jacobian of C, is defined by

$$h_{J,\mathrm{Kum}} = \widehat{h}_{J,2\Theta} \colon J(\overline{K}) \to \mathbb{R}.$$

The *canonical Kummer height pairing* is then defined by

$$h_{J\times J,\mathrm{Kum}} \colon J(\overline{K}) \times J(\overline{K}) \to \mathbb{R}$$

$$(P,Q) \mapsto \tfrac{1}{2}(h_{J,\mathrm{Kum}}(P+Q) - h_{J,\mathrm{Kum}}(P) - h_{J,\mathrm{Kum}}(Q)).$$

Remark 1.6.9. As 2Θ is a symmetric divisor, the linear part of $h_{J,\mathrm{Kum}}$ is 0. Hence, the pairing $h_{J\times J,\mathrm{Kum}}$ is bilinear. It is the bilinear pairing satisfying

$$h_{J\times J,\mathrm{Kum}}(P,P) = h_{J,\mathrm{Kum}}(P).$$

Remark 1.6.10. The divisor 2Θ is not very ample. However, it is symmetric. Therefore, it descends to a divisor on the Kummer variety $J/\{\pm 1\}$ associated to J. This divisor on $J/\{\pm 1\}$ is very ample. The height that you get is the height associated to the embedding of $J/\{\pm 1\}$ in $\mathbb{P}^{2^g-1}$ associated to 2Θ. That is the reason why we call this height the canonical Kummer height.

Moreover, the divisor Θ also gives rise to a principal polarisation $\theta \colon J \to J^\vee$. The Néron-Tate and canonical Kummer height pairing are related in the following way.

Theorem 1.6.11. *Let $C/\operatorname{Spec} K$ be a smooth curve, let J be its Jacobian and let $\theta \colon J \to J^\vee$ be the principal polarisation associated to the Theta divisor of J. Then*

$$h_{J\times J^\vee,\mathrm{NT}} \circ (\mathrm{id}_J, \theta) = h_{J,\mathrm{Kum}}.$$

Proof. Let $\mathcal{P}$ be the Poincaré bundle on $J \times J^\vee$ and let Θ be the Theta divisor on J. Then, cf. [Mumf70, sect. 13, p. 123–125], we have

$$D := (\mathrm{id}_J \times \theta)^*\mathcal{P} \cong m^*\Theta \otimes (p_1^*\Theta)^{-1} \otimes (p_2^*\Theta)^{-1},$$

where $m \colon J \times J \to J$ is the multiplication and $p_1, p_2 \colon J \times J \to J$ are the projections onto the first and second coordinate. Now, if you use the additivity and functoriality of the heights, see Proposition 1.6.4, then you see that we get

$$\begin{aligned} h_{J\times J^\vee,\mathcal{P}}(P,\theta(Q)) &= h_{J\times J,D}(P,Q) \\ &= h_{J\times J,m^*\Theta}(P,Q) - h_{J\times J,p_1^*\Theta}(P,Q) - h_{J\times J,p_2^*\Theta}(P,Q) \\ &= h_{J,\Theta}(P+Q) - h_{J,\Theta}(P) - h_{J,\Theta}(Q) \\ &= \tfrac{1}{2}\left(h_{J,2\Theta}(P+Q) - h_{J,2\Theta}(P) - h_{J,2\Theta}(Q)\right). \end{aligned}$$

Hence, the functions $h_{J\times J^\vee,\mathrm{NT}}\circ(\mathrm{id}_J,\theta)$ and $h_{J,\mathrm{Kum}}$ differ by a bounded function. As both of the functions are quadratic, they are equal. □

Remark 1.6.12. Even though Θ is not well-defined, $h_{J,\Theta}$ is. The difference between any two choices of Θ is torsion, and the height at a torsion divisor is 0, by the additivity of the height (cf. Proposition 1.6.4).

Now we define the regulator of a Jacobian as follows.

Definition 1.6.13 (Regulator)**.** Let J/K be a Jacobian over a number field. Consider the finitely generated group $J(K)$. Let $x_1,\dots,x_r$ be generators $J(K)/J(K)_{\mathrm{tors}}$. The *regulator of* J is defined as

$$\left|\det\left(h_{J\times J,\,\mathrm{Kum}}(x_i,x_j)\right)_{i,j=1}^{r}\right|.$$

1.6.2 Calculation of the regulator

Using the points on J that we found when computing the algebraic rank, we will compute the regulator. In order to do that, we need to calculate the height pairing for several pairs of points. For genus 2, it is still possible to use the embedding described in Remark 1.6.10. For genus 3 and higher, this is not feasible, due to the number of equations describing the image of $J/\{\pm1\}$ inside $\mathbb{P}^{2^g-1}$ growing exponentially.

Due to work of Holmes ([Holm12]) and Müller ([Müll14]) it is now known how arithmetic intersection theory could be used to do this calculation. This has also been implemented in `Magma` for hyperelliptic curves by Müller, and works in practice for genus up to 10.

In many cases, especially in genus 3, 4 and 5, the height bound we use for point finding is not high enough to provably compute the regulator. The upper bounds for difference between the naive and canonical height are quite big in some cases (for genus 2, this is a bit better, see for example [MüSt16]). In that case, we can only obtain a finite index subgroup of the Mordell-Weil group. Therefore, the regulator that we get might be a square multiple of the actual regulator of J. Hence, the conjectural order of Ш, assuming BSD, might be a square multiple of the order that we compute.

Again, we might end up with more elements in the Mordell-Weil group than the algebraic rank. In case this happens, when trying to find the regulator, we use the same trick with the 'greatest common divisor' as we did with the real period, making use of Lemma 1.3.15 again.

For our distinguished examples we obtained the following.

Example 1.6.14. For H_1, the algebraic rank of J_1 is 0. Hence, the regulator is 1.

Example 1.6.15. For H_2, the algebraic rank of J_2 is 1. In this particular case, the bound for the naive height of a generator was not too large. Having looked for points below this bound, we found that the point $(x-1,1)$, in `Magma`'s Mumford representation, is a generator for $J_2(\mathbb{Q})/J_2(\mathbb{Q})_{\mathrm{tors}}$. The height pairing of the point with itself, the regulator, is

$$0.0474425704742192075988905184458.$$

Example 1.6.16. For H_3, the algebraic rank of J_3 is 1. Having looked for points of very small height, we found that the point $(x, -1)$, in `Magma`'s Mumford representation, is probably a generator for $J_3(\mathbb{Q})/J_3(\mathbb{Q})_{\mathrm{tors}}$. The height pairing of the point with itself is

$$0.230972622186586831975393030694.$$

The other values for the height pairing of points with itself are all square multiples of this number, which indicates that this point is very likely a generator for $J_3(\mathbb{Q})/J_3(\mathbb{Q})_{\mathrm{tors}}$. Hence, we assume the regulator equals the aforementioned number.

1.7 Tamagawa numbers

We consider the situation of a general abelian variety A/K over a number field K, having Néron model $\mathcal{A}/\mathcal{O}_K$. Let v be a finite place of K and let $\mathcal{A}_v$ be the reduction of $\mathcal{A}$ at $k(v)$. Then we can define the Tamagawa number as follows.

Definition 1.7.1 (Tamagawa number)**.** The *Tamagawa number of A at v* is

$$[\mathcal{A}_v(k(v)) : \mathcal{A}_v^0(k(v))],$$

where $\mathcal{A}_v^0$ is the connected component of 0 in $\mathcal{A}_v$, in other words, the number of connected components of $\mathcal{A}_v$ having a rational point.

Suppose that we have a regular model $\mathcal{H}^{\mathrm{s}}$ of H over the strict henselisation of $\mathbb{Z}_{(p)}$. Then in [BoLi99, Thm. 1.1, p. 277], Bosch and Liu give an exact sequence

$$0 \to \operatorname{Im}\overline{\alpha} \to \operatorname{Ker}\overline{\beta} \to \phi_A(\overline{\mathbb{F}_p}) \to 0$$

of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$-modules. Here $\phi_A(\overline{\mathbb{F}_p})$ is the geometric component group of the Néron model of $\mathcal{J}$. The map $\overline{\alpha}\colon \mathbb{Z}^{\overline{I}} \to \mathbb{Z}^{\overline{I}}$, with $\overline{I}$ indexing the components $\{\Gamma_i : i \in I\}$ of the special fibre of $\mathcal{H}^{\mathrm{s}}$, maps each component Γ_j to $\sum_{i\in\overline{I}} e_i^{-1}\langle\Gamma_j, \Gamma_i\rangle \cdot \Gamma_i$, where $\langle\cdot,\cdot\rangle$ is the intersection pairing and e_i is the geometric multiplicity of Γ_i (in itself, which is 1 in our case). The map $\overline{\beta}\colon \mathbb{Z}^{\overline{I}} \to \mathbb{Z}$ maps each component Γ_j to $d_j e_j$, where d_j is the multiplicity of Γ_j in the special fibre. Here, the Galois group $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ acts on $\mathbb{Z}^{\overline{I}}$ by its natural action on the components of the special fibre.

Due to Donnelly, `Magma` is able to compute this geometric component group using this theorem, and moreover, because explicit equations exist for a regular model $\mathcal{H}$ of H over $\mathbb{Z}_{(p)}$, we are able to compute the action of Frobenius on $\operatorname{Im}\overline{\alpha}$ and $\operatorname{Ker}\overline{\beta}$.

The way regular models are constructed in `Magma` is by repeatedly blowing up non-regular points until the fibred surface is regular. To compute the Galois action on the components of the special fibre, we traced down this blow-up procedure, and in each step we computed the action of Galois on the points blown-up, and on the new components which appeared in the special fibre on the new blown-up charts.

The result is an implementation of a `Magma` package on top of the existing regular models package, which computes the action of the Galois group on $\phi_A(\overline{\mathbb{F}_p})$, and then computes the Tamagawa number, the order of $\phi_A(\mathbb{F}_p)$. The source code for this package will be released together with this thesis. It has been used to compute Tamagawa numbers for almost all of the 66,158 genus 2 curves present in [LMFDB] (see also [BSSVY16]). Due to a specific problem in the implementation of the author's code there are a few Tamagawa numbers left to compute. This computation was finished within a few hours.

For our distinguished examples we obtained the following.

Example 1.7.2. The curve H_1 has only one bad prime, which is 5. The Tamagawa number at 5 is 5.

Example 1.7.3. The curve H_2 has three bad primes: 2, 5 and 7. The Tamagawa number at 2 is 4, the Tamagawa numbers at 5 and 7 are 1.

Example 1.7.4. The curve H_3 has three bad primes: 2, 3 and 31. The Tamagawa number at 2 is 2, the Tamagawa numbers at 3 and 31 are 1.

1.8 Tate-Shafarevich group

1.8.1 Definition

Let V/K be a group scheme over a field K. Let $\overline{K}$ be an algebraic closure of K and let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Then we define the following group.

Definition 1.8.1 (Weil-Châtelet group)**.** The Weil-Châtelet group of V/K is defined as

$$\mathrm{WC}(V/K) = H^1(G_K, V(\overline{K})).$$

It is a well-known fact that the Weil-Châtelet group is in canonical bijection with the set of K-isomorphism classes of torsors of V over K.

Let A/K be an abelian variety over a number field. Let v be a place of K and let K_v be a completion of K at v. We fix an extension of the place v to $\overline{K}$ and an algebraic closure $\overline{K_v}$ of K_v. This gives an embedding $\overline{K} \subset \overline{K_v}$. Let G_K and G_{K_v} be the absolute Galois groups of K and K_v, respectively. Then we have natural maps $G_{K_v} \to G_K$ and $\mathrm{WC}(A/K) \to \mathrm{WC}(A_{K_v}/K_v)$.

Definition 1.8.2 (Tate-Shafarevich group)**.** The *Tate-Shafarevich group* $\text{Ш}(A/K)$ is defined as

$$\bigcap_v \ker\left(\mathrm{WC}(A/K) \to \mathrm{WC}(A_{K_v}/K_v)\right).$$

The Tate-Shafarevich group can be viewed as the set of isomorphism classes of torsors X of A over K, such that X has a K_v-rational point for every place v. The Tate-Shafarevich group measures the failure of the Hasse principle for torsors.

It is a well-known conjecture that the Tate-Shafarevich group is finite. It is known that $Ш(A/K)$ is torsion and that for every positive integer n the group $Ш(A/K)[n]$ is finite. However, the conjecture has only been proven for elliptic curves over $\mathbb{Q}$ of analytic rank at most 1.

Remark 1.8.3. Jacobians J of curves over K have a principal polarisation over an algebraic extension of K. By composing this polarisation with the Cassels-Tate pairing, we find that the order of $Ш(J/K)$, assuming it is finite, is either a square or two times a square, see for example [PoSt99, Cor. 9, p. 1123-1124]. `Magma` contains a procedure for hyperelliptic curves over number fields, to determine whether the order of $Ш(J/K)$ is a square.

1.8.2 Computation

In general, it is hard to compute the Tate-Shafarevich group. For our calculations, we do not calculate the order of the Tate-Shafarevich group. Instead, we only check whether the conjectural order, given by the BSD conjecture, is (up to a certain precision) a rational square or two times a rational square (with a small denominator), and that this corresponds to the result of the procedure described in Remark 1.8.3.

For our distinguished examples, we obtained the following.

Example 1.8.4. For H_1, the BSD formula would give

$$|Ш(J_1)| = \frac{L^{(r)}(J_1,1)\cdot|J_1(\mathbb{Q})_{\mathrm{tors}}|^2}{r!\cdot P_{J_1}R_{J_1}\cdot\prod_p c_p} \approx 4.00000000000000000000000000001,$$

which is almost equal to 4, which agrees with the results from [FLSSSW01].

Example 1.8.5. For H_2, the BSD formula would give

$$|Ш(J_2)| = \frac{L^{(r)}(J_2,1)\cdot|J_2(\mathbb{Q})_{\mathrm{tors}}|^2}{r!\cdot P_{J_2}R_{J_2}\cdot\prod_p c_p} \approx 1.00000000000000000000000000049,$$

which is almost equal to 1, which agrees with the fact that the order of $Ш(J_2)$ is expected to be a square, and that the 2-Selmer group has order 4.

Example 1.8.6. For H_3, the BSD formula would give

$$|Ш(J_3)| = \frac{L^{(r)}(J_3,1)\cdot|J_3(\mathbb{Q})_{\mathrm{tors}}|^2}{r!\cdot P_{J_3}R_{J_3}\cdot\prod_p c_p} \approx 1.00000000000000000000000000003,$$

which is almost equal to 1, which agrees with the fact that the order of $Ш(J_3)$ is expected to be a square, and that the 2-Selmer group has order 8.

Chapter 2

The BSD conjecture for an elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$

Abstract. In this chapter we show that the Birch and Swinnerton-Dyer conjecture for a certain elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$ is equivalent to the same conjecture for a certain pair of hyperelliptic curves of genus 2 over $\mathbb{Q}$. We numerically verify the conjecture for these hyperelliptic curves. Moreover, we explain the methods used to find this example, which turned out to be a bit more subtle than expected.

2.1 Introduction

The Birch and Swinnerton-Dyer conjecture ([BiSw65]) has been generalised by Tate ([Tate66]) to abelian varieties of higher dimension and over general number fields.

