UNIVERSITÄT ULM · SCIENDO · DOCENDO · CURANDO ·

ulm university universität
uulm

L-functions of curves of genus ≥ 3

Dissertation zur Erlangung des Doktorgrades Dr. rer. nat. der Fakultät für Mathematik und Wirtschaftswissenschaften der Universität Ulm

Vorgelegt von **Michel Börner** aus Meerane im Jahr 2016

Tag der Prüfung

14.10.2016

Gutachter

Prof. Dr. Stefan Wewers
Jun.-Prof. Dr. Jeroen Sijsling

Amtierender Dekan

Prof. Dr. Werner Smolny

Contents

Chapter 1

Introduction

In this thesis, we consider superelliptic curves over number fields K, i.e. algebraic curves (Definition 2.1.1) given by an equation of the form

$$y^n = f(x) \ \ , \text{ with } f \in K[x] \ \text{ and } \ n \in \mathbb{N}. \tag{1.1.1}$$

For two classes of such curves, hyperelliptic curves and Picard curves, we give computational evidence for one of the big open problems concerning L-functions of curves — the question whether the L-function satisfies a functional equation.

L-functions of curves are part of a larger class of L-functions. The best-known example of this class is the Riemann zeta function with its functional equation and meromorphic continuation. An interesting property of this function is the fact that it encodes information about the distribution of primes in the ring of integers $\mathbb{Z}$. For other objects besides $\mathbb{Z}$, such as curves, characters or modular forms, one may define a function similar to the Riemann zeta function. These generalizations of the Riemann zeta function are called L-functions. Each class of objects has its own type of L-function, which provides information about the underlying object from that class.

For most classes of objects, L-functions are far from being completely understood and there is a wide range of open problems. Two well-known examples are the Birch–Swinnerton-Dyer conjecture [Wil06] for elliptic curves and the Riemann hypothesis [Sar04]. Both are among the *Millennium Problems* stated by the *Clay Mathematics Institute*. The open challenges stated above are closely related to the *Langlands program*, which was proposed in the 1960s by Robert Langlands. It aims to close gaps between algebraic number theory, automorphic forms, and representation theory to formulate and prove conjectures on more general types of L-functions [BCG$^+$04], [Gel84].

In this thesis we consider L-functions of curves, and like the Riemann zeta function they are analytic continuations of so-called L-series. The L-series of a curve Y defined over a number field K can be written as a *Dirichlet series*

$$L(Y,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ \ , \text{ for } \Re(s) > 3/2 \ \ , \ s \in \mathbb{C} \tag{1.1.2}$$

(Theorem 3.2.4) or as an *Euler product*

$$L(Y,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(Y,s),$$

where the product runs over the prime ideals $\mathfrak{p}$ of the ring of integers of K.

In the case $K = \mathbb{Q}$, these are just the prime numbers. The Euler product representation may be interpreted as using the information of the *local* L-factors $L_\mathfrak{p}$ at all primes $\mathfrak{p}$ to create a meromorphic function $L(Y, s)$. Here 'local' emphasizes that $L_\mathfrak{p}$ only depends on the reduction behavior of the curve at a prime ideal $\mathfrak{p}$, cf. Proposition 3.4.3 for details. We will see that all but finitely many of the $L_\mathfrak{p}$ are easy to calculate by a computer. However, in general it is not clear how to compute all $L_\mathfrak{p}$ for an arbitrary curve.

There is a conjectured functional equation for $L(Y, s)$,

$$\Lambda(Y, s) = \pm\Lambda(Y, 2 - s), \tag{FEq}$$

with $\Lambda(Y, s) := \sqrt{N}^s \cdot (2\pi)^{-g_Y s} \cdot \Gamma(s)^{g_Y} \cdot L(Y, s)$ ([dS04], [Ser70]). This notation uses two important integer invariants of the curve Y: the *genus* g_Y and the *conductor* N, as well as the Gamma function $\Gamma(s)$.

The conjecture is a theorem only in very special cases, e.g. for elliptic curves. In this case, the functional equation (FEq) is a consequence of the modularity theorem [Wil95], [BCDT01]. For some classes of curves of genus larger than one, there is empirical and experimental evidence for the correctness of this conjecture. It has been verified for a large number of examples in numerous articles — with various attempts in the computation of the local factors $L_\mathfrak{p}$ and the conductor N, see e.g. [BW16], [Boo05], [DdJZ06], [Liu96], and [BBW16]. However, for a proof of (FEq) in the case of genus larger than one, *'existing methods [. . .] provide no insight [. . .] [and] an entirely new approach is needed'* (see [Har14a]).

To make computational results on L-functions publicly available, the *L-functions and modular forms database* (*LMFDB*, [LMF16]) was launched in May 2016 (see [Voi16] for an overview). The database mostly concerns L-functions of elliptic curves and some genus-two curves. This is a further motivation to explore L-functions of genus ≥ 3.

Goals and results

The first main goal of this thesis is to give computational and experimental evidence for (FEq) for curves of genus ≥ 2 over a number field. We will use a method of Dokchitser [Dok04] to verify (FEq) numerically up to arbitrarily high precision. For this method we need the conductor N and a finite number of local factors $L_\mathfrak{p}$. The conductor N is the main limiting factor in the verification of (FEq), as the computation time for Dokchitser's method has order $\mathcal{O}(N)$ (Section 4.3.5).

We distinguish between the primes $\mathfrak{p}$ of good and bad reduction of the curve Y (see Definition 2.3.1 for a precise definition). The local factors $L_\mathfrak{p}$ are called good and bad factors, accordingly. For superelliptic curves we have a concrete and explicit way of calculating $L_\mathfrak{p}$ for all but finitely many primes $\mathfrak{p}$ by point counting on Equation (1.1.1), considered as a curve over the residue field of $\mathfrak{p}$. For a precise statement, we refer to Section 4.2.1.

At the primes of bad reduction we cannot find equations for the curve such that the curve is smooth in reduction, i.e. over the residue field of $\mathfrak{p}$. These bad primes are the essential point of the computation of the L-series. The behavior of the curve at the bad primes completely defines the conductor N, and computing $L_{\mathfrak{p}}$ at these primes may be highly non-trivial. For elliptic curves this is well understood, and for hyperelliptic curves (genus 2 and higher) and over fields of odd characteristic one can use methods similar to those used to compute the $L_{\mathfrak{p}}$ in the elliptic curve case (see e.g. [Liu96]). For the case of genus 2 and arbitrary characteristic some sophisticated attempts were made by Dokchitser, de Jeu and Zagier [DdJZ06], as well as Booker [Boo05]. These authors assume (FEq) to hold and use it to deduce the bad factors and the conductor. In contrast to these approaches, we compute the bad $L_{\mathfrak{p}}$ and N directly and provably correctly. Then we use this to verify (FEq).

We use representation theory and étale cohomology to give an algorithm to compute the $L_{\mathfrak{p}}$ at all primes and the conductor N for two classes of curves of genus larger than two. These curves are certain hyperelliptic curves, which are of genus ≥ 2, and Picard curves, a class of curves of genus 3. To compute the $L_{\mathfrak{p}}$ and N we follow the instructions described in [BW16] by Bouw and Wewers. Their approach is based on the description of the semistable reduction of superelliptic curves. In [BW16], the problem is discussed in a less computable way, yet in a more general set-up. For the two classes of curves considered, we formulate conditions on the curves such that the instructions given in [BW16] can be implemented as an algorithm executable by a computer.

We have computed several hundreds of L-series of curves using an implementation of our algorithm written in *Sage*. We verified the functional equation (FEq) numerically for all these examples using Dokchitser's method. Within our class of hyperelliptic curves, the ability to verify (FEq) for a curve of arbitrarily high genus is only limited by our computational power.

The second main goal of this thesis is to systematically search for curves with given parameters. In particular, we sketch a first step towards finding the Picard curve over $\mathbb{Q}$ with minimal conductor in Theorem 5.3.12. Picard curves are a natural choice for this discussion, since (for a defined set of bad primes) they can be classified into a finite number of $\mathbb{Q}$-equivalence classes.

We discuss an algorithm by Malmskog and Rasmussen [MR14] that creates a list of all Picard curves over $\mathbb{Q}$ with good reduction away from 3. We implemented this algorithm and our results show that the original list in [MR14] was incomplete. We discussed this with Malmskog and Rasmussen whereupon they found an implementational error. In the current version of the paper [MR16], they present a completed list that agrees with our results. Moreover, we present a generalization to Picard curves with good reduction away from a finite set of small primes. An important part in these algorithms are solutions of *S-unit equations*, based on work by Smart [Sma97], where we benefit from recent improvements by Koutsianas and Cremona [Kou15].

For each curve in the completed Malmskog–Rasmussen list of Picard curves over $\mathbb{Q}$ with good reduction away from 3 we have computed all bad factors and the conductor. Moreover, we give a construction for a Picard curve that has minimal conductor among all Picard curves over $\mathbb{Q}$. For an explicit minimal conductor, better insight into the solution of S-unit equations is needed.

With our methods and in abundance of computational power it is possible to construct any number of coefficients of the L-series of a curve from the two classes stated above. Thus our results enable further research on L-series of curves of genus ≥ 2.

Outline

In Chapter 2 we introduce the key concepts *curve* and *curve given by one equation*. We introduce the two settings for our computations in Chapters 4 and 5. In both settings we give conditions on a curve Y such that there is a model $\mathcal{Y}$ with special fiber at $\mathfrak{p}$ given by the same equation as Y, modulo $\mathfrak{p}$. Next we define good, bad, and semistable reduction and introduce the Semistable Reduction Theorem by Deligne and Mumford. For an absolutely irreducible smooth projective curve over a local field $K_\mathfrak{p}$, this theorem guarantees the existence of a semistable model over a finite extension of $K_\mathfrak{p}$.

The main part of Chapter 3 concerns L-functions and their properties. We start with a general definition of the L-function and the local factor $L_\mathfrak{p}$. Then we discuss the easier case of a good factor and give a connection to the Hasse–Weil zeta function. For the computation of the bad factors, we give an alternative definition of $L_\mathfrak{p}$ in terms of a certain curve in positive characteristic. After that, we present a detailed description of the conjectured functional equation (FEq). We also explain how we numerically verify (FEq) in *Sage* and discuss sources of error that may occur.

Chapter 4 is an adapted version of the paper [BBW16], which summarizes part of our findings. We give a class of hyperelliptic curves of arbitrarily high genus over $\mathbb{Q}$ that acquires semistable reduction at all primes $\mathfrak{p}$ already over $\mathbb{Q}$. There we compute $L_\mathfrak{p}$ and N algorithmically and verify (FEq) for various examples.

In Chapter 5 we consider L-functions of Picard curves over $\mathbb{Q}$. Picard curves over $\mathbb{Q}$ never have semistable reduction at $p = 3$. Hence it is futile to look for such curves over $\mathbb{Q}$ with semistable reduction everywhere (as we did for hyperelliptic curves). We elaborate the computation of the bad factors and conductor of a Picard curve over $\mathbb{Q}$ for two examples with good reduction away from $\{2, 3\}$. After that, we define Picard curves and state some important properties. Moreover, we describe the structure of the bad factors and the conductor for typical examples of Picard curves good away from a finite set of small primes. Another important point is the description of Malmskog and Rasmussen's algorithm for the construction of all Picard curves over $\mathbb{Q}$ with good reduction away from 3. We discuss a generalization of this algorithm to Picard curves over $\mathbb{Q}$ good away from a finite set of small primes. This is used to examine lower bounds on the size of the conductor N of a Picard curve.

Chapter 2

Curves and models

In this chapter we introduce two key concepts of this thesis: curves and models of curves. Throughout this thesis we deal with plane curves over number fields given by one equation. In Section 2.1 we introduce this class of curves and discuss some basic properties and alternative descriptions of the curves in this class. We introduce models of curves and discuss basic properties in Section 2.2. Finally, we discuss the terms good, bad, and semistable reduction in Section 2.3.

Take a plane curve Y given by one equation over a number field K and let $\mathfrak{p} \lhd \mathcal{O}_K$ be a prime. The main goal of this chapter is to give conditions on Y such that there is a model $\mathcal{Y}$ of Y where the special fiber of $\mathcal{Y}$ at $\mathfrak{p}$ is given by the same equation as Y, reduced modulo $\mathfrak{p}$.

2.1 Curves

Definition 2.1.1 (Curve)

A *curve* over any field k is a separated scheme Y of finite type over $\operatorname{Spec}(k)$ of pure dimension one. $\lhd$

Note that we do not assume that a curve is necessarily smooth or projective. We do not even assume that a curve is integral. The reason is that the special fiber of a model of a curve Y, which we introduce in Section 2.2, is in general not reduced, and hence not integral.

Assumption 2.1.2 (Perfect field K)

All curves considered in this thesis are defined over a finite field or a field of characteristic zero. Moreover, for our purposes, we do not gain anything from distinguishing between regularity as an absolute property and smoothness of a finite morphism of schemes. Therefore from now on we assume that K is a perfect field. Fix an algebraic closure K^{alg} of K. $\lhd$

Remark 2.1.3 (reduced, irreducible)

Let $F \in K[x,y]$ be a non-constant polynomial. It is easy to see that the scheme $\operatorname{Spec}(K[x,y]/(F))$ is

i) reduced $\iff$ F has no square factor,

ii) irreducible $\iff$ F only consists of powers of one irreducible factor,

iii) integral $\iff$ F is irreducible. $\triangleleft$

Remark 2.1.4 (Projective curve given by one equation)

We construct the *projective curve Y_F given by F* as follows.
Let Y_1 be an affine curve given as $Y_1 = \operatorname{Spec}(K[x,y]/(F))$ for an absolutely irreducible non-constant polynomial $F \in K[x,y]$. For simplicity, we additionally assume that $F \notin K[x]$. This amounts to F being a minimal polynomial for y in the extension $K(Y_1)/K(x)$, and $K(Y_1)/K(x)$ is finite. Thus we can write the function field of Y_1 as $K(Y_1) = K(x)[y]/(F)$. In general, the affine curve $Y_1 := \operatorname{Spec}(K[x,y]/(F))$ has a finite set of singularities, which we denote Y_1^{sing}. Define $A_1 := K[x]$, $A_2 := K[1/x]$ and denote $X_1 := \operatorname{Spec} A_1$, $X_2 := \operatorname{Spec} A_2$. Write $A_1[y] = K[x,y]/(F)$ and define B_2 as the normalization of A_2 in $K(Y_1) = K(x)[y]/(F)$.

Define X_1^{sing} to be the image of Y_1^{sing} under the map

$$\pi : Y_1 = \operatorname{Spec} A_1[y] \to X_1 = \operatorname{Spec} A_1 \quad \text{given by} \quad (x,y) \mapsto x. \tag{2.1.1}$$

Define $\tilde{A}_2$ by $\operatorname{Spec} \tilde{A}_2 = X_2 \setminus X_1^{\text{sing}}$. Then the normalization $\tilde{B}_2$ of $\tilde{A}_2$ in the function field $K(x)[y]/(F)$ yields a patch at infinity where the points in $\operatorname{Spec} \tilde{B}_2 \setminus Y_1$ are smooth by construction. The gluing of $\operatorname{Spec} \tilde{B}_2$ and $\operatorname{Spec} A_1[y]$ yields an integral projective curve Y_F with affine patch Y_1. We call this curve Y_F *the projective curve given by F*.

The curve constructed above still has the same singularities as Y_1, i.e. $Y_F \setminus Y_1$ is smooth. By normalizing the curve Y_F in the function field $K(Y_F) := K(x)[y]/(F)$, we obtain a smooth projective curve. This may be done as follows. In $K(Y_F)$, we construct the integral closures B_1 and B_2 of $A_1 = K[x]$ and $A_2 = K[1/x]$, respectively. As K is perfect, the affine curves $\operatorname{Spec} B_1$ and $\operatorname{Spec} B_2$ are smooth over K, and gluing yields an integral smooth projective curve $Y_F^{\text{norm}} \supseteq \operatorname{Spec} B_1, \operatorname{Spec} B_2$. Due to the one-to-one correspondence between function fields of transcendence degree one and K^{alg}-isomorphism classes of integral smooth projective curves, this curve is unique (up to isomorphism) as a curve over K^{alg}. $\triangleleft$

Definition 2.1.5 (Projective curve given by one equation)

From now on, we will use the following terms and notation. Let $F \in K[x,y]$ be a polynomial which is not in $K[x]$.

i) Since $(K(x)[y]/(F))/K(x)$ is finite, we can extend the map $\pi : Y_1 \to X_1$ from Equation (2.1.1) to a cover $Y \to \mathbb{P}^1_x$ by sending all points in $Y \setminus Y_1$ to $x = \infty$. Throughout this thesis, we use π for the map

$$\pi : Y \to \mathbb{P}^1_x, \ (x,y) \mapsto x.$$

Note that we assume that this is a finite morphism, due to the assumption on F above. So π is a *cover*, i.e. a dominant finite separable morphism.

ii) Let Y be a projective curve with cover $\pi : Y \to \mathbb{P}^1_x$. We call the elements of Y lying above $x = \infty$ *the points at infinity*.

iii) The *projective curve given by* F is the (possibly singular) curve Y_F constructed in Remark 2.1.4.

iv) The *smooth projective curve given by* F is the curve Y_F^{norm} constructed in Remark 2.1.4.

Note that we omit the index $_F$ if the defining equation is clear from context.

Notation 2.1.6 (Situations in this thesis)

There are two main situations that are important in this thesis. We can characterize them by the types of equations $F \in K[x,y]$ that define the curve $Y = Y_F$.

- ***Case AS***
  Let p be a prime number. The polynomial F is of the form

  $$F = y^p + h(x)y - g(x),$$

  with non-zero polynomials $g, h \in K[x]$ and F absolutely irreducible.

- ***Case S***
  Let $n \geq 2$ be an integer with $\mathrm{char}\,(K) \nmid n$. The polynomial F is of the form

  $$F = y^n - f(x),$$

  where $f \in K[x]$ is non-constant and splits over K^{alg} as

  $$f(x) = \prod_{i=1}^{r} (x - x_i)^{a_i},$$

  with $0 < a_i < n$ and $\gcd(n, a_1, \ldots, a_r) = 1$. This guarantees that F is absolutely irreducible.

Note that ***Case AS*** is a variant of an Artin–Schreier curve. For $p = 2$, ***Case AS*** describes a hyperelliptic curve. Curves given by an equation as in ***Case S*** are superelliptic curves. We will use the terms ***Case AS*** and ***Case S*** in the rest of this chapter. ◁

Note that $\mathrm{char}\,(K) \nmid n$ is a necessary assumption in ***Case S***, because if $\mathrm{char}\,(K) \mid n$, the map $Y \to \mathbb{P}^1_x$, $(x,y) \mapsto x$ is inseparable. In ***Case AS***, the map $(x,y) \mapsto x$ is not inseparable for $\mathrm{char}\,(K) \mid p$ since h is non-zero .

We will discuss most of the theory in this chapter for both ***Case AS*** and ***Case S***.

We have already seen that for a (possibly singular) curve Y given by one equation, the points at infinity are smooth by construction. The following lemma gives a condition guaranteeing that a curve (in the respective case) has a unique point at infinity.

As normalization is complicated in general, we restrict in ***Case AS*** to the case that $\deg(g) > \deg(h) \cdot \frac{p}{p-1}$, which ensures that the behavior at $z = 0$ does not depend on the term $h(x)y$. This assumption also holds in the class of hyperelliptic curves discussed in Chapter 4.

Lemma 2.1.7 (Point at infinity)

*i) Let Y be as in **Case AS** and let $\deg(g) > \deg(h) \cdot \frac{p}{p-1}$.*
If $p \nmid \deg(g)$, then Y has a unique point at infinity, which is K-rational.

*ii) Let Y be as in **Case S**.*
If $\gcd(n, \deg(f)) = 1$, then Y has a unique point at infinity, which is K-rational.

Proof: To prove *i)*, we construct an equation for Y around ∞.
After replacing K by a suitable finite extension and replacing the coordinates (x, y) with suitable multiples, if necessary, we may assume that g is monic. Define $z := 1/x$, $\delta := \left\lceil \frac{\deg g}{p} \right\rceil$, and $w := z^\delta y$. Rewriting $y^p + h(x)y - g(x)$ in terms of z and w yields an *equation at infinity*

$$w^p + h^*(z)w - g^*(z), \tag{2.1.2}$$

where

$$g^*(z) = z^{\delta p} g(1/z) \quad \text{and} \quad h^*(z) = z^{\delta(p-1)} h(1/z).$$

Note that $h^*(z)$ is divisible by z to the power $\delta(p-1) - \deg h$. This is a positive integer, since $\deg h < \frac{p-1}{p} \cdot \deg g$ and $\delta \geq \frac{\deg g}{p}$. The polynomial $g^*(z)$ is also divisible by z, due to the fact that $\delta p - \deg g > 0$, whenever $p \nmid \deg g$.

Choose a maximal integer $\ell > 0$ such that z^ℓ simultaneously divides $h^*(z)$ and $g^*(z)$ and write

$$w^p = z^\ell \left(\frac{g^*(z)}{z^\ell} - w \frac{h^*(z)}{z^\ell} \right).$$

For $p \nmid \ell$ this equation describes the normalization of $k[z]$ in the function field $K(Y)$. Hence in this case, Y has a unique point in $z = 0$. Note that ℓ is equal to the maximal power of z dividing $g^*(z)$. To see this, subtract the maximal powers of z dividing h^* and g^*

$$(\delta(p-1) - \deg h) - (\delta p - \deg g) > -\delta - \deg h + \deg g > \frac{\deg g}{p} - \delta > -1.$$

So we have $\ell = \delta p - \deg g$. Thus for $p \nmid \deg g$, we have that p does not divide ℓ. Hence

Y has a unique point at infinity.

For *ii)*, define the nonnegative integer $a_{r+1} < n$ such that $\sum_{i=1}^{r+1} a_i \equiv 0 \pmod{n}$. Then by a similar argument as in *i)* with $\delta := \left\lceil \frac{\deg f}{n} \right\rceil$ and $z = 1/x$, $w = z^\delta y$, we get as an equation around $z = w = 0$:

$$w^n = f^*(z), \tag{2.1.3}$$

with $f^*(z) = z^{\delta n} f(1/z)$. Therefore we have $\gcd(n, a_{r+1})$ points at $z = 0$ in the normalization of $K[z] := K[1/x]$ in $K(Y)$. Since $\gcd(n, \deg(f)) = \gcd\left(n, \sum_{i=1}^{r+1} a_i - \deg(f)\right) = \gcd(a_{r+1}, n)$, the statement follows. $\square$

Remark 2.1.8

Let Y be in one of the cases of Lemma 2.1.7.

i) We denote the unique point at infinity by $\infty \in Y$.

ii) Equations (2.1.2) and (2.1.3) describe a plane affine curve containing ∞ in the cases ***Case AS*** and ***Case S***, respectively. We call the respective equation the *equation at infinity*. $\lhd$

We now look at the normalization as a desingularization tool for a curve Y in ***Case AS*** with ordinary double points, under the assumptions $p = 2$ (hyperelliptic case), $\deg(g) > \deg(h) \cdot \frac{p}{p-1}$, and $p \nmid \deg g$ (unique point at infinity). We additionally assume that $\mathrm{char}\,(K) = p$. We will see that the setting for the class of hyperelliptic curves in Chapter 4 fulfills these requirements (see Section 4.3.1). Moreover, ordinary double points are a class of singularities that are easier to handle in terms of the theory on L-functions in Chapter 3.

Consider a closed point $(a, b) \in Y \setminus \{\infty\}$. We may use Corollary 4.3.4. It states that (a, b) is an ordinary double point if and only if a is a simple, yet not double zero of $h(x)$ and a double zero of $g(x)$. For details, see Section 4.3.3.

Lemma 2.1.9 (Resolution of ordinary double points)

*Let Y be in **Case AS**, under the additional assumptions $p = 2$, $\deg(g) > \deg(h) \cdot \frac{p}{p-1}$, $p \nmid \deg g$, and* $\mathrm{char}\,(K) = p$. *We assume that Y has only ordinary double points on the affine patch as singularities.*
Define the following polynomials in $K^{alg}[x]$

$$\tilde{h} := h(x) / \prod_i (x - x_i) \qquad \tilde{g} := g(x) / \prod_i (x - x_i)^2$$

where the products run over all ordinary double points (x_i, b_i) of Y.

Write $r := \prod_i (x - x_i)$ and $w := y/r$. Then the normalization Y^{norm} of Y is the smooth projective curve over K with function field

$$K(Y^{\mathrm{norm}}) = K(x)[w]/(w^2 + \tilde{h}w - \tilde{g}).$$

Proof: The statement follows from the fact that Y^{norm} is unique (up to isomorphism) and from the normalization of $K[x]$ in $L := K(x)[y]/(y^2 + h(x)y - g(x))$.