Conjecture 2.1.1 (BSD, [Gros86, Conj. 2.10, p. 224])**.** *Let A/K be an abelian variety of dimension d and algebraic rank r over a number field K of discriminant Δ. Let $L(s)$ be its L-function, $A^\vee$ its dual, R its regulator,* Ш *its Tate-Shafarevich group and Ω the product of its real and complex periods. For each prime $\mathfrak{p}$ of $\mathcal{O}_K$, let $c_\mathfrak{p}$ be the Tamagawa number of A at $\mathfrak{p}$. Then* Ш *is finite, $L(s)$ admits an analytic continuation to $\mathbb{C}$ having a zero of order r at $s = 1$, and*

$$\lim_{s\to 1} (s-1)^{-r} L(s) = \frac{\Omega \cdot R \cdot |Ш| \cdot \prod_\mathfrak{p} c_\mathfrak{p}}{|A(K)_{\mathrm{tors}}| \cdot |A^\vee(K)_{\mathrm{tors}}| \cdot |\Delta|^{d/2}}.$$

In 1989, Kolyvagin ([Koly89, Koly91]) proved equality of the analytic and algebraic rank for modular elliptic curves over $\mathbb{Q}$ of analytic rank at most 1. After the proof of the modularity theorem ([BCDT01]), this part of the conjecture is now known for all elliptic curves over $\mathbb{Q}$ of analytic rank at most 1.

For elliptic curves with complex multiplication more is known. In 1991, Rubin ([Rub91]) proved the correctness of the p-part of BSD for elliptic curves over an imaginary quadratic field K with complex multiplication by K, analytic rank equal to 0, and p coprime to $|\mathcal{O}_K^*|$.

Originally, the Birch and Swinnerton-Dyer conjecture has been conceived based on numerical calculations with elliptic curves. In Chapter 1, we numerically verified the conjecture for hundreds of hyperelliptic curves of genus 2 and 3 over $\mathbb{Q}$, extending the work of Flynn, Leprévost, Schaefer, Stein, Stoll and Wetherell ([FLSSSW01]), who numerically verified BSD for 32 modular hyperelliptic curves of genus 2 over $\mathbb{Q}$, using modularity.

This verification consists of two parts. First, we check that the analytic rank (established numerically) and the algebraic rank are equal. Then we numerically compute all terms in the BSD formula except for $|Ш|$ (to more than 20 digits precision), and by rearranging the formula we deduce a predicted value for $|Ш|$. This will a priori be some real number, but if the BSD conjecture is true then it should in fact be the square of a positive integer, cf. earlier results of Poonen and Stoll ([PoSt99]). So if our conjectural value of $|Ш|$ is indeed the square of a positive integer to high precision, then this provides strong numerical evidence for the conjecture.

After finishing this verification, a natural question that arose was if the numerical verification for genus 2 curves over $\mathbb{Q}$, could provide us with examples of elliptic curves E over quadratic number fields for which BSD numerically seems to hold. The Weil restriction of E to $\mathbb{Q}$ is an abelian variety of dimension 2 over $\mathbb{Q}$ and might have the chance of being the Jacobian of a genus 2 curve over $\mathbb{Q}$. As the Jacobi locus is dense in the moduli space, one might expect this to happen very often. This was not the case. While trying many examples, all seemed to fail.

However, this Weil restriction becomes a product of two elliptic curves, after base change. The product of two elliptic curves, taken with the associated product polarisation, does not lie in the Jacobi locus. The best we could hope for is the existence of another polarisation, which makes it isomorphic (as polarised abelian variety) to the Jacobian of a curve of genus 2. This is actually only possible in a few special cases. By trying other polarisations in these special cases, we found an example of an elliptic curve over $\mathbb{Q}(\sqrt{5})$, whose Weil restriction is isogenous to the Jacobian of a curve of genus 2 over $\mathbb{Q}$. However, the isogeny was only defined over $\mathbb{Q}(\sqrt[8]{5}, i)$. We applied some reduction steps to reduce the size of this field and arrive at the following theorem

Theorem 2.1.2. *Let E over $\mathbb{Q}(\sqrt[4]{5})$ be the elliptic curve given by*

$$y^2 = x^3 + \sqrt[4]{5} \cdot x^2 - \left(5 + 3\sqrt{5}\right) \cdot x + \sqrt[4]{5}\left(5 + \sqrt{5}\right).$$

Let H and H' over $\mathbb{Q}$ be the hyperelliptic curves given by $y^2 = x^5 - x^3 + \frac{1}{5} \cdot x$, and $y^2 = x^5 - 5 \cdot x^3 + 5 \cdot x$, respectively. Then the generalised Birch and Swinnerton-Dyer conjecture holds for E over $\mathbb{Q}(\sqrt[4]{5})$ if and only if it holds for the Jacobians $\operatorname{Jac} H$ *and* $\operatorname{Jac} H'$ *over $\mathbb{Q}$.*

Finally, because of this reduction of the size of the field, we were able to numerically verify the BSD conjecture for the mentioned hyperelliptic curves.

We could also phrase the problem we solved as a moduli problem. For fixed N, we consider the space $\mathcal{M}$ of quintuples $(E_1, E_2, A, \phi, \rho)$, where E_1 and E_2 are elliptic curves, (A, ϕ) is a principally polarised abelian surface, and $\rho : E_1 \times E_2 \to A$ is an isogeny of degree N. If $\iota : \mathcal{M} \to \mathcal{M}$ is the involution that swaps E_1 and E_2, then our problem is the finding of rational points of $\mathcal{M}/\iota$, for which (A, ϕ) is the Jacobian of a smooth genus-2 curve with its natural principal polarisation.

This moduli problem (or variations thereof) has been studied extensively by others. This started with Hayashida and Nishi in [HaNi65]. More recently, there is work of Rodriguez-Villegas ([Rodr00]), Lange ([Lan06]), and Kani ([Kani14], [Kani16]). However, as far as we are aware, none of these results gives a way to control the size of the field of definition for the isogeny ρ, which is needed for our verification of the BSD conjecture.

The organisation of this chapter is as follows. In the first section, the final results will be shown, the equivalence of BSD for a certain elliptic curve over a quartic field and BSD for a certain pair of hyperelliptic curves of genus 2 over $\mathbb{Q}$. In the second section, the methods used to find this example will be demonstrated. First we study which elliptic curves could have the potential to become isogenous to the Jacobian of a genus 2 curve after Weil restriction. Then we explain how the required isogenies, which are very easy to find analytically, were algebraised. Finally, we describe some steps that had to be taken to reduce the size of the number field over which these maps are defined, which was actually necessary to be able to complete the verification.

The author wishes to thank his supervisors David Holmes and Fabien Pazuki. Moreover Maarten Derickx is thanked for useful discussions that led to improvements of this chapter.

2.2 Verification for an elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$

Throughout this section, let E be the elliptic curve over $\mathbb{Q}(\sqrt[4]{5})$ given by the Weierstraß equation

$$y^2 = x^3 + \sqrt[4]{5} \cdot x^2 - \left(5 + 3\sqrt{5}\right) \cdot x + \sqrt[4]{5}\left(5 + \sqrt{5}\right).$$

Even though it has j-invariant $282880\sqrt{5} + 632000$, it is not the base change of an elliptic curve over $\mathbb{Q}(\sqrt{5})$, which can be verified using the isomorphism criteria from [Silv09, Sect. III.1, p. 42–51]. Even though the following lemma is not strictly necessary for the proof, it does turn out to be an important property of E.

Lemma 2.2.1. *The elliptic curve E geometrically has complex multiplication by $\mathbb{Z}[\sqrt{-5}]$.*

Proof. The Hilbert class polynomial for discriminant -20 is

$$x^2 - 1264000 \cdot x - 681472000,$$

see for example [BLP16, Table 2, p. 400]. Its zeros are $632000 \pm 282880\sqrt{5}$. The j-invariant for E is $632000 + 282880\sqrt{5}$, which proves that E geometrically has complex multiplication by $\mathbb{Z}[\sqrt{-5}]$. □

Let H be the hyperelliptic curve of genus 2 over $\mathbb{Q}$ given by the Weierstraß equation $y^2 = x^5 - x^3 + \frac{1}{5} \cdot x$. Let $H'\colon y^2 = x^5 - 5 \cdot x^3 + 5 \cdot x$ over $\mathbb{Q}$ be the quadratic twist of H over $\mathbb{Q}(\sqrt{5}\,)$.

The following propositions will be used to prove Theorem 2.1.2.

Proposition 2.2.2. *Let* $K = \mathbb{Q}(\sqrt[4]{5}\,)$ *and*

$$\varphi\colon H_K \to E\colon (x : y : 1) \mapsto (\varphi_x : \varphi_y : 1)\,, \quad \textit{with}$$

$$\varphi_x = \frac{\sqrt{5} \cdot x^2 - \sqrt[4]{5} \cdot x + 1}{x}, \qquad \varphi_y = \frac{-\sqrt[4]{5}^3 \cdot xy + \sqrt{5} \cdot y}{x^2}$$

Then the map $\psi\colon H_{\mathbb{Q}(\sqrt{5}\,)} \to W := \operatorname{Res}^K_{\mathbb{Q}(\sqrt{5}\,)} E$ *naturally induced by* φ *induces an isogeny* $\nu\colon \operatorname{Jac} H_{\mathbb{Q}(\sqrt{5}\,)} \to W$ *over* $\mathbb{Q}(\sqrt{5}\,)$.

Proof. For the Weil restriction we have

$$W_K = E \times E',$$

where E' over K is the pull-back of E under the automorphism $\sigma\colon \sqrt[4]{5} \mapsto -\sqrt[4]{5}$ of K over $\mathbb{Q}(\sqrt{5}\,)$. Using this identification, after base change, the map ψ becomes

$$\psi_K\colon H_K \overset{(\varphi,\varphi^\sigma)}{\longrightarrow} E \times E'.$$

Suppose that the map ν_K induced by ψ_K is not an isogeny. Then the image of ν_K in $E \times E'$ is an elliptic curve F over K and we have the following diagram.

$$\begin{tikzcd}
 & & & E \\
H_K \arrow[urrr, "\varphi{,}2"] \arrow[r, "\geq 2"] \arrow[drrr, "\varphi^\sigma{,}2"'] & F \arrow[urr, "1"'] \arrow[r] \arrow[drr, "1"] & E \times E' \arrow[ur] \arrow[dr] & \\
 & & & E'
\end{tikzcd}$$

As the morphisms φ and φ^σ are of degree 2, and the morphism $H_K \to F = \nu(H_K)$ is of degree at least 2, the two morphisms $F \to E$ and $F \to E'$ are of degree 1 and defined over K. Hence, E and E' must be isomorphic over K. Even though E and E' are isomorphic over $\mathbb{Q}\big(i, \sqrt[4]{5}\,\big)$, it is easily verified that they are not isomorphic over K. Therefore, ν_K must be an isogeny and hence also ν is an isogeny. □

Remark 2.2.3. The map $\varphi\colon H_K \to E$ is the quotient of H_K by the automorphism

$$H_K \to H_K\colon \quad x \mapsto \frac{1}{\sqrt{5}\cdot x}, \quad y \mapsto \frac{-y}{\sqrt[4]{5}^3 \cdot x^3}.$$

In fact, the geometric automorphism group of H is the dihedral group D_4 of order 8, and the Jacobian of any curve of genus 2 over $\mathbb{Q}$ whose automorphism group is non-abelian, is isogenous to the square of an elliptic curve, over a finite extension of $\mathbb{Q}$, cf. [CGLR99, Lem. 2.4, p. 42]. Note that this result does not give control on the degree of the field extension needed to define the isogeny.

Now let us generalise the notion of quadratic twists of elliptic curves to abelian varieties over number fields.

Definition 2.2.4. Let A be an abelian variety over a number field K, and let $K \subset L$ be an extension of degree 2. Then the *L-quadratic twist* of A over L is the twist of A corresponding to the cocycle $\mathrm{Gal}(L/K) \to \mathrm{Aut}_L(A)$ mapping the non-trivial element $\sigma \in \mathrm{Gal}(L/K)$ to the automorphism $-1\colon A \to A$.

Example 2.2.5. Let $E\colon y^2 = x^3 + x$ over $\mathbb{Q}$. Then its $\mathbb{Q}(i)$-quadratic twist can be determined using the following procedure. Let $G = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \langle\sigma\rangle$. Then we consider the cocycle $\rho\colon G \to \mathrm{Aut}_{\mathbb{Q}(i)}(E)$ mapping σ to -1.

Let $R = \mathbb{Q}(i)(x)[y]/(y^2 - x^3 - x)$ be the function field of E over $\mathbb{Q}(i)$. Then the group G already acts on $\mathbb{Q}(i)$. We extend this action to R by $g \cdot x = \rho(g)(x)$ and $g \cdot y = \rho(g)(y)$ for $g \in G$, i.e. G acts trivially on these coordinates except for $\sigma \cdot y = -y$.

Next, we compute $R^G = \mathbb{Q}(x, iy) \subset R$, and note that $R^G \cong \mathbb{Q}(x)[y]/(-y^2 - x^3 - x)$. Hence, the $\mathbb{Q}(\sqrt{-1})$-quadratic twist is $E'\colon\ -y^2 = x^3 + x$, as in the classical theory.

Note that E and E' are actually isomorphic over $\mathbb{Q}$ in this case. So, the quadratic twist does not have to be non-trivial. In fact, there is a non-trivial twist of E over $\mathbb{Q}(i)$, which is given by $E''\colon y^2 = x^3 - 4x$. It can be obtained by twisting using the cocycle $G \to \mathrm{Aut}_{\mathbb{Q}(i)}(E)$ mapping σ to the automorphism

$$E_{\mathbb{Q}(i)} \to E_{\mathbb{Q}(i)}\colon \quad x \mapsto -x, \quad y \mapsto iy.$$

The following proposition is probably well-known to the experts.

Proposition 2.2.6. *Let A be an abelian variety over a number field K, and let $K \subset L$ be an extension of degree 2. Then the Weil restriction $W := \mathrm{Res}_K^L A_L$ of the base change A_L to K is isogenous to the product $A \times A'$, where A' over K is the L-quadratic twist of A.*

Proof. Recall that $\mathrm{Hom}_K(T, W) = \mathrm{Hom}_L(T_L, A_L)$ for any scheme T over K. Consider the morphism $\nu\colon A \times A' \to W$, given by the morphism

$$\kappa\colon A_L \times A'_L \to A_L\colon (x, y) \mapsto x + \rho(y),$$

where the isomorphism $\rho : A'_L \cong A_L$ comes from the twist data. Then the map

$$\nu_L\colon A_L \times A'_L \to A_L \times A^\sigma_L$$

is given by κ on the first component and κ^σ on the second component, where $\sigma\colon L \to L$ is the non-trivial element of $\mathrm{Gal}(L/K)$. Then κ^σ is

$$A_L \times A'_L \to A^\sigma_L = A_L\colon (x, y) \mapsto \sigma(x) + \rho(\sigma(y)).$$

As $\rho(\sigma(y)) = -\sigma(\rho(y))$, by definition of the L-quadratic twist, we now find that the kernel of ν_L is finite and that ν is an isogeny. □

Example 2.2.7. For example, for an elliptic curve $E\colon y^2 = f(x)$ over K, the L-quadratic twist is the curve $E'\colon dy^2 = f(x)$ over K and the isomorphism ρ is given by $E'_L \to E_L\colon (x, y) \mapsto (x, y/\sqrt{d})$, and

$$\nu_L\colon E_L \times E'_L \to E_L \times E_L\colon (x, y) \mapsto (x + \rho(y), \sigma(x - \rho(y))).$$

The kernel of ν_L consists of the pairs $(x, \rho^{-1}(x))$ where $x \in E[2]$. Hence, the isogeny $E \times E' \to W$ has degree 4.

Proposition 2.2.8. *Let A and B be abelian varieties over a number field K, let $K \subset L$ be a finite extension of number fields and let C be an abelian variety over L. Then*

(1) BSD holds for $A \times B$ over K if and only if it holds for A and B over K;

(2) if A and B are isogenous over K, then BSD holds for A over K if and only if it holds for B over K;

(3) BSD holds for the Weil restriction $\mathrm{Res}^L_K C$ over K if and only if it holds for C over L;

(4) if L/K is quadratic, BSD holds for the base change A_L over L if and only if it holds for A over K and its L-quadratic twist A' over K.

Proof. For (1) and (2), see [Tate66, p. 422]. For (3), see [Mil72]. In the case L/K is a quadratic extension, $\mathrm{Res}^L_K A_L$ is isogenous over K to $A \times A'$, where A'/K is the L-quadratic twist of A, cf. Prop. 2.2.6 or [Kida95, Thm., p. 53]. Now (4) follows from (1), (2) and (3). □

Proof (Theorem 2.1.2). By Proposition 2.2.8 part (4), BSD holds for $\mathrm{Jac}\, H$ and $\mathrm{Jac}\, H'$ over $\mathbb{Q}$ if and only if it holds for $\mathrm{Jac}\, H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$. The latter is isogenous over $\mathbb{Q}(\sqrt{5})$ to $\mathrm{Res}^{\mathbb{Q}(\sqrt[4]{5})}_{\mathbb{Q}(\sqrt{5})} E$ by Proposition 2.2.2. Hence, by parts (2) and (3) of Proposition 2.2.8, BSD holds for $\mathrm{Jac}\, H_{\mathbb{Q}(\sqrt{5})}$ over $\mathbb{Q}(\sqrt{5})$ if and only if it holds for E over $\mathbb{Q}(\sqrt[4]{5})$. □

Using the methods in Chapter 1, we can numerically verify that the Birch and Swinnerton-Dyer conjecture holds for $\operatorname{Jac} H$ and $\operatorname{Jac} H'$ in the following sense. We numerically verified that the analytic and algebraic rank agree, and we computed all terms except for $|Ш|$, with more than 20 digits precision. Then we used the conjectural formula to predict the order of Ш. This predicted order, $|Ш_{\mathrm{an}}|$, appears to equal 1 in both cases. This gives strong evidence for the conjecture, especially since 1 is the square of an integer, which is to be expected according to [PoSt99].

In fact, we found the following values for the BSD-invariants:

	$\operatorname{Jac} H$	$\operatorname{Jac} H'$
r	1	1
$\lim_{s\to 1}(s-1)^{-r}L(s)$	4.54183774632835249986	4.54183774632835249986
R	4.70213971014416647713	0.94042794202883329543
Ω	1.93181743899697988452	9.65908719498489942260
$c_{\mathfrak{p}}$	$c_2 = 1,\ c_5 = 2$	$c_2 = 1,\ c_5 = 2$
$\lvert J_{\mathrm{tors}}\rvert$	2	2
$Ш_{\mathrm{an}}$	1.00000000000000000000	1.00000000000000000000

Remark 2.2.9. The values of these invariants suggest that $\operatorname{Jac} H$ and $\operatorname{Jac} H'$ are isogenous; they all seem to differ by an integer multiple. Since, the numerical verification succeeded for both curves, the author did not try to actually find an isogeny.

2.3 Methodology

In this section, I will try to answer the question how you find an elliptic curve E over a number field K, with $L \subset K$ of degree 2, such that its Weil restriction to L is isogenous as abelian variety (without fixed polarisation) to the base change of a Jacobian of a hyperelliptic curve of genus 2 defined over $\mathbb{Q}$.

2.3.1 Which elliptic curves?

The product of two elliptic curves over a number field, E and E', taken with the associated product polarisation, does not lie in the Jacobi locus in the moduli space of polarised abelian varieties, cf. [Weil57, Satz 2, p. 37]. However, in some cases it might happen that the abelian variety has another polarisation which makes it into the Jacobian of a smooth curve of genus 2. Heuristically, most polarised abelian varieties lie in the Jacobi locus, but also most polarised abelian varieties have only one polarisation, up to multiplication by an integer. So, heuristically it is not so clear whether such E and E' actually exist. Hence, we should be looking for elliptic curves E and E', such that $E \times E'$ contains a smooth curve of genus 2.

The work of Hayashida and Nishi, [HaNi65], contains sufficient conditions on E and E' for this situation to arise. In particular, [HaNi65, Thm., §4, p. 14] states: if E and E' have complex multiplication by the principal order of the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$ and m is not 1, 3, 7 or 15, then $E \times E'$ contains a smooth curve of genus 2.

2.3.2 Reconstruction of the hyperelliptic curve

Assume that E over K geometrically has complex multiplication by $\mathcal{O}_{-m} = \mathbb{Z}[\alpha_m]$, where

$$\alpha_m = \begin{cases} \sqrt{-m} & \text{if } m \not\equiv 3 \mod 4; \\ \frac{1}{2}(\sqrt{-m}+1) & \text{if } m \equiv 3 \mod 4. \end{cases}$$

Now consider the complexification $E_{\mathbb{C}}$ and fix an embedding of $\mathcal{O}_{-m}$ in $\mathbb{C}$. Then $E_{\mathbb{C}} \cong \mathbb{C}/\Lambda$, where Λ is a lattice of the form $\mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \frac{\beta}{\gamma}$ with β and $\gamma \neq 0$ generating, as $\mathbb{Z}$-module, an ideal of $\mathcal{O}_{-m}$. Moreover, $E_{\mathbb{C}}$ has a Hermitian form, whose imaginary part, without loss of generality, gives the standard antisymmetric form

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

on Λ, with respect to the basis just given.

The idea is now to consider the complex lattice $\mathbb{Z}\binom{1}{0} + \mathbb{Z}\binom{0}{1} + \mathbb{Z}\binom{\alpha_m}{0} + \mathbb{Z}\binom{0}{\alpha_m}$ inside $\mathbb{C}^2$. We try to put other antisymmetric forms on the lattice, and for each such a form, we choose a basis, such that the antisymmetric form with respect to this basis is of the standard form

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

After this, we apply a transformation in $\mathrm{GL}_2(\mathbb{C})$ to obtain a basis that is of the form $\binom{1}{0}, \binom{0}{1}, \binom{v_1}{v_2}, \binom{w_1}{w_2}$, cf. [Sch89, §5]. If the antisymmetric form satisfies the Riemann relations, cf. [Lang82, Lem. 1.1 & 1.2, Chap. VII, §1, p. 132], then the matrix

$$M = \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix}$$

will be symmetric and its imaginary part will be positive definite, i.e. M has the potential to be the small period matrix of a hyperelliptic curve H of genus 2.

One can then evaluate the theta functions in M and use these to reconstruct the Igusa invariants of H. These Igusa invariants can only be computed numerically, up to a certain precision, but we expect them to be rational. If the precision is high enough, we can guess the rational values for the Igusa invariants. Then we can use Mestre's algorithm ([Mes91]) to construct a hyperelliptic curve with these Igusa invariants. This part of the reconstruction procedure is explained in more detail in [Weng03].

2.3.3 Constructing algebraic maps

Now we are in the situation that we found an elliptic curve E over K and a hyperelliptic curve H over $\mathbb{Q}$ (i.e. given with explicit equations in $\mathbb{P}^2$ over K and $\mathbb{Q}$, respectively), such that the base change of $E \times E$ and $J := \mathrm{Jac}(H)$ to $\mathbb{C}$ numerically seem to be isogenous. If such an isogeny exists, we know by GAGA that it is algebraisable and defined over a finite extension of K. The only problem that remains is to find such an algebraic isogeny explicitly.

It is possible to numerically construct an analytic isogeny $\tau\colon H_{\mathbb{C}} \to J_{\mathbb{C}} \to E_{\mathbb{C}} \times E_{\mathbb{C}}$. We consider the four composite maps

$$\begin{tikzcd} \tau_{1,x}, \tau_{1,y}, \tau_{2,x}, \tau_{2,y}\colon H_{\mathbb{C}} \arrow[r] & E_{\mathbb{C}} \times E_{\mathbb{C}} \arrow[r, shift left] \arrow[r, shift right] & E_{\mathbb{C}} \arrow[r, shift left, "x"] \arrow[r, shift right, "y"'] & \mathbb{P}^1_{\mathbb{C}} \end{tikzcd} ,$$

where the middle two maps are the two projections, and x and y are coordinate maps, and try to 'guess' them. We assume that the map $\tau_{1,x}\colon H_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ (and analogously for $\tau_{1,y}, \tau_{2,x}, \tau_{2,y}$) is of the shape

$$(x, y) \mapsto \frac{\sum_{i=0}^{N} \sum_{j=0}^{1} a_{i,j} x^i y^j}{\sum_{i=0}^{M} \sum_{j=0}^{1} b_{i,j} x^i y^j},$$

for certain $a_{i,j}, b_{i,j} \in \mathbb{C}$ and $N, M \in \mathbb{Z}_{\geq 0}$. We pick $R := 2N + 2M$ complex-valued points $P_k := (\alpha_k, \beta_k) \in H_{\mathbb{C}}(\mathbb{C})$ for $k = 1, \ldots, R$ and numerically compute $Q_k := \tau_{1,x}(P_k)$. Each such point gives rise to a linear equation

$$\sum_{i=0}^{N} \sum_{j=0}^{1} a_{i,j} \alpha_k^i \beta_k^j - Q_k \cdot \sum_{i=0}^{M} \sum_{j=0}^{1} b_{i,j} \alpha_k^i \beta_k^j = 0$$

in the coefficients $a_{i,j}$ and $b_{i,j}$. Or, to phrase it in other words, the vector of coefficients $(a_{0,0}, \ldots, a_{N,1}, b_{0,0}, \ldots, b_{M,1})$ is in the kernel of the matrix

$$A = \begin{pmatrix} \alpha_1^0 \beta_1^0 & \cdots & \alpha_1^N \beta_1^1 & -Q_1 \alpha_1^0 \beta_1^0 & \cdots & -Q_1 \alpha_1^M \beta_1^0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \alpha_R^0 \beta_R^0 & \cdots & \alpha_R^N \beta_R^1 & -Q_R \alpha_R^0 \beta_R^0 & \cdots & -Q_R \alpha_R^M \beta_R^1 \end{pmatrix}.$$

We can compute this kernel numerically and choose N and M such that the kernel is 1-dimensional. In this way, we can be sure to find a basis vector, which is a $\mathbb{C}$-multiple of a vector with algebraic entries, instead of obtaining a random $\mathbb{C}$-linear combination of two or more.

We compute a generator for the kernel and rescale it to make one of the non-zero entries equal to 1. Then we use LLL to guess algebraic relations for the other entries. In this way, we found a solution $(a_{0,0}, \ldots, b_{M,1}) \in \overline{\mathbb{Q}}^R$ and, if M and N were chosen appropriately, it can be verified algebraically that these functions indeed define a morphism $\varphi\colon H_L \to E_L \times E_L$, where L is the field extension of K generated by all $a_{i,j}, b_{i,j}$, whose base change to $\mathbb{C}$ is $((\tau_{1,x}, \tau_{1,y}), (\tau_{2,x}, \tau_{2,y}))$.

2.3.4 Smaller fields

A priori, the field L might be way too big for a feasible numerical verification of BSD. For example, in our specific case, a priori the curve H and E were defined over $\mathbb{Q}$ and

$\mathbb{Q}(\sqrt{5})$, respectively, but the maps φ and ψ were only defined over $L = \mathbb{Q}(\sqrt[8]{5}, i)$ and $\varphi\colon H \to E\colon (x : y : 1) \mapsto (\varphi_x : \varphi_y : 1)$ was given by

$$\varphi_x = \frac{\frac{1}{2} i \sqrt[4]{5} \cdot x^4 - x^3 - \frac{1}{2} i \left(\frac{4}{5} \sqrt[4]{5}^3 - \sqrt[4]{5}\right) \cdot x^2 + \frac{1}{5}\sqrt{5} \cdot x + \frac{1}{10} i \sqrt[4]{5}}{x^3 + \frac{2i}{5}\sqrt[4]{5}^3 \cdot x^2 - \frac{1}{5}\sqrt{5} \cdot x},$$

$$\varphi_y = \frac{\frac{1}{4}\varepsilon \sqrt[8]{5}^3 \cdot x^4 y + \delta \sqrt[8]{5} \cdot x^3 y - \frac{1}{4}\varepsilon \left(\frac{4}{5}\sqrt[8]{5}^7 + \sqrt[8]{5}^3\right) \cdot x^2 y - \frac{\delta}{5}\sqrt[8]{5}^5 \cdot xy + \frac{1}{20}\varepsilon \sqrt[8]{5}^3 \cdot y}{x^5 + \frac{3i}{5}\sqrt[4]{5}^3 \cdot x^4 - \frac{3}{5}\sqrt{5} \cdot x^3 - \frac{1}{5} i \sqrt[4]{5} \cdot x^2},$$

where $\varepsilon = 1 - i$ and $\delta = 1 + i$. Of course this still proves that $\operatorname{Jac} H_L$ and $E_L \times E_L$ are isogenous.

However, it is not feasible yet to numerically verify BSD for H_L. The situation is not as good as in Proposition 2.2.8 part (4). In the isogeny decomposition of the Weil restriction $\operatorname{Res}^{L}_{\mathbb{Q}(\sqrt{5})} \operatorname{Jac}(H_L)$, there will not only be twists of $\operatorname{Jac} H$ occuring, but also higher dimensional factors, see also [DiNa03]. Even if we are lucky, and all these factors are Jacobians of hyperelliptic curves over $\mathbb{Q}$, these curves will be of genus greater than 3. Numerical verification of BSD for such curves might take too much time.

In order to reduce the size of L and reduce to the case of a quadratic field extension, we performed some twists, for example on E by $\varepsilon\sqrt[8]{5}$ and on H by -1. We then repeated the procedure in the previous paragraph and even managed to find a map of smaller degree over the smaller field $\mathbb{Q}(\sqrt[4]{5})$.

Having found the appropriate map defined over $\mathbb{Q}(\sqrt[4]{5})$, we were able to get the result in Proposition 2.2.2 in order to finally prove Theorem 2.1.2.

Chapter 3

Inverse Galois problem for ordinary curves

Abstract. We consider the inverse Galois problem over function fields of positive characteristic p, for example, over the projective line. We describe a method to construct certain Galois covers of the projective line and other curves, which are ordinary in the sense that their Jacobian has maximal p-torsion. We do this by constructing Galois covers of ordinary semi-stable curves, and then deforming them into smooth Galois covers.

3.1 Introduction

In [GlPr05], Glass and Pries prove that there is an ordinary (in the sense that the Jacobian has maximal p-torsion) hyperelliptic curve of every genus in characteristic $p > 2$. Viewing hyperelliptic curves as $\mathbb{Z}/2\mathbb{Z}$-covers of the projective line $\mathbb{P}^1$, this leads to the following question: is it possible, for any finite group G, to construct an ordinary curve which is a Galois cover of $\mathbb{P}^1$ whose Galois group is G?