Obviously we have $w^2 + \tilde{h}(x)w = y^2/r^2 + \tilde{h}(x)w = \tilde{g}(x) \in K[x]$, so w is integral over $K[x]$. Now take an element $\alpha \in L \setminus K(x)$ which is integral over $K[x]$. Then

$$\alpha = \beta_1(x) + \beta_2(x)y \quad \text{with} \quad \beta_i \in K(x).$$

The element α has minimal polynomial $u^2 + (h\beta_2 - 2\beta_1)u + \beta_1^2 - \beta_2(g\beta_2 + \beta_1 h)$, which is in $K(x)[u]$. By Gauss' Lemma the coefficients of this polynomial are already in $K[x]$. By a standard argument, this is equivalent to $\beta_2 \cdot r \in K[x]$. Thus

$$\alpha \in K[x] + \frac{y}{r}K[x] \simeq K[x,w]/(w^2 + \tilde{h}w - \tilde{g}).$$

We have shown that $K[x,w]/(w^2 + \tilde{h}w - \tilde{g})$ is the normalization of $K[x]$ in L. Since Y is nonsingular at ∞, the statement follows. □

For an application as singularization, see Section 4.2.2 and Step 3 of the algorithm in Section 4.3.5.

The situation of the cover $Y \to X := \mathbb{P}^1_x$, together with the normalization map $Y^{\mathrm{norm}} \to Y$ is depicted in Figure 2.1. Each ordinary double point corresponds to a loop in Y and maps to $x = x_i$ on X.

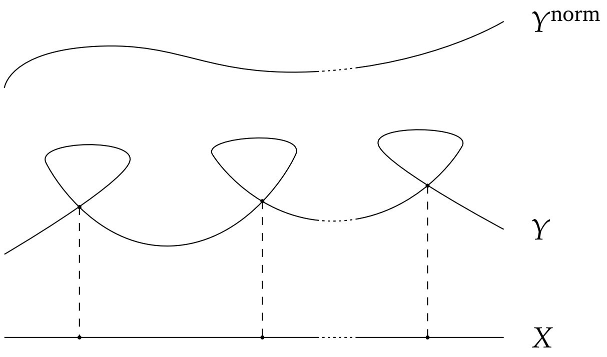


Figure 2.1: Normalization of Y.

Recall that for a projective curve Y over a field K, the *geometric genus* (or just *genus*) is defined as

$$g_Y := g(Y) := \dim_K H^1(Y, \mathcal{O}_Y).$$

We compute the genus $g(Y_F^{\mathrm{norm}})$ of the normalization Y_F^{norm} of a possibly singular curve Y_F both for ***Case AS*** and ***Case S***. For simplicity we pass to the base change $Y_{K^{\mathrm{alg}}}$.

Proposition 2.1.10 (Genus)
Consider a curve Y_F over K^{alg} given by a polynomial $F \in K[x,y]$ in the respective case.

i) Y_F^{norm} *in* ***Case S*** *with* $\mathrm{char}\,(K) \nmid n$ *has genus*

$$g(Y_F^{norm}) = 1 + \frac{1}{2} \cdot \big(n(\deg f - 1) - \sum_i \gcd(n, a_i)\big).$$

Here we denote by a_i the multiplicities of the roots of f over K^{alg} and define a_{r+1} as the positive integer $< n$ with $\sum_i a_i \equiv 0 \pmod{n}$.

ii) Y_F^{norm} *in* ***Case AS*** *with* $\deg(g) > \deg(h) \cdot \frac{p}{p-1}$ *has genus*

$$g(Y_F^{norm}) = 1 + \frac{1}{2} \cdot \big(p(\deg g - 1) - \sum_i \gcd(p, a_i)\big).$$

Here we consider the roots x_i of g over K^{alg} and set

$$a_i := \max\{\ell \in \mathbb{N}_{>0} \mid x_i \textit{ is an } \ell\textit{-fold root of } g \textit{ and an } (\ell - 1)\textit{-fold root of } h\}.$$

Moreover, we define a_{r+1} as the nonnegative integer $< p$ with $\sum_i a_i \equiv 0 \pmod{p}$.

Proof: As Y is a cover of $\mathbb{P}^1$, we use the Riemann–Hurwitz formula in the following form

$$g(Y_F^{\mathrm{norm}}) = 1 + \frac{1}{2} \cdot \left(-2n + \sum_P (e_P - 1)\right),$$

where e_P is the ramification index and P ranges over all ramification points (in the normalization).

First consider *i)*. Then the ramification index is $e_P = n/\gcd(n, a_i)$.
We already showed in the proof of Lemma 2.1.7 ii), that we have $\gcd(n, a_i)$ ramification points in the normalization. So the formula simplifies in ***Case S*** to

$$g(Y_F^{\mathrm{norm}}) = 1 + \frac{1}{2} \cdot \Big(-2n + \sum_{i=1}^{r+1} \big((n/\gcd(n, a_i) - 1) \cdot \gcd(n, a_i)\big)\Big).$$

We get with a simple calculation

$$g(Y_F^{\mathrm{norm}}) = 1 + \frac{1}{2} \cdot \big(n(\deg f - 1) - \sum_{i=1}^{r+1} \gcd(n, a_i)\big).$$

This proves *i)*. The second statement follows similarly. □

2.2 Models of curves

In this section, let $K_\mathfrak{p}$ be a field which is complete with respect to a discrete valuation $v_\mathfrak{p} : K_\mathfrak{p}^\times \to \mathbb{Q}$. The ring of integers $\mathcal{O}_{K_\mathfrak{p}}$ is the set of elements of $K_\mathfrak{p}$ with nonnegative valuation. Denote the residue field by k and write $\mathfrak{p}$ for the unique maximal (and prime) ideal of $\mathcal{O}_{K_\mathfrak{p}}$.

Example 2.2.1

Let $K = \mathbb{Q}$. Then by completing at $\mathfrak{p} = (p) \lhd \mathbb{Z}$ we obtain $K_\mathfrak{p} = \mathbb{Q}_p$ with ring of integers $\mathbb{Z}_p$ and residue field $k = \mathbb{F}_p$. ◁

Let Y be an irreducible smooth projective curve over $K_\mathfrak{p}$, together with a cover

$$Y \to X := \mathbb{P}^1_{K_\mathfrak{p}}.$$

Definition 2.2.2 (Model of a curve)

A *model* of Y is a normal, integral, proper, and flat $\mathcal{O}_{K_\mathfrak{p}}$-scheme $\mathcal{Y}$ together with an isomorphism $\mathcal{Y} \otimes_{\mathcal{O}_{K_\mathfrak{p}}} K_\mathfrak{p} \simeq Y$. ◁

We fix the isomorphism above and use $\mathcal{Y} \otimes_{\mathcal{O}_{K_\mathfrak{p}}} K_\mathfrak{p}$ and Y interchangeably.

Note that in this thesis, every model is normal by definition. We easily see that $\mathcal{X} = \mathbb{P}^1_{\mathcal{O}_{K_\mathfrak{p}}}$ is a model of $X = \mathbb{P}^1_{K_\mathfrak{p}}$. We now use the model $\mathcal{X}$ of X to construct a model $\mathcal{Y}$ of Y by normalizing $\mathcal{X}$ in the function field of Y. This construction is one of the main reasons why we always consider Y as a cover of $X = \mathbb{P}^1_{K_\mathfrak{p}}$.

Definition 2.2.3 ($\mathcal{Y}$)

We define the scheme $\mathcal{Y}$ as the normalization of $\mathcal{X} = \mathbb{P}^1_{\mathcal{O}_{K_\mathfrak{p}}}$ in the function field $K_\mathfrak{p}(Y)$ of Y. ◁

Lemma 2.2.4 (Model $\mathcal{Y}$)

The normalization of $\mathcal{X} = \mathbb{P}^1_{\mathcal{O}_{K_\mathfrak{p}}}$ in the function field $K_\mathfrak{p}(Y)$ of Y is indeed a model of Y.

Proof: As $\mathcal{Y}$ is the normalization of the irreducible $\mathcal{O}_{K_\mathfrak{p}}$-scheme $\mathcal{X}$ in $K_\mathfrak{p}(Y)$, it is normal, integral, and proper. Flatness of $\mathcal{Y}$ over $\mathcal{O}_{K_\mathfrak{p}}$ comes from the fact that the morphism $\mathcal{Y} \to \mathcal{X}$ is non-constant and $\mathcal{Y}$ dominates $\mathcal{X}$ [Liu06, Prop 4.3.9]. Finally, the scheme $\mathcal{Y} \otimes_{\mathcal{O}_{K_\mathfrak{p}}} K_\mathfrak{p}$ is normal in $K_\mathfrak{p}(Y)$. This scheme is isomorphic to Y since Y is smooth, hence normal. □

We give a useful criterion to check whether a given $\mathcal{O}_{K_\mathfrak{p}}$-curve is a model in the following lemma.

Lemma 2.2.5 (Normal scheme)

Let R be a discrete valuation ring, with field of fractions $K_{\mathfrak{p}}$ and residue field k. Let $\tilde{\mathcal{Y}}$ be an R-scheme such that $\mathcal{O}_{\tilde{\mathcal{Y}}}(U)$ is flat over R for every affine open subset U of $\tilde{\mathcal{Y}}$. We suppose that the generic fiber $\tilde{\mathcal{Y}}_{K_{\mathfrak{p}}}$ is normal and that the special fiber $\tilde{\mathcal{Y}}_k$ is reduced. Then $\tilde{\mathcal{Y}}$ is normal.

Proof: See [Liu06, Lemma 4.1.18]. □

We consider the smooth projective curve Y over a field $K_{\mathfrak{p}}$ with discrete valuation $v_{\mathfrak{p}}$, given by a non-constant polynomial F. The construction of this curve (in the case of a perfect field $K_{\mathfrak{p}}$) is discussed in Remark 2.1.4. The curve $\mathcal{X}$ is given by the gluing of $A_1 = \mathcal{O}_{K_{\mathfrak{p}}}[x]$ and $A_2 = \mathcal{O}_{K_{\mathfrak{p}}}[z = 1/x]$. So we may construct a model $\mathcal{Y}$ of Y by gluing $\operatorname{Spec} B_1$ and $\operatorname{Spec} B_2$, where the B_i are the normalizations of the A_i in $K_{\mathfrak{p}}(Y)$.

Theorem 2.2.6

*Let Y be an irreducible smooth projective curve over $K_{\mathfrak{p}}$ given by a polynomial $F \in K_{\mathfrak{p}}[x,y]$ in **Case AS** resp. **Case S**. Assume in **Case S** that the residue characteristic* char (k) *does not divide n. Let F_2 be the 'equation at infinity', i.e. the minimal polynomial of w over $K_{\mathfrak{p}}[z = 1/x]$ (as defined in Equation (2.1.2) resp. (2.1.3)). Moreover, assume that F and F_2 are irreducible modulo $\mathfrak{p}$, the maximal ideal of $\mathcal{O}_{K_{\mathfrak{p}}}$.*

Then the special fiber $\bar{Y} := \mathcal{Y} \otimes_{\mathcal{O}_{K_{\mathfrak{p}}}} k$, is a projective curve over k with function field $k(\bar{Y}) = k(\bar{x})[\bar{y}]/(\bar{F})$. Here $\bar{x}, \bar{y}$ are the images of x, y in $k(\bar{Y})$ and $\bar{F} = F \pmod{\mathfrak{p}}$.

Proof: Define $\tilde{\mathcal{Y}}$ as the gluing of $\operatorname{Spec} \tilde{B}_1$ and $\operatorname{Spec} \tilde{B}_2$ with

$$\tilde{B}_1 = \mathcal{O}_{K_{\mathfrak{p}}}[x][y] \quad \text{and} \quad \tilde{B}_2 = \mathcal{O}_{K_{\mathfrak{p}}}[z][w].$$

Here z, w are as in Equations (2.1.2) and (2.1.3) for ***Case AS*** and ***Case S***, respectively. The rest of the proof is identical for both cases.

We first use the criterion of Lemma 2.2.5 for $R = \mathcal{O}_{K_{\mathfrak{p}}}$ to show that $\tilde{\mathcal{Y}}$ is normal. Both B_1 and B_2 are torsion-free $\mathcal{O}_{K_{\mathfrak{p}}}$-modules and thus flat over $\mathcal{O}_{K_{\mathfrak{p}}}$. Moreover, $\tilde{\mathcal{Y}}_{K_{\mathfrak{p}}} = Y$ is normal, since we assume that Y is smooth. As the reductions of F and F_2 modulo $\mathfrak{p}$ are irreducible, $\tilde{\mathcal{Y}}_k$ is reduced. Thus $\tilde{\mathcal{Y}}$ is normal in $K_{\mathfrak{p}}(Y)$, hence isomorphic to $\mathcal{Y}$. □

We summarize some important implications on $\bar{Y}$ in the following corollary.

Corollary 2.2.7 (Reduced curve)

We use the notation and assumptions of Theorem 2.2.6. Then the following holds:

i) $\bar{Y}$ is reduced and absolutely irreducible.

ii) $\bar{Y}$ has a unique, smooth point $\bar{\infty}$ at infinity.

iii) The affine open $\bar{Y} \setminus \{\bar{\infty}\}$ is a plane curve given by the reduction of F modulo $\mathfrak{p}$.

Proof: The statements follow from the fact that $\mathcal{Y}$ is normal and given by $B_1 = \mathcal{O}_{K_\mathfrak{p}}[x][y]$ and $B_2 = \mathcal{O}_{K_\mathfrak{p}}[z][w]$. □

The corollary is a key result on models of curves in the setting of chapters 4 and 5, cf. Theorem 4.3.1 and Remark 5.2.2.

2.3 Good and bad reduction

Let Y be an absolutely irreducible smooth projective curve over the local field $K_\mathfrak{p}$, as defined in the previous section. We write k for the residue field, $\mathcal{O}_{K_\mathfrak{p}}$ for the ring of integers of $K_\mathfrak{p}$, and $\widehat{\mathcal{O}}_{K_\mathfrak{p}}$ for the p-adic completion of $\mathcal{O}_{K_\mathfrak{p}}$.

Definition 2.3.1 (Good and bad reduction)

i) We say that Y has *good reduction at* $\mathfrak{p}$ if there is a model $\mathcal{Y}$ of Y over $\widehat{\mathcal{O}}_{K_\mathfrak{p}}$ such that the special fiber

$$\bar{Y} := \mathcal{Y} \otimes_{\widehat{\mathcal{O}}_{K_\mathfrak{p}}} k$$

is a smooth curve.If Y has good reduction at $\mathfrak{p}$, we also say that $\mathfrak{p}$ is a *prime of good reduction* (or *good prime*) of Y.

ii) We say that Y has *bad reduction at* $\mathfrak{p}$ if no such model exists. In this case we say that $\mathfrak{p}$ is a *bad prime* of Y.

We further define two special cases important for our study.

iii) The curve Y has *potentially good reduction at* $\mathfrak{p}$ if there exists a finite extension $L/K_\mathfrak{p}$ such that $Y_L := Y \otimes_{K_\mathfrak{p}} L$ has good reduction.

iv) The curve Y has *semistable reduction at* $\mathfrak{p}$ if there exists an $\widehat{\mathcal{O}}_{K_\mathfrak{p}}$-model $\mathcal{Y}$ of Y whose special fiber is semistable, i.e. the special fiber is reduced and has at most ordinary double points as singularities. ◁

Remark 2.3.2 (Semistable reduction)

Recall that we defined $K_\mathfrak{p}$ to be a field which is complete with respect to a discrete valuation $v_\mathfrak{p}$. Consider an absolutely irreducible smooth projective curve Y of genus ≥ 2 over $K_\mathfrak{p}$. The Semistable Reduction Theorem by Deligne and Mumford [DM69, Cor. 2.7] states that there exists a finite extension L of $K_\mathfrak{p}$ such that $Y_L = Y \otimes_{K_\mathfrak{p}} L$ has semistable reduction. In other words, there exists an $\mathcal{O}_L$-model $\mathcal{Y}$ whose special fiber $\bar{Y}$ is reduced and has at most ordinary double points as singularities.

Without going into details, note that the assumption $g(Y) \geq 2$ implies that there is a minimal semistable model over L, called *stable model* of Y_L. Its special fiber is called *stable reduction of* Y_L. For details we refer to [DM69, Lem. 1.12]. ◁

Chapter 3

L-functions

The first aim of this chapter is to give an exact definition of the L-function of a curve Y of genus g_Y defined over a number field K (Definition 3.2.1). Moreover, we develop a connection to the Hasse–Weil zeta function and give a more manageable expression for the local factor $L_\mathfrak{p}$ in Section 3.4. The description of the L-function follows the discussion in [BW16, §§ 2.1 – 2.3].

We also introduce the functional equation (FEq) and explain a method to check (FEq) numerically up to arbitrarily high precision. We first recall some facts from algebraic number theory that are important for the following sections.

Denote by $\mathcal{O}_K$ the ring of integers of a number field K with ideal norm $\mathsf{N}(\cdot)$ defined as $\mathsf{N}(\mathfrak{p}) := |\mathcal{O}_K/\mathfrak{p}|$. The residue field and residue characteristic of a prime $\mathfrak{p} \lhd \mathcal{O}_K$ are denoted $k = k(\mathfrak{p})$ and p, respectively. For a prime $\mathfrak{p} \lhd \mathcal{O}_K$ we define the following *valuation* on $\mathcal{O}_K$:

$$v_\mathfrak{p}(a) := \max\{d \in \mathbb{N}_0 \mid a \in \mathfrak{p}^d\} \text{ , for } a \in \mathcal{O}_K.$$

3.1 Ramification of ideals in number fields

Let K be a number field. Recall that the *discriminant of a polynomial* $f(x) \in K[x]$ of degree m with leading coefficient c_m and roots $r_1, \dots, r_m$ (in the splitting field of f) is defined as

$$\Delta(f) := c_m^{2m-2} \prod_{i<j} (r_i - r_j)^2.$$

Let $(\alpha_1, \dots, \alpha_t)$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$ and $\{\sigma_1, \dots, \sigma_t\}$ the set of embeddings of K into $\mathbb{C}$. Recall that the *discriminant* of K is $\delta_K := (\det(\sigma_i(\alpha_j)))^2$.

Remark 3.1.1 (Discriminant)

i) Let K be of the form $K = \mathbb{Q}(\alpha)$, and denote the minimal polynomial of α by $f = \min_\mathbb{Q}(\alpha)$. If the roots of f form an integral basis of K we have

$$\Delta(f) = \delta_K.$$

This is the case e.g. for cyclotomic fields $K/\mathbb{Q}$ and α a root of unity generating that field extension. However, it is not true in general if the roots of f do not form such an integral basis. Take for instance $f = x^4 - x + 1$ with $\Delta(f) = 229$, $\delta_K = 229^{12}$. In this case we have $\Delta(f) \neq \delta_K$.

ii) If we only assume that $K = \mathbb{Q}(\alpha)$, the following holds:

$$\Delta(f)/\delta_K = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2,$$

where $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is the determinant of the base change matrix from an integral basis of $\mathbb{Z}[\alpha]$ to an integral basis of $\mathcal{O}_K$. ◁

Let L/K be a Galois extension with Galois group Γ. We denote the decomposition group of a prime $\mathfrak{P} \lhd \mathcal{O}_L$ lying over a prime $\mathfrak{p} \lhd \mathcal{O}_K$ by $D := D_{\mathfrak{P}}$. The inertia group of $\mathfrak{P}$ is denoted by $I := I_{\mathfrak{P}}$. Recall that any inertia group is of the form $I = C_m \ltimes P$, where C_m denotes the unique cyclic group of some order m (with m prime to p) and P is the Sylow p-subgroup of I [Ser79, Cpt. IV, § 2, Cor. 4].

Definition 3.1.2 (Higher ramification groups)

Let L/K be Galois and let $\mathfrak{P} \lhd \mathcal{O}_L$ be a prime. For each $i \in \{-1, 0, 1, 2, \ldots\}$ we define the *higher ramification groups* by

$$\Gamma_i := \{\sigma \in \Gamma \mid v_{\mathfrak{P}}\left((\sigma(\pi) - \pi)/\pi\right) \geq i \text{ for all } \pi \in \mathcal{O}_L\}.$$

In the case $\Gamma_1 \neq \{\mathrm{id}\}$, we define the set of *jumps* as the numbers $h_1, \ldots, h_r \in \mathbb{N}$ with

$$\Gamma_1 = \ldots = \Gamma_{h_1} \supsetneq \Gamma_{h_1+1} = \ldots = \Gamma_{h_r} \supsetneq \{\mathrm{id}\}\,. \qquad ◁$$

Note that by definition, $\Gamma_{-1} = \mathrm{Gal}(L/K)$, $\Gamma_0 = I_{\mathfrak{P}}$, and Γ_1 is the Sylow p-subgroup of $I_{\mathfrak{P}}$, i.e. the second term in $C_m \ltimes P$. Moreover, the jumps are well-defined since $\Gamma_k \supseteq \Gamma_{k+1}$ and eventually $\{\mathrm{id}\} = \Gamma_n = \Gamma_{n+1} = \ldots$ for some $n \in \mathbb{N}_0$.

3.2 The *L*-function of a curve

Let Y be a smooth projective curve defined over a number field K. For our computations, a distinction between the L-series and the conjectured analytic continuation, i.e. L-function (Conjecture 3.5.1) is not relevant. Therefore, we define the *L-function of* Y as a product

$$L(Y, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(Y, s)$$

of local factors $L_{\mathfrak{p}}$, where $\mathfrak{p}$ runs over the prime ideals of $\mathcal{O}_K$.

In the following, we motivate the definition of the local L-factor $L_{\mathfrak{p}}$ we will use throughout this thesis (Definition 3.2.1). This definition originates from the *Artin L-function* [Neu92, Def. VII.10.1]. We follow the argumentation in [Neu92, VII.10] and [Mil80, Cpt. VI, § 13]. Fix a number field K and a prime $\mathfrak{p} \lhd \mathcal{O}_K$. Write $k := k(\mathfrak{p})$ for the residue field. Also fix an auxiliary prime number ℓ different from the residue characteristic p of $\mathfrak{p}$. Write $K_{\mathfrak{p}}$ for the $\mathfrak{p}$-adic completion of K, which is a finite extension of $\mathbb{Q}_p$.

As we are dealing with a local problem, we consider smooth projective curves Y over $K_{\mathfrak{p}}$. This is important for the definition of the étale cohomology group later.

Write $J := \mathrm{Jac}(Y)$ for the Jacobian of Y. We denote by $J[\ell^n]$ the ℓ^n-torsion points of $J(Y)$ as $\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{alg}}/K_{\mathfrak{p}})$-module for $n \in \mathbb{N}$. The starting point of the construction of the L-function is the *ℓ-adic Tate module* of $J(Y)$. It is the inverse limit of the system $J[\ell^n]$ under multiplication by ℓ,

$$T_\ell(J(Y)) := \varprojlim_n J[\ell^n] \simeq (\varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z})^{2g_Y} \simeq \mathbb{Z}_\ell^{2g_Y}\,.$$

We denote the absolute Galois group of $K_{\mathfrak{p}}$ by $\Gamma_{K_{\mathfrak{p}}} := \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{alg}}/K_{\mathfrak{p}})$. For the absolute Galois group of the residue field k we write

$$\Gamma_k := \mathrm{Gal}(k^{\mathrm{alg}}/k) = \langle \sigma_q \rangle, \tag{3.2.1}$$

generated by the Frobenius element σ_q. More precisely, $\sigma_q : k^{\mathrm{alg}} \to k^{\mathrm{alg}}$ is the q-Frobenius defined by $x \mapsto x^q$ ($q = |k|$). If we denote by $K_{\mathfrak{p}}^{\mathrm{ur}} \subset K_{\mathfrak{p}}{}^{\mathrm{alg}}$ the maximal unramified extension of $K_{\mathfrak{p}}$, the inertia group of $K_{\mathfrak{p}}$ can be defined as

$$I_{K_{\mathfrak{p}}} := \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{alg}}/K_{\mathfrak{p}}^{\mathrm{ur}})\,.$$

We have a short exact sequence $1 \to I_{K_{\mathfrak{p}}} \hookrightarrow \Gamma_{K_{\mathfrak{p}}} \twoheadrightarrow \Gamma_k \to 1\,.$

Now $\Gamma_{K_{\mathfrak{p}}}$ acts on each $J[\ell^n]$ and hence on $T_\ell(J(Y))$, providing a representation

$$\rho_\ell :\, \Gamma_{K_{\mathfrak{p}}} \to \mathrm{Aut}(T_\ell(J(Y))) \simeq \mathrm{GL}_{2g_Y}(\mathbb{Z}_\ell)\,.$$

We define the vector space V to be the dual of $T_\ell(J(Y)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and ρ_ℓ^* to be the dual representation of ρ_ℓ. Our definition of the local L-factor comes from the local L-factor of the Artin L-series of (ρ_ℓ^*, V). The dual of $\rho_\ell(\sigma_q)$ is $\rho_\ell^*(\sigma_q^{-1})$ and by [Del74, Sec. 2], $V = (T_\ell(J(Y)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^*$ is the *first ℓ-adic cohomology group*

$$H^1_{\text{ét}}(Y_{K_{\mathfrak{p}}^{\mathrm{alg}}}, \mathbb{Q}_\ell) := \Big(\varprojlim_n H^1_{\text{ét}}(Y_{K_{\mathfrak{p}}^{\mathrm{alg}}}, \mathbb{Z}/\ell^n)\Big) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\,.$$

In the following, let $q = \mathsf{N}(\mathfrak{p}) = |k(\mathfrak{p})|$. By abuse of notation, write σ_q instead of $\rho_\ell^*(\sigma_q)$.

Definition 3.2.1 (Local *L*-factor)

Let $I_{K_\mathfrak{p}} = \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{alg}}/K_\mathfrak{p}^{\mathrm{ur}})$ and let $\sigma_q \in \Gamma_{K_\mathfrak{p}}$ be an arithmetic Frobenius element (i.e. $\sigma_q(\alpha) = \alpha^q \pmod{\mathfrak{p}}$). Then

$$L_\mathfrak{p}(Y,s) = \frac{1}{\det(1 - \sigma_q^{-1} q^{-s} \mid V^{I_{K_\mathfrak{p}}})},$$

where $V := H^1_{\text{ét}}(Y \otimes_{K_\mathfrak{p}} K_\mathfrak{p}^{\mathrm{alg}}, \mathbb{Q}_\ell)$ denotes the first étale cohomology group of Y and ℓ is an auxiliary prime distinct from the residue characteristic of $\mathfrak{p}$. We refer to [BW16, § 2.2] for more details. ◁

Definition 3.2.1 does not depend on the choice of a prime ℓ coprime to the residue characteristic of $\mathfrak{p}$, [dS04, p. 94].

Theorem 3.2.2 (Rationality of the local factor)

We have

$$L_\mathfrak{p}(Y,s) = \frac{1}{P(q^{-s})},$$

where $P(T) \in \mathbb{Z}[T]$ is a polynomial with values in $\mathbb{Z}$ and independent of ℓ. ◁

Proof: For the general case, see [Del74, Thm. 1.6]. The easier case of a good prime $\mathfrak{p}$ is discussed in Remark 3.3.2. □

We now state some general properties of L-factors. We start by linking the local factors to the Dirichlet series. More precisely, we give a connection between the coefficients a_n from Equation (1.1.2)

$$L(Y,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

and the coefficients of the polynomial $P(T = q^{-s}) = L_\mathfrak{p}(Y,s)^{-1}$. We define the coefficients of $P(T)$ as follows:

$$P(T) = \sum_{i=0}^{\deg(P)} c_i T^i. \tag{3.2.2}$$

Lemma 3.2.3 (Expansion of $L_\mathfrak{p}$ at prime powers)

We have

$$L_\mathfrak{p}(Y,s) = \sum_{k=0}^{\infty} \frac{a_{q^k}}{q^{ks}} = 1 + \frac{a_q}{q^s} + \frac{a_{q^2}}{q^{2s}} + \ldots \quad \textit{with} \quad a_{q^e} = -\sum_{1 \le i \le e} c_i a_{q^{e-i}}\,.$$

Here the a_{q^e} are given by the coefficients c_i of $P(T)$ (Theorem 3.2.2, Equation (3.2.2)). The polynomial P is seen as a power series in T, i.e. we set $c_i = 0$ for all $i > \deg(P)$.

Proof: This follows from the Taylor expansion of $L_{\mathfrak{p}}$ with respect to the variable T. Alternatively, consider the identity

$$1 = L(Y,s) \cdot \prod_{\mathfrak{p}} P(q^{-s}) =: \left(\sum_n \frac{a_n}{n^s}\right) \cdot \left(\sum_n \frac{b_n}{n^s}\right),$$

set $b_i = c_i$ for $i \leq 2g_Y$, $b_i = 0$ for $i > 2g_Y$ and use the Dirichlet product

$$\left(\sum_n \frac{a_n}{n^s}\right) \cdot \left(\sum_n \frac{b_n}{n^s}\right) = \sum_n \frac{\sum_{d|n} a_{n/d} b_d}{n^s} = \sum_n \frac{\sum_{d|n} a_d b_{n/d}}{n^s} =: \sum_n \frac{g_n}{n^s} = 1\,. \qquad \square$$

We now easily see (analogously to the Riemann zeta function):

$$L(Y,s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(Y,s) = \prod_{\mathfrak{p}} \sum_{k=0}^{\infty} \frac{a_{q^k}}{q^{ks}} = \sum_n \frac{a_n}{n^s}, \tag{3.2.3}$$

where $a_1, a_q, \ldots, a_{q^e}$ as defined above. This implies that for $n = \prod_i p_i^{k_i}$ we have $a_n = \prod_i a_{p_i^{k_i}}$. Hence the a_n are weakly multiplicative.

Theorem 3.2.4 (Convergence of the L-series)

For smooth projective curves Y the Dirichlet series

$$L(Y,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

converges in the right half-plane where $\Re(s) > 3/2$.

Proof: The statement is a corollary to Proposition 3.3.4. For details, see [Sau03]. □

3.3 Good factors

We will show that all but finitely man local factors may be expressed in terms of the Hasse–Weil zeta function of a certain curve $\bar{Y}$ over the residue field $k(\mathfrak{p})$ (Remark 3.3.3). We therefore start by recalling the definition and some properties of the Hasse–Weil zeta function.

Definition 3.3.1 (Hasse–Weil zeta function)

Let X be a (not necessarily smooth) projective curve over a finite field $\mathbb{F}_q$. Denote by $N_{q^m} = \#X(\mathbb{F}_{q^m})$ the number of closed points of X defined over $\mathbb{F}_{q^m}$. Then the (local) Hasse–Weil zeta function is defined as

$$Z(X,T) := \exp\left(\sum_{m=1}^{\infty} \frac{N_{q^m} T^m}{m}\right). \tag{3.3.1}$$

Note that it is more natural to define $Z(X,T)$ not as a power series, but as a converging series ζ_X in one complex variable $s \in \mathbb{C}$ by setting $T = q^{-s}$: $\zeta_X(s) := Z(X, q^{-s})$. Nevertheless, we will mainly use the first version for better readability. ◁

Let X be as in Definition 3.3.1 and assume for now that X is absolutely irreducible. For the general case, see Section 4.2.1. As a consequence of the Weil conjectures (proven by Dwork, Grothendieck, and Deligne, [Har77, p. 449 ff.]), $Z(X,T)$ is a rational function of the following form

$$Z(X,T) = \frac{P_q(T)}{(1-T)(1-qT)}.$$

Here $P_q(T)$ is a polynomial in $\mathbb{Z}[T]$ depending on q that can be written as

$$P_q(T) = 1 + c_1 T + \ldots + q^{g_Y} T^{2g_Y} =: \sum_{i=0}^{2g_Y} c_i T^i\,. \tag{3.3.2}$$

We use the functional equation of $Z(X,T)$ [Har77, C.1.2] to get

$$P_q(T) = P_q\left(\frac{1}{qT}\right) \cdot q^{g_Y} T^{2g_Y}.$$

This yields a mirror rule for the c_i:

$$c_0 = 1\,,\ c_n = c_{2g_Y - n} \cdot q^{n-g_Y}\,.$$

Hence only $c_1, \ldots, c_{g_Y}$ are needed to construct $P_q(T)$. We define

$$t_{q^m} := N_{q^m} - 1 - q^m. \tag{3.3.3}$$

For the calculation of the $c_1, \ldots, c_{g_Y}$, we use logarithmic derivation of (3.3.1) to obtain

$$(i+1) \cdot c_{i+1} = \sum_{\substack{j+m+1=i+1\\ 1\le m+1\,;\,0\le j\le i}} t_{q^{m+1}} c_j, \tag{3.3.4}$$

where $c_0 = 1$ and $i \in \{0, \ldots, g_Y - 1\}$.

Remark 3.3.2 (Local L-factor at primes of good reduction)

We will see later (Proposition 3.4.4) that for a prime $\mathfrak{p}$ of good reduction, the local factor $L_{\mathfrak{p}}(Y,s)$ is given by the inverse of the numerator of the Hasse–Weil zeta function (Definition 3.3.1). This implies that $L_{\mathfrak{p}}(Y,s)$ satisfies

$$L_{\mathfrak{p}}(Y,s) = \left(1 + c_1 q^{-s} + \ldots + q^{g_Y(1-2s)}\right)^{-1}, \tag{3.3.5}$$

where the c_i are defined as in Equation (3.3.4) and $q = |k(\mathfrak{p})|$. Hence to compute the good local factors of a smooth projective curve Y over a number field K, it suffices to compute $c_1, \dots, c_{g_Y}$. For this one simply has to count the number of closed points on the reduced curve $\bar{Y}$ (Definition 2.3.1) over the finite fields $\mathbb{F}_q, \dots, \mathbb{F}_{q^{g_Y}}$. $\lhd$

Remark 3.3.3 (Number of good factors)

Recall that a smooth projective curve over K has good reduction outside finitely many primes [Liu06, Prop. 10.1.21]. Moreover, there are no projective algebraic curves over $\mathbb{Q}$ of genus ≥ 1 with everywhere good reduction [Fon85, 3.4.6 Cor. 2]. This implies that for a smooth projective curve over a number field K all but finitely many local factors $L_\mathfrak{p}$ are of the form in Equation (3.3.5). For $K = \mathbb{Q}$ at least one local factor is not of this form. $\lhd$

We are now able to prove the basis for the convergence statement of the L-series (Theorem 3.2.4).

Proposition 3.3.4 (Asymptotic behavior of the a_n)

The terms a_n in the L-series of a smooth projective curve Y of genus g_Y over K grow as $\mathcal{O}(\sqrt{n})$.

Proof: Recall that $t_{q^k} = \#\bar{Y}(\mathbb{F}_{q^k}) - q^k - 1$ by Equation (3.3.3). The statement follows from the Hasse–Weil bound $|t_{q^k}| \leq 2g_Y\sqrt{q^k}$, the finiteness of the set of bad primes (Remark 3.3.3), and the fact that for the good primes the a_n are a linear combination of the t_{q^k} (Lemma 3.2.3, Equation (3.3.4)). $\square$

3.4 Bad factors

In this section we give an expression for $L_\mathfrak{p}$ in terms of a certain reduced curve $\bar{Z}$ over the residue field $k = k(\mathfrak{p})$. With this expression we will be able to compute the bad factors for the two classes of curves discussed in Chapters 4 and 5. We closely follow the argumentation in [BW16, § 2.3].

As in Section 3.2 we assume that Y is a smooth projective curve over a p-adic field $K_\mathfrak{p}$. For the scope of this thesis we may also assume that the genus g_Y is larger than one. Recall from Remark 2.3.2 that there exists a finite extension L of $K_\mathfrak{p}$ and a semistable model $\mathcal{Y}$ of Y over $\mathcal{O}_L$. Replacing L by a finite extension, we may additionally assume that $L/K_\mathfrak{p}$ is Galois and denote the Galois group by

$$\Gamma := \mathrm{Gal}(L/K_\mathfrak{p}) \,.$$

We further may choose the model $\mathcal{Y}$ such that Γ naturally acts on $\mathcal{Y}$. Such a model is called *quasi-stable*, see [BW16, § 2.3] for details.

Denote by

$$\bar{Y} := \mathcal{Y} \otimes_{\mathcal{O}_L} k \tag{3.4.1}$$

the special fiber of such a quasi-stable model $\mathcal{Y}$ of Y.

The Galois group Γ acts on $\bar{Y}$, since $\mathcal{Y}$ is quasi-stable. We therefore define the following curve.

Definition 3.4.1 (Inertial reduction)

Let $\bar{Y}$ as in Equation (3.4.1). We define the *inertial reduction* by

$$\bar{Z} := \bar{Y}/\Gamma. \qquad \triangleleft$$

In the following, write $\bar{Z}_{k^{\mathrm{alg}}}$ for the base change $\bar{Z}_{k^{\mathrm{alg}}} = \bar{Z} \otimes_k k^{\mathrm{alg}}$.

Theorem 3.4.2 (Action of $I_{K_\mathfrak{p}}$ on the cohomology)

We have

$$H^1_{\acute{e}t}(Y_{K_\mathfrak{p}^{alg}}, \mathbb{Q}_\ell)^{I_{K_\mathfrak{p}}} \simeq H^1_{\acute{e}t}(\bar{Z}_{k^{alg}}, \mathbb{Q}_\ell).$$

Proof: See [BW16, Thm. 2.4]. □

We have already seen (Theorem 3.2.2) that the bad factors, like the good factors, can be expressed as the inverse of a polynomial in $\mathbb{Z}[T]$. With Theorem 3.4.2, we obtain a practical expression for the local L-factor, depending on $\bar{Z}_{k^{\mathrm{alg}}}$ instead of $Y_{K_\mathfrak{p}^{\mathrm{alg}}}$. This means that, as in the good case (Remark 3.3.2), the bad factors $L_\mathfrak{p}$ can be expressed in terms of a curve over a finite field in characteristic $p = \mathrm{char}\,(k(\mathfrak{p}))$. We summarize this in the following proposition.

Proposition 3.4.3 (Local L-factor)

The following definition of the local L-factor is equivalent to Definition 3.2.1:

$$L_\mathfrak{p}(Y, s) = L_\mathfrak{p}(Y, T = q^{-s}) = \frac{1}{\det(1 - \mathrm{Frob}_q \cdot T \mid H^1_{\acute{e}t}(\bar{Z}_{k^{alg}}, \mathbb{Q}_\ell))},$$

where Frob_q *is the relative q-Frobenius endomorphism on* $\bar{Z}$ $\big(q = |k|\big)$.

Proof: See [BW16, Cor. 2.5]. □

For a good prime $\mathfrak{p}$ we have $\Gamma = I_{K_\mathfrak{p}} = \{\mathrm{id}\}$. So we obtain the following result.

Proposition 3.4.4 (Local L-factor and the Hasse–Weil zeta function)

Let Y be a smooth projective and absolutely irreducible curve over a number field K.

For a prime $\mathfrak{p}$ of good reduction of Y and $\bar{Y}$ as defined in 2.3.1 it holds that $L_{\mathfrak{p}}(Y,T)$ is the inverse of the numerator of the Hasse–Weil zeta function $Z(\bar{Y},T)$.

Proof: Note that on $H^1_{\text{ét}} := H^1_{\text{ét}}(\bar{Y}_{k^{\text{alg}}}, \mathbb{Q}_\ell)$, the arithmetic q-Frobenius σ_q on k^{alg} (Equation (3.2.1)) induces a map $f : H^1_{\text{ét}} \to H^1_{\text{ét}}$ that fulfills the *Lefschetz trace formula* [Lef37]:

$$\#\bar{Y}(\mathbb{F}_{q^m}) = \#\{x \mid x \text{ fixed by } f^m\} = \sum_{j=0}^{2} (-1)^j \cdot \operatorname{tr}(f^m \mid H^j_{\text{ét}})\,.$$

(Note that by [Chê04, Prop 4.2], σ_q^{-1} and Frob_q induce the same map f in $H^i_{\text{ét}}$.) Using the identity

$$\exp\left(\sum_{m=1}^{\infty} \operatorname{tr}(f^m \mid V)\frac{T^m}{m}\right) = \det(1 - fT \mid V)^{-1},$$

and

$$\det(1 - fT \mid H^0_{\text{ét}}) = (1-T) \quad , \quad \det(1 - fT \mid H^2_{\text{ét}}) = (1-qT)$$

(cf. Remark 4.2.2), we get

$$Z(\bar{Y},T) = \prod_{j=0}^{2} \det\left(1 - fT \mid H^j_{\text{ét}}\right)^{(-1)^{j+1}} = \frac{\det\left(1 - fT \mid H^1_{\text{ét}}\right)}{(1-T)(1-qT)}.$$

The statement follows. □

Remark 3.4.5 (Local factors)

- For elliptic curves over number fields, there are only three cases of bad factors: $L_{\mathfrak{p}} = 1$ and $L_{\mathfrak{p}} = 1 \pm T$, [Hus04, 14.3.4].
- For curves of genus ≥ 2, the main difficulty in checking (FEq) is to compute the bad $L_{\mathfrak{p}}$ and the conductor N. We define the conductor in the following section. Moreover, we discuss algorithms for the computation of the bad factors and N for two classes of curves in Sections 4.2, 5.2.2, and 5.2.3. ◁

3.5 The functional equation (FEq)

Throughout this section, let Y be a smooth projective curve of genus g_Y over a number field K. Moreover, we write δ_K for the discriminant of K (Remark 3.1.1).

In the following we state the functional equation we will use throughout this thesis. We use the notation $V = H^1_{\text{ét}}(Y_{K_{\mathfrak{p}}^{\text{alg}}}, \mathbb{Q}_\ell)$.

Conjecture 3.5.1 (Functional equation)

i) $L(Y,s)$ has an analytic continuation to the whole complex plane (without poles).

ii) There is an integer N — the conductor of the L-function — whose prime factors are identical to those of the product of δ_K and the norms of the primes $\mathfrak{p}$ of bad reduction, with the following property.
The *modified* L*-function*

$$\Lambda(Y,s) := N^{s/2} \cdot (2\pi)^{-g_Y s} \cdot \Gamma(s)^{g_Y} \cdot L(Y,s)$$

satisfies the functional equation

$$\Lambda(Y,s) = \mu \cdot \Lambda(Y, 2-s), \tag{FEq}$$

where $\mu \in \{\pm 1\}$.

iii) The conductor N in ii) is given by

$$N := \delta_K^{2g} \cdot \prod_{\mathfrak{p}} \mathsf{N}(\mathfrak{p})^{f_{\mathfrak{p}}},$$

where δ_K is the discriminant of the number field K and $\mathsf{N}(\cdot)$ is the ideal norm defined as $\mathsf{N}(\mathfrak{p}) := |\mathcal{O}_K/\mathfrak{p}|$. The product runs over the bad primes $\mathfrak{p}$ of $\mathcal{O}_K$. For details, see [Ser70, §§ 2.1, 2.3, and 4.1].

More explicitly, we have $f_{\mathfrak{p}} = \epsilon + \delta$ with

$$\epsilon = \operatorname{codim}(V^{I_{K_\mathfrak{p}}}) = \dim V - \dim(V^{I_{K_\mathfrak{p}}}),$$

and the *Swan conductor* δ.
For a precise definition of δ we refer to [Kat89, § 2]. ◁

Definition 3.5.2 (Conductor, root number)

The integer N from Conjecture 3.5.1 is called the *conductor of the L-function* of Y. We refer to the $f_{\mathfrak{p}}$ as *conductor exponents* and the number μ is called *sign* or *root number* of the functional equation. ◁

We will see later (proof of Corollary 4.4.6, or [BW16, Thm. 2.9]) that ϵ and δ correspond to tame and wild ramification at $\mathfrak{p}$, respectively.

Instead of discussing a precise definition of the Swan conductor, we will give definitions in special cases, e.g. certain hyperelliptic curves and Picard curves in due course. For the time being, keep in mind that δ vanishes if and only if the Sylow p-subgroup of $I_{K_\mathfrak{p}}$ acts trivially on the cohomology group V.

Remark 3.5.3 (Conjectured functional equation)

- It suffices to show analytic continuation for $\Lambda(Y,s)$ to prove i), since the gamma function $\Gamma(s)$ only has poles at $0,-1,-2,\ldots$ and no zeros.
- If Λ is entire, $L(Y,s)$ has trivial zeros of order at least g_Y at $0,-1,-2,\ldots$, due to the first point.
- The sign μ defines the parity of the order of vanishing of $L(Y,s)$ at $s=1$, cf. the Birch and Swinnerton-Dyer conjecture [Wil06].
- The term $\Lambda(2-s)$ indicates a symmetry around the line $\Re(s)=1$. It is conjectured that all non-trivial zeros of L lie on this critical line — even for more general L-functions, see [IS00].
- For elliptic curves over $\mathbb{Q}$ and curves with complex multiplication, Conjecture 3.5.1 is a theorem, [BCDT01], (see [HS00, p. 461] and [dS04, Eqn. 5.3.17] for an overview). This follows from the modularity theorem, yet the modularity theorem doesn't give direct proof of the functional equation. The proof is based on two important facts. First, an L-series of a modular form satisfies Conjecture 3.5.1. Second, the Shimura–Taniyama–Weil conjecture (i.e. modularity theorem) states that $L(Y,s)=L(f,s)$ for a suitable modular form f, [MP05, Cpt. 7]. One of the goals of the Langlands program is to find such a connection for more general curves.

3.6 Verifying (FEq) numerically — Dokchitser's algorithm

We give a brief description of the procedure we use to check the functional equation (FEq) numerically.

Obviously, $L(Y,s)$ is either described as an infinite product or an infinite sum. We therefore need to find a way to check (FEq) without computing the whole L-series. For our computations, we use the `Dokchitser` package in the free computer algebra software *Sage* [St16]. It is based on Tim Dokchitser's paper [Dok04], where — among other things — he describes an algorithm to verify (FEq) up to a chosen numerical precision for curves of genus g_Y over $\mathbb{Q}$.

The idea of the algorithm is to find a different representation of the L-function which also fulfills a functional equation, assuming (FEq) holds. For this, Dokchitser uses *Mellin transforms*, as in the proof of the functional equation of the Riemann zeta function [Neu92, Sec. VII.1]. With this representation, the contribution of *all* coefficients a_n with n larger than a certain bound M is smaller than a chosen error. In fact, this bound M can even be computed *a priori* and only depends on g_Y and N.

The calculation of M is based on somewhat heuristic arguments, and the output of the (FEq)-check in the `Dokchitser` package is open to some interpretation. The manual of the accompanying *PARI/GP* implementation [Dok06] states the following:

> *'The output of* `check_functional_equation()` *should ideally return 0* [meaning the machine epsilon `eps`].
> *If* `check_functional_equation()` *does not look like 0 at all, probably some of the parameters* [i.e. N or the a_n] *are wrong.'*

Since a typical output of `check_functional_equation()` with an obviously wrong input ranges around 0.1 – 100 in absolute value, we have to be satisfied with the following rule: If the absolute value of the output is smaller than a certain bound, namely 10^{-14} (approx. $100 \cdot$`eps`), we consider (FEq) to hold for this curve.

One might think that there are several sources of uncertainty here, and it may seem unclear which statistical hypothesis one wants to test. But keep the following things in mind:

- Opposed to other approaches where (FEq) is used to find suitable data at the bad primes ([Boo05], [DdJZ06]), we are able to *provably compute* the bad local factors and the conductor without making use of (FEq). This is performed for two classes of superelliptic curves in Chapters 4 and 5. After that we rather verify (FEq) with our data than use (FEq) to see if our data is correct.
- Assuming (FEq) to hold, a type I error in our case would be an output larger than 10^{-14} although all data of the curve is correct. This would imply an error in Dokchitser's calculations, e.g. a too small bound M. It could also indicate that Conjecture 3.5.1 is wrong. Yet this never occurred within our experimental results (cf. the first point).
- The corresponding type II error is a sufficiently small output although some data is incorrect. All the data at the bad primes (integer coefficients of $L_\mathfrak{p}$ (Proposition 3.4.3), prime powers in N (Conjecture 3.5.1)) is discrete. So (FEq) is very sensitive to errors in this data. This means that such a type II error is very unlikely, assuming that the point counting at the good primes works correctly. Moreover, we never fed guessed or random bad prime data into (FEq), hoping that the output is small enough.
- In principle, one can perform the (FEq)-check with arbitrarily high precision by changing some of the parameters of `check_functional_equation()`, e.g. lowering the machine epsilon `eps` (see [Dok06] for details). This would make the conclusions drawn from this (FEq)-check even more reliable. However, it results in larger values for the bound M and thus in more computation time.

In practice, we use *Sage* to first compute $M(g_Y, N)$. Then we do the necessary point counting over finite fields of size up to $q^k \leq M$ (Remark 3.3.2), compute the bad factors

(Sections 4.3.5, 5.2.2, and 5.2.3), and assemble the truncated L-series

$$\sum_{n=1}^{M} \frac{a_n}{n^s}$$

(Equation (3.2.3)). After that, we load this data into the `Dokchitser` package to check (FEq). We will discuss the algorithm for all $L_\mathfrak{p}$ and N, as well as some computational aspects in more detail in the hyperelliptic setting in Section 4.3.5. There we also show that M is of order $\mathcal{O}(\sqrt{N})$ and therefore the computational cost of computing the necessary a_n is $\mathcal{O}(N)$.