The inverse Galois problem over function fields has been studied extensively. In [Harb84] and [Harb87], Harbater solved the problem for $\overline{\mathbb{F}}_p(t)$ and for $k(t)$ where k is a complete ultrametric field (see also [MaMa99, Sect. V.2]). The problem is solved by constructing covers of $\mathbb{P}^1$ over $\overline{\mathbb{F}}_p$ or k using rigid analytic methods. These methods, however, do not seem to give us a way to easily determine whether the curves constructed are ordinary.

In this chapter, we will construct Galois covers which are ordinary using a different method: deformation theory. We will reprove the aforementioned result by Glass and Pries in a different way, that will also allow us to construct ordinary covers of $\mathbb{P}^1$ (and other curves) with other Galois groups.

For our method, we will consider Galois covers of ordinary semi-stable curves. We will then use deformation theory on semi-stable curves, [DeMu69], and in particular on curves with an action of a group, [Sai12], to smoothen the cover. Our key result in this direction is the following.

Theorem 3.1.1. *Let G be a finite group and let $\gamma\colon C \to D$ be a Galois cover (cf. Def. 3.4.1, p. 43), with Galois group G, of semi-stable curves over an algebraically closed field k of characteristic p coprime to the order of G. Moreover, suppose that for each $P \in C^{\mathrm{sing}}$ and each $\sigma \in \mathrm{Stab}(P) \subset G$, the determinant of the action of σ on the tangent space at P is -1 if σ swaps the two branches of C at P and 1 otherwise. Then there exists a smoothening $\Gamma\colon \mathcal{C} \to \mathcal{D}$ of the cover γ, where $\mathcal{C}$ and $\mathcal{D}$ are semi-stable curves over $k[[X]]$. In case C is ordinary, the curve $\mathcal{C}$ is also ordinary.*

For example, using a configuration of copies of $\mathbb{P}^1$, whose associated graph is an n-gon, we will realise the dihedral group D_n with $2n$ elements.

Example 3.1.2 (Prop. 3.5.5, p. 48)**.** Let n be a positive integer and let p be a prime number not dividing $2n$. Then there exists a Galois cover $C \to \mathbb{P}^1$ with group D_n such that C is a smooth ordinary curve over $\overline{\mathbb{F}}_p$.

In section 2, we will treat the definitions necessary to extend the notion of ordinarity to semi-stable curves. In section 3, we will look at graphs associated to semi-stable curves and their quotients by group actions. In section 4, we show how to deform these singular curves to smooth curves, while preserving the group action. The proof of the main theorem will be given in section 5. Finally, in section 6, we will list some examples of groups for which we can construct ordinary Galois covers, using this method.

The author wishes to thank his PhD advisors David Holmes and Fabien Pazuki. Moreover, Bas Edixhoven, Maarten Derickx, Peter Koymans and an anonymous referee are thanked for their thorough reading and their useful comments for improvements.

3.2 Ordinarity of semi-stable curves

Let us first recall the notion of semi-stable curves.

Definition 3.2.1. A curve over an algebraically closed field is semi-stable if it is reduced, proper, connected and has at-worst nodal singularities. Over a scheme S, a semi-stable curve is a proper flat scheme over S whose geometric fibres are semi-stable curves.

Let k be an algebraically closed field of characteristic $p > 0$ and let $C/\operatorname{Spec} k$ be a semi-stable curve. Consider the map $\mathcal{O}_C \to \mathcal{O}_C$ raising all sections to the power p and let $F\colon H^1(C, \mathcal{O}_C) \to H^1(C, \mathcal{O}_C)$ be the induced map on cohomology. This map satisfies the conditions of [Mumf70, Cor., chap. 14, p. 143], hence $H^1(C, \mathcal{O}_C)$ decomposes as the sum of a semisimple part and a nilpotent part.

Definition 3.2.2 ([Mumf70, sect. 15, p. 146–150])**.** We say C is ordinary if the semisimple rank of F is maximal or, in other words, if the dimension of the semisimple part of

$H^1(C, \mathcal{O}_C)$ is equal to $\dim_k(H^1(C, \mathcal{O}_C))$. More generally, for a scheme S, a semi-stable curve C/S is called ordinary if C_s is ordinary for every geometric point s of S.

Remark 3.2.3. It is well-known that for smooth curves this definition coincides with the classical definition, i.e. a smooth curve is ordinary if the p-torsion of the Jacobian of the curve is maximal.

An easy well-known corollary of [Mumf70, Cor., chap. 14, p. 143] is the following lemma.

Lemma 3.2.4. *Let $C/\operatorname{Spec} k$ and F be as before. Then C is ordinary if and only if F is an isomorphism.*

The goal of this section is to prove that a semi-stable curve is ordinary (in the sense of Definition 3.2.2) if and only if all irreducible components of its normalisation are.

Proposition 3.2.5. *Let C/k be a semi-stable curve over an algebraically closed field. Let $C_1, \ldots, C_n$ be the irreducible components of its normalisation. Then C is ordinary if and only if for all $i = 1, \ldots, n$ the smooth curve C_i is ordinary.*

Proof. Let $\widetilde{C}$ be the normalisation of C, and consider the exact sequence

$$0 \longrightarrow \mathcal{O}_C \longrightarrow \pi_*\mathcal{O}_{\widetilde{C}} \longrightarrow \pi_*\mathcal{O}_{\widetilde{C}}/\mathcal{O}_C \longrightarrow 0.$$

The sheaf $\pi_*\mathcal{O}_{\widetilde{C}}/\mathcal{O}_C$ is a direct sum of skyscraper sheaves, one for each singular point P of C, having k as stalk in P. As π is an affine morphism, we have $H^i(C, \pi_*\mathcal{F}) = H^i(\widetilde{C}, \mathcal{F})$ for any quasi-coherent sheaf $\mathcal{F}$ of $\mathcal{O}$-modules on $\widetilde{C}$. Hence, for the associated long exact sequence we get

$$0 \longrightarrow k \longrightarrow k^n \longrightarrow k^{\mathrm{Sing}(C)} \longrightarrow H^1(C, \mathcal{O}_C) \longrightarrow \bigoplus_{i=1}^{n} H^1(C_i, \mathcal{O}_{C_i}) \longrightarrow 0.$$

Now consider the action of Frobenius on this exact sequence. On k, k^n and $k^{\mathrm{Sing}(C)}$ it acts componentwise, hence it induces an isomorphism. By Lemma 3.2.4, on the one hand, Frobenius acts on $H^1(C, \mathcal{O}_C)$ as an isomorphism if and only if C is ordinary. On the other hand, Frobenius acts on $H^1(C_i, \mathcal{O}_{C_i})$ as an isomorphism if and only if C_i is ordinary. Now we can use the five-lemma to conclude the desired result. □

3.3 Quotients of curves and their associated graphs

In this section, we will build a formalism for graphs associated to semi-stable curves. It should commute with the operation of taking the quotient under the action of a finite group. Throughout this section S will be $\operatorname{Spec} k$, the spectrum of an algebraically closed field. The following two examples will serve as motivation for the definition that follows.

Example 3.3.1. Let C/S be a curve obtained by gluing three copies of $\mathbb{P}^1$ to form a triangle. We let $G = \mathbb{Z}/3\mathbb{Z}$ act on C by cyclically permuting these $\mathbb{P}^1$'s. Then the quotient of C by G is a $\mathbb{P}^1$ with two of its points glued together.

Example 3.3.2. Let C/S be the same curve as in the previous example. We let $G = S_3$ act on C in the natural way. Then the quotient of C by G is $\mathbb{P}^1$.

Definition 3.3.3 (Graph)**.** A graph consists of the data of a set of vertices V, for every $v \in V$ a set E_v of edge ends, and an involution $n\colon \bigsqcup_v E_v \to \bigsqcup_v E_v$ without fixed point, giving the opposite of each edge end.

A morphism of graphs from $(V, (E_v)_v, n_V)$ to $(W, (E_w)_w, n_W)$ consists of a morphism $\varphi\colon V \to W$ and morphisms $\psi_v\colon E_v \to E_{\varphi(v)} \cup \{\varphi(v)\}$ for every $v \in V$ satisying the following conditions:

- an edge end $e \in E_v$ is mapped to $\varphi(v)$ (i.e. it is contracted) if and only if the opposite end $n_V(e)$ is mapped to the same point;
- when an edge $e \in E_v$ is not contracted, its opposite end $n_V(e)$ is mapped to $n_W(\psi_v(e))$, i.e. opposite edge ends stay opposite.

Remark 3.3.4. Edges are allowed to be contracted for the reason that morphisms of semi-stable curves could map singular points to smooth points. We would like these morphisms to give rise to morphisms on their associated graphs (cf. Definition 3.3.7).

Another solution for this problem would be to allow edge ends to be connected to themselves. This would correspond to a suitable notion of graphs for semi-stable curves with a finite set of smooth marked points. In this case, morphisms of marked semi-stable curves are supposed to map singular points to singular or marked points.

Proposition 3.3.5. *Colimits exist in the category of graphs.*

Proof. Consider a diagram of graphs $(V_i, (E_v)_{v \in V_i}, n_i)_{i \in I}$ (with morphisms between them). The set of vertices V of the colimit graph will be the colimit in the category of sets of the diagram $(V_i)_{i \in I}$ obtained by forgetting the edge ends.

For each vertex $v \in V$, we consider the set of vertices w in the original diagram that map to v. Its sets of edge ends form a diagram $(E_w)_{w \mapsto v}$. Let E'_v be the colimit of this diagram in the category of sets. Moreover, we glue the maps $n_i|_{E_w}$ to a map $n'_v\colon E'_v \to E'_v$. The set of edge ends E_v of v is then defined as $E'_v \setminus \{e \in E'_v : n'_v(e) = e\}$. The map $n\colon \bigcup_{v \in V} E_v \to \bigcup_{v \in V} E_v$ is constructed by gluing the n'_v.

It is clear from the construction that the graph $(V, (E_v)_{v \in V}, n)$ is the colimit of the diagram $(V_i, (E_v)_{v \in V_i}, n_i)_{i \in I}$. □

Remark 3.3.6. In particular, if a finite group G acts on a graph Γ, then the quotient graph Γ/G exists and can be constructed as follows:

- its set of vertices is V/G (quotient in the category of sets);
- for each $v \in V$, reducing to $\overline{v} \in V/G$, the edge end set $E_{\overline{v}}$ is obtained as follows: first take E_v/G_v, where $G_v \subset G$ is the stabiliser of v, and then remove all elements that have been identified with their opposite (i.e. the edge ends e for which there is an element of G mapping e to $n_V(e)$).

Definition 3.3.7 (Associated graph)**.** Let C be a semi-stable curve over S. Then we can associate to it a graph, whose vertices are the irreducible components of C. There are two opposite edge ends for each singular point P: one for each of the two (possibly the same) components that are intersecting there.

Proposition 3.3.8. *Let C/S be a possibly singular reduced curve. Let $\pi\colon \widetilde{C} \to C$ be its normalisation. Then C is semi-stable if and only if there exist two maps $\ell_1, \ell_2\colon L \to \widetilde{C}$ from the singular locus of C to $\widetilde{C}$ such that $\pi \circ \ell_1 = \pi \circ \ell_2$ is the inclusion of the singular locus in C and C is the colimit of the following diagram with these two arrows:*

$$L \rightrightarrows \widetilde{C}.$$

Proof. If C is semi-stable, then there lie two points above each singular point of C and by ordering them for each singular point, we get two maps ℓ_1 and ℓ_2 as required. Using [Liu02, Prop. 7.5.15, p. 310] and reducing to the affine case, we find that C is the colimit of the diagram.

If C is such a colimit, then above each singular point of C there are one or two points. If there is only one, then C would be smooth at that point, which is not the case, hence there are two. Then by [Liu02, Prop. 7.5.15, p. 310] the singularities are nodal and we are done. □

Proposition 3.3.9. *Let C/S be a semi-stable curve. Let $G \subset \mathrm{Aut}_S(C)$ be a finite group. Let Γ be the graph associated to C. Then there exists a semi-stable curve D/S that is a categorical quotient of C by G in the category of schemes. Its associated graph is Γ/G.*

Proof. Let $\pi\colon \widetilde{C} \to C$ be the normalisation of C. For each singular point $p \in C$ choose an ordering on the two points in $\pi^{-1}(p)$. Let L be the union of the singular points of C. Then the ordering chosen gives us two maps $\ell_1, \ell_2\colon L \to \widetilde{C}$ mapping p to the first respectively second point in $\pi^{-1}(c)$. Observe, cf. Proposition 3.3.8, that C is the colimit of the diagram

$$L \rightrightarrows \widetilde{C},$$

where the two maps are ℓ_1 and ℓ_2.

The universal property of the normalisation gives us an extension of the action of G on C to $\widetilde{C}$. Now the irreducible components of $\widetilde{C}$ are connected and G permutes them. Using [Mumf70, Thm. 1, chap. 12, p. 111], we see that the categorical quotient $q\colon \widetilde{C} \to \widetilde{D}$ of $\widetilde{C}$ by the group action of G identifies components sent to each other and each such component is replaced by the quotient of that component by the action of its stabiliser. Now we will recall the standard argument to prove that these quotients of the components are smooth curves.

As a subring of an integral ring is integral, the quotients of the components are integral. Furthermore, they are normal, as for an integrally closed domain A with an action of a group G, the ring A^G is integrally closed. As A is an integral extension of A^G, it has the going-up property and A^G is noetherian and of dimension 1. Hence, the quotients of the components are normal integral of dimension 1. Hence, the quotients of the components of $\widetilde{C}$ are smooth curves, see also [Stacks, 0BX2].

Now we will re-glue the points. Let D be the colimit of the diagram

$$L \rightrightarrows \widetilde{D},$$

where the two maps are $q \circ \ell_1$ and $q \circ \ell_2$. Let $\zeta\colon \widetilde{D} \to D$ be the natural map. Now, we will prove that this is also a categorical quotient of C by G.

$$\begin{tikzcd}
L \arrow[r, bend left, "\ell_1"] \arrow[r, bend right, "\ell_2"'] & \widetilde{C} \arrow[r, "q"] \arrow[d, "\pi"] & \widetilde{D} \arrow[d, "\zeta"] \arrow[ddl, dashed, bend left=60, "\rho"] \\
 & C \arrow[r, dashed, "Q"] \arrow[d, "\psi"] & D \arrow[dl, dashed, "\nu"] \\
 & T &
\end{tikzcd}$$

First of all, the maps $\zeta \circ q \circ \ell_1$ and $\zeta \circ q \circ \ell_2$ are the same by construction. Hence, there is a map $Q\colon C \to D$, such that $Q \circ \pi = \zeta \circ q$.

Let T be a test scheme with a trivial action of G and $\psi\colon C \to T$ be a G-equivariant map. Then the map $\psi \circ \pi\colon \widetilde{C} \to T$ is also G-equivariant and gives rise to a unique map $\rho\colon \widetilde{D} \to T$, such that $\rho \circ q = \psi \circ \pi$. Now we have

$$\rho \circ q \circ \ell_1 = \psi \circ \pi \circ \ell_1 = \psi \circ \pi \circ \ell_2 = \rho \circ q \circ \ell_2,$$

and hence by the universal property of the colimit there is a unique map $\nu\colon D \to T$ such that $\nu \circ \zeta = \rho$. Now the compositions $\psi \circ \pi$ and $\nu \circ \zeta \circ q = \nu \circ Q \circ \pi$ are equal. Since the normalisation is surjective on schemes and injective on the underlying rings, it is an epimorphism. This yields $\psi = \nu \circ Q$ as desired.