Chapter 4

L-functions of hyperelliptic curves

4.1 Introduction

In this chapter, we present an algorithm for the computation of all $L_\mathfrak{p}$ and $f_\mathfrak{p}$ for a family of hyperelliptic curves over $\mathbb{Q}$ with semistable reduction everywhere. The chapter is a slightly modified version of a paper by Irene I. Bouw, Stefan Wewers, and the author of this thesis [BBW16]. We adapted the notation and removed § 1.1 and some duplicate discussions especially in § 4.2 of [BBW16].

Throughout this chapter let Y be a smooth projective curve of genus $g_Y \geq 2$ over a number field K.

4.1.1 Current developments

The main motivation for this paper, which continues a project begun in [BW16], is the question how to compute the local L-factor $L_\mathfrak{p}(Y,s)$ and the conductor exponent $f_\mathfrak{p}$ explicitly, given the curve Y and the prime $\mathfrak{p}$. If the curve Y has good reduction at $\mathfrak{p}$, which is true for almost all $\mathfrak{p}$, it is well known how to do that. Namely, $f_\mathfrak{p} = 0$ and $L_\mathfrak{p}(Y,s) = P(\bar{Y},(\mathsf{N}(\mathfrak{p}))^{-s})^{-1}$, where $P(\bar{Y},T) \in \mathbb{Z}[T]$ is the numerator of the zeta function of the reduction $\bar{Y}$ of Y at $\mathfrak{p}$. To compute $P(\bar{Y},T)$ it suffices to count the number of $\mathbb{F}_{q^n}$-rational points on $\bar{Y}$, for $q = \mathsf{N}(\mathfrak{p})$ and $n = 1,\ldots,g_Y$. The complexity of this approach is bounded by $\mathcal{O}(q^{g_Y})$. There is an extensive literature dealing with various methods for lowering this asymptotic bound, see e.g. [GH00], [Ked01], and [KS08].

If Y has bad reduction at $\mathfrak{p}$ it is not so easy to compute $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ directly from the curve Y, even if $\mathsf{N}(\mathfrak{p})$ is very small. Prior to [BW16], a general and systematic approach was known for $g_Y = 1$ and for $g_Y = 2$ in the case that q is odd. Alternative approaches do not allow one to compute $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ directly at the finitely many primes of bad reduction. For example, Dokchitser, de Jeu, and Zagier [DdJZ06] guess $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ for the primes $\mathfrak{p}$ of bad reduction and verify the guess by checking that the functional equation holds. Booker ([Boo05], [Boo03]) assumes (FEq) to hold and uses a sophisticated approach to numerically construct candidates for the coefficients at the bad primes.

In this paper we compute $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ directly for a certain class of hyperelliptic curves at all primes $\mathfrak{p}$, including the primes of bad reduction. Our result does not depend on the assumption that the functional equation holds. Instead, we use our results to verify the functional equation (FEq) numerically in many concrete cases, using the method of Dokchitser [Dok04].

Our approach to calculate the local L-factor $L_\mathfrak{p}$ and the conductor exponent $f_\mathfrak{p}$ for the bad primes $\mathfrak{p}$ is based the results of [BW16] and [RW]. The key ingredient is the calculation of the semistable reduction of Y at the bad primes. Prior to [BW16] and this paper, a direct computation of $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ at bad primes was usually done using regular models (see e.g. [Sto08] and [FHS07]). In [BW16] we argue that using semistable reduction is actually easier and more powerful. One intention of the present paper is to provide further evidence for this claim by applying our method to many curves over $\mathbb{Q}$ of genus up to 6.

The sign of the functional equation (FEq) is also known to be a product of local factors, the so-called *local root numbers* ([DM69]). In principle, it should be possible to compute the local root numbers using our methods, but we have not tried to do that. Assuming that the functional equation holds, the sign is of course determined by our numerical verification.

We expect that our approach enables the computation of the L-series of chosen curves with much larger conductor N and genus g_Y than was previously possible. However, we have not tried to push computations to their limit. Our largest case is a curve with $g_Y = 6$ and $N = 7 \cdot 11 \cdot 13 \cdot 89 \cdot 431 \cdot 857 \approx 3 \cdot 10^{10}$. This conductor is comparable to the largest conductor that was considered in [DdJZ06].

4.1.2 Outline

In [BW16] we discussed how to determine the local factor $L_\mathfrak{p}(Y,s)$ and the conductor exponent $f_\mathfrak{p}$ from the *stable reduction* of Y at $\mathfrak{p}$. Furthermore, we discussed how to do this explicitly for *superelliptic curves*, i.e. curves Y given by an equation of the form

$$y^n = f(x),$$

where $f \in K[x]$ is a polynomial with coefficients in K. A serious restriction that we imposed in [BW16] was that the exponent n is prime to the residue characteristic of $\mathfrak{p}$. This restriction can be removed using the results of [Arz12], [AW12], and [Rüt14]. In principle we can therefore compute $L_\mathfrak{p}(Y,s)$ and $f_\mathfrak{p}$ for all primes $\mathfrak{p}$ and all superelliptic curves. There is also no fundamental difficulty to extend our methods to curves that are not superelliptic. However, the details can get tricky, and it is rather hard to implement algorithms which work for general classes of curves.

The class of curves we consider in the present paper is constructed to illustrate the use of stable reduction in computing the local L-factor $L_\mathfrak{p}$ and the conductor exponent $f_\mathfrak{p}$. At the same time, this class is as simple as possible so that the calculations are manageable by a straightforward algorithm. It is a rather general class of hyperelliptic curves over $\mathbb{Q}$ of fixed genus $g_Y \geq 2$ described in Section 4.3.1. Within this class we search for particular curves Y that have semistable reduction at every prime number p. For each curve satisfying this condition, we compute its L-series and conductor exponent and numerically verify the functional equation.

Our method also applies to the case that Y has potentially semistable, but not semistable, reduction at a prime $\mathfrak{p}$. However, in this case the calculations get more involved, and we have not implemented algorithms that can handle such cases in a routine fashion. In Section 4.4 we discuss three cases in detail, illustrating the difficulties occurring. For a more detailed discussion and further examples we refer to [BW15].

4.1.3 Overview of the paper

The structure of the paper is as follows. In Section 4.2 we recall how to compute the local L-factor and the conductor exponent at a prime $\mathfrak{p}$ where the curve Y has semistable reduction. The explicit expression for the local L-factor and the conductor exponent can be found in Proposition 4.2.4 and Corollary 4.2.5, respectively.

In Section 4.3 we consider a rather general class of hyperelliptic curves and determine necessary and sufficient conditions for these curves to have semistable reduction everywhere (Lemmas 4.3.3 and 4.3.7). In Section 4.3.5 we summarize the algorithm for computing the local L-factor and the conductor exponent at the primes of bad reduction of the curves satisfying these conditions and for verifying the functional equation numerically. Examples are given in Section 4.3.6. In Section 4.4 three superelliptic curves that do not have semistable reduction everywhere are discussed.

All data from the examples discussed in this paper can be retrieved from
`https://github.com/reinbot/hyperell`.

Acknowledgment

We thank the referees for very useful comments and suggestions. We are grateful to one of the referees for pointing out the reference [Liu96], which contains many of the arguments from Section 4.3 to describe models of hyperelliptic curves in a similar form.

4.2 Étale cohomology of a semistable curve

Let Y be a smooth projective and absolutely irreducible curve of genus greater than or equal to 2 defined over a number field K. In this section we recall from Section 2 of [BW16] the description of the local L-factor and the conductor exponent at a prime $\mathfrak{p}$ of $\mathcal{O}_K$ in the case that Y has semistable reduction at $\mathfrak{p}$. In general, the curve Y only admits semistable reduction after passing to a finite extension. The main result of this section is an explicit, computable expression for the local L-factor and the conductor exponent in the case that no field extension is needed.

4.2.1 Local factors at good primes

For a prime $\mathfrak{p}$ of $\mathcal{O}_K$ we denote the local ring by $\mathcal{O}_{\mathfrak{p}}$, the residue field by $k = k(\mathfrak{p})$, and the norm by $q := \mathsf{N}(\mathfrak{p}) = |k(\mathfrak{p})|$.

Throughout this section we assume that Y has semistable reduction at $\mathfrak{p}$. Recall that this means that there exists a proper and flat model $\mathcal{Y}$ of Y over $\mathcal{O}_{\mathfrak{p}}$ whose special fiber $\bar{Y} := \mathcal{Y} \otimes_{\mathcal{O}_{\mathfrak{p}}} k$ is semistable, i.e. $\bar{Y}$ is reduced and has only ordinary double points as singularities. We keep the semistable model $\mathcal{Y}$ fixed and call its special fiber $\bar{Y}$ the *semistable reduction* of Y at $\mathfrak{p}$ — even though $\bar{Y}$ is not uniquely determined without further assumptions. We write $\bar{Y}_{k^{\mathrm{alg}}} := \bar{Y} \otimes_k k^{\mathrm{alg}}$ for the base change of $\bar{Y}$ to the algebraic closure k^{alg} of k. We denote the absolute Galois group of k by Γ_k. Let $\mathrm{Frob}_{\mathfrak{p}} \in \Gamma_k$ denote the arithmetic Frobenius element on k^{alg}, i.e. the element determined by

$$\mathrm{Frob}_{\mathfrak{p}}(a) = a^q \,,\ a \in k^{\mathrm{alg}} .$$

If $\mathfrak{p}$ is a prime of good reduction, it is well known that the local L-factor $L_{\mathfrak{p}}(Y, s)$ may be computed by point counting on $\bar{Y}$ (Remark 3.3.2). Moreover, the conductor exponent is zero.

In our case, where $\bar{Y}$ is semistable, this generalizes as follows. Let $H^i_{\text{ét}}(\bar{Y}_{k^{\mathrm{alg}}}, \mathbb{Q}_\ell)$ be the ith ℓ-adic étale cohomology group of $\bar{Y}_{k^{\mathrm{alg}}}$, for an auxiliary prime ℓ different from the residue characteristic of $\mathfrak{p}$. Write $\mathrm{Frob}_{\bar{Y}} : \bar{Y} \to \bar{Y}$ for the relative k-Frobenius morphism. For $n \in \mathbb{N}$ let $\mathbb{F}_{q^n} \subset k^{\mathrm{alg}}$ be the finite extension of $k = \mathbb{F}_q$ of degree n. The *zeta function* of $\bar{Y}$ is defined as

$$Z(\bar{Y}, T) := \exp\Big(\sum_{n \geq 1} |\bar{Y}(\mathbb{F}_{q^n})| \cdot \frac{T^n}{n} \Big).$$

It is well known that $Z(\bar{Y}, T)$ is a rational function of the form

$$Z(\bar{Y}, T) = \frac{P_1(T)}{P_0(T) \cdot P_2(T)},$$

where

$$P_i(T) := \det(1 - T \cdot \mathrm{Frob}_{\bar{Y}} \mid H^i_{\text{ét}}(\bar{Y}_{k^{\mathrm{alg}}}, \mathbb{Q}_\ell)).$$

See e.g. [Mil80, Cpt. VI, Thm. 13.1]. The following proposition expresses the local L-factor $L_{\mathfrak{p}}$ and the conductor exponent $f_{\mathfrak{p}}$ in terms of invariants of the semistable reduction $\bar{Y}$ of Y at $\mathfrak{p}$ in our situation, where Y has semistable reduction at $\mathfrak{p}$.

Proposition 4.2.1 (Local L-factor)

The local L-factor is given by the formula

$$L_{\mathfrak{p}}(Y/K, s) = P_1(q^{-s})^{-1},$$

where $P_1(T) \in \mathbb{Z}[T]$ is the numerator of the zeta function of $\bar{Y}$. The conductor exponent is

$$f_{\mathfrak{p}} = 2g_Y - \dim H^1_{ét}(\bar{Y}_{k^{\mathrm{alg}}}, \mathbb{Q}_\ell) = 2g_Y - \deg(P_1).$$

Proof: This follows directly from [BW16, Cor. 2.5 and 2.6], since we assume that Y has semistable reduction at $\mathfrak{p}$. □

Remark 4.2.2 (Zeta function)

Proposition 4.2.1 relates the local L-factor $L_{\mathfrak{p}}(Y/K, s)$ to the zeta function of the semistable reduction $\bar{Y}$ of Y at $\mathfrak{p}$. To see this, we first note that the numerator of the zeta function can be expressed as follows. Since $\bar{Y}_{k^{\mathrm{alg}}}$ is connected we have $H^0_{\text{ét}}(\bar{Y}_{k^{\mathrm{alg}}}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell$. The Frobenius morphism $\mathrm{Frob}_{\bar{Y}}$ acts trivially, hence we obtain

$$P_0(T) = 1 - T.$$

Let $\bar{Y}_i$ denote the irreducible components of $\bar{Y}$, and let m_i denote the number of irreducible components of $\bar{Y}_i \otimes k$. Then

$$P_2(T) = \prod_i \left(1 - (qT)^{m_i}\right). \tag{4.2.1}$$

We conclude that to determine the numerator $P_1(T)$ of the zeta function, and hence the local L-factor, it suffices to determine the zeta function of $\bar{Y}$. We conclude that if the semistable reduction $\bar{Y}$ of Y at $\mathfrak{p}$ is known explicitly, in a suitable sense, we can compute both P_2 and the zeta function of $\bar{Y}$ by point counting. This yields an expression for the local L-factor. By 'explicit description' we mean, for example, that we have given the irreducible components of $\bar{Y}$ by equations and have a description of the intersections.

As seen in Equation (3.3.2), the polynomial $P_1(T)$ has the form

$$P_1(T) = 1 + c_1 T + \ldots + c_{2g_Y} T^{2g_Y} \in \mathbb{Z}[T].$$

If $\bar{Y}$ is smooth, the zeta function of $\bar{Y}$ satisfies a functional equation ([Mil80, Cpt. VI, Thm. 12.6]). Therefore the c_i fulfill the mirror rule

$$c_{2g_Y - i} = q^{g_Y - i} c_i, \quad i = 0, \ldots, g_Y.$$

Hence P_1 is already determined by the coefficients $c_0, \ldots, c_{g_Y}$.

In the case that $\bar{Y}$ is semistable, but not smooth, the numerator of the zeta function does not necessarily satisfy a functional equation. In order to reduce the cost of the calculation of P_1, we use that P_1 decomposes into a part determined by the loops and a part coming from the normalization of $\bar{Y}$. The last part satisfies a functional equation, and to compute it we may again use the functional equation to reduce the calculation costs. We refer to Proposition 4.2.4 for a description in the the case that $\bar{Y}$ is absolutely irreducible. ◁

Remark 4.2.3 (Bounds on point counting)

We numerically verify the functional equation using the method of Dokchitser [Dok04]. To do this, it suffices to know the first coefficients a_n of the L-function $L = \sum_n a_n/n^s$ for n up to a certain bound M (see also Section 4.3.5). In terms of the Euler-product representation of the L-series this means that for many of the local L-factors we do not need to compute all coefficients up to c_{2g_Y}. Hence we only count points on $\bar{Y}$ over fields $\mathbb{F}_{q^n}$ for $q^n \leq M$. ◁

4.2.2 Local factors and conductor exponent at bad primes

In the rest of this paper we always consider one prime $\mathfrak{p}$ at a time. For convenience, we therefore mostly drop $\mathfrak{p}$ from the notation, if no confusion may arise. Moreover, we write from now on

$$L_{\mathfrak{p}}(\bar{Y}, T)^{-1} = P(\bar{Y}, T)$$

for the numerator P_1 of the zeta function of $\bar{Y}$.

In Remark 4.2.2 we showed that we can compute the local L-factor of Y at a prime $\mathfrak{p}$ of semistable reduction, provided we know an explicit description of the stable reduction $\bar{Y}$ at $\mathfrak{p}$. In this section, we assume that the curve $\bar{Y}$ is absolutely irreducible. This assumption is satisfied for all examples considered in this paper, in particular the class of curves considered in Section 4.3.

Let

$$\pi : \bar{Y}_0 \to \bar{Y}$$

be the normalization of $\bar{Y}$. Then $\bar{Y}_0$ is a smooth projective absolutely irreducible curve and π a finite birational morphism.

Let $\xi \in \bar{Y}$ be a closed point. The fiber $\pi^{-1}(\xi)$ has degree one over $k(\xi)$ if ξ is a smooth point and degree two if ξ is an ordinary double point. An ordinary double point ξ is called *split* (resp. *nonsplit*) if $\pi^{-1}(\xi)$ consists of two points (resp. of one point).

The zeta function of $\bar{Y}_0$ has the form:

$$Z(\bar{Y}_0, T) = \frac{P(\bar{Y}_0, T)}{(1-T)(1-qT)}.$$

Since $\bar{Y}_0$ is smooth, Remark 4.2.2 applies to $P(\bar{Y}_0, T)$. The form of the denominator follows from the assumption that the reduced curve $\bar{Y}$ is absolutely irreducible.

The following result reduces the calculation of the local L-factor in our situation to a characterization of the ordinary double points and point counting on the normalization $\bar{Y}_0$ of $\bar{Y}$.

Proposition 4.2.4 (Decomposition of local factor)

Let $\mathcal{S}$ denote the set of singular points of $\bar{Y}$. For $\xi \in \mathcal{S}$ we let $d_\xi := [k(\xi) : k]$ denote the degree of ξ. Furthermore, define $\varepsilon_\xi := 1$ (resp. $\varepsilon_\xi := -1$) if ξ is a split (resp. a nonsplit) double point. Then

$$P(\bar{Y}, T) = P(\bar{Y}_0, T) \cdot \prod_{\xi \in \mathcal{S}} (1 - \varepsilon_\xi T^{d_\xi}).$$

Proof: Lemma 2.7.(1) of [BW16] implies that the ℓ-adic étale cohomology group of $\bar{Y}$ decomposes as a direct sum of Γ_k-modules

$$H^1_{\text{ét}}(\bar{Y}_{k^{\text{alg}}}, \mathbb{Q}_\ell) = H^1_{\text{ét}}(\bar{Y}_{0,k^{\text{alg}}}, \mathbb{Q}_\ell) \oplus H^1(\Delta_{\bar{Y}_{k^{\text{alg}}}}, \mathbb{Q}_\ell),$$

where $\Delta_{\bar{Y}_{k^{\text{alg}}}}$ denotes the graph of components of $\bar{Y}_{k^{\text{alg}}}$. Therefore, it suffices to show that

$$\det(1 - T \cdot \text{Frob}_{\mathfrak{p}} \mid H^1(\Delta_{\bar{Y}_{k^{\text{alg}}}}, \mathbb{Q}_\ell)) = \prod_{\xi \in \mathcal{S}} (1 - \varepsilon_\xi T^{d_\xi}).$$

This amounts to computing the character of the representation of Γ_k acting on $H^1(\Delta_{\bar{Y}_{k^{\text{alg}}}}, \mathbb{Q}_\ell)$. This is described in Lemma 2.7.(2) of [BW16].

Since we assume that $\bar{Y}$ is a semistable, absolutely irreducible curve, the graph of components $\Delta_{\bar{Y}_{k^{\text{alg}}}}$ is a bouquet of

$$\sum_{\xi \in \mathcal{S}} d_\xi$$

simple loops. This is exactly the number of ordinary double points of $\bar{Y}_{k^{\text{alg}}}$.

An element $\xi \in \mathcal{S}$ corresponds to a Γ_k-orbit of edges of $\Delta_{\bar{Y}_{k^{\text{alg}}}}$. Furthermore, ξ is a split (resp. nonsplit) ordinary double point if and only if the stabilizer $\Gamma_{k(\xi)}$ acts trivially (resp. acts by reversing orientation) on any of the edges in the orbit corresponding to ξ.

Lemma 2.7.(2) of [BW16] implies that the character of $H^1(\Delta_{\bar{Y}_{k^{\mathrm{alg}}}}, \mathbb{Q}_\ell)$ considered as Γ_k-representation is

$$\chi_{\mathrm{sing}} := \bigoplus_{\xi \in \mathcal{S}} \mathrm{Ind}_{\Gamma_{k(\xi)}}^{\Gamma_k} \varepsilon_\xi. \tag{4.2.2}$$

Here we interpret the integer $\varepsilon_\xi \in \{\pm 1\}$ as the character of a 1-dimensional representation of $\Gamma_{k(\xi)}$. Namely, ε_ξ is the trivial character if $\varepsilon_\xi = 1$ and the unique character of order 2 if $\varepsilon_\xi = -1$. The statement of the proposition now follows from an elementary calculation. For a proof which does not use étale cohomology, see [AP96]. □

Corollary 4.2.5 (Conductor exponent)

The conductor exponent is

$$f_{\mathfrak{p}} = \sum_{\xi \in \mathcal{S}} d_\xi.$$

Proof: This is a special case of [BW16, Cor. 2.6]. □

4.3 Hyperelliptic curves with semistable reduction everywhere

In this section we consider a class of hyperelliptic curves of genus greater than or equal to 2 that are defined over a number field K. We find conditions on the defining equation which guarantee that the curve has semistable reduction at every prime. This makes it relatively easy to calculate the local L-factor at the bad primes, even for residue characteristic $p = 2$.

4.3.1 Setting

We fix a number field K, an integer $g_Y \geq 2$, and two polynomials $g, h \in \mathcal{O}_K[x]$ satisfying the following three conditions.

- The polynomial g is monic, of degree $2g_Y + 1$.
- The degree of h is at most g_Y.
- The polynomial $f := 4g + h^2$ has no multiple roots.

Let Y be the smooth projective curve over K that is birationally given by the affine equation

$$y^2 + h(x)y = g(x). \tag{4.3.1}$$

The assumptions imply that Y is a hyperelliptic, absolutely irreducible curve of genus g_Y. An alternative equation for Y is

$$u^2 = f(x) = 4g(x) + h(x)^2, \tag{4.3.2}$$

where $u := 2y + h(x)$. Depending on the residue characteristic considered either (4.3.1) or (4.3.2) will be more useful.

Equation (4.3.1) defines a smooth affine plane curve, which is an affine open of Y. Let $\infty \in Y$ denote the unique point not contained in this affine open. It will be useful to have a similar equation for a neighborhood of ∞. For this we set $z := x^{-1}$, $w := z^{g_Y+1}y$, $g^* := z^{2g_Y+2}g$ and $h^* := z^{g_Y+1}h$. Considering g^*, h^* as polynomials in z, (4.3.1) can be rewritten as

$$w^2 + h^*(z)w = g^*(z). \tag{4.3.3}$$

This is again an equation for a smooth plane curve, and the point ∞ has coordinates $(z, w) = (0, 0)$. Note that we used the assumption that g has odd degree to prove smoothness at ∞. See also [Liu96, Sec. 1.1].

4.3.2 Reduction

We choose a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. As in Section 4.2 we denote by $\mathcal{O}_\mathfrak{p}$ the local ring and by $k = k(\mathfrak{p})$ the residue field of $\mathfrak{p}$. Let $\mathcal{X} = \mathbb{P}^1_{\mathcal{O}_\mathfrak{p},x}$ be the projective line over $\mathcal{O}_\mathfrak{p}$, with coordinate x. Write $\mathcal{Y}$ for the normalization of $\mathcal{X}$ in the function field $K(Y)$ of Y. For convenience, we write X for the generic fiber of $\mathcal{X}$ and $K(X)$ for its function field.

We denote by $\bar{Y}$ and $\bar{X}$ the special fibers of $\mathcal{Y}$ and $\mathcal{X}$, respectively. These are proper curves over k and $\bar{X} = \mathbb{P}^1_k$. The following proposition states that the curve $\bar{Y}$ is completely determined by the reduction of the affine equation (4.3.1) modulo $\mathfrak{p}$.

Proposition 4.3.1 (Special fiber)

The curve $\bar{Y}$ is reduced and absolutely irreducible. The point ∞ reduces to a smooth point $\bar{\infty} \in \bar{Y}$, and the affine open part $\bar{Y} \setminus \{\bar{\infty}\}$ is a plane curve with equation

$$\bar{y}^2 + \bar{h}(\bar{x})\bar{y} = \bar{g}(\bar{x}). \tag{4.3.4}$$

Here $\bar{x}, \bar{y}$ are the images of x, y in the function field of $\bar{Y}$, and $\bar{g}$ (resp. $\bar{h}$) are the images of g (resp. h) in $k[\bar{x}]$.

Proof: This is a special case of Corollary 2.2.7. □

4.3.3 Even characteristic

We continue with the notation and assumptions of Sections 4.3.1 and 4.3.2. Additionally, we assume that the residue field k has characteristic $p = 2$.

Notation 4.3.2

Let $\xi \in \bar{Y} \setminus \{\bar{\infty}\}$ be a closed point and $k(\xi)$ the residue field of ξ. We consider $\bar{Y} \setminus \{\bar{\infty}\}$ as an affine plane curve with coordinate functions $\bar{x}, \bar{y}$. Define $a, b \in k(\xi)$ by $\xi = (a, b)$, which implies $k(\xi) = k(a, b)$.

Lemma 4.3.3 (Conditions for singularities)

Let $\xi = (a, b) \in \bar{Y} \setminus \{\bar{\infty}\}$ be a closed point.

i) The point ξ is a singularity of $\bar{Y}$ if and only if

$$\bar{h}(a) = 0 = (\bar{h}'(a))^2 \bar{g}(a) + (\bar{g}'(a))^2. \tag{4.3.5}$$

Here $\bar{h}', \bar{g}' \in k[\bar{x}]$ are the formal derivatives of $\bar{h}, \bar{g}$ with respect to $\bar{x}$.

ii) Assume that ξ is a singularity. Then ξ is an ordinary double point if and only if $\bar{h}'(a) \neq 0$.

A similar statement can be found in [Liu96, Lem. 5 and 6].

Proof: Since $\xi = (a, b) \neq \{\bar{\infty}\}$ we may use the affine equation (4.3.4) and get

$$b^2 + \bar{h}(a) b = \bar{g}(a). \tag{4.3.6}$$

The Jacobian criterion implies that ξ is singular if and only if

$$\bar{h}(a) = 0, \quad \bar{h}'(a) b = \bar{g}'(a). \tag{4.3.7}$$

Inserting (4.3.7) into (4.3.6) yields (4.3.5), as we are in characteristic 2.

For the proof of *ii)* we assume that ξ is singular and compute the tangent cone of $\bar{Y}$ at ξ using (4.3.6) and (4.3.7). It is given by

$$(\bar{y} + b)^2 + \bar{h}'(a)(\bar{y} + b)(\bar{x} + a) + \bar{g}_2 (\bar{x} + a)^2 = 0,$$

where $\bar{g}_2$ is the coefficient of $\bar{x}^2$ in the Taylor expansion of $\bar{g}$ at $\bar{x} = a$. As we are in characteristic 2, the underlying quadratic form is nondegenerate if and only if $\bar{h}'(a) \neq 0$. This proves *ii)*. □

Corollary 4.3.4 (Semistable reduction)

The curve $\bar{Y}$ is semistable if and only if $\bar{h} \neq 0$ and

$$\gcd(\bar{h}, \bar{h}', \bar{g}') = 1.$$

Proof: It suffices to show that $\xi = (a, b) \in \bar{Y} \setminus \{\bar{\infty}\}$ is a smooth or an ordinary double point if and only if $(\bar{h}(a), \bar{h}'(a), \bar{g}'(a)) \neq (0, 0, 0)$. This follows from Lemma 4.3.3. □

From now on we assume that $\bar{Y}$ is semistable and use the results from Section 4.2 to compute the local L-factor and the conductor exponent of Y at $\mathfrak{p}$. Let

$$\pi : \bar{Y}_0 \to \bar{Y}$$

be the normalization of $\bar{Y}$, as in Section 4.2.

In order to use Proposition 4.2.4 and Corollary 4.2.5 we need to know the set $\mathcal{S}$ of singular points of $\bar{Y}$, the invariants d_ξ and ε_ξ for all $\xi \in \mathcal{S}$, and an explicit equation for $\bar{Y}_0$. This will be achieved by the following proposition and Corollary 4.3.6.

Proposition 4.3.5 (Singularities in terms of g and h)

Assume that $\bar{Y}$ is semistable. Set

$$r := \gcd(\bar{h}, (\bar{h}')^2\bar{g} + (\bar{g}')^2) \in k[\bar{x}].$$

Then the following holds.

i) A point $\xi = (a,b) \in \bar{Y} \setminus \{\bar{\infty}\}$ is singular if and only if $r(a) = 0$.

ii) The polynomial r is separable, i.e. all roots of r over the algebraic closure k^{alg} of k are simple. Moreover, $\tilde{h} := \bar{h}/r \in k[\bar{x}]$ is prime to r.

iii) There exists an $s \in k[\bar{x}]$ such that

$$r^2 \mid \bar{g} + s^2 + \bar{h}s.$$

iv) Set $\tilde{g} := (\bar{g} + s^2 + \bar{h}s)/r^2 \in k[\bar{x}]$ and $\tilde{y} := (\bar{y} + s)/r \in k(\bar{Y})$. Then $\tilde{y}$ satisfies

$$\tilde{y}^2 + \tilde{h}\tilde{y} = \tilde{g}, \tag{4.3.8}$$

which is an equation for the smooth plane affine curve $\bar{Y}_0 \setminus \{\bar{\infty}\}$.

A similar statement can be found in [Liu96, Rem. 2].

Proof: Claim *i)* follows directly from Lemma 4.3.3.i). Assume that a is a root of r. Then there is a unique point $\xi = (a,b) \in \bar{Y}$, and it is a singularity. Since we assume that $\bar{Y}$ is semistable, ξ is even an ordinary double point. Therefore, it follows from Lemma 4.3.3.ii) that $\bar{h}'(a) \neq 0$. We conclude that all roots of r are simple roots of $\bar{h}$. This proves *ii)*.

Since k is a perfect field of characteristic 2 and r is separable by *ii)*, there exists a polynomial $s \in k[\bar{x}]$ such that

$$s^2 \equiv \bar{g} \pmod{r}.$$

Set $\tilde{y} := (\bar{y} + s)/r \in k(\bar{Y})$, then $\tilde{y}$ satisfies Equation (4.3.8).

For *iii)* we have to show that $\tilde{g} = (\bar{g} + s^2 + \bar{h}s)/r^2$ is a polynomial. Assume that $a \in k$ is a pole of $\tilde{g}$. By *ii)* r has a simple zero at a. The choice of s implies that $\bar{h}$ also has a simple zero at a, and hence that $\tilde{g}$ has a simple pole at $\bar{x} = a$. But this implies that the map $\bar{Y}_0 \to \bar{X} = \mathbb{P}^1_k$ is branched at $\bar{x} = a$. Hence there exists a unique smooth point $\xi = (a, b) \in \bar{Y}$ above $\bar{x} = a$, contradicting the fact that $r(a) = 0$. Now *iii)* is proved.

It follows from *iii)* that there is a finite birational morphism $\bar{Y}_1 \to \bar{Y}$ which is an isomorphism at $\bar{\infty}$ and such that $\bar{Y}_1 \setminus \{\bar{\infty}\}$ is the plane affine curve given by (4.3.8). Let $\xi = (a, b) \in \bar{Y}_1 \setminus \{\bar{\infty}\}$ be a closed point. If ξ is a singular point, then $\tilde{h}(a) = 0$ by the Jacobian criterion. But then $r(a) \neq 0$ by *ii)* and the definition of $\tilde{h}$. Therefore ξ lies above a smooth point of $\bar{Y}$. Since $\bar{Y}_1 \to \bar{Y}$ is finite, it follows that ξ is also a smooth point. We obtain a contradiction and conclude that $\bar{Y}_1$ is smooth. So $\bar{Y}_1 = \bar{Y}_0$ is the normalization of $\bar{Y}$. □

The following corollary follows from Proposition 4.3.5 and Corollary 4.2.5.

Corollary 4.3.6

Assume that $\bar{Y}$ is semistable.

i) There is a bijection between the set $\mathcal{S}$ of singular points of $\bar{Y}$ and the irreducible factors of the polynomial $r \in k[\bar{x}]$ defined in Proposition 4.3.5.

ii) A singular point $\xi = (a, b) \in \bar{Y}$ is a split (resp. a non split) ordinary double point if the polynomial

$$T^2 + \tilde{h}(a)T + \tilde{g}(a) \in k(a)[T]$$

is reducible (resp. irreducible).

iii) The conductor exponent at $\mathfrak{p}$ is

$$f_{\mathfrak{p}} = \deg(r).$$

4.3.4 Odd characteristic

We now switch to the case of a prime $\mathfrak{p}$ with residue characteristic $p \geq 3$. It will be more convenient to use Equation (4.3.2) to describe the curve Y:

$$u^2 = f(x) := 4g(x) + h(x)^2.$$

Recall that this equation is derived from (4.3.1) by the substitution $y = (u - h)/2$. Since 2 is a unit in $\mathcal{O}_{\mathfrak{p}}$, the same substitution works for the model $\mathcal{Y}$. It follows that the special fiber $\bar{Y}$ of $\mathcal{Y}$ is given by the equation

$$\bar{u}^2 = \bar{f}(\bar{x}). \tag{4.3.9}$$

Here $\bar{f} \in k[\bar{x}]$ denotes the image of f in $k[\bar{x}]$ and $\bar{u}$ the image of u in $k(\bar{Y})$. We also adopt Notation 4.3.2 to this new equation and write a closed point $\xi \in \bar{Y} \setminus \{\bar{\infty}\}$ in the form $\xi = (a, b)$, where (a, b) is a solution to (4.3.9).

Note that the assumption that g is a monic polynomial of degree $2g_Y + 1$ and that h has degree $\leq g_Y$ implies that both f and $\bar{f}$ have degree $2g_Y + 1$. The polynomial f is separable by assumption, but in general this will not be true for $\bar{f}$. The following statement is easy to show — the proof is left to the reader.

Lemma 4.3.7 (Condition for semistable curve)

The curve $\bar{Y}$ is semistable if and only if $\bar{f}$ has at most double roots.

We assume from now on that the curve $\bar{Y}$ is semistable. Lemma 4.3.7 implies that the polynomial $\bar{f}$ has at most double roots. It follows that there is a unique decomposition

$$\bar{f} = r^2 \cdot s,$$

where $r, s \in k[\bar{x}]$ are separable and relatively prime.

Proposition 4.3.8

We assume that $\bar{Y}$ is semistable. Let $\xi = (a, b) \in \bar{Y} \setminus \{\bar{\infty}\}$ be a closed point.

i) The point ξ is a singularity of $\bar{Y}$ if and only if $r(a) = 0$.

ii) Assume that ξ is a singularity. Then ξ is a split (resp. a nonsplit) ordinary double point if and only if $s(a)$ is a square (resp. a nonsquare) in $k(\xi)^\times$.

iii) The normalization $\bar{Y}_0$ of $\bar{Y}$ is given by the equation

$$\bar{v}^2 = s(\bar{x}).$$

More precisely, the map $\bar{Y}_0 \to \bar{Y}$ is determined by $\bar{u} = r\bar{v}$.

Proof: The proof is similar to but easier than the proof of Proposition 4.3.5 and is therefore omitted. □

The following corollary is the analogous statement to Corollary 4.3.6 for odd primes. It follows from Proposition 4.3.8.

Corollary 4.3.9

Assume that $\bar{Y}$ is semistable.

i) There is a bijection between the set $\mathcal{S}$ of singular points of $\bar{Y}$ and the irreducible factors of the polynomial r.

ii) For $\xi = (a,b) \in \mathcal{S}$ we have $\varepsilon_\xi = 1$ (resp. $\varepsilon_\xi = -1$) if and only if $s(a)$ is a square (resp. a nonsquare) in $k(a)^\times$.

iii) The conductor exponent is

$$f_\mathfrak{p} = \deg(r).$$

4.3.5 Algorithm

In this section we summarize the results obtained so far and describe the resulting algorithm for computing the L-function of the curve Y. We also make some comments on implementation, running time and numerical precision. For simplicity we assume from now on that $K = \mathbb{Q}$.

We are interested in computing the L-series of a curve Y/K given as an Euler product,

$$L(Y/K,s) = \sum_{n\geq 1} \frac{a_n}{n^s} = \prod_p L_p(Y,s).$$

More specifically, we want to give evidence for the conjectured functional equation (FEq). We use the `Dokchitser` package in the free computer algebra software *Sage*, based on Tim Dokchitser's paper [Dok04]. We can verify the functional equation in this package up to a given numerical precision. For that we need to know the conductor of the L-function,

$$N = \prod_p p^{f_p},$$

and the coefficients a_n need to be calculated for all $n \leq M$ up to a certain heuristic constant M, depending on N and g_Y. The constant M can be computed using the `Dokchitser` package. Since the determination of M in [Dok04] relies on heuristic arguments, we do not have a proof that our computations are correct up to a certain precision. Using the results of [Bra10] it might be possible to give provably correct bounds for the precision, but we have not tried to do that.

Within *Sage*, the numerical verification of the functional equation was carried out using 53 bits of precision, which corresponds to a significand with 15 decimal digits. We defined the functional equation to be verified if the return value of `check_functional_equation()` from the `Dokchitser` package was below 10^{-14}.

The coefficients a_n of the series expansion of the L-function are weakly multiplicative. Therefore it suffices to compute the coefficients a_{p^k} for all prime powers $p^k \leq M$. This can be done by point counting. If one uses naive point counting methods, the calculation of each a_{p^k} has a complexity of about $\mathcal{O}(p^k)$. By the Prime Number Theorem, we get a complexity of $\mathcal{O}((M/2) \cdot (M/\log(M)))$ for each L-series. For fixed genus, M is proportional to the square root of the conductor N of the curve (cf. [Dok04]). So the complexity of checking the functional equation is bounded by $\mathcal{O}(N/\log N)$.

Finding examples of suitable curves Y satisfying the condition from Section 4.3.1 and checking the functional equation of $L(Y,s)$ can be performed as follows. We fix an integer $g_Y \geq 2$.

1. Choose polynomials $g,h \in \mathbb{Z}[x]$ with g monic, $\deg(g) = 2g_Y + 1$, $h \not\equiv 0 \pmod 2$, and $\deg(h) \leq g_Y$. Consider their reductions $\bar{g}, \bar{h}$ modulo 2. If

$$\gcd(\bar{h}, \bar{h}', \bar{g}') \neq 1,$$

the model $\mathcal{Y}$ from Section 4.3.2 is not semistable at $p = 2$ (Corollary 4.3.4). In this case we dismiss our choice of g and h and start over. Otherwise, compute the polynomial

$$r := \gcd(\bar{h}, (\bar{h}')^2\bar{g} + (\bar{g}')^2).$$

2. Calculate the discriminant $\Delta \in \mathbb{Z}$ of the polynomial $f := 4g + h^2$, and define S' as the set of prime factors of Δ, ignoring the prime factor 2. Check for each $p \in S'$ whether

$$\gcd(\bar{f}, \bar{f}', \bar{f}'') = 1,$$

where $\bar{f}$ is the reduction of $\bar{f}$ mod p for the given prime p. If the test fails for one $p \in S'$, we cannot guarantee that Y has semistable reduction (Lemma 4.3.7). So we dismiss our example and go back to the beginning.

In the case that $\gcd(\bar{f}, \bar{f}', \bar{f}'') = 1$ we consider the degree of r. If $\deg r > 1$ then we set $S := S' \cup \{2\}$, otherwise set $S := S'$.

Now we know that Y has bad semistable reduction at all primes $p \in S$ and good reduction everywhere else.

3. For each bad prime $p \in S$, we do the following.

3*a*. If $p = 2$, decompose the polynomial $r \in \mathbb{F}_2[\bar{x}]$ into irreducible factors:

$$r = \prod_i r_i.$$

Each factor r_i corresponds to a singularity $\xi_i \in \bar{Y}$ with $\deg(\xi_i) = \deg(r_i)$. Check for each i whether ξ_i is split or not (Prop. 4.2.4 and Corollary 4.3.6 ii)) and set $\varepsilon_i \in \{\pm 1\}$, accordingly.

Now calculate the numerator $P(\bar{Y}_0, T)$ of the zeta function of the normalization $\bar{Y}_0$ of $\bar{Y}$, using Equation (4.3.8) and point counting (Remark 4.2.2 and Remark 4.2.3).

The local L-factor at $p = 2$ is

$$L_2(\bar{Y}, T) = P(\bar{Y}_0, T)^{-1} \cdot \prod_i (1 - \varepsilon_i T^{d_i})^{-1}$$

(Proposition 4.2.4). Also, set $f_2 = \deg(r)$ (Corollary 4.3.6.iii)).

3*b*. If $p \in S'$, compute the decomposition

$$\bar{f} = r^2 s.$$

Decompose $r = \prod_i r_i \in \mathbb{F}_p[\bar{x}]$ into irreducible factors. Set $d_i := \deg(r_i)$ and $\varepsilon_i := \pm 1$, as in Corollary 4.3.9.ii).

Calculate the numerator $P(\bar{Y}_0, T)$ of the zeta function of the normalization $\bar{Y}_0$ of $\bar{Y}$ using the equation from Proposition 4.3.8.iii). As in 3a, the local L-factor is

$$L_p(\bar{Y}, T) = P(\bar{Y}_0, T)^{-1} \cdot \prod_i (1 - \varepsilon_i T^{d_i})^{-1}.$$

Set $f_p := \deg(r)$ (Corollary 4.3.9.iii)).

4. Compute the conductor

$$N := \prod_{p \in S} p^{f_p}$$

and the constant M using the `Dokchitser` package.

5. Calculate the local L-factor $L_p(Y, s)$ for all good primes $p \notin S$, $p \leq M$ via point counting (Remarks 4.2.2 and 4.2.3).

6. Compute the truncated L-series

$$L(Y, s)' = \sum_{n=1}^{M} \frac{a_n}{n^s}$$

from the local factors $L_p(Y, s)$, $p \leq M$. Check (FEq) using the `Dokchitser` package for the root number 1. If this fails, repeat with root number -1.

Remark 4.3.10 (Improvements)

The algorithm described above can be slightly improved using Remark 4.2.3. Recall that we only need coefficients a_n of the L-series with $n \leq M$. Thus we can use the bound M to truncate the polynomial $P(\bar{Y}_0, T)$, resp. the local L-factor L_p in Step 3a and 3b. For an example, we refer to Example 4.3.14 in Section 4.3.6. $\triangleleft$

In the above algorithm the time needed to compute the set of bad primes, the conductor N, the bad factors, and the constant M is insignificant compared with the time needed for the point counting. The numerical verification of the functional equation is not expensive either. Therefore, the running time of our algorithm for an individual curve Y is bounded by $\mathcal{O}(N/\log N)$ with almost all the running time spent on point counting. For the class of hyperelliptic curves considered in this section, the functional equation of curves with conductor up to about 10^{10} can be verified numerically within a reasonable time. The largest curve we considered has conductor $N = 7 \cdot 11 \cdot 13 \cdot 89 \cdot 431 \cdot 857 \approx 3 \cdot 10^{10}$. Using more sophisticated point-counting methods (see e.g. [KS08], [Ked01], [GH00], [Har14b], or [Min10]) would probably allow the computation of significantly larger examples.

The running time of the algorithm for a curve in the class we consider is essentially determined by the conductor. Although the constant M depends on N and the genus g_Y of Y, the dependence on g_Y is insignificant within the range of genera that we consider (see [Dok04, Eqn. (4-2)]). This is an advantage of our approach, as opposed to for example that of Booker ([Boo05, Sec. 2.3.2]). However, the discriminant of the polynomial $f = 4g + h^2$ (Remark 3.1.1) determines the odd prime factors of the conductor. The genus $g_Y = (\deg(g) - 1)/2$ of Y is directly connected to the degree $\deg(g) = \deg(f)$. Polynomials of larger degree obviously tend to have larger discriminants. So the larger g_Y is, the harder it is to find instances of curves Y with conductor of reasonable size, i.e. $N \leq 3 \cdot 10^{10}$. So far, we found curves that fall within this range for all $g_Y \leq 6$.

We have verified the functional equation for several hundreds of examples. These examples were constructed by searching for polynomials $g, h \in \mathbb{Z}[x]$ that satisfy the conditions of Steps 1 and 2 of the above algorithm. Among those we only picked pairs (g, h) such that the discriminant of $f := h^2 + 4g$ is relatively small. However, we did not try to do an exhaustive search for examples of this form. One can easily construct a lot more examples, especially for small genus. On our homepage, we provide a selection of examples — each with slightly different set of bad primes, conductor, and bad factors — where the functional equation has been verified. The data can be found on `https://github.com/reinbot/hyperell`.

4.3.6 Examples

In this section we give a few explicit examples in detail. All given examples fulfill (FEq). Note that the chosen examples do not necessarily have the smallest possible conductor for the given genus — it is merely a selection of showpiece examples.

Example 4.3.11 (Genus two)

The polynomials

$$g = x^5 - 3x^4 - 3x^3 - 3x^2 - 3x - 1, \quad h = x^2 + 3x + 1$$

define a genus-two curve $Y/\mathbb{Q}$.

We find five bad primes: $2, 3, 7, 101, 163$. The L-factors corresponding to these primes are as follows.

$$\begin{aligned}
L_2^{-1} &= 1 + T^2, \\
L_3^{-1} &= (1+T)(3T^2 - T + 1), \\
L_7^{-1} &= (1-T)(7T^2 + 3T + 1), \\
L_{101}^{-1} &= (1+T)(101T^2 + 3T + 1), \\
L_{163}^{-1} &= (1-T)(163T^2 + 11T + 1).
\end{aligned}$$

The conductor is $N = 2^2 \cdot 3 \cdot 7 \cdot 101 \cdot 163 \approx 10^6$.

We briefly review the computations for $p = 2, 3$. For the reduction of Y at $p = 2$ we find

$$\bar{Y}/\mathbb{F}_2 : \ \bar{y}^2 + (1 + \bar{x} + \bar{x}^2)\bar{y} = 1 + \bar{x} + \bar{x}^2 + \bar{x}^3 + \bar{x}^4 + \bar{x}^5.$$

Since $\bar{h}' = (1 + \bar{x} + \bar{x}^2)' = 1$, the curve $\bar{Y}$ is semistable. The singular locus is determined by the polynomial

$$r := \gcd(\bar{h}, (\bar{h}')^2\bar{g} + (\bar{g}')^2) = \bar{h} = 1 + \bar{x} + \bar{x}^2.$$

Hence there is a unique ordinary double point $\xi = (a, b)$ of degree 2, where a is a solution to $a^2 + a + 1 = 0$. Substituting $\bar{y} = \bar{h}\tilde{y}$ into the equation of $\bar{Y}$ and dividing by $\bar{h}^2$ we obtain as equation for the normalization $\bar{Y}_0$ of $\bar{Y}$:

$$\tilde{y}^2 + \tilde{y} = \bar{g}/\bar{h}^2 = 1 + \bar{x}.$$

This defines a curve of genus zero. So $\bar{Y}_0$ does not contribute to the local L-factor.

The inverse image $\pi^{-1}(\xi)$ of the singular point ξ in $\bar{Y}_0$ corresponds to the solutions of the equation

$$\tilde{y}^2 + \tilde{y} = 1 + a$$

in $\mathbb{F}_2(a) = \mathbb{F}_4$. Clearly, this equation is irreducible and ξ is a non-split ordinary double point. We conclude that

$$L_2^{-1} = 1 + T^2.$$

For the reduction of Y at $p = 3$ we find

$$\bar{Y}/\mathbb{F}_3 : \ \bar{u}^2 = \bar{x}^2(2 + \bar{x}^2 + \bar{x}^3).$$

This is a semistable curve with one $\mathbb{F}_3$-rational ordinary double point $\xi = (0, 0)$.

Substituting $\bar{u} = \bar{x}\bar{v}$ and dividing by $\bar{x}^2$ yields the following equation for the normalization $\bar{Y}_0$ of $\bar{Y}$:

$$\bar{Y}_0 : \ \bar{v}^2 = 2 + \bar{x}^2 + \bar{x}^3.$$

Hence $\bar{Y}_0$ is a smooth curve of genus 1 over $\mathbb{F}_3$. Since $|\bar{Y}_0(\mathbb{F}_3)| = 3$, we conclude that the numerator of the zeta function of $\bar{Y}_0$ is $P(\bar{Y}_0, T) = 1 - T + 3T^2$.

The inverse image $\pi^{-1}(\xi)$ of the singular point ξ in $\bar{Y}_0$ corresponds to the solutions of the equation

$$\bar{v}^2 = 2.$$

We conclude that ξ is a non-split double point and that

$$L_3^{-1} = (1+T)(1-T+3T^2).$$

The computation of the local L-factors for $p = 7, 101, 163$ is similar.

The numerical verification of the functional equation in *Sage* was successful, and we found that the root number is 1.

Example 4.3.12 (Genus three)

The polynomials $g = x^7 + x^6 + 2x^5 + 2x^4 + 2x^3 - 1$ and $h = -x^3 + x^2 + x + 2$ define a genus-three curve. We find four bad primes: $2, 3, 11, 37$. The local L-factors corresponding to these primes are

$$\begin{aligned} L_2^{-1} &= (1-T)(1+T)(2T^2 - T + 1), \\ L_3^{-1} &= (1+T)(1-T^2), \\ L_{11}^{-1} &= (1+T)^2(11T^2 - 4T + 1), \\ L_{37}^{-1} &= (1-T)(37^2T^4 + 148T^3 + 14T^2 + 4T + 1), \end{aligned}$$

the conductor is $N = 2^2 \cdot 3^3 \cdot 11^2 \cdot 37 \approx 10^5$, and the root number is 1.