Now the existence of the categorical quotient D follows by using Proposition 3.3.8. We analyse its associated graph. Its irreducible component are orbits, under the action of G, of irreducible components of C, which corresponds exactly to the set of vertices of Γ/G (cf. Remark 3.3.6). In order to study the singular points of D, we consider a singular point $P \in C$. It has two preimages $P_1, P_2 \in \widetilde{C}$, and it gives rise to a singular point in D if and only if $q(P_1)$ and $q(P_2)$ have not been identified with each other. Now $q(P_1)$ and $q(P_2)$ have been identified with each other, if and only if there is an automorphism $g \in G$ swapping P_1 and P_2. That is, they are identified, if and only if there is an automorphism swapping the two edge ends. In other words, if and only if the edge end does not survive in Γ/G (cf. Remark 3.3.6).

Therefore, the graph associated to D is Γ/G. □

Example 3.3.10. The graph $\Gamma(C)$ corresponding to the curve C from Examples 3.3.1 and 3.3.2 consists of three vertices C_1, C_2 and C_3. The set of edge ends for C_i is $\{C_{i,j}\}_{j \neq i}$, where $n(C_{i,j}) = C_{j,i}$. In both cases, the graph associated to the quotient curve (a single vertex with a loop, and a single vertex, respectively) is the quotient of $\Gamma(C)$ by the action of $\mathbb{Z}/3\mathbb{Z}$ and S_3, respectively.

3.4 Proof of the main theorem

In this section, we will treat deformations of Galois covers in order to prove the main theorem, Theorem 3.1.1. Let us first define this notion.

Definition 3.4.1 (Galois cover)**.** Let $f\colon X \to Y$ be a morphism of noetherian schemes, and let G be (isomorphic to) a finite group of automorphisms of X. Then f is called a Galois cover with group G if Y is the quotient of X by G as a scheme, and each $g \in G \setminus \{\mathrm{id}\}$ does not act as the identity on any of the irreducible components of X.

Set-up 3.4.2. Let C be a semi-stable curve over $S = \operatorname{Spec} k$, the spectrum of an algebraically closed field. Let $G \subset \operatorname{Aut}_S(C)$ be a finite group of order coprime to $p := \operatorname{char} k$ such that for each component of C the stabiliser acts faithfully on the component. Let D be the quotient of C by G (as in Proposition 3.3.9). Then $\gamma\colon C \to D$ is a Galois cover with group G.

Remark 3.4.3. Suppose we are in the setting of Set-up 3.4.2. Then γ is tame admissible in the sense of [Wew99, Def. 2.3.1, p. 260]. However, we will describe the local structure of the cover more explicitly.

Let $Q \in C^{\mathrm{sing}}$ be a node and let $P \in D$ be its image $\gamma(Q)$. Then P could be either singular or smooth. We consider the cases separately.

- If $P \in D^{\mathrm{sing}}$, then we know that $\widehat{\mathcal{O}}_{C,Q} \cong k[[a,b]]/(ab)$ and moreover we have that $\widehat{\mathcal{O}}_{D,P} \cong k[[s,t]]/(st)$ (cf. [Liu02, Prop. 7.5.15, p. 310]) and, swapping the variables if necessary, one easily checks that the original cover is given by

$$\widehat{\gamma}_Q : k[[s,t]]/(st) \to k[[a,b]]/(ab) : \quad s \mapsto a^m \cdot u, \quad t \mapsto b^\ell \cdot v,$$

  for some integers m and ℓ and units $u \in k[[a]]$ and $v \in k[[b]]$. The stabiliser $\operatorname{Stab}(Q) \subset G$ acts faithfully on both components through Q. Hence, we find that $k((a))/k((s))$ and $k((b))/k((t))$ are Galois extensions of degree $m = |\operatorname{Stab}(Q)| = \ell$. In particular, m is not divisible by p and, by Hensel's lemma, u and v are m-th powers in $k[[a,b]]/(ab)$ and we may and will assume, by composing with an automorphism if necessary, that $u = v = 1$.

  In particular, the group $\operatorname{Stab}(Q)$ is cyclic and acts on a and b by multiplication with (not necessarily the same) m-th roots of unity.

- In the case that P is a smooth point of D, the local cover $\widehat{\gamma}_Q$ is given by

$$\widehat{\gamma}_Q : k[[s]] \to k[[a,b]]/(ab) : \quad s \mapsto a^m \cdot u + b^\ell \cdot v,$$

for some integers m and ℓ and units $u \in k[[a]]$ and $v \in k[[b]]$. Analogous to the first case, we get that $m = \ell = \frac{1}{2} \cdot |\mathrm{Stab}(Q)|$ and we may assume that $u = v = 1$.

The group $\mathrm{Stab}(Q)$ is either cyclic, generated by an element g swapping the two components, such that g^2 acts by multiplication with primitive m-th roots of unity, or $\mathrm{Stab}(Q)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, where the first factor is acting by swapping the two components and the second one by multiplication with m-th roots of unity.

In the part that follows, we will assume that the action of G is orientation preserving in the following sense.

Definition 3.4.4. Let k be an algebraically closed field and let C be a semi-stable curve over $\operatorname{Spec} k$. Let $G \subset \mathrm{Aut}_k(C)$ be a finite group. For every $P \in C^{\mathrm{sing}}$, the subgroup $\mathrm{Stab}(P)$ acts on the completed local ring $(\widehat{\mathcal{O}}_{C,P}, \mathfrak{m}_P)$ of C at p, and on its cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$. The action of G on C is called orientation preserving at P, if for each $\sigma \in \mathrm{Stab}(P)$, this action of σ on $\mathfrak{m}_P/\mathfrak{m}_P^2$ has determinant $\mathrm{sgn}_P(\sigma)$, where $\mathrm{sgn}_P(\sigma)$ is the sign of the action of σ on the set of branches of C through P. The action of G on C is called orientation preserving if it is orientation preserving at every $P \in C^{\mathrm{sing}}$.

Remark 3.4.5. This condition is easily seen to be verified in case $\mathrm{Stab}(P)$ is isomorphic to either $1, \mathbb{Z}/2\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ for each $P \in C^{\mathrm{sing}}$. In these cases, after changing coordinates if necessary, the action of $\mathrm{Stab}(P)$ on $\widehat{\mathcal{O}}_{C,P} \cong k[[a,b]]/(ab)$ only involves swapping a and b and multiplying them simultaneously by -1.

Proposition 3.4.6. *Suppose we are in the situation of Set-up 3.4.2 and that the action of G on C is orientation preserving. Over the complete discrete valuation ring $R = k[[X]]$, with residue field k, there exists a G-Galois cover $\Gamma\colon \mathcal{C} \to \mathcal{D}$ of semi-stable curves over* $\operatorname{Spec} R$ *such that $\Gamma_s \cong \gamma$, and $\mathcal{C}_\eta$ and $\mathcal{D}_\eta$ are smooth, where η and s are the generic and special point of* $\operatorname{Spec} R$*, respectively.*

Proof. First we shall consider the local structure of the map γ above the singular points of D in order to define the scheme $\mathcal{D}$ using deformation theory of stable curves.

For each singular point $P \in D$, the completed local ring $\widehat{\mathcal{O}}_{D,P}$ is isomorphic to $k[[s,t]]/(st)$. Now we take $\mathcal{D}/\operatorname{Spec} R$ to be any deformation of D such that we have an isomorphism $\widehat{\mathcal{O}}_{\mathcal{D},P} \cong k[[s,t,X]]/(st - X^m)$, using [Bert13, Prop. 4.37, p. 117], where $m = |\mathrm{Stab}(Q)|$ is the size of the stabiliser inside G of any point $Q \in \varphi^{-1}(P)$.

To lift γ we will use [Sai12, Prop. 1.2.4, p. 8]. Let $P \in D$ be a singular point or a point where γ is ramified. Then, in order to get the patching data as in loc. cit., it suffices to étale-locally extend the action of G to the local deformation ring of $\gamma^{-1}(P)$. Let $Q \in \gamma^{-1}(P)$ be an arbitrary point.

We consider two cases.

(i) First consider the case P is smooth. If also Q is smooth, the lifting is straightforward, so we only consider the case when Q is singular. As in Remark 3.4.3, in this case, after changing coordinates if necessary, $\widehat{\gamma}_Q$ is of the form

$$k[[s]] \to k[[a,b]]/(ab)\colon \quad s \mapsto a^m + b^m,$$

where $m = \frac{1}{2}|\mathrm{Stab}(Q)|$. The group $\mathrm{Stab}(Q)$ acts by swapping a and b and multiplying them with m-th roots of unity (the cyclic case from Remark 3.4.3 is not orientation-preserving). We lift this part of the cover to $R = k[[X]]$ by taking the local deformation

$$k[[s,X]] \to k[[a,b,X]]/(ab - X)\colon s \mapsto a^m + b^m, \quad X \mapsto X.$$

It is immediate how the action of $\mathrm{Stab}(Q)$ can be extended, observing that we need to use that the action is orientation preserving, as the element $X = ab$ needs to be preserved by $\mathrm{Stab}(Q)$. To extend this to an action of G, we choose a representative σ for each right coset of $G/\mathrm{Stab}(Q)$. We then create a copy of this local cover above $\sigma(Q)$, using σ to identify the cover with the cover above Q.

(ii) Now suppose P is singular (and hence Q is singular as well). In this case, cf. Remark 3.4.3, after changing coordinates if necessary, $\widehat{\gamma}_Q$ is of the form

$$k[[s,t]]/(st) \to k[[a,b]]/(ab)\colon \quad s \mapsto a^m, \quad t \mapsto b^m,$$

where $m = |\mathrm{Stab}(Q)|$. The group $\mathrm{Stab}(Q)$ is acting on $a, b \in k[[a,b]]/(ab)$ by multiplication with (possibly distinct) powers of m-th roots of unity. We lift this part of the cover to $R = k[[X]]$ by taking the local deformation

$$\begin{gathered} k[[s,t,X]]/(st - X^m) \to k[[a,b,X]]/(ab - X) \\ s \mapsto a^m, \quad t \mapsto b^m, \quad X \mapsto X, \end{gathered}$$

observing that we need to use that the action is orientation preserving again. We extend the natural action of $\mathrm{Stab}(Q)$ to G in the same way as in case (i).

Using [Sai12, Prop. 1.2.4, p. 8], we find a G-Galois cover $\Gamma\colon \mathcal{C} \to \mathcal{D}$ of schemes over $\mathrm{Spec}\,(k[[X]])$, such that the special fibre is γ, and locally above singular points Q as above we have $\widehat{\mathcal{O}}_{\mathcal{C},Q} \cong k[[a,b,X]]/(ab - X)$. On these local charts, the only non-smooth point are given by $s = t = 0$ (in case (ii)) and $a = b = 0$ (in both cases), respectively, and hence lie on the special fibre $X = 0$. The points on the generic fibre specialising to a smooth point on the special fibre are smooth automatically, as smoothness is an open condition. Hence, the generic fibres $\mathcal{C}_\eta$ and $\mathcal{D}_\eta$ are smooth. The semi-stability of $\mathcal{C}_\eta$ and $\mathcal{D}_\eta$ follows from the deformation theory of nodal singularities (see for example [DeMu69]). □

Now we can combine this with the results from the previous section to prove Theorem 3.1.1.

Proof. (Theorem 3.1.1) Take a deformation $\mathcal{C} \to \mathcal{D}$ as in Proposition 3.4.6. Then, if C is ordinary, also $\mathcal{C}_\eta$ is ordinary, as the p-rank is lower semi-continuous, cf. [FvdG04, sect. 2] and [Katz79, Th. 2.3.1]. □

Remark 3.4.7. Using an argument like Harbater's, see [MaMa99, Thm. 2.7, p. 376], we can find an ordinary G-Galois cover over k instead of the much larger field $k((X))$. The idea is that $\mathcal{C}_\eta$ is defined over a finitely generated algebra over k. By Bertini-Noether, the locus where the curves are irreducible is Zariski open and dense. Moreover, the ordinary and the smooth locus are also Zariski open and dense. Hence, as k was assumed to be algebraically closed, we can find a point to specialise to in order to find an ordinary G-Galois cover of smooth curves over k.

3.5 Examples of ordinary curves

In this section, we will apply the theory developed in the previous chapter to construct examples of ordinary curves, which are Galois covers of some other curve. We will treat the following examples.

Galois group	Galois cover of
C_2 (arbitrary genus hyperelliptic curve)	projective line
gen. by two elements, one of order 2, one of higher order	elliptic curve
$G \rtimes C_2$ for abelian groups G as above	projective line
D_n	projective line
A_5	projective line

As a first example, we will show that there exist ordinary hyperelliptic curves of arbitrary genus in odd characteristic. The following reproves a result of Glass and Pries ([GlPr05, Thm. 1, sect. 2, p. 301]) using the tools that we developed.

Proposition 3.5.1. *Let $p > 2$ be a prime number and let $g \geq 1$ an integer. Then there exists an ordinary hyperelliptic curve of genus g over $k = \overline{\mathbb{F}}_p$.*

Proof. We will prove this statement by induction on the genus. For $g = 1$, in order to obtain an ordinary elliptic curve, take two copies of $\mathbb{P}^1$ and glue them in two points to obtain a curve C. Let $G := \mathbb{Z}/2\mathbb{Z}$ act on C by swapping the two components. Then the quotient D of C by G is isomorphic to $\mathbb{P}^1$ by Proposition 3.3.9, and the action of G on C is orientation preserving by Remark 3.4.5. We deform this, using Theorem 3.1.1. The resulting curve $\mathcal{C}/\overline{\mathbb{F}}_p[[X]]$ is a G-cover of $\mathcal{D} = \mathbb{P}^1$. As the arithmetic genus is constant on flat families, the generic fibre of $\mathcal{C}$ gets the structure of an ordinary elliptic curve over $\overline{\mathbb{F}}_p((X))$. Using Remark 3.4.7, we obtain an ordinary elliptic curve over $\overline{\mathbb{F}}_p$.

Now suppose that we managed to obtain an ordinary hyperelliptic curve $H/\overline{\mathbb{F}}_p$ of genus $\ell - 1 \geq 1$. We will construct an ordinary hyperelliptic curve of genus ℓ out of this.

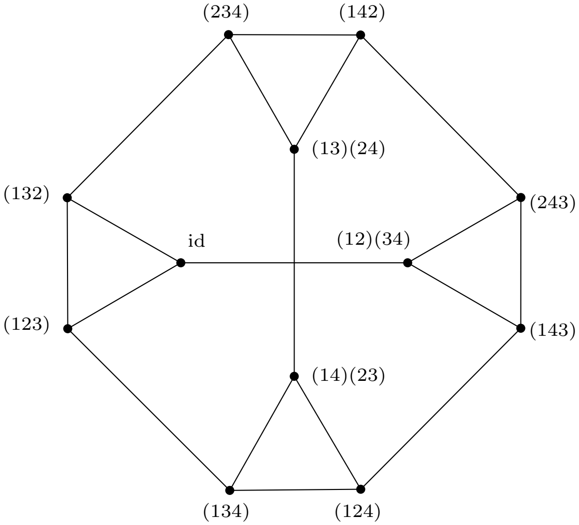
Take an ordinary elliptic curve E over $\overline{\mathbb{F}}_p$. Let $\varphi_H \colon H \to \mathbb{P}^1$ and $\varphi_E \colon E \to \mathbb{P}^1$ be the associated 2:1-covers to $\mathbb{P}^1$. Pick points $P \in E(\overline{\mathbb{F}}_p)$ and $Q \in H(\overline{\mathbb{F}}_p)$ such that φ_E (resp. φ_H) is ramified at P (resp. Q). Let C be the curve obtained by gluing E and H in P and Q respectively. Let D be the curve obtained by gluing $\mathbb{P}^1$ and $\mathbb{P}^1$ in $\varphi_E(P)$ and $\varphi_H(Q)$, respectively.

Then there is a natural map $\varphi\colon C \to D$ and the action of $G := \mathbb{Z}/2\mathbb{Z}$ on E and H extends to C, giving φ the structure of a G-Galois cover. Moreover, C is ordinary as both E and H are, cf. Proposition 3.2.5. As of Remark 3.4.5, the action of G on C is orientation preserving. As before, we can use Theorem 3.1.1 and Remark 3.4.7 in order to obtain an ordinary hyperelliptic curve of genus ℓ over $\overline{\mathbb{F}}_p$. □

Proposition 3.5.2. *Let G be a finite group, generated by two elements, of which one has order 2 and the other has order greater than 2 (e.g. $G = S_n$ or $G = D_n$ for $n \geq 3$). Let p be a prime number coprime to $|G|$. Then there exists an elliptic curve E over $\overline{\mathbb{F}}_p$ and a Galois cover $C \to E$ with group G of smooth curves over $\overline{\mathbb{F}}_p$ such that C is ordinary and of genus $\frac{1}{2}|G| + 1$.*

Proof. Let h_1, h_2 be two generators of G, of which h_1 is of order 2 and h_2 of higher order. Then we can consider the Cayley graph Γ, whose vertices are elements $g \in G$ and for each vertex $g \in G$, the edge end set E_g consists of three elements, opposite to edge ends of gh_1, gh_2 and gh_2^{-1}. This graph has the property that every vertex is connected to exactly three other vertices. The group G acts on the graph by

$$G \to \mathrm{Aut}(\Gamma)\colon g \mapsto (h \mapsto gh).$$



An illustration of the graph constructed in the proof of Proposition 3.5.2 with $G = A_4$ and generators $h_1 = (12)(34)$ and $h_2 = (123)$.

Next, we will construct an ordinary semi-stable curve C out of this graph. As components we take copies of $\mathbb{P}^1$, one for each element $g \in G$, glued together in any arbitrary way such that Γ is the graph associated to C. For any pair of triples of distinct points in $\mathbb{P}^1$, there is a unique automorphism sending the first triple of points to the second triple. In this way, we can extend the action of G on Γ to an action of G on C. By construction the graph has $|G|$ nodes and $\frac{3}{2}|G|$ edges, hence the aritmetic genus of C is $\frac{1}{2}|G| + 1$.

Any edge between some vertex g and gh_2 (or gh_2^{-1}) is only stabilised by the identity element of G. Edges between g and gh_1 are stabilised by the subgroup $\langle gh_1 g^{-1} \rangle \subset G$ of order 2. In both cases, Remark 3.4.5 applies and the action of G on C is orientation preserving.

As the automorphism $h \mapsto gh_1 g^{-1} h$ does swap the two edge ends of the edge between g and gh_1, these edge ends disappear in the quotient. As the automorphism group acts transitively on the vertices, the quotient graph is one vertex with one loop. Using Proposition 3.3.9 we then find that the quotient C/G is isomorphic to $\mathbb{P}^1$ glued to itself in one point.

Now we can use Theorem 3.1.1 to deform this cover into a G-Galois cover of an elliptic curve E by an ordinary smooth curve over $\overline{\mathbb{F}}_p((X))$. The arithmetic genus is invariant under this deformation. Using Remark 3.4.7, we obtain the desired cover of smooth curves over $\overline{\mathbb{F}}_p$. □

Remark 3.5.3. Any non-abelian finite simple group can be realised in this way. Because of the odd order theorem, such a group G has even order. Take any element h_1 of order 2. Then there exists, cf. [Stei98], another element h_2 such that h_1 and h_2 generate G. By taking $h_1 \cdot h_2$ instead of h_2 if necessary, we may assume that h_2 has order greater than 2.

Proposition 3.5.4. *If in addition to the hypotheses in Proposition 3.5.2 the group G is abelian, let H be the group $G \rtimes C_2$, where C_2 acts on G by inverting all elements. Then there exists a Galois cover $C \to \mathbb{P}^1$ with group H, such that C is a smooth ordinary curve over $\overline{\mathbb{F}}_p$ of genus $\frac{1}{2}|G| + 1$.*

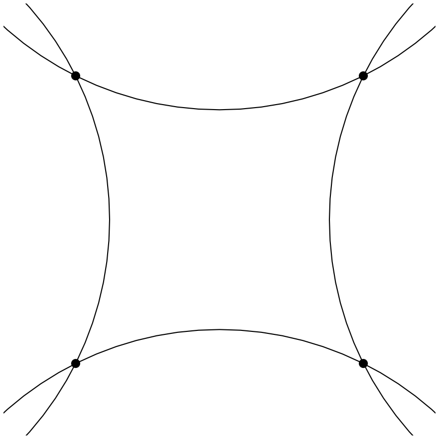
Proof. In the case G is abelian, also

$$\Gamma \to \Gamma \colon g \mapsto g^{-1}$$

is an automorphism of Γ. Using this automorphism, we obtain an action of H of Γ. Again the action extends to C and the quotient C/H is isomorphic to $\mathbb{P}^1$. In order to verify that this action is still orientation preserving, it suffices to consider the edge between the vertices $\mathrm{id} \in G$ and h_1. The new automorphism does fix this edge, but it also commutes with the multiplication by h_1. Hence, the stabiliser of the edge is $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and Remark 3.4.5 applies. Using Theorem 3.1.1 and Remark 3.4.7 again, we get a H-Galois cover of $\mathbb{P}^1$ by an ordinary smooth curve over $\overline{\mathbb{F}}_p$. □

Proposition 3.5.5. *Let n be an integer and let p be a prime number coprime to $2n$. Then there exists a Galois cover $C \to \mathbb{P}^1$ with group D_n, the dihedral group of order $2n$, such that C is a smooth ordinary curve over $\overline{\mathbb{F}}_p$ of genus 1.*

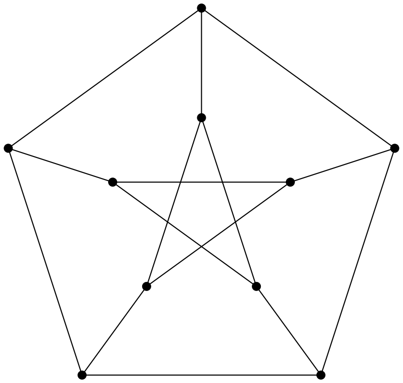
Proof. Consider the regular n-gon as a graph Γ and let D_n act on it. By gluing n copies of $\mathbb{P}^1$ subsequently in the points 0 and ∞ (gluing the 0 of one curve to the ∞ of the next one), we can construct an ordinary semi-stable curve C of arithmetic genus 1 whose associated graph is Γ.



An example with $n = 4$: four copies of $\mathbb{P}^1$ glued in a square form.

The group D_n acts on Γ in a natural way and this action can be extended to C, using the automorphism $(x : y) \mapsto (y : x)$ to mirror the sides of the n-gon, if necessary. The quotient C/D_n is isomorphic to $\mathbb{P}^1$ (cf. Proposition 3.3.9), the action of D_n on C is orientation preserving (cf. Remark 3.4.5), and by deforming it, using Theorem 3.1.1 and Remark 3.4.7, we find a D_n-Galois cover of $\mathbb{P}^1$ by an ordinary smooth curve over $\overline{\mathbb{F}}_p$. □

Proposition 3.5.6. *Let $p > 5$ be a prime number. Then there exists a Galois cover $C \to \mathbb{P}^1$ with group A_5 such that C is a smooth ordinary curve over $\overline{\mathbb{F}}_p$ of genus 6.*



The Petersen graph.

Proof. This time take Γ to be the Petersen graph. Its automorphism group is S_5. We construct the curve C, of arithmetic genus 6, by taking 10 copies of $\mathbb{P}^1$ and gluing them arbitrarily to obtain a stable curve, whose associated graph is Γ. We extend the action of the subgroup $A_5 \subset S_5$ on Γ to C, like in the previous examples. This action satisfies all the necessary conditions. The quotient C/A_5 is $\mathbb{P}^1$ and by deforming again, we find a A_5-Galois cover of $\mathbb{P}^1$ by an ordinary smooth curve. □

Chapter 4

Primes of ordinary reduction for hyperelliptic curves

Abstract. In this chapter we show for all positive integers M and g, and all number fields K except for $\mathbb{Q}$, 100% of hyperelliptic curves of genus g over K have at least M primes of ordinary good reduction.

4.1 Introduction

In arithmetic statistics, the occurrence of different types of reduction is often studied. For example Wong proved that 17.9% of elliptic curves over $\mathbb{Q}$ are everywhere semistable ([Wong01]), and Elkies showed that every elliptic curve over $\mathbb{Q}$ has infinitely many primes of good supersingular reduction ([Elk87]).

Ogus proved that elliptic curves and abelian surfaces over number fields have infinitely many primes of ordinary good reduction ([Ogus82, Cor. 2.9, p. 372]). In this chapter, we study the occurrence of ordinary good primes for Jacobians of hyperelliptic curves of genus greater than 2 over number fields.

The organisation of this chapter is as follows. First, we generalise Yui's criterion to determine whether a hyperelliptic curve over a finite field is ordinary to hyperelliptic curves given by an even degree model. Then we define several notions of density on $\operatorname{Specmax} \mathcal{O}_K$ and on $\mathcal{O}_K^N$, where $\mathcal{O}_K$ the ring of integers of a number field. Then we combine several results to prove, for all positive integers M and g, all number fields K except for $\mathbb{Q}$, that 100% of hyperelliptic curves of genus g over K have at least M primes of ordinary good reduction.

4.2 Generalisation of Yui's criterion

The following criterion by Yui gives a practical way to determine whether a hyperelliptic curve has ordinary reduction.

Theorem 4.2.1 ([Yui78, Cor. 2.3, p. 387]). *Let g be a positive integer. Let k be a perfect field of characteristic $p > 2$ and let C be a proper smooth curve over k defined by $y^2 = f(x)$ for some separable polynomial $f \in k[x]$ of degree $2g + 1$. Write $f(x)^{(p-1)/2} = \sum_j c_j x^j$. Then C is ordinary, i.e. the p-rank of $J(C)$ is g, if and only if* $\det(A) \neq 0$, *where*

$$A = \left(c_{ip-j}\right)_{i,j=1}^{g}$$

is the Cartier-Manin matrix.

Example 4.2.2. Consider the hyperelliptic curve

$$H\colon y^2 = f(x) = x^5 + x^4 + x^3 + 3x^2 + x + 2$$

of genus 2 over $\mathbb{F}_5$. Then $f(x)^2 = x^{10} + 2x^9 + 3x^8 + 3x^7 + 4x^6 + 2x^5 + 3x^2 + 4x + 4$, and the Cartier-Manin matrix is

$$\begin{pmatrix} 0 & 2 \\ 0 & 3 \end{pmatrix},$$

and its determinant is 0, which means that $\mathrm{Jac}(H)$ is not ordinary.

The criterion is only formulated for hyperelliptic curves defined by an odd degree model. We prove that the criterion also holds for an even degree model.

Theorem 4.2.3. *Let g be a positive integer. Let k be a perfect field of characteristic $p > 2$ and let C be a proper smooth curve over k defined by $y^2 = f(x)$ for some separable polynomial $f \in k[x]$ of degree $2g + 2$. Suppose that $g \leq p$. Write $f(x)^{(p-1)/2} = \sum_j c_j x^j$. Then C is ordinary, i.e. the p-rank of $J(C)$ is g, if and only if* $\det(A) \neq 0$, *where*

$$A = \left(c_{ip-j}\right)_{i,j=1}^{g}$$

is the Cartier-Manin matrix.

Proof. To prove the statement, we may extend the field k if necessary. Hence, we may and will assume that $f \in k[x]$ has a zero $\alpha \in k^*$. Now C has another model $y^2 = h(x)$ where $h(x) = f(x + \alpha)$. We will prove that the condition $\det A \neq 0$ does not depend on the model chosen.

Write $h(x) = \sum_j d_j x^j$. Then $d_j = \sum_{\ell \geq j} c_\ell \cdot \binom{\ell}{j} \cdot \alpha^{\ell - j}$. Then we find that

$$d_{ip-j} = \sum_{g \geq I \geq i} \sum_{1 \leq J \leq j} \binom{I-1}{i-1} \cdot \binom{p-J}{p-j} \cdot c_{Ip-J} \cdot \alpha^{Ip-J-ip+j}, \tag{4.1}$$

as $\binom{pI-J}{pi-j} \equiv \binom{I-1}{i-1} \cdot \binom{p-J}{p-j} \mod p$ by Lucas's theorem (note that $i, j \leq g \leq p$) and using the fact that

$$\binom{\ell}{pi-j} \equiv 0 \mod p$$

if $\ell \not\equiv -1, -2, \ldots, -j \mod p$. Note that the coefficient in front of c_{ip-j} in the right hand side of Eq. 4.1 is 1 and hence this shows that the matrix $(d_{ip-j})_{i,j=1}^g$ can be obtained from the matrix $(c_{ip-j})_{i,j=1}^g$ by means of elementary row and column operations: for $I > i$ you add $\binom{I-1}{i-1} \cdot \alpha^{Ip-ip}$ times the I-th row to the i-th row, starting from $i = 1$, working up to $i = g-1$, and for $J < j$ you add $\binom{p-J}{p-j} \cdot \alpha^{j-J}$ times the J-th column to the j-th column, starting from $j = g$. In other words, we have

$$\left(d_{pi-j}\right)_{i,j=1}^g = \left(\binom{I-1}{i-1} \cdot \alpha^{Ip-ip}\right)_{i,I=1}^g \cdot \left(c_{pi-j}\right)_{i,j=1}^g \cdot \left(\binom{p-J}{p-j} \cdot \alpha^{j-J}\right)_{J,j=1}^g,,$$

and the second and fourth matrix occuring in the formula are triangular with 1's on the diagonal. Here, it should also be understood that $\binom{n}{k} = 0$ in case $k > n$.