Example 4.3.13 (Genus four)

The polynomials $g = x^9 - 2x^8 + x^7 - 2x^4 + 2x^3 + 2x^2 + x$ and $h = -2x^4 + x^3 - 2x^2 - x - 1$ define a genus-four curve. We find four bad primes: $3, 7, 31, 53$. The L-factors corresponding to these primes are

$$\begin{aligned} L_3^{-1} &= (1-T)(1+T)(9T^4 + 6T^3 + 4T^2 + 2T + 1), \\ L_7^{-1} &= (1+T^3)(7T^2 + 3T + 1), \\ L_{31}^{-1} &= (1-T)(31^3T^6 + 1581T^4 + 36T^3 + 51T^2 + 1), \end{aligned}$$

$$L_{53}^{-1} = (1+T)(53^3T^6 + 8427T^5 + 1537T^4 + 670T^3 + 29T^2 + 3T + 1),$$

the conductor is $N = 3^2 \cdot 7^3 \cdot 31 \cdot 53 \approx 10^8$, and the root number is 1.

Example 4.3.14 (Genus five)

The polynomials $g = x^{11} + 3x^4 + 2x^3 - 3x^2 - 2x$ and $h = -3x^3 + x^2 + 3x + 1$ define a genus-five curve. We find four bad primes: $7, 227, 1277, 1609$. The truncated L-factors corresponding to these primes are

$$\begin{aligned}
L_7^{-1} &= (1-T)(7^4T^8 - 588T^6 + 134T^4 - 12T^2 + 1),\\
L_{227}^{-1} &= (1+T)(\ldots + 200T^2 + 13T + 1),\\
L_{1277}^{-1} &= (1+T)(\ldots - 35T + 1),\\
L_{1609}^{-1} &= (1+T)(\ldots - 26T + 1).
\end{aligned}$$

The conductor is $N = 7 \cdot 227 \cdot 1277 \cdot 1609 \approx 10^9$, and the root number is 1. We truncated the last three L-factors to save computation time, since the bound in this example is $M = 1112661 < \{227^3, 1277^2, 1609^2\}$. Hence no further information is needed to verify the functional equation, see Remark 4.3.10.

Example 4.3.15 (Genus six)

The polynomials $g = x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 - x^7 - x^6 + x^5 + x^4 + x^3$ and $h = x^6 + x^5 - x^3 + x^2 + x + 1$ define a genus-six curve. We find six bad primes: $7, 11, 13, 89, 431, 857$. The truncated L-factors corresponding to these primes are

$$\begin{aligned}
L_7^{-1} &= (1+T)(7^5T^{10} + 1372T^8 + 1127T^7 + 112T^6 + 122T^5 + 16T^4 + 23T^3 +\\
&\qquad 4T^2 + 1),\\
L_{11}^{-1} &= (1+T)(11^5T^{10} - 43923T^9 - 10648T^8 + 2662T^7 + 781T^6 - 390T^5 +\\
&\qquad 71T^4 + 22T^3 - 8T^2 - 3T + 1),\\
L_{13}^{-1} &= (1+T)(13^5T^{10} - 114244T^9 + 43940T^8 - 10140T^7 + 1040T^6 +\\
&\qquad - 342T^5 + 80T^4 - 60T^3 + 20T^2 - 4T + 1),\\
L_{89}^{-1} &= (1-T)(\ldots + 320T^3 + 43T^2 - 5T + 1),\\
L_{431}^{-1} &= (1+T)(\ldots + 859T^2 + 31T + 1),\\
L_{857}^{-1} &= (1-T)(\ldots + 1448T^2 - 41T + 1)
\end{aligned}$$

The conductor is $N = 7 \cdot 11 \cdot 13 \cdot 89 \cdot 431 \cdot 857 \approx 3 \cdot 10^{10}$, and the root number is 1. As in the previous example, we truncated the last three L-factors, as the bound is $M = 2549728 < \{89^4, 431^3, 857^3\}$.

4.4 Generalizations

In this section we consider some cases of superelliptic curves over $K = \mathbb{Q}$ that do not have semistable reduction at all primes p. As stated in Section 4.1.2, it is in principle possible to compute the semistable reduction of any superelliptic curve of prime degree at all primes of bad reduction. From this one may compute the local L-factor and the conductor exponent for each bad prime. However, in the general situation, the calculations needed are more involved than those of the previous section. One of the main difficulties is that in general one has to pass to an extension of $\mathbb{Q}_p$. We have not implemented an algorithm in the more general situation. Still we hope that the cases we discuss here illustrate the usefulness of our method for general superelliptic curves.

4.4.1 First hyperelliptic example

The polynomials

$$g = x^7 - 2x^6 - 2x^4 + x^3 + 3x^2 + x, \quad h = 3x^3 + 3x^2 + 2x + 1$$

substituted in (4.3.1) define a hyperelliptic curve $Y/\mathbb{Q}$ of genus 3 that has good reduction at $p = 2$. We ignore the prime $p = 2$ from now on and describe Y by

$$Y/\mathbb{Q}: \; y^2 = f(x) = 4x^7 + x^6 + 18x^5 + 13x^4 + 22x^3 + 22x^2 + 8x + 1, \tag{4.4.1}$$

with $f := h^2 + 4g$. The discriminant of f is $\Delta = -2^{12} \cdot 3 \cdot 5^3 \cdot 13^2 \cdot 97$, so there are four bad primes: $p = 3, 5, 13, 97$.

For $p \in \{3, 13, 97\}$ the condition $\gcd(\bar{f}, \bar{f}', \bar{f}'') = 1$ holds, where $\bar{f}$ denotes the reduction of f mod p. We conclude that Y has semistable reduction at $p \in \{3, 13, 97\}$. The local L-factor and the conductor exponent can be computed as before, and we obtain

$$\begin{aligned} L_3^{-1} &= (1-T)(3^2T^4 + 3T^3 + T + 1), \quad f_3 = 1, \\ L_{13}^{-1} &= (1+T^2)(13T^2 + 5T + 1), \quad f_{13} = 2, \\ L_{97}^{-1} &= (1+T)(97^2T^4 + 582T^3 + 78T^2 + 6T + 1), \quad f_{97} = 1. \end{aligned}$$

The reduction of Equation (4.4.1) at $p = 5$ does not define a semistable curve. More precisely, let $\mathcal{Y}^{\text{naive}}$ denote the normalization of $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}}$ in the function field of Y, and let $\bar{Y}^{\text{naive}}$ denote the fiber of $\mathcal{Y}^{\text{naive}}$ at $p = 5$. Then $\bar{Y}^{\text{naive}}$ is an integral curve over $\mathbb{F}_5$ with an affine open subset of the form

$$\bar{Y}^{\text{naive}}/\mathbb{F}_5: \; \bar{y}^2 = \bar{f} = 4(\bar{x}+1)^4(\bar{x}^3 + \bar{x} + 4). \tag{4.4.2}$$

We see that $\bar{Y}^{\text{naive}}$ has a unique $\mathbb{F}_5$-rational singularity $(\bar{x}, \bar{y}) = (4, 0)$, which is not an ordinary double point. The curve $\bar{Y}^{\text{naive}}$ is smooth everywhere else. In particular, $\bar{Y}^{\text{naive}}$ is not semistable, and the algorithm of Section 4.3 is not directly applicable.

Using the results of [BW16, § 2], can easily compute the semistable reduction of Y at $p = 5$. Computing the stable reduction is a local problem. We may therefore consider Y as a curve over the 5-adic numbers $\mathbb{Q}_5$. Let $L := \mathbb{Q}_5[\pi]$ be the extension of degree 4 with $\pi^4 = 5$. Clearly, $L/\mathbb{Q}_5$ is a Galois extension, which is totally and tamely ramified. The Galois group of $L/\mathbb{Q}_5$ is cyclic, generated by the element σ determined by

$$\sigma(\pi) = \zeta_4\pi.$$

Here $\zeta_4 \in \mathbb{Z}_5$ is the 4th root of unity with $\zeta_4 \equiv 2 \pmod 5$. Let $\mathfrak{p} = (\pi) \lhd \mathcal{O}_L$ denote the unique prime ideal, which has residue field $k = k(\mathfrak{p}) = \mathbb{F}_5$. The following lemma states that Y acquires semistable reduction over L.

The semistable model is general not unique. In the case that we need a base extension for Y to acquire stable reduction, not every semistable model may be used to calculate the local L-factor and the conductor exponent. Since $g_Y \geq 2$, there exists a unique minimal semistable model $\mathcal{Y}$ of Y, which may be used to calculate $L_\mathfrak{p}$ and $f_\mathfrak{p}$. We refer to [BW16, § 2.3], for an explanation.

Lemma 4.4.1 (Semistable reduction)

i) The curve $Y_L = Y \otimes_{\mathbb{Q}_5} L$ has semistable reduction at $\mathfrak{p}$.

ii) Let $\mathcal{Y}/\mathcal{O}_L$ denote the minimal semistable model of Y_L and $\bar{Y}$ its special fiber. The curve $\bar{Y}$ is the union of two smooth, absolutely irreducible curves over $\mathbb{F}_5$. The first component $\bar{Y}_1$ has an affine open subset given by

$$\bar{y}_1^2 = 4(\bar{x}^3 + \bar{x} + 4). \tag{4.4.3}$$

The second component $\bar{Y}_2$ has an affine open subset given by

$$\bar{y}_2^2 = 3\bar{x}_2^4 + 2. \tag{4.4.4}$$

iii) The components $\bar{Y}_1, \bar{Y}_2$ intersect in a unique split ordinary double point ξ of degree 2. As a point on $\bar{Y}_1$, we have $\xi = (4, b)$, where $b \in \mathbb{F}_5(\xi) = \mathbb{F}_{5^2}$ is a solution to $b^2 = 3$.

iv) The generator σ of the Galois group $\mathrm{Gal}(L/\mathbb{Q}_5) = \langle\sigma\rangle$ acts trivially on $\bar{Y}_1$ and on $\bar{Y}_2$ via the automorphism of order 4

$$\bar{x}_2 \mapsto 3\bar{x}_2, \quad \bar{y}_2 \mapsto -\bar{y}_2.$$

Proof: We follow the recipe in [BW16, § 4]. The equations for $\bar{Y}_i$, $i = 1, 2$, are obtained as follows. For $\bar{Y}_1$, we substitute $y = (x+1)y_1$ in (4.4.1), divide by $(x+1)^4$ and reduce modulo $\mathfrak{p}$. Using (4.4.2) we see that we obtain Equation (4.4.3). For $\bar{Y}_2$, we substitute $x = 4 + \pi x_2$ and $y = \pi^2 y_2$, divide by 5 and reduce modulo $\mathfrak{p}$. A short computation yields (4.4.4). Statements *iii)* and *iv)* are straightforward. □

The semistable model $\mathcal{Y}$ dominates the naive model $\mathcal{Y}^{\text{naive}}$. More precisely, there is a modification, i.e. a map which is an isomorphism on the complement of a nowhere dense subset of the target space, $\mathcal{Y} \to \mathcal{Y}^{\text{naive}} \otimes_{\mathbb{Z}_5} \mathcal{O}_L$. The resulting map $\bar{Y} \to \bar{Y}^{\text{naive}}$ may be visualized as in Figure 4.1.

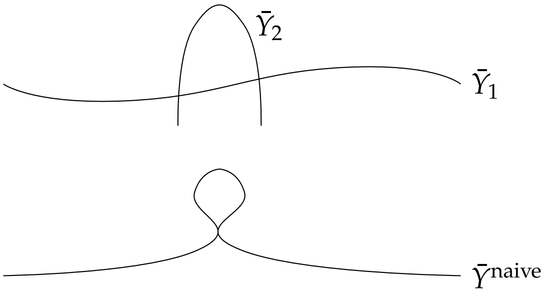


Figure 4.1: $\bar{Y} \to \bar{Y}^{\text{naive}}$

We see that $\bar{Y}_2$ is contracted to the singular point on $\bar{Y}^{\text{naive}}$ and that $\bar{Y}_1$ can be identified with the normalization of $\bar{Y}^{\text{naive}}$.

Corollary 4.4.2

The local L-factor and the conductor exponent of the curve Y at $p = 5$ are

$$L_5^{-1} = (1+T)(1+3T+5T^2), \quad f_5 = 3.$$

Proof: Let $\bar{Z} := \bar{Y}/\mathrm{Gal}(L/\mathbb{Q}_5)$ be the quotient of $\bar{Y}$ by the action of the Galois group of the extension $L/\mathbb{Q}_5$. In the terminology of [BW16], $\bar{Z}$ is the *inertial reduction* of Y at $p = 5$. It follows from Lemma 4.4.1 that $\bar{Z}$ is a semistable curve over $\mathbb{F}_5$, consisting of two irreducible components $\bar{Z}_1, \bar{Z}_2$, which intersect in a unique nonsplit ordinary double point of degree 2. The curve $\bar{Z}_1$ may be identified with $\bar{Y}_1$ and the curve $\bar{Z}_2$ with the quotient $\bar{Y}_2/\langle\sigma\rangle$. One sees from (4.4.4) and Lemma 4.4.1.iv) that $\bar{Z}_2$ has genus 0. By [BW16], Corollary 2.5, the local L-factor is

$$L_5(Y,T) = P(\bar{Z},T)^{-1},$$

where $P(\bar{Z},T)$ is the numerator of the zeta function of $\bar{Z}$. From the above description of $\bar{Z}$ we see that

$$P(\bar{Z},T) = (1+T)(1+3T+5T^2).$$

The second factor is the numerator of the zeta function of the genus-one curve $\bar{Z}_1$, which is given by (4.4.3), and the first factor comes from the action of $\Gamma_{\mathbb{F}_5}$ on $H^1(\Delta_{\bar{Z}})$, as in the proof of Proposition 4.2.4. Finally, we use [BW16, Cor. 2.6], to conclude that

$$f_5 = 2g_Y - \dim H^1_{\text{ét}}(\bar{Z}_{k^{\text{alg}}}, \mathbb{Q}_\ell) = 6 - 3 = 3. \qquad \square$$

We computed the local L-factors and conductor exponents at all bad primes, so we can continue with Step 4 of the algorithm from Section 4.3.5. The conductor of the L-function is $N = 3 \cdot 5^3 \cdot 13^2 \cdot 97 \approx 10^8$, and we obtain $M = 55956$. We compute the local L-factors for all good primes $p \leq M$ and the truncated L-series $L(Y,s)'$ as described in Section 4.3.5. Feeding these data into Dokchitser's algorithm, we checked that the L-function of Y satisfies the expected functional equation with root number -1.

4.4.2 Second hyperelliptic example

We now treat an example of a hyperelliptic curve that does not have semistable reduction at $p = 2$. In this case, the methods of [BW16] to compute the semistable reduction do not apply, and we have to use a different method. The techniques used in this case are developed in [AW12], [Arz12] and [Rüt14]. A proof that this method always succeeds will appear in [RW]. We refer to [BW15], Section 4, for an introduction and more examples.

The polynomials

$$g = x^9 - x^8 + x^7 + x^5 + x^3, \quad h = -x^4 + 1$$

define a hyperelliptic curve of genus four. The discriminant of $f := h^2 + 4g$ is $\Delta = -2^{32} \cdot 317$. So $p = 317$ is the only odd prime where Y has bad reduction.

Running through Step 2 and 3b of the algorithm from Section 4.3.5 we see that Y has semistable reduction at $p = 317$ and the local L-factor and the conductor exponent are

$$L_{317}^{-1} = (1+T)(1 - 32T + 991T^2 + \ldots), \quad f_{317} = 1.$$

It will follow from the calculation of the conductor N below that this is indeed the correct truncation.

For the rest of this section we consider Y as a curve over $\mathbb{Q}_2$. Unfortunately, the condition $\gcd(\bar{h}, \bar{h}', \bar{g}') = 1$ from Step 1 of Section 4.3.5 is not satisfied. The naive model $\mathcal{Y}^{\text{naive}}$ of Y over $\mathbb{Z}_2$, given by (4.3.1), has special fiber

$$\bar{Y}^{\text{naive}}/\mathbb{F}_2 : \bar{y}^2 + (\bar{x}+1)^4\bar{y} = \bar{g}(\bar{x}) = \bar{x}^9 + \bar{x}^8 + \bar{x}^7 + \bar{x}^5 + \bar{x}^3. \tag{4.4.5}$$

One sees that the (unique) singularity $(\bar{x}, \bar{y}) = (1,1)$ of $\bar{Y}^{\text{naive}}$ is not an ordinary double point. Substituting

$$\bar{y} = (\bar{x}+1)^3\bar{y}_0 + \bar{x}^4 + \bar{x}^2 + 1$$

into (4.4.5) and dividing by $(\bar{x}+1)^6$ we obtain an equation for the normalization $\bar{Y}_0'$ of $\bar{Y}^{\rm naive}$:

$$\bar{Y}_0'/\mathbb{F}_2: \qquad \bar{y}_0^2 + (\bar{x}+1)\bar{y}_0 = \bar{x}^2(\bar{x}+1). \tag{4.4.6}$$

We see that $\bar{Y}_0'$ is a smooth curve of genus one. The numerator of its zeta function is

$$P(\bar{Y}_0', T) = 1 + T + 2T^2. \tag{4.4.7}$$

The computation of the semistable reduction of Y at $p = 2$ is rather challenging. We only state the result (Lemma 1 below). A detailed proof will be given elsewhere.

Using the methods of [AW12] we produce the following polynomial:

$$\begin{aligned}\Delta = x^{12} &+ 20x^{11} + 154x^{10} + 664x^9 + 1873x^8 + 3808x^7 + 5980x^6 \\ &+ 7560x^5 + 7799x^4 + 6508x^3 + 4290x^2 + 2224x + 887 \in \mathbb{Z}_2[x]. \end{aligned} \tag{4.4.8}$$

One checks that Δ is irreducible over $\mathbb{Q}_2$. Let $L/\mathbb{Q}_2$ be the splitting field of Δ, $\Gamma = \mathrm{Gal}(L/\mathbb{Q}_2)$ the Galois group, and $K_i := L^{\Gamma_i}$ the fixed field of the ith higher ramification group, for $i \geq 0$. One also checks that $K_0/\mathbb{Q}_2$ has degree 2 and that K_1/K_0 has degree 9. We find that $K_0/\mathbb{Q}_2$ is the unique unramified extension of degree 2, and Γ_0/Γ_1 is a cyclic group of order 9. Unfortunately, we do not know the exact size and structure of the wild subgroup of the inertia group Γ_1. Nevertheless, we can prove the following.

Lemma 4.4.3 (Semistable reduction)

i) *The curve Y_L has semistable reduction.*

ii) *Let $\mathcal{Y}$ be the minimal semistable model of Y over $\mathcal{O}_L$ and $\bar{Y}$ the special fiber of $\mathcal{Y}$. Then $\bar{Y}$ consists of five irreducible components $\bar{Y}_0, \ldots, \bar{Y}_4$ over the residue field $k = \mathbb{F}_4$ of L. Here $\bar{Y}_0$ may be identified with the pullback to k of the curve $\bar{Y}_0'$, the normalization of $\bar{Y}^{\rm naive}$. The components $\bar{Y}_1, \bar{Y}_2, \bar{Y}_3$ are smooth curves of genus one over k, given by equations*

$$\bar{Y}_i/k: \ \bar{y}_i^2 + \bar{y}_i = \bar{x}_i^3, \qquad i = 1, 2, 3.$$

The component $\bar{Y}_4$ is a projective line and intersects each of the other four components in a unique point. The genus-one components $\bar{Y}_0, \ldots, \bar{Y}_3$ do not intersect (Figure 4.2).

iii) *The inertia group Γ_0 fixes $\bar{Y}_0$ and $\bar{Y}_4$ and permutes the components $\bar{Y}_1, \bar{Y}_2, \bar{Y}_3$ transitively. The wild inertia group Γ_1 fixes every component.*

iv) *Let $\Gamma_0' \subset \Gamma_0$ be the stabilizer of the component $\bar{Y}_1$, $H \subset \Gamma_0'$ the kernel of the map*

$\Gamma_0' \to \mathrm{Aut}(\bar{Y}_1)$, and $\tilde{\Gamma}_0 = \Gamma_0'/H$ the quotient. Then $\tilde{\Gamma}_0$ is cyclic of order 6. Its unique element of order two acts on $\bar{Y}_1$ via the automorphism

$$\bar{x}_1 \mapsto \bar{x}_1, \quad \bar{y}_1 \mapsto \bar{y}_1 + 1.$$

Moreover, the filtration of higher ramification groups on $\tilde{\Gamma}_0$ has the form

$$\tilde{\Gamma}_0 \supsetneq \tilde{\Gamma}_1 = \ldots = \tilde{\Gamma}_{15} \supsetneq \tilde{\Gamma}_{16} = 1.$$

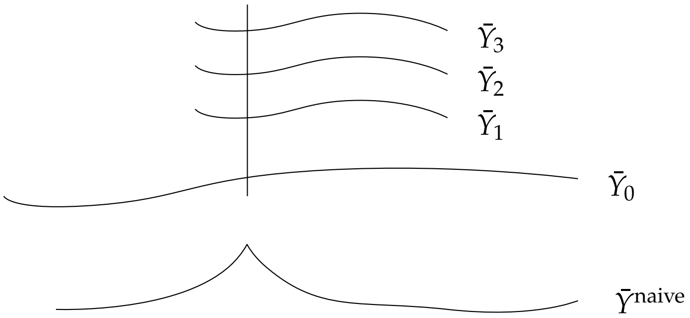


Figure 4.2: $\bar{Y} \to \bar{Y}^{\mathrm{naive}}$

Corollary 4.4.4

The local L-factor and the conductor exponent of Y at $p = 2$ are

$$L_2^{-1} = 1 + T + 2T^2, \qquad f_2 = 16.$$

Proof: Let $\bar{Z} = \bar{Y}/\Gamma$ be the quotient curve. It follows directly from Lemma 1 that $\bar{Z}$ is a semistable curve over $\mathbb{F}_2$, consisting of three irreducible components — corresponding to the three orbits of the action of Γ_1 on the set of irreducible components of $\bar{Y}$. The first component is the genus-one curve $\bar{Z}_0 := \bar{Y}_0/\Gamma \cong \bar{Y}_0'$, given by (4.4.6). The other two components have genus zero. Moreover, the graph of components of $\bar{Z}$ is a tree. It follows that the zeta function of $\bar{Z}$ is the same as the zeta function of $\bar{Y}_0'$, and hence

$$P(\bar{Z}, T) = P(\bar{Y}_0', T) = 1 + T + 2T^2,$$

by (4.4.7). The claim $L_2^{-1} = 1 + T + 2T^2$ now follows from [BW16, Cor. 2.5].

By [BW16, § 2.6], the conductor exponent f_2 has the form

$$f_2 = \epsilon + \delta,$$

where

$$\epsilon = 2g_Y - \dim H^1_{\text{ét}}(\bar{Z}_{k^{\mathrm{alg}}}, \mathbb{Q}_\ell) = 8 - 2 = 6$$

and $\delta = \delta_V$ is the *Swan conductor* of the Γ-module $V := H^1_{\text{ét}}(Y_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$.

Since the graph of components of $\bar{Y}$ is a tree, the cospecialization map induces a Γ-equivariant isomorphism

$$V \cong \oplus_{i=0}^{3} H^1_{\text{ét}}(\bar{Y}_{i,k^{\text{alg}}}, \mathbb{Q}_\ell).$$

The Swan conductor of V only depends on the action of Γ_0. By Lemma 1.iii), the Γ_0-module V has a direct sum decomposition

$$V = V_0 \oplus V_1,$$

where

$$V_0 = H^1_{\text{ét}}(\bar{Y}_{0,k^{\text{alg}}}), \quad V_1 = \oplus_{i=1}^{3} H^1_{\text{ét}}(\bar{Y}_{i,k^{\text{alg}}}).$$

Moreover, V_0 has trivial Γ_0-action. This implies that $\delta = \delta_{V_1}$ is the Swan conductor of the induced Γ_0-module

$$V_1 = \operatorname{Ind}_{\tilde{\Gamma}_0}^{\Gamma_0} \tilde{V}, \quad \tilde{V} := H^1_{\text{ét}}(\bar{Y}_{1,k^{\text{alg}}}, \mathbb{Q}_\ell),$$

where the group $\tilde{\Gamma}_0$ is defined in Lemma 1.iv). We have $\delta = \delta_{V_1} = \delta_{\tilde{V}}$ by standard properties of the Swan conductor. To compute $\delta_{\tilde{V}}$ we may use the formula

$$\delta_{\tilde{V}} = \sum_{i=1}^{\infty} \frac{|\tilde{\Gamma}_i|}{|\tilde{\Gamma}_0|} \cdot \dim \tilde{V}/\tilde{V}^{\tilde{\Gamma}_i},$$

see [BW16], proof of Theorem 2.9. By Lemma 1.(iv.) we obtain

$$\frac{|\tilde{\Gamma}_i|}{|\tilde{\Gamma}_0|} \cdot \dim \tilde{V}/\tilde{V}^{\tilde{\Gamma}_i} = \begin{cases} \frac{2}{6} \cdot 2, & i = 0, \dots, 15, \\ 0, & i \geq 16. \end{cases}$$

We conclude that $\delta = \delta_{\tilde{V}} = 10$ and hence

$$f_2 = \epsilon + \delta = 6 + 10 = 16. \qquad \square$$

It follows that the conductor of the L-function is $N = 2^{16} \cdot 317 \approx 10^7$. Using the bound $M = 101248$, we verified the functional equation for $L(Y, s)$ and obtained the root number -1.