Hence, the matrices $(c_{ip-j})_{i,j=1}^g$ and $(d_{ip-j})_{i,j=1}^g$ have the same determinant, which proves the claim. Now we may and will reduce without loss of generality to the case in which $x \mid f$. The curve given by

$$y^2 = f(x) = \sum_{i=1}^{2g+2} f_i x^i$$

has another model, namely $Y^2 = F(X)$, where we write $X = \frac{1}{x}$ and $Y = \frac{y}{x^{g+1}}$, and where

$$F(X) := \sum_{i=0}^{2g+1} f_{2g+2-i} X^i$$

is the polynomial f but with its coefficients in reversed order. Note that $f_1 \neq 0$ as f is separable and hence F has degree $2g+1$. Now we apply Theorem 4.2.1 to the model $Y^2 = F(X)$. Write

$$F(X)^{(p-1)/2} = \sum_j C_j X^j.$$

It is the polynomial $f^{(p-1)/2}$ (as polynomial of degree $(g+1)(p-1)$) with its coefficients in reversed order, i.e. $C_j = c_{(g+1)(p-1)-j}$. Then

$$\left(C_{ip-j}\right)_{i,j=1}^g = \left(c_{(g+1-i)p-(g+1-j)}\right)_{i,j=1}^g = \left(c_{ip-j}\right)_{i,j=g,g-1,\ldots,2,1}.$$

Hence, the statement we want to prove follows from Theorem 4.2.1. □

4.3 Counting ordinary polynomials over $\mathbb{F}_q$

Definition 4.3.1. Let g be a positive integer. A monic polynomial f of degree $2g+2$ in $\mathbb{F}_q[x]$ is said to be *ordinary* if it has non-zero discriminant and the hyperelliptic curve C of genus g defined by $y^2 = f$ is ordinary.

Corollary 4.3.2. *Let $g > 0$ be an integer and let $q = p^a$ be an odd prime power. Suppose that $g \leq p$. Then there are at least $q^{2g+2} - (4g + 3 + \frac{p-1}{2} \cdot g) \cdot q^{2g+1}$ ordinary polynomials of degree $2g+2$ in $\mathbb{F}_q[x]$.*

Proof. Let $f = x^{2g+2} + c_{2g+1}x^{2g+1} + \ldots + c_0$ be a generic monic polynomial of degree $2g+2$. Its discriminant $\Delta(f)$ is a polynomial of total degree at most $2(2g+2)-1 = 4g+3$ in $\mathbb{F}_q[c_0, \ldots, c_{2g+1}]$. On the other hand, $\det(A)$ from Theorem 4.2.3 is a polynomial of total degree at most $g \cdot \frac{p-1}{2}$. Hence, the curve $y^2 = f$ is an ordinary hyperelliptic curve if and only if $h := \Delta(f) \cdot \det(A) \in \mathbb{F}_q[c_0, \ldots, c_{2g+1}]$, which is of total degree at most $4g + 3 + \frac{p-1}{2} \cdot g$, is not vanishing in the coefficients of f.

First of all note that $h \neq 0$, because there do exist ordinary hyperelliptic curves of genus g over $\mathbb{F}_q$, see [GlPr05, Thm. 2.3], or Chapter 3 of this thesis. Hence, we have $0 \leqslant \deg h \leqslant 4g + 3 + \frac{p-1}{2} \cdot g$. By standard counting arguments, there can be at most $\deg h \cdot q^{2g+1}$ rational zeros of h. This proves the statement. □

4.4 Density in $\operatorname{Specmax} \mathcal{O}_K$

Let $K = \mathbb{Q}(\alpha)$ be a number field of degree $n > 1$. Let $\mathcal{O} = \mathcal{O}_K$ be its ring of integers. We will put the following density on the set of primes $\operatorname{Specmax} \mathcal{O}$ of $\mathcal{O}$.

Definition 4.4.1. For a subset $I \subset \operatorname{Specmax} \mathcal{O}$ we define its *natural density*, if it exists, as

$$\lim_{N \to \infty} \frac{\sum_{p \in \operatorname{Specmax} \mathbb{Z} : p \leqslant N} \sum_{\mathfrak{p} \in I : p\mathcal{O} \subset \mathfrak{p}} \kappa(\mathfrak{p})}{n \cdot |\{p \in \operatorname{Specmax} \mathbb{Z} : p \leqslant N\}|},$$

where $\kappa(\mathfrak{p})$ is the absolute residue field degree of $\mathfrak{p}$.

Remark 4.4.2. This density is non-standard. Often primes are weighted by $\frac{1}{|\mathbb{F}|}$, where $\mathbb{F}$ is the residue field. In other cases, the primes are ordered by the size of $|\mathbb{F}|$, rather than the size of the underlying prime number p. Here we chose to weigh the primes by the degree of their residue fields. The reason is that we want the set of primes having residue field degree 1 not to have density 1 (which it would have using the other notion of density).

Let $\mathcal{P}$ be the set of odd prime numbers that ramify nowhere in $\mathcal{O}$ and at which $\mathbb{Z}[\alpha]$ is regular. This set contains almost all prime numbers. By Kummer-Dedekind the splitting pattern of $p \in \mathcal{P}$ in the ring $\mathcal{O}$ is the factorisation pattern of $g := f_{\mathbb{Q}}^{\alpha}$ in $\mathbb{F}_p[X]$. By using the Frobenius density theorem ([LS96, p. 32]) in combination with Burnside's orbit-counting theorem, we can determine the proportion of linear primes in $\mathcal{O}$, i.e. primes of $\mathcal{O}$ having residue field degree 1.

Lemma 4.4.3. *Let Ω be the set of primes in* $\operatorname{Specmax} \mathcal{O}$ *with residue field degree 1. Then Ω has natural density $\frac{1}{n}$.*

Proof. As all but finitely many prime numbers are in $\mathcal{P}$, it suffices to only consider primes lying above elements of $\mathcal{P}$. Let G be the Galois group of a Galois closure of K, considered as a subgroup of S_n, permuting the roots of g.

By the Frobenius density theorem the usual natural density of the set of prime numbers (in $\mathbb{Z}$) for which g has decomposition type $(n_1, \ldots, n_t)$, where $n_1 \leq \ldots \leq n_t$ are positive integers such that $n_1 + \ldots + n_t = n$, equals the proportion of elements in G having cycle type $(n_1, \ldots, n_t)$.

Hence, the density of the set of primes in Ω is

$$\sum_{(n_1,\ldots,n_t)} \frac{|\{g \in G : g \text{ has cycle type } (n_1, \ldots, n_t)\}|}{|G|} \cdot \frac{|\{i : n_i = 1\}|}{n},$$

i.e., $\frac{1}{n}$ times the average, over the elements of G, of the number of fixed points. By Burnside's orbit-counting theorem, this average equals the number of orbits under G, which is 1 as g is irreducible. Hence, the density of Ω is $\frac{1}{n}$. □

Corollary 4.4.4. *Both Ω and* $\operatorname{Specmax} \mathcal{O} \setminus \Omega$ *are infinite.*

4.5 Density in $\mathcal{O}^N$

Let K and $\mathcal{O}$ be as before. Let N be a positive integer. First, let us define a density on the set $\mathcal{O}^N$ (which we will then later identify with the set of monic polynomials of degree N with coefficients inside $\mathcal{O}$).

Definition 4.5.1. Let $x = (x_1, \ldots, x_N) \in \mathcal{O}^N$, then we define its height as

$$h(x) := \sqrt{\sum_{i=1,\ldots,N} \sum_{\iota\colon K \hookrightarrow \mathbb{C}} |\iota(x_i)|^2}.$$

Proposition 4.5.2. *For every $M \in \mathbb{R}_{>0}$ there are only finitely many elements $x \in \mathcal{O}^N$ with $h(x) \leqslant M$.*

Proof. For every $i \in \{1, \ldots, N\}$ and every $\iota\colon K \hookrightarrow \mathbb{C}$ we have $|\iota(x_i)| \leqslant M$. Order the set $\{\iota\colon K \hookrightarrow \mathbb{C}\}$ and consider the map $\mathcal{O} \to \mathbb{C}^n\colon x \mapsto (\iota(x))_{\iota\colon K \hookrightarrow \mathbb{C}}$, which embeds $\mathcal{O}$ inside $\mathbb{C}^n$ as a discrete subgroup. The cube $\{(y_1, \ldots, y_n) \in \mathbb{C}^n : \forall j : |y_j| \leqslant M\}$ is compact. Hence, its intersection with the image of $\mathcal{O}$ is finite. In particular, there are only finitely many possibilities for the x_i inside $\mathcal{O}$. □

The previous proposition proves that the following definition makes sense.

Definition 4.5.3. Let S be a subset of $\mathcal{O}^N$, then the *natural density* of S, if it exists, is:

$$\lim_{M\to\infty} \frac{|\{x \in S : h(x) \leqslant M\}|}{|\{x \in \mathcal{O}^N : h(x) \leqslant M\}|}.$$

Proposition 4.5.4. *For each $M \in \mathbb{R}_{>0}$, let $E(M)$ be the number of elements in $\mathcal{O}$ of height at most M. Then there exists a constant $c \in \mathbb{R}_{>0}$ such that*

$$E(M) = c \cdot M^n + \varepsilon(M),$$

where ε is such that $\lim_{M\to\infty} \varepsilon(M)/M^n = 0$.

Proof. Proof omitted. In fact, much stronger results are true, see [Div76]. □

The following lemma tells us that the natural density of a coset of a non-zero ideal is what one would expect.

Lemma 4.5.5. *Let $I \subset \mathcal{O}$ be a non-zero ideal and let I' be a coset of I. Then the natural density of I' is $[\mathcal{O} : I]^{-1}$.*

Proof. As abelian group, I' is a union of cosets of $[\mathcal{O} : I]\mathcal{O}$, hence we may and will assume that I is generated by an element in $\mathbb{Z}$, say $I = L\mathcal{O}$ for $L \in \mathbb{Z}$. Now choose some $x \in I'$ and let $s := h(x)$ be its height.

Let $M \in \mathbb{R}_{>s}$ and consider the elements in $\mathcal{O}$ of height at most M. There are $c \cdot M^n + \varepsilon(M)$ of them, where c and ε are as in Proposition 4.5.4. On the other hand, there are $c \cdot \left(\frac{M-s}{L}\right)^n + \varepsilon\left(\frac{M-s}{L}\right)$ elements $y \in \mathcal{O}$ of height at most $\frac{M-s}{L}$. For each such y, the point $L \cdot y + x$ has height at most M and is in I'. Hence,

$$\liminf_{M\to\infty} \frac{|\{x \in I' : h(x) \leqslant M\}|}{|\{x \in \mathcal{O} : h(x) \leqslant M\}|} \geqslant \lim_{M\to\infty} \frac{c \cdot \left(\frac{M-s}{L}\right)^n + \varepsilon\left(\frac{M-s}{L}\right)}{c \cdot M^n + \varepsilon(M)} = \frac{1}{L^n}.$$

As this is true for every of the L^n cosets of I, it follows that I' has natural density $\frac{1}{L^n}$ as desired. □

4.6 Density of hyperelliptic curves with ordinary primes

Again, let K be a number field of degree $n > 1$ over $\mathbb{Q}$, and let $\mathcal{O}$ be its ring of integers. Let g be a positive integer and take $N = 2g + 2$. Now we will consider the hyperelliptic curves defined by monic polynomials of degree N with coefficients in $\mathcal{O}$ with non-zero discriminant. We identify this set of polynomials with $\mathcal{O}^N$ to define a density on it.

Theorem 4.6.1. *Let M be a positive integer. Let S_M be the subset of $\mathcal{O}^N$ consisting of polynomials f for which there exist at least M distinct prime ideals $\mathfrak{p}$ such that $\overline{f} \in k_{\mathfrak{p}}[x]$ is ordinary. Then S_M has (natural) density 1.*

Proof. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be those elements of $\operatorname{Specmax} \mathcal{O} \setminus \Omega$, the set of primes with residue field degree greater than 1, such that the prime numbers p_i lying above the $\mathfrak{p}_i$ are all greater than g. For every $i = 0, 1, \ldots$, let $I_i := \prod_{j=i+1}^{i+M} \mathfrak{p}_i$. Then by Corollary 4.3.2 for at least

$$\prod_{j=i+1}^{i+M} \left(1 - \left(4g + 3 + \frac{p_i - 1}{2} \cdot g\right) \cdot q_i^{-1}\right) \geqslant 1 - \sum_{j=i+1}^{i+M} \left(4g + 3 + \frac{p_i - 1}{2} \cdot g\right) \cdot q_i^{-1}$$

of the residue classes modulo I_i, hyperelliptic curves reducing to this residue class are ordinary at $\mathfrak{p}_{i+1}, \ldots, \mathfrak{p}_{i+M}$. Here, q_i is the order of $k(\mathfrak{p}_i)$. As the primes have residue field degree at least 2, we have $q_i \geqslant p_i^2$ and hence

$$\sum_{j=i+1}^{i+M} \left(4g + 3 + \frac{p_i - 1}{2} \cdot g\right) \cdot q_i^{-1} \leqslant (5g+3) \cdot \sum_{j=i+1}^{i+M} p_i^{-1}.$$

This converges to 0 as $i \to \infty$. By applying Lemma 4.5.5 we find that the density of S_M equals 1. □

Remark 4.6.2. The methods used in this chapter seem to be unable to yield any result stronger than Theorem 4.6.1. In fact, even if one can prove, for example, that a proportion of at most $\frac{\log \log q}{q}$ of hyperelliptic curves over $\mathbb{F}_q$ are not ordinary, then it still seems to be possible that these hyperelliptic curves are exactly the ones with the smallest coefficients, in which case you cannot even prove the existence of a single hyperelliptic curve with infinitely many primes of ordinary good reduction.

Bibliography

[Bert13] J. Bertin, Algebraic stacks with a view toward moduli stacks of covers. *Arithmetic and geometry around Galois theory.* Edited by P. Dèbes, M. Emsalem, M. Romagny and A. M. Uludağ. Birkhäuser/Springer, Basel, 2013.

[BLP16] Y. Bilu, F. Luca, A. Pizarro-Madariaga, Rational products of singular moduli. *J. Number Theory* **158** (2016), 397–410.

[vB18] R. van Bommel, Inverse Galois problem for ordinary curves. *Int. J. Number Theory* **14** (2018), no. 5, 1305–1315.

[BSSVY16] A. R. Booker, J. Sijsling, A. Sutherland, J. Voight, D. Yasaki. A database of genus-2 curves over the rational numbers. *LMS J. Comput. Math.* **19** (2016), suppl. A, 235–254.

[BiSw65] B. J. Birch, H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.* **218** (1965), 79–108.

[BoLi99] S. Bosch, Q. Liu, Rational points of the group of components of a Néron model. *Manuscripta Math.* **98** (1999), no. 3, 275–293.

[BLR90] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models.* Springer-Verlag, Berlin, 1990.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[CGLR99] G. Cardona, J. González, J. C. Lario, A. Rio, On curves of genus 2 with Jacobian of GL_2-type. *Manuscripta Math.* **98** (1999), no. 1, 37–54.

[DeMu69] P. Deligne, D. Mumford, The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.* **36**, 75–109.

[DiNa03] C. Diem, N. Naumann, On the structure of Weil restrictions of abelian varieties. *J. Ramanujan Math. Soc.* **18** (2003), no. 2, 153–174.

[Div76] B. Divis, Lattice point theory of irrational ellipsoids with an arbitrary center. *Monatsh. Math.* **83** (1997), no. 4, 279–307.

[Dokc04] T. Dokchitser, Computing special values of motivic L-functions. *Experiment. Math.* **13** (2004), no. 2, 137–149.

[Elk87] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* **89** (1987), no. 3, 561–567.