4.4.3 Non-hyperelliptic example

Finally, we treat a non-hyperelliptic example. Let $Y/\mathbb{Q}$ be the superelliptic curve of genus three given by the equation

$$y^3 = f(x) = x^4 - x^2 + 1. \tag{4.4.9}$$

The discriminant of f is $144 = 2^4 \cdot 3^2$, hence Y has good reduction at $p \neq 2, 3$.

The local L-factor and the conductor exponent of Y at $p = 2$ have been computed in [BW16, § 7]. The result is

$$L_2^{-1} = 1 + 2T^2, \qquad f_2 = 8.$$

The methods of [BW16] do not allow the computation of the semistable reduction of Y at $p = 3$, because the exponent of y in (4.4.9) is equal to $p = 3$. Again, we have to use the algorithm of [RW], see also [AW12], [Arz12] and [Rüt14]. However, this case is much easier than that treated in Section 4.4.2. One of the key difficulties in general is to find a field extension L of $\mathbb{Q}_p$ over which Y acquires semistable reduction, together with the centers and radii of the blow ups that have to be performed. In this section, we produce these data without referring to [RW], and then check that we have indeed found the desired semistable model $\mathcal{Y}$ of Y. Similar examples, with more motivation and more details, can be found in [BW15, § 4].

Let $L := \mathbb{Q}_3[\zeta_4, \pi]$, where ζ_4 is a primitive 4th root of unity and π satisfies $\pi^{12} = 3$. This is a Galois extension of $\mathbb{Q}_3$ whose Galois group is the dihedral group of order 24, generated by

$$\tau(\pi, \zeta_4) = (\zeta_{12}\pi, \zeta_4) \qquad \sigma(\pi, \zeta_4) = (\pi, -\zeta_4).$$

Here $\zeta_{12} := \zeta_4^3(-1 + \pi^6\zeta_4)/2 \in L$ is a primitive 12th root of unity. We put $\zeta_3 = \zeta_{12}^4$. The residue field of the unique prime $\mathfrak{p} = (\pi) \lhd \mathcal{O}_L$ is $k = k(\mathfrak{p}) = \mathbb{F}_3[\zeta_4] = \mathbb{F}_9$.

Lemma 4.4.5 (Semistable reduction)

i) The curve $Y_L = Y \otimes_{\mathbb{Q}_3} L$ has semistable reduction at $\mathfrak{p}$.

ii) Let $\mathcal{Y}$ be the minimal semistable model of Y over $\mathcal{O}_L$ and $\bar{Y}$ the special fiber of $\mathcal{Y}$. Then $\bar{Y}$ consists of 4 smooth, absolutely irreducible components over k. The normalization $\bar{Y}_0$ of the naive model has genus zero. The other three components $\bar{Y}_i$ ($i = 1, 2, 3$) have genus 1 and each intersects $\bar{Y}_0$ in a unique ordinary double point of degree 1 (Figure 4.3).

iii) The Galois group $\Gamma := \mathrm{Gal}(L/\mathbb{Q}_3)$ acts trivially on $\bar{Y}_0$. It acts as a cyclic group $\langle\tau^3\rangle$ of order 4 on $\bar{Y}_1$, the quotient by this action has genus 0. The components $\bar{Y}_2$ and $\bar{Y}_3$ are conjugate under the action on $\bar{Y}$ induced by σ. The Galois group Γ acts on $\bar{Y}_2$ (resp. $\bar{Y}_3$) as a cyclic group $\Gamma = \langle\tau\rangle$ of order 12. The quotients of $\bar{Y}_2$ (resp. $\bar{Y}_3$) both by $\langle\tau\rangle$ and by the wild subgroup $\langle\tau^4\rangle$ have genus 0.

Proof: As in Section 4.3, we write $\bar{f}$ for the image of f in $\mathbb{F}_3[\bar{x}]$. The formal derivative of $\bar{f}$ satisfies $\bar{f}' = \bar{x}(\bar{x}^2 + 1) \in \mathbb{F}_3[\bar{x}]$. The Jacobi criterion therefore implies that the special

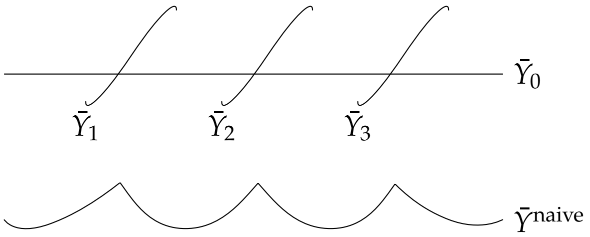


Figure 4.3: $\bar{Y} \to \bar{Y}^{\mathrm{naive}}$

fiber $\bar{Y}^{\mathrm{naive}}_{k^{\mathrm{alg}}}$ of the naive model of Y has singularities in the 3 points with $\bar{x} = 0, \pm\zeta_4$. The normalization $\bar{Y}_0$ of $\bar{Y}^{\mathrm{naive}}_{k^{\mathrm{alg}}}$ has genus 0, since the map

$$(\bar{x}, \bar{y}) \mapsto \bar{x}, \qquad \bar{Y}^{\mathrm{naive}}_{k^{\mathrm{alg}}} \to \mathbb{P}^1_{k^{\mathrm{alg}}}$$

is purely inseparable. This immediately follows from Equation (4.4.9).

To compute a semistable model of Y we construct a certain modification $\mathcal{Y} \to \mathcal{Y}^{\mathrm{naive}} \otimes \mathcal{O}_L$. This modification is determined explicitly as a blowup with centers the three singular points of $\bar{Y}^{\mathrm{naive}}_{k^{\mathrm{alg}}}$; its exceptional divisor consists of three irreducible components $\bar{Y}_1, \bar{Y}_2, \bar{Y}_3$, as indicated in Figure 4.3. Once we now the components $\bar{Y}_i$, $i = 1, 2, 3$, explicitly, we can show that $\bar{Y}$ is semistable and hence that $\mathcal{Y}$ is a semistable model of $Y \otimes_K L$.

To find the component $\bar{Y}_1$ corresponding to the singularity with $\bar{x} = 0$ we define the coordinates

$$x = \pi^9 x_1, \qquad y = (\zeta_3 - 1)y_1 + 1$$

We substitute this into Equation (4.4.9) and divide the resulting equation by $(\zeta_3 - 1)^2$. Reducing the result modulo $\mathfrak{p}$ yields

$$\bar{Y}_1 : \qquad \bar{y}_1^3 - \bar{y}_1 = \bar{x}_1^2.$$

Here we used that $(\zeta_3 - 1)^2 = -3\zeta_3$ and that $\pi^6 \equiv 1 - \zeta_3 \pmod{\pi^7}$. Note that $\bar{Y}_1$ has genus 1.

The automorphism $\tau \in \Gamma$ induces the trivial automorphism on $\mathcal{Y}^{\mathrm{naive}}$, since $\mathcal{Y}^{\mathrm{naive}}$ is defined over $\mathbb{Z}_3$. It acts nontrivially on the model of Y defined by the coordinates (x_1, y_1), via its action of the coefficients. An easy calculation shows that in reduction τ acts on $\bar{Y}_1$ as

$$(\bar{x}_1, \bar{y}_1) \mapsto (\zeta_4 \bar{x}_1, -\bar{y}_1).$$

It follows that Γ acts on $\bar{Y}_1$ via a group of order 4, and that the quotient of $\bar{Y}_1$ by this group is a curve of genus zero.

To find the component $\bar{Y}_2$, we similarly define the coordinates

$$x = a\pi^{15}x_2 - 2\zeta_4, \qquad y = \zeta_4\pi^{10}y_2 + b\pi^4\left(-\frac{4}{7}\zeta_4 x + 1\right),$$

where $a, b \in \mathbb{Q}_3[\zeta_4]$ satisfy $a^2 = \zeta_4$ and $b^3 = 7$. Suitably normalizing a and b and arguing as for $\bar{Y}_1$, we find in reduction:

$$\bar{Y}_2 : \qquad \bar{y}_2^3 - \bar{y}_2 = \bar{x}_2^2.$$

Note that $\bar{Y}_2$ has genus 1, as well.

The automorphism $\sigma \in \Gamma$, which sends ζ_4 to $-\zeta_4$, induces an automorphism of $\mathcal{Y}^{\mathrm{naive}}$ that permutes the two singularities with $\bar{x} = \pm\zeta_4^3$. Defining coordinates

$$(x_3, y_3) = (\sigma(x_2), \sigma(y_3))$$

therefore yields a further component:

$$\bar{Y}_3 : \qquad \bar{y}_3^3 - \bar{y}_3 = \bar{x}_3^2.$$

The components $\bar{Y}_2$ and $\bar{Y}_3$ are permuted by σ.

We obtain a model $\mathcal{Y}$ of Y such that the reduction $\bar{Y}$ exactly consists of the 4 irreducible components $\bar{Y}_1, \bar{Y}_2, \bar{Y}_3$, and the normalization $\bar{Y}_0$ of $\bar{Y}^{\mathrm{naive}}$. The fact that Y is semistable follows from the observation that

$$\sum_{i=0}^{3} g(\bar{Y}_i) = 3 = g(Y).$$

The fact that the intersection behavior of the components is as in Figure 4.3 is easily deduced from the definition of the coordinates. The minimality of the semistable model follows from this. Statements *i)* and *ii)* follow. The largest part of Statement *iii)* has already been checked. The rest follows similarly. □

Corollary 4.4.6

The local L-factor and conductor exponent of Y at $p = 3$ are

$$L_3^{-1} = 1, \qquad f_3 = 12.$$

Proof: The proof is similar to the proof of Corollaries 4.4.2 and 4.4.4. The statement on the local L-factor immediately follows from Lemma 4.4.5.iii), since the inertial reduction $\bar{Z}$ of Y at $p = 3$ has genus 0.

We compute the conductor exponent using [BW16, § 2.6]. We find that $f_3 = \epsilon + \delta$, where

$$\epsilon = 2g_Y - \dim H^1_{\text{ét}}(\bar{Z}_{k^{\text{alg}}}, \mathbb{Q}_\ell) = 6 - 0 = 6.$$

We compute the Swan conductor δ of the Γ-module $V := H^1_{\text{ét}}(\bar{Z}_{k^{\text{alg}}}, \mathbb{Q}_\ell)$ using [BW16, Thm. 2.9]. Note that the wild subgroup of the decomposition group of $\mathfrak{p}$ satisfies

$$\tau^4(\pi) - \pi = (\zeta_{12}^4 - 1)\pi.$$

Since $v_L(\zeta_{12}^4 - 1) = 6$, we conclude that the higher ramification filtration of Γ is

$$\Gamma_0 = \langle \tau \rangle \supsetneq \Gamma_1 = \cdots = \Gamma_6 = \langle \tau^4 \rangle \supsetneq \Gamma_7 = \{1\}.$$

Lemma 4.4.5.iii) implies that the quotient $\bar{Y}/\Gamma_i$ has genus one for all $1 \leq i \leq 6$. We conclude from [BW16, Thm. 2.9], that

$$\delta = \sum_{i=1}^{\infty} \frac{|\Gamma_i|}{|\Gamma_0|} (2g_Y - 2g(\bar{Y}/\Gamma_i)) = \frac{6 \cdot 3}{12}(6 - 2) = 6.$$

It follows that $f_3 = \epsilon + \delta = 6 + 6 = 12$. □

We verified the functional equation for $L(Y/\mathbb{Q})$, using the bound $M = 274994$ and the root number 1.

Chapter 5

L-functions of Picard curves

In this chapter, we compute conductor and L-factors at all primes for another class of curves — *Picard curves*. These curves have genus 3 and bad reduction at $p = 3$. As in Chapter 4, we use the description of semistable reduction of superelliptic curves in [BW16] to compute the bad local factors.

In Section 5.1, we elaborate the calculations of the bad factors and conductor exponents for the two Picard curves $y^3 = x^4 \pm 1$ to show in more detail how the semistable reduction described in [BW16] works. In contrast to the class of hyperelliptic curves discussed before, we do not achieve semistable reduction over $\mathbb{Q}$. This requires non-trivial extensions of $\mathbb{Q}$ and makes the computations rather involved.

We continue with a general description of Picard curves and some properties (Section 5.2.1). For Picard curves with good reduction away from a defined set S, we discuss the computation of the conductor and the bad factors. In Section 5.3.1, we describe the construction of all Picard curves over $\mathbb{Q}$ with good reduction away from 3 [MR14]. We also discuss a generalization of this construction in Section 5.3.2. This is used to describe the search for a Picard curve over $\mathbb{Q}$ with minimal conductor.

5.1 Two examples for the computation of $L_\mathfrak{p}$ and N

5.1.1 Outline of the approach

Consider a superelliptic curve Y, i.e. a smooth projective absolutely irreducible curve given by

$$y^n = f(x)$$

over a finite extension $K_\mathfrak{p}$ of $\mathbb{Q}_p$. We make the process described in [BW16] explicit to calculate the local L-factors $L_\mathfrak{p}$ at all bad primes, as well as the conductor exponents $f_\mathfrak{p}$. For this, we first compute the semistable reduction of Y at $\mathfrak{p}$. For the time being, we restrict ourselves to the case that the residue characteristic p does not divide the degree n of the cover. For the other, more complicated case, see Section 5.2.3.

We consider the degree-n Kummer cover $Y \to \mathbb{P}^1_{K_\mathfrak{p}}$ given by $(x, y) \mapsto x$ over a field extension $L/K_\mathfrak{p}$ with the following properties:

a) L contains the splitting field L_0 of f,

b) L contains a primitive n-th root of unity,

c) the extension $L/K_\mathfrak{p}$ is Galois with $\Gamma := \mathrm{Gal}(L/K_\mathfrak{p})$,

d) L contains an n-th root of π, where $\mathfrak{P} = (\pi) \lhd \mathcal{O}_{L_0}$ is the prime ideal above $\mathfrak{p}$.

The curve Y acquires semistable reduction over L, i.e. we can construct a semistable model $\mathcal{Y}$ of Y over $\mathcal{O}_L$ [BW16, § 5]. Denote $\mathcal{X}$ the minimal semistable model of X such that the branch divisor specializes to distinct smooth points of the special fiber $\bar{X}$. We define $\mathcal{Y}$ as the normalization of $\mathcal{X}$ in the function field $K_\mathfrak{p}(Y)$. One can show that $\mathcal{Y}$ is a semistable model of Y_L [BW16, Thm. 3.4].

The cover $Y \to X$ extends to a finite Γ-equivariant morphism $\mathcal{Y} \to \mathcal{X}$ on the models. Its restriction to the special fibers is a finite Γ-equivariant map $\bar{Y} \to \bar{X}$ between semistable curves over the residue field. This map in turn induces a finite map $\bar{Y}/\Gamma \to \bar{X}/\Gamma$ between semistable curves over $k(\mathfrak{p}) = \mathbb{F}_q$ for some integer q.

We write $\bar{Z} := \bar{Y}/\Gamma$ for the the inertial reduction of Y. Note that $\bar{Z} \to \bar{X}/\Gamma$ completely defines the local L-factor, whereas for the conductor exponent f_p we may also have to compute reductions $\bar{Y}/\Gamma_i$ for higher ramification groups $\Gamma_i < \Gamma$, cf. Definition 3.1.2 and Section 4.4.

The first step in analyzing $\bar{Y}$ is to analyze the stably marked tree $(\bar{X}, \bar{D})$, where $\bar{D}$ is the divisor of the ramification points. To construct it, we separate the branch points of the cover such that $\bar{X}$ consists of a tree of components $\bar{X}_i$. These components are all isomorphic to the projective line and contain at least three points which are either singular points of $\bar{X}$ or branch points [BW16, Prop. 3.2 (4)]. Moreover, the branch points specialize to smooth pairwise distinct points.

Then we determine the action of the inertia group I of Γ on $\bar{X}$ and $\bar{Y}$. This action describes the local L-factor and the conductor exponent of $\mathfrak{p}$ completely if $g(\bar{Y}/I) = 0$. If this is not the case, we look at the semilinear action of Γ/I on $\bar{Y}/I$ which yields our final result $\bar{Z} \to \bar{X}/\Gamma$. For the f_p, we compute the action of the Γ_i on $\bar{Y}$, if necessary.

Notation

For the fields occurring in the examples we use the following notation. As we only consider one fixed prime $\mathfrak{p}$ at a time, the ground field is denoted $K_0 = K_\mathfrak{p}$, without naming the prime $\mathfrak{p}$. The splitting field of the polynomial defining the curve is denoted L_0, and the field L is defined as above. Further intermediate fields between K_0 and L are denoted K, M, and N, if necessary.

5.1.2 First example: $y^3 = x^4 + 1$

Consider the curve $Y/\mathbb{Q}$ given by $y^3 = x^4 + 1$. We have a degree-3-cover of $\mathbb{P}^1$:

$$\begin{aligned} Y &\longrightarrow X := \mathbb{P}^1_{\mathbb{Q},x} \\ (x,y) &\longmapsto x \end{aligned}$$

with branch points $z_1 = \zeta_8$, $z_2 = \zeta_8^3$, $z_3 = \zeta_8^5$, $z_4 = \zeta_8^7$, and $z_5 = \infty$, where ζ_8 denotes a primitive 8th root of unity.

The polynomial $x^4 + 1$ splits completely over the cyclotomic field L_0 of degree 4:

$$y^3 = (x - \zeta_8) \cdot (x - \zeta_8^3) \cdot (x - \zeta_8^5) \cdot (x - \zeta_8^7) \,.$$

For each root we denote the multiplicity by a_i, hence $a_1 = a_2 = a_3 = a_4 = 1$. Moreover, at $x = \infty$ we have $a_5 := -\sum_i a_i \pmod 3 = 2$.

We denote the degree of the cover by $n = 3$ and compute the ramification indices $e_i := n/(n, a_i)$ at the z_i: $e_1 = e_2 = e_3 = e_4 = e_5 = 3$. For each i we have $(n, a_i) = 1$ ramification point in the normalization. With this data, we can verify that the curve has genus $g(Y) = 1 + \frac{1}{2}(-2 \cdot 3 + 5 \cdot (3 - 1)) = 3$.

We have bad reduction at $p = 3$ (the exponent of y, cf. Lemma 5.2.3) and $p = 2$ (since $\Delta_{\mathbb{Q}(\zeta_8)} = \Delta\,(x^4 + 1) = 2^8$. As we are dealing with a local problem at $\mathfrak{p} = (p)$, we may regard the curve Y over the p-adic completion $\mathbb{Q}_p$. So in the following we consider Y over a finite extension of $\mathbb{Q}_2$, with the respective valuation $v_{\mathfrak{p}}$ as defined on page 15.

The case $p = 2$

We first extend $K_0 = \mathbb{Q}_2$ to a field containing ζ_8, i.e. the splitting field of $f = x^4 + 1$:

$$L_0 := \mathbb{Q}_2(\zeta_8) = \mathbb{Q}_2(\sqrt{2}, i) \,.$$

Its Galois group is $\mathrm{Gal}(L_0/K_0) = C_2 \times C_2$, where C_m denotes the cyclic group of order m. For $L_0 = \mathbb{Q}_2(\sqrt{2}, i)$ the ring of integers is $\mathcal{O}_{L_0} = \mathbb{Z}_2[\zeta_8 = (1+i)/\sqrt{2}]$. Consider the prime ideal $\mathfrak{p} := (2)$ in $\mathbb{Z}_2 = \mathcal{O}_{K_0}$ and the discrete valuation $v_{\mathfrak{p}}$ with $v_{\mathfrak{p}}(2) = 1$. We obtain the following prime ideals and residue fields, using $(1 + \zeta_8)^2 = (1 + i)$ (as ideals in $\mathcal{O}_{L_0}$).

$$\begin{tikzcd}
\mathbb{Q}_2(\zeta_8) \arrow[d, dash, "2"] & \mathfrak{P} := (1+\zeta_8) \arrow[d, dash, "2"] & k = \mathcal{O}_{L_0}/\mathfrak{P} = \mathbb{F}_2 \arrow[d, dash, "1"] \\
\mathbb{Q}_2(i) \arrow[d, dash, "2"] & (1+i) \arrow[d, dash, "2"] & k = \mathbb{F}_2 \arrow[d, dash, "1"] \\
\mathbb{Q}_2 & \mathfrak{p} := (2) & k = \mathbb{F}_2
\end{tikzcd}$$

The extension $\mathbb{Q}_2(\zeta_8)/\mathbb{Q}_2$ is Galois and we have: $\mathfrak{p} = (2) = (1 + \zeta_8)^4 = \mathfrak{P}^4$ in $\mathcal{O}_{L_0}$.

We see that $g = 1$, $e = 4$, and $f = [k(\mathfrak{P}) : k(\mathfrak{p})] = 1$. The valuation $v_\mathfrak{p}$ extends to a valuation $v_\mathfrak{P}$ with $v_\mathfrak{P}(2) = 4 \cdot v_\mathfrak{p}(2) = 4$. We denote by x the coordinate on a component X and by $\bar{x}$ their reductions modulo $\mathfrak{p}$.

Keep in mind that by the conditions on the extension L/K_0 posed in Section 5.1.1, the semistable model is defined over $L := \mathbb{Q}_2(\zeta_8, \zeta_3, \sqrt[3]{2})$.

Separating points

We now construct $\mathcal{X}$ resp. $\bar{X}$ step by step by separating points on the special fiber $\bar{X}^{\text{naive}}$ of the naive model $\mathcal{X} = \mathbb{P}^1$. Modulo $\mathfrak{P} = (1 + \zeta_8)$ we have the following situation (Figure 5.1). The cover Y of $\mathbb{P}^1$ is ramified over the four zeros of $x^4 + 1$ and ∞. Moreover, all zeros specialize to the same point $\bar{x} = 1$. Note that in Figure 5.1 the points on $\bar{X}^{\text{naive}}$ are labeled according to their respective points on X.

x	ζ_8	ζ_8^3	ζ_8^5	ζ_8^7	∞
$\bar{x} = x \mod \mathfrak{P}$	1	1	1	1	∞

Table 5.1: Coordinate x

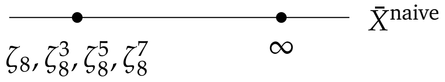


Figure 5.1: Coordinate x

Recall that we want to construct a tree $\bar{X}$ with separated branch points. We choose to separate ζ_8 from ζ_8^3. This corresponds to the Möbius transformation

$$x_1 = \frac{x - \zeta_8}{\zeta_8^3 - \zeta_8}. \tag{5.1.1}$$

The new component $\bar{X}_1$ arising from this separation of points is depicted in Figure 5.2.

x	ζ_8	ζ_8^3	ζ_8^5	ζ_8^7	∞
$x \mod \mathfrak{P}$	1	1	1	1	∞
x_1	0	1	$1+i$	i	∞
$\bar{x}_1 = x_1 \mod \mathfrak{P}$	0	1	0	1	∞ ,

Table 5.2: Coordinate x_1

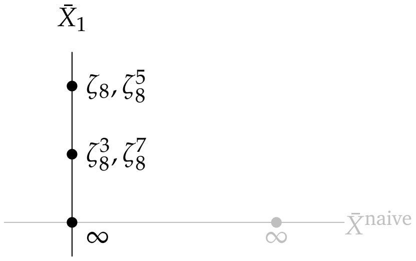


Figure 5.2: Coordinate x_1

Before we consider the implications of the new coordinates for the equation $y^3 = x^4 + 1$, we completely separate the two pairs of points via the Möbius transformations

$$x_2 = \frac{x - \zeta_8}{\zeta_8^5 - \zeta_8} = \frac{x_1}{1+i} \qquad \text{and} \qquad x_3 = \frac{x - \zeta_8^3}{\zeta_8^7 - \zeta_8} = \frac{x_1 - 1}{i - 1}. \tag{5.1.2}$$

Thus we obtain the following situation (Figure 5.3):

x	ζ_8	ζ_8^3	ζ_8^5	ζ_8^7	∞
x_2	0	$\frac{1}{1+i}$	1	$\frac{i}{1+i}$	∞
$\bar{x}_2 \equiv x_2 \mod \mathfrak{P}$	0	∞	1	∞	∞
x_3	$\frac{1}{1-i}$	0	$\frac{-i}{1-i}$	1	∞
$\bar{x}_3 \equiv x_3 \mod \mathfrak{P}$	∞	0	∞	1	∞ ,

Table 5.3: Coordinates x_2, x_3

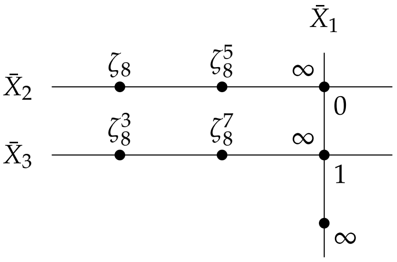


Figure 5.3: $\bar{X}$

Note that on every component $\bar{X}_i$, the sum of the multiplicities a_i of the points is a multiple of $n = 3$, cf. Figures 5.4 and 5.5.