[FvdG04] C. Faber, G. van der Geer, Complete subvarieties of moduli spaces and the Prym map. *J. Reine Angew. Math.* **573** (2004), 117–137.

[FLSSSW01] E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll, J. 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.

[GlPr05] D. Glass, R. Pries, Hyperelliptic curves with prescribed p-torsion. *Manuscripta Math.* **117**, no. 3 (2005), 299–317.

[Gros86] B. H. Gross, Local Heights on Curves. *Arithmetic geometry (Storrs, Conn., 1984)*, 327–339. Springer, New York, 1986.

[Harb84] D. Harbater, Mock covers and Galois extensions. J. Algebra **91**, no. 2 (1984), 281–293.

[Harb87] D. Harbater, Galois coverings of the arithmetic line. *Number theory (New York, 1984–1985),* 165–195. Springer, Berlin, 1987.

[Harr18] M. Harrison, *Small hyperelliptic curves over* $\mathbb{Q}$. Retreived on 26 June 2018 from `https://people.maths.bris.ac.uk/~matyd/HE/`.

[HMS16] D. Harvey, M. Massierer, A.S. Sutherland Computing L-series of geometrically hyperelliptic curves of genus three. *LMS J. Comput. Math.* **19** (2016), suppl. A, 220–234.

[HaNi65] T. Hayashida, M. Nishi, Existence of curves of genus two on a product of two elliptic curves. *J. Math. Soc. Japan* **17** (1965), 1–16.

[HiSi00] M. Hindry, J.H. Silverman. *Diophantine geometry. An introduction.* Springer-Verlag, New York, 2000.

[Holm12] D. Holmes, Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory* **132** (2012), no. 6, 1295–1305.

[Kani14] E. Kani, Jacobians isomorphic to a product of two elliptic curves and ternary quadratic forms. *J. Number Theory* **139** (2014), 138–174.

[Kani16] E. Kani, The moduli space of Jacobians isomorphic to a product of two elliptic curves. *Collect. Math.* **67** (2016), no. 1, 21–54.

[Katz79] N. Katz, Slope filtration of F-crystals. *Journées de Géometrie Algébrique de Rennes (Rennes, 1978)*, Vol. I, 113–163, Astérisque **63**, 1979.

[Kida95] M. Kida, Galois descent and twists of an abelian variety. *Acta Arith.* **73** (1995), no. 1, 51–57.

[Koly89] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $\text{Ш}(E, \mathbb{Q})$ for a subclass of Weil curves. *Math. USSR-Izv.* **32** (1989), no. 3, 523–541.

[Koly91] V. A. Kolyvagin, On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves. *International Congress of Mathematicians*, vol. I, II (Kyoto, 1990), 429–436. Math. Soc. Japan, Tokyo, 1991.

[Lang82] S. Lang. *Introduction to algebraic and abelian functions.* Second edition. Graduate Texts in Mathematics, 89. *Springer-Verlag, New York-Berlin*, 1982.

[Lang83] S. Lang, *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Lan06] H. Lange, Principal polarizations on products of elliptic curves. *The geometry of Riemann surfaces and abelian varieties*, 153–162, Contemp. Math. 397, *Amer. Math. Soc., Providence, RI*, 2006.

[LS96] H. W. Lenstra Jr., P. Stevenhagen. Chebotarëv and his density theorem. *Math. Intelligencer* **18** (1996), no. 2, 26–37.

[Liu94] Q. Liu, Conducteur et discriminant minimal de courbes de genre 2. *Compositio Math.* **94** (1994), no. 1, 51–79.

[Liu96] Q. Liu, Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.* **348** (1996), no. 11, 4577–4610.

[Liu02] Q. Liu, *Algebraic Geometry and Arithmetic Curves.* Oxford University Press, Oxford, 2002. Translated by R. Erné.

[LMFDB] The LMFDB Collaboration, *The L-functions and Modular Forms Database.* Available at: `http://www.lmfdb.org`.

[MaMa99] G. Malle, B. H. Matzat, *Inverse Galois Theory.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.

[Mes91] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules. *Effective methods in algebraic geometry (Castiglioncello, 1990)*, 313–334. Progr. Math., 94, *Birkhäuser Boston, Boston, MA,* 1991.

[Mil72] J. S. Milne, On the arithmetic of abelian varieties. *Invent. Math.* **17** (1972), 177–190.

[Mil86] J. S. Milne, Jacobian varieties. *Arithmetic geometry (Storrs, Conn., 1984)*, 167–212. Springer, New York, 1986.

[Müll14] J. S. Müller, Computing canonical heights using arithmetic intersection theory. *Math. Comp.* **83** (2014), no. 285, 311–336.

[MüSt16] J. S. Müller, M. Stoll, Canonical heights on genus-2 Jacobians. *Algebra Number Theory* **10** (2016), no. 10, 2153–2234.

[Mumf70] D. Mumford, *Abelian varieties.* Pubished for Tata Institute of Fundamental Research, Bombay. Oxford University Press, London, 1970.

[Nér65] A. Néron, Quasi-fonctions et hauteurs sur les Variétés abéliennes. *Ann. of Math.* **82** (1965), no. 2, 249–331.

[Ogus82] A. Ogus, Hodge cycles and crystalline cohomology. In: *Hodge cycles, motives, and Shimura varieties.* Lecture Notes in Mathematics, 900. *Springer-Verlag, Berlin-New York*, 1982.

[PoSt99] B. Poonen, M. Stoll, The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math.* **150** (1999), no. 3, 1109–1149.

[Rayn70] M. Raynaud, Spécialisation du foncteur de Picard. *Inst. Hautes Études Sci. Publ. Math.* (1970), No. 38, 27–76.

[Rodr00] F. Rodriguez-Villegas, Explicit models of genus 2 curves with split CM. *Algorithmic number theory (Leiden, 2000)*, 505–513, Lecture Notes in Comput. Sci., 1838, *Springer, Berlin*, 2000.

[Rub91] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* **103** (1991), no. 1, 25–68.

[Sai12] M. Saidi, Fake liftings of Galois covers between smooth curves. *Galois-Teichmuller theory and arithmetic geometry, Advanced Studies in Pure Mathematics* (2012), Tokyo, Mathematical Society of Japan, 457–501.

[Sch89] M. Schlichenmaier. *An introduction to Riemann Surfaces, algebraic curves and moduli spaces.* Lecture Notes in Physics, 322. *Springer-Verlag, Berlin*, 1989.

[Ser70] J. P. Serre. Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures). *Séminaire Delange-Pisot Poitou. Théorie des nombres, Vol. 11* (1969–1970), no. 2, Talk no. 19, p. 1–15.

[Stacks] The Stacks Project Authors. *Stacks Project.* Available at: `http://stacks.math.columbia.edu`.

[Silv09] J. H. Silverman. *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. *Springer, Dordrecht,* 2009.

[Stei98] A. Stein, $1\frac{1}{2}$-generation of finite simple groups. *Beiträge Algebra Geom.* **39**, no. 2 (1998), 349–358.

[Stol17] M. Stoll, An explicit theory of heights for hyperelliptic Jacobians of genus three. *Algorithmic and experimental methods in algebra, geometry, and number theory*, 665–715, *Springer, Cham*, 2017.

[Tate66] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki, Vol. 9* (1964–1966), Exp. No. 306, 415–440, Soc. Math. France, Paris, 1995.

[Weil57] A. Weil, Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. 1957* (1957), 33–53.

[Weng03] A. Weng, Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.* **72** (2003), no. 241, 435–458.

[Wew99] S. Wewers, Deformation of tame admissible covers of curves. *Aspects of Galois Theory (Gainesville, FL, 1996)*, 239–282. Cambridge Univ. Press, Cambridge, 1999.

[Wong01] S. Wong, On the density of elliptic curves. *Compositio Math.* **127** (2001), no. 1, 23–54.

[Yui78] N. Yui. On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *Journal of algebra*, **52** (1978), no. 2, 378–410.

Samenvatting

Wiskundigen zijn al sinds mensenheugenis geïnteresseerd in het oplossen van vergelijkingen. Nog leuker vinden ze het om te laten zien dat een vergelijking geen oplossing heeft. Zo heeft de vergelijking

$$x^2 + y^2 = -1$$

bijvoorbeeld geen oplossing, omdat kwadraten nooit negatief zijn. Een andere manier om te laten zien dat een vergelijking geen oplossing heeft, is door te kijken naar de rest bij deling. Als we bijvoorbeeld de vergelijking

$$x^2 - y^2 = 1\,000\,002 \tag{1}$$

bekijken, waarbij x en y gehele getallen moeten zijn, dan zien we dat $1\,000\,002$ een veelvoud van 4 plus 2 is. Kwadraten van gehele getallen zijn altijd ofwel een veelvoud van 4, ofwel een veelvoud van 4 plus 1. Bijvoorbeeld, $2^2 = 4$, $4^2 = 16$ en $6^2 = 36$ zijn veelvouden van 4, en $1^2 = 1$, $3^2 = 9$ en $5^2 = 25$ zijn veelvouden van 4 plus 1. Als x^2 en y^2 allebei een veelvoud van 4 of een veelvoud van 4 plus 1 zijn, dan kan $x^2 - y^2$ een veelvoud van 4, een veelvoud van 4 plus 1 of een veelvoud van 4 plus 3 zijn, maar zeker geen veelvoud van 4 plus 2.

Als we nu x vervangen door $a + \frac{1}{2}$ en y door $b + \frac{1}{2}$, dan krijgen we de vergelijking

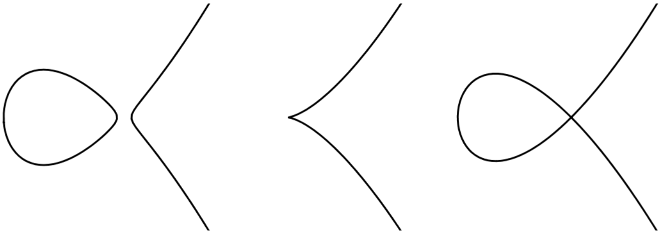
$$a^2 + a - b^2 - b = (a + \tfrac{1}{2})^2 - (b + \tfrac{1}{2})^2 = 1\,000\,002. \tag{2}$$

Deze vergelijking heeft wel een oplossing, namelijk $a = 83\,336$ en $b = 83\,330$. Oplossingen van vergelijking (1) geven aanleiding tot oplossingen van vergelijking (2) en omgekeerd, omdat $x = a + \frac{1}{2}$ en $y = b + \frac{1}{2}$. We vinden dus de oplossing $x = 83\,336 + \frac{1}{2}$ en $y = 83\,330 + \frac{1}{2}$ voor onze oorspronkelijke vergelijking (1).

Dit is geen tegenspraak. We hadden namelijk laten zien dat onze vergelijking (1) geen oplossingen x en y heeft, waarbij x en y gehele getallen zijn, en die hebben we nu ook niet gevonden. Ondanks dat er een correspondentie is tussen de rationale (breuken) oplossingen van vergelijking (1) en vergelijking (2), kan het zo zijn dat de ene vergelijking geen geheeltallige oplossingen heeft, terwijl de andere die wel heeft.

We zeggen dat vergelijkingen (1) en (2) verschillende *modellen* geven voor de kromme gedefinieerd door één van deze twee vergelijkingen over de rationale getallen. Het blijkt dat er voor een bepaalde categorie van krommen, elliptische krommen, één model is dat, in zekere zin, het beste model van alle modellen is. Dat model heet het *Néron-model.*

Dit Néron-model bevat een hoop informatie over de kromme. Deze zogenaamde aritmetische informatie bestaat onder andere uit het reductietype, maar ook een tal van andere invarianten.



De verschillende reductietypes voor een elliptische kromme

Een andere manier om naar de kromme te kijken is door te kijken naar de oplossingen, waarbij x en y reële getallen zijn, of zelfs complexe getallen. Er kunnen diverse integralen over de kromme worden uitgerekend, die aanleiding geven tot zogenaamde meetkundige informatie over de kromme.

Het *vermoeden van Birch and Swinnerton-Dyer* geeft een diep verband tussen deze aritmetische en meetkundige informatie. Birch and Swinnerton-Dyer zijn op dit vermoeden gekomen, doordat ze heel veel berekeningen hadden gedaan met elliptische krommen en zodoende een verband zagen tussen de verschillende dingen die zij berekend hadden.

In hoofdstuk 1 van dit proefschrift bekijk ik dit vermoeden van Birch and Swinnerton-Dyer, maar dan niet voor krommen, maar voor oppervlakken, drie-, vier- en vijfdimensionale variëteiten. Op dezelfde manier als Birch en Swinnerton-Dyer dat gedaan hebben, probeer ik door middel van computerberekeningen het vermoeden te bekrachtigen. In hoofdstuk 2 bekijk ik het vermoeden voor een kromme die niet gedefinieerd is over de rationale getallen, maar over een getallenlichaam van graad 4 over de rationale getallen.

In hoofdstuk 3 bekijk ik juist de reductietypes van krommen, de zogenaamde *gewone reductie* in het bijzonder. Ik laat zien dat je een kromme die gewone reductie heeft maar niet glad is, kunt omvormen tot een gladde kromme met gewone reductie. Dit resultaat gebruik ik dan vervolgens in hoofdstuk 4 om de statistieken over gewone reductie te bestuderen voor hyperelliptische krommen over een getallenlichaam.

Acknowledgements

First, I would like to thank my supervisors David Holmes and Fabien Pazuki. I learned a lot from the discussions I had with them, and I am very grateful for their guidance. Moreover, I would like to thank the members of the reading committee, the members of the opposition committee, Bas Edixhoven, Tim Dokchitser, Steffen Müller, Carlo Pagano, Maarten Derickx, Peter Koymans, and several anonymous referees for their comments and other contributions that led to improvements of this thesis.

Finally, I would like to thank my current and former colleagues, my family, my friends from the sports centre, the math olympiad, the chess club, high school, my previous studies and Copenhagen, and all my other personal friends that contributed to my positive experience of the last four years.

Curriculum vitae

Raymond van Bommel is born on 5 August 1991 in Haarlem, The Netherlands. From 2003 to 2009 he attended high school at Atheneum College Hageveld in Heemstede, The Netherlands, where he obtained his Dutch vwo diploma. During his time in high school, he already studied mathematics on university level, and he participated three times to the International Mathematical Olympiad in 2007, 2008 and 2009, winning bronze medals in 2008 and 2009.

After high school, Raymond continued studying mathematics. First he went to Universiteit Leiden, The Netherlands, for his bachelor's from 2009 until 2012, where he graduated cum laude. Then from 2012 until 2014 he studied for his master's at Université Paris-Sud, France, for the first year, and Universiteit Leiden for the second year, within the Erasmus Mundus program ALGANT, graduating cum laude.

From 2014 until 2018, Raymond finished his PhD in mathematics at Universiteit Leiden under the supervision of dr. David Holmes (Universiteit Leiden) and prof. dr. Fabien Pazuki (Københavns Universitet, Denmark). His work resulted in a number of published articles and this thesis.

During his life, Raymond also participated to many programming contests, winning the Benelux Algorithm Programming Contest in 2011 and 2013, and has also been a member of the jury for several programming contests. Moreover, since 2009, he has been an active volunteer for the Nederlandse Wiskunde Olympiade, the organisation behind the mathematical olympiad in The Netherlands. Among other tasks, he is (co-)responsible for the problem selection for the national rounds and the financial administration of the foundation.