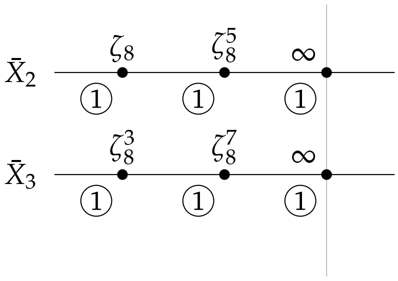


Figure 5.4: Multipl. on $\bar{X}_2, \bar{X}_3$

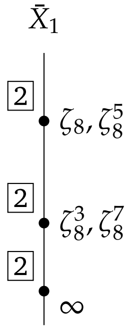


Figure 5.5: Multiplicities on $\bar{X}_1$

New equation

Now look at $\bar{Y}$. We apply the changes of variables to our equation $y^3 = x^4 + 1$. Recall that $\mathfrak{P} = (1 + \zeta_8)$ and $x_1 = (x - \zeta_8)/(-\sqrt{2})$, hence $x = \zeta_8 - \sqrt{2}x_1$. In terms of x_1, the naive (and not semistable) model $\mathcal{Y}^{\text{naive}}$ is given by

$$\begin{aligned} y^3 &= x^4 + 1 \\ &= 4x_1^4 - 8\sqrt{2}\zeta_8 x_1^3 + 12\zeta_8^2 x_1^2 - 4\sqrt{2}\zeta_8^3 x_1 \\ &= 4 \cdot (x_1^4 - 2\sqrt{2}\zeta_8 x_1^3 + 3\zeta_8^2 x_1^2 - \sqrt{2}\zeta_8^3 x_1) \,. \end{aligned}$$

Now set $y =: \lambda y_1$ with an element λ satisfying $v_{\mathfrak{P}}(\lambda^3) = v_{\mathfrak{P}}(4) = 8$. We choose $\lambda := 2^{2/3} = \sqrt[3]{2}^2$. For this we extend the field $\mathbb{Q}_2(\zeta_8)$ to $\mathbb{Q}_2(\zeta_8, \sqrt[3]{2})$. Since this extension is not Galois, we also adjoin ζ_3 and obtain a field $L := \mathbb{Q}_2(\zeta_8, \sqrt[3]{2}, \zeta_3)$, which is Galois over $\mathbb{Q}_2$.

By [BW16, Thm. 4.5], there is a unique irreducible component $\bar{Y}_i$ of $\bar{Y}$ above each $\bar{X}_i$. With the above notation we get an equation for the cover $\bar{Y}_1 \to \bar{X}_1$:

$$\begin{aligned} & y_1^3 = x_1^4 - 2\sqrt{2}\zeta_8 x_1^3 + 3\zeta_8^2 x_1^2 - \sqrt{2}\zeta_8^3 x_1 \\ \bar{Y}_1 : \quad & \bar{y}_1^3 \equiv \bar{x}_1^4 + \bar{x}_1^2 \pmod{\mathfrak{P}_L} \,, \end{aligned}$$

where $\mathfrak{P}_L$ is the prime ideal of $\mathcal{O}_L$.

The cover's branch points are depicted in Figure 5.2 (double points at 0 and 1).

We use $x_1 = (1+i)x_2$ and $x_1 = 1 + (i-1)x_3$ from Equation (5.1.2) to get the following equations for the covers $\bar{Y}_2 \to \bar{X}_2$ and $\bar{Y}_3 \to \bar{X}_3$:

$$\begin{aligned} y_1^3 &= (1+i)^4 x_2^4 - \sqrt{2}^3 \zeta_8 (1+i)^3 x_2^3 + \zeta_8^2 (1+i)^2 x_2^2 - \sqrt{2}\zeta_8^3 (1+i) x_2 \\ &= 2 \cdot \left((1+i)^2 i x_2^4 - \sqrt{2}\zeta_8 (1+i)^3 x_2^3 + \zeta_8^2 i x_2^2 - \zeta_8^4 x_2 \right). \end{aligned}$$

Now substitute $y_1 = \sqrt[3]{2} y_2$ to obtain

$$y_2^3 = (1+i)^2 i x_2^4 - \sqrt{2}\zeta_8 (1+i)^3 x_2^3 + \zeta_8^2 i x_2^2 - \zeta_8^4 x_2 \,.$$

Thus we get

$$\bar{Y}_2 : \quad \bar{y}_2^3 \equiv \bar{x}_2^2 + \bar{x}_2 \pmod{\mathfrak{P}_L},$$

and with an analogous calculation

$$\bar{Y}_3 : \quad \bar{y}_3^3 \equiv \bar{x}_3^2 + \bar{x}_3 \pmod{\mathfrak{P}_L},$$

cf. Figure 5.3 (two elliptic curves ramified at $0, 1, \infty$).

All field extensions used so far are (sorted from unramified to wildly ramified):

$$\begin{tikzcd} L = \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}, \zeta_8) \arrow[d, dash, "4"] & \mathfrak{P}_L \arrow[d, dash, "4"] & k(\mathfrak{P}_L) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "1"] \\ M := \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}) \arrow[d, dash, "3"] & \mathfrak{P}_M := (\sqrt[3]{2}) \arrow[d, dash, "3"] & k(\mathfrak{P}_M) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "1"] \\ K := \mathbb{Q}_2(\zeta_3) \arrow[d, dash, "2"] & \mathfrak{P}_K := (2) \arrow[d, dash, "1"] & k(\mathfrak{P}_K) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "2"] \\ \mathbb{Q}_2 & \mathfrak{p} = (2) & k = \mathbb{F}_2 \end{tikzcd}$$

Note that L fulfills all conditions posed in Section 5.1.1 for a semistable model $\mathcal{Y}$.

We see that M/K is tamely ramified ($e = 3$). Moreover, L/M is wildly ramified as $p = \operatorname{char}(k(\mathfrak{P}_L)) = 2$ divides $4 = e$. Since $\mathbb{Q}_2(\zeta_8) \cap \mathbb{Q}_2(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}_2$, we have

$$|\mathrm{Gal}(L/\mathbb{Q}_2)| = 24 = 4 \cdot 3 \cdot 2 = |\mathrm{Gal}(\mathbb{Q}_2(\zeta_8)/\mathbb{Q}_2)| \cdot |\mathrm{Gal}(\mathbb{Q}_2(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}_2)|,$$

cf. [Lan02, Cpt. VI, § 1, Thm. 1.14]. Therefore the Galois group is

$$\Gamma := \mathrm{Gal}(L/\mathbb{Q}_2) = C_2 \times C_2 \times S_3 .$$

Inertia group

We know that the inertia group I is a normal subgroup of $D_{\mathfrak{P}_L} = \Gamma$ of order $|I| = e_{L/K_0} = 4 \cdot 3 \cdot 1 = 12$. Thus I is either the non-abelian dihedral group $D_6 = S_3 \times C_2$ or the abelian group $C_6 \times C_2$.

We know that $I = \langle \alpha, \beta, \gamma \rangle$ with $\alpha(\zeta_8) = \zeta_8^3$, $\beta(\zeta_8) = \zeta_8^5$, $\alpha\beta(\zeta_8) = \zeta_8^{3\cdot 5} = \zeta_8^7$, as well as $\gamma(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}$. And $\Gamma/I = \langle \delta \rangle$ with $\delta(\zeta_3) = \zeta_3^2$. The subextensions $\mathbb{Q}_2(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_2(\zeta_3)$ and $\mathbb{Q}_2(\zeta_3, \zeta_8)/\mathbb{Q}_2(\zeta_3)$ are both abelian and $I = \mathrm{Gal}(L/K)$ is the direct product of those two groups. We conclude that I is abelian and hence

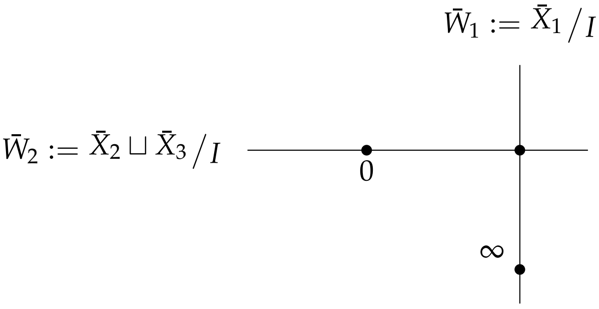
$$I = C_6 \times C_2 = C_3 \ltimes (C_2 \times C_2),$$

with Sylow 2-subgroup $C_2 \times C_2$.

Consequences

The action of the elements α, β of I on $\bar{X}$ are depicted in Figure 5.6.

$$\alpha : \quad \zeta_8 \leftrightarrow \zeta_8^3, \zeta_8^5 \leftrightarrow \zeta_8^7 \qquad \beta : \quad \zeta_8 \leftrightarrow \zeta_8^5, \zeta_8^3 \leftrightarrow \zeta_8^7 \qquad \alpha\beta : \quad \zeta_8 \leftrightarrow \zeta_8^7, \zeta_8^3 \leftrightarrow \zeta_8^5.$$


$\bar{W}_1 := \bar{X}_1/I$
$\bar{W}_2 := \bar{X}_2 \sqcup \bar{X}_3/I$
0
∞

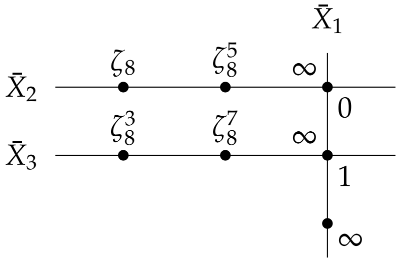


Figure 5.6: Action of I on $\bar{X}$

Figure 5.7: $\bar{X}$

So the six points collapse into one and $(\bar{X}_2 \sqcup \bar{X}_3)/I = \bar{W}_2$, with coordinate $\bar{w}_2 := \bar{x}_2^2 + \bar{x}_2$, as well as $\bar{X}_1/I = \bar{W}_1$, with coordinate $\bar{w}_1 := \bar{x}_1^2 + \bar{x}_1$. We see that both covers $\bar{Y}_1/I \to \bar{W}_1$, $\bar{Y}_{2,3}/I \to \bar{W}_2$ of $\mathbb{P}^1$ are ramified over at most two points. The Riemann–Hurwitz formula yields that $(\bar{Y}/I)$ has genus zero, so the contribution to L_2 is trivial.

Recall that $y =: \pi y_1$ with $\pi = \sqrt[3]{2}^2$. Hence $y_1 = \sqrt[3]{2}^{-2} y$. And I acts on $\bar{Y}_1$ via $\gamma : y_1 \mapsto \zeta_3 y_1$. Thus the three points above each point on $\bar{W}_1$ collapse into one.

We get an action of $\langle \gamma \rangle$ on the function field of $\bar{Y}_1$:

$$\left(\mathbb{F}_4(\bar{x}_1)[\bar{y}_1]/(\bar{y}_1^3 - \bar{x}_1)\right)^{\langle \gamma \rangle} = \mathbb{F}_4(\bar{x}_1)$$

As a result, we obtain $\mathbb{F}_4(\bar{x}_1)$ as function field of $\bar{Y}_1/I$. We will come back to this result in the computation of the action of the higher ramification groups on $\bar{Y}$.

Hence we have shown that the local factor at $p = 2$ is

$$L_2 = 1.$$

Higher ramification groups, exponent of conductor

Recall that $L = \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}, \zeta_8)$ with Galois group $\Gamma = \mathrm{Gal}(L/\mathbb{Q}_2) = C_2 \times C_2 \times S_3$ and

$$\begin{tikzcd}
\mathbb{Q}_2 \arrow[r, dash, "2"] \arrow[rr, dash, bend left, "S_3"] \arrow[r, dash, bend right, "C_2 = {}^{\Gamma}/_{I}"'] \arrow[d, dash] & K \arrow[r, dash, "3"] \arrow[rr, dash, bend left, "I"] \arrow[r, dash, bend right, "C_3"'] \arrow[d, dash] & M \arrow[r, dash, "4"] \arrow[r, dash, bend right, "C_2 \times C_2"'] \arrow[d, dash] & L \arrow[d, dash] \\
(2) = \mathfrak{p} \arrow[r, dash, "e{=}1"] & \mathfrak{P}_K \arrow[r, dash, "e{=}3"] & \mathfrak{P}_M \arrow[r, dash, "e{=}4"] & \mathfrak{P}_L\,.
\end{tikzcd}$$

Consider $L = \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}, \zeta_8)$ and $\mathcal{O}_L = \mathbb{Z}_2[\zeta_3, \sqrt[3]{2}, \zeta_8]$ with prime ideal $\mathfrak{P}_L$ above the prime ideal $\mathfrak{P}_K = (\sqrt[3]{2})$. The coordinates of all branch points are powers of ζ_8, with respect to the coordinate x. Therefore it suffices to look at the actions of the higher ramification groups on $\mathfrak{P}_{L_0} = (1 + \zeta_8) \lhd \mathcal{O}_{L_0}$. Note that in $\mathcal{O}_L$ we have $(\mathfrak{P}_L)^{12} = (2) = \mathfrak{P}_{L_0}^4$, which implies $(\mathfrak{P}_L)^3 = \mathfrak{P}_{L_0}$ and $v_{\mathfrak{P}_L} = 3v_{\mathfrak{P}_{L_0}}$.

We now compute the filtration of Γ into higher ramification groups Γ_i, as defined in Definition 3.1.2. As we have seen, the first higher ramification group is $\Gamma_0 = I = C_3 \ltimes (C_2 \times C_2)$. Its generators α, β, γ are given above.

The next ramification group is the wild inertia subgroup $P := \Gamma_1$, which is the Sylow 2-subgroup of I, hence $\Gamma_1 = C_2 \times C_2$, generated by α and β.

Now $\Gamma_2 = \{\sigma \in \Gamma_1 \mid v_{\mathfrak{P}_{L_0}}((\sigma(\pi) - \pi)/\pi) \geq 2 \text{ for all } \pi \in \mathcal{O}_{L_0}\}$ is a subgroup of $\langle \alpha, \beta \rangle$. Considering the actions of α, β, and $\alpha\beta$ on the uniformizer $\pi_0 := 1 + \zeta_8$ of $\mathcal{O}_{L_0}$, we get

$$\begin{aligned}
v_{\mathfrak{P}_{L_0}}\left(\frac{\alpha(\pi) - \pi}{\pi}\right) &= v_{\mathfrak{P}_{L_0}}\left(\frac{\zeta_8^3 - \zeta_8}{1 + \zeta_8}\right) = v_{\mathfrak{P}_{L_0}}(\zeta_8 - 1) = 1 &&\Rightarrow v_{\mathfrak{p}_L}\left(\frac{\alpha(\pi) - \pi}{\pi}\right) &&= 3 \\
v_{\mathfrak{P}_{L_0}}\left(\frac{\beta(\pi) - \pi}{\pi}\right) &= v_{\mathfrak{P}_{L_0}}\left(\frac{\zeta_8^5 - \zeta_8}{1 + \zeta_8}\right) = v_{\mathfrak{P}_{L_0}}(2\sqrt{2}) - 1 = 3 &&\Rightarrow v_{\mathfrak{p}_L}\left(\frac{\beta(\pi) - \pi}{\pi}\right) &&= 9 \\
v_{\mathfrak{P}_{L_0}}\left(\frac{\alpha\beta(\pi) - \pi}{\pi}\right) &= v_{\mathfrak{P}_{L_0}}\left(\frac{\zeta_8^7 - \zeta_8}{1 + \zeta_8}\right) = v_{\mathfrak{P}_{L_0}}(\sqrt{2}) - 1 = 1 &&\Rightarrow v_{\mathfrak{p}_L}\left(\frac{\alpha\beta(\pi) - \pi}{\pi}\right) &&= 3\,.
\end{aligned}$$

In conclusion,

$$\Gamma_1 = \Gamma_2 = \Gamma_3 = \langle \alpha, \beta \rangle = C_2 \times C_2, \qquad \Gamma_4 = \ldots = \Gamma_9 = \langle \beta \rangle = C_2,$$

and all groups Γ_i with index $i \geq 10$ are trivial.

Now we look at the action of the Γ_i on the components of $\bar{Y}$. We have already seen that $\bar{Y}/I$ is a projective line. Since γ does not act on the ζ_8^i, we have $(\bar{X}_2 \sqcup \bar{X}_3)/\langle \alpha, \beta \rangle = \bar{W}_2$, hence $\bar{Y}/\Gamma_1, \ldots, \bar{Y}/\Gamma_3$ are curves of genus zero.

The element β yields $(\bar{X}_2 \sqcup \bar{X}_3)/\langle\beta\rangle = \bar{W}_2 \sqcup \bar{W}_2$, yet β acts trivially on $\bar{X}_1, \bar{Y}_1$. So $\bar{Y}/\Gamma_4, \ldots, \bar{Y}/\Gamma_9$ are curves of genus one. All curves $\bar{Y}/\Gamma_i$ with higher index are identical to $\bar{Y}$.

With the formula in [BW16, Thm. 2.9], we compute the conductor exponent f_2 to

$$f_2 = 2g(Y) - 2g(\bar{Y}/\Gamma) + \sum_{i=1}^{\infty} \frac{|\Gamma_i|}{|\Gamma_0|}(2g(Y) - 2g(\bar{Y}/\Gamma_i)) = 6 - 0 + 3 \cdot \frac{4}{12} \cdot 6 + 6 \cdot \frac{2}{12} \cdot 4 = 16.$$

The case $p = 3$

First, by renaming the variables we get the equation $y^4 = x^3 - 1$ of an isomorphic curve and avoid the more complicated case where p divides the degree of the cover, cf. [BW16, Section 3.1]. The cover $Y \to \mathbb{P}^1_x, (x, y) \mapsto x$, given by $y^4 = x^3 - 1$ has branch points $z_1 = 1$, $z_2 = \zeta_3$, $z_3 = \zeta_3^2$, and $z_4 = \infty$. Since

$$y^4 = (x - 1) \cdot (x - \zeta_3) \cdot (x - \zeta_3^2),$$

we get multiplicities $a_1 = a_2 = a_3 = 1$ and thus $a_4 := -\sum_i a_i \pmod 4 = 1$. Therefore we have $e_1 = e_2 = e_3 = e_4 = 4$ and $(n, a_i) = 1$ ramification point (with $n = 4$).

Separation of points

We extend $\mathbb{Q}_3$ to $L_0 = \mathbb{Q}_3(\zeta_3)$, which is Galois and the splitting field of f. The corresponding prime ideal in $\mathcal{O}_{L_0}$ is $\mathfrak{P}_{L_0} = (1 - \zeta_3)$ with $\mathfrak{P}_{L_0}^2 = (3)$. Modulo $\mathfrak{P}_{L_0}$, all zeros of $x^3 - 1$ specialize to 1. To separate the three points we set

$$x_1 := \frac{x - 1}{\zeta_3 - 1}$$

and find the following situation on the component $\bar{X}_1$.

x	1	ζ_3	ζ_3^2	∞
$x \mod \mathfrak{P}_{L_0}$	1	1	1	∞
$\bar{x}_1 = x_1 \mod \mathfrak{P}_{L_0}$	0	1	2	∞

Table 5.4: Coordinate x_1

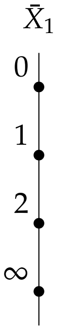


Figure 5.8: Coordinate x_1

Denote $\pi := \zeta_3 - 1$ and note that $3 = -\pi^2\zeta_3^2$. Then the new equation (in terms of y and x_1) is

$$\begin{aligned} y^4 &= x^3 - 1 \\ &= (\zeta_3 - 1)^3 x_1^3 + 3(\zeta_3 - 1)^2 x_1^2 + 3(\zeta_3 - 1)x_1 \\ &= \pi^3\left(x_1^3 - (\zeta_3 - 1)\zeta_3^2 x_1^2 - \zeta_3^2 x_1\right). \end{aligned}$$

We set $y_1 = \sqrt[4]{\pi^3}y$ and get

$$\begin{aligned} y_1^4 &= x_1^3 + (1 - \zeta_3)\zeta_3^2 x_1^2 - \zeta_3^2 x_1 \\ \bar{y}_1^4 &\equiv \bar{x}_1^3 - \bar{x}_1 \pmod{\mathfrak{P}_{L_0}}, \end{aligned}$$

as an equation for the new component $\bar{Y}_1 \to \bar{X}_1$. According to Section 5.1.1 we have semistable reduction over the Galois closure L of $L_0(i, \alpha := \sqrt[4]{\pi}) = \mathbb{Q}_3(\zeta_3, i, \alpha)$, which is a degree-32 extension of $\mathbb{Q}_3$.

We obtain the following prime ideals and residue fields.

$$\begin{tikzcd} L := \mathbb{Q}_3(\zeta_3, \alpha, i, \beta) \arrow[d, dash, "4"] & \mathfrak{P}_L \arrow[d, dash, "1"] & k = \mathbb{F}_3(i) \arrow[d, dash, "2"] \\ \mathbb{Q}_3(\zeta_3, \alpha) \arrow[d, dash, "4"] & (\alpha) \arrow[d, dash, "4"] & k = \mathbb{F}_3 \arrow[d, dash, "1"] \\ L_0 = \mathbb{Q}_3(\zeta_3) \arrow[d, dash, "2"] & (\pi) \arrow[d, dash, "2"] & k = \mathbb{F}_3 \arrow[d, dash, "1"] \\ \mathbb{Q}_3 & (3) & k = \mathbb{F}_3 \end{tikzcd}$$

Here β is the generator of the degree-two extension $L/\mathbb{Q}_3(\zeta_3, \alpha, i)$.

The Galois group Γ has order 32. The above diagram yields that the order of the inertia group I is 8.

Inertia group

The inertia group is the semidirect product of an m-cyclic group (with m prime to 3) and a Sylow 3-group. Thus the only possibility is $I = C_8$. This group contains an element σ which exchanges ζ_3 and ζ_3^2. Hence $\bar{Y}_1/I$ is a degree-4 cover ramified over at most three points and has genus zero (by Riemann–Hurwitz). So the contribution to the L-factor is trivial.

Since $\Gamma_1 = P$ is the Sylow 3-subgroup of I, we have $\Gamma_1 = \{\mathrm{id}\}$ and thus $\delta = 0$. Or equivalently: $L/\mathbb{Q}_3$ is a tamely ramified extension, hence $\delta = 0$ by [BW16, Cor. 2.6]. The conductor exponent is

$$f_3 = \epsilon + \delta = 2g(Y) - 2g(\bar{Y}/\Gamma) + 0 = 6 - 0 + 0 = 6.$$

We have shown that $L_2 = 1, L_3 = 1$ and the conductor exponents are $f_2 = 16, f_3 = 6$.

5.1.3 Second example: $y^3 = x^4 - 1$

Note that the map

$$(x, y) \mapsto (\zeta_8 x, \zeta_6 y)$$

provides an isomorphism from the curve defined by $y^3 = x^4 + 1$ to the one given by $y^3 = x^4 - 1$. It is defined over $\mathbb{Q}(\zeta_6, \zeta_8) \simeq \mathbb{Q}[x]/(x^8 - x^4 + 1)$. So the two curves are twists of each other, cf. the twists in Section A.1.

Consider the degree-3-cover of $\mathbb{P}^1$:

$$\begin{aligned} Y &\longrightarrow \mathbb{P}^1_x \\ (x, y) &\longmapsto x, \end{aligned}$$

birationally given by $y^3 = x^4 - 1$. Its branch points are $z_1 = 1$, $z_2 = -1$, $z_3 = i$, $z_4 = -i$, and $z_5 = \infty$. As with the former example, Y has bad reduction exactly at $p = 2$ and $p = 3$.

The case $p = 2$

Again, we work over the local field $\mathbb{Q}_2$. Write $L_0 = \mathbb{Q}_2(i)$ for the splitting field of $x^4 - 1$. We get the following situation modulo $\mathfrak{P}_{L_0} = (1 + i) \lhd \mathcal{O}_{L_0}$ (Figure 5.9):

x	1	-1	i	$-i$	∞
$x \mod \mathfrak{P}_{L_0}$	1	1	1	1	∞

Table 5.5: Coordinate x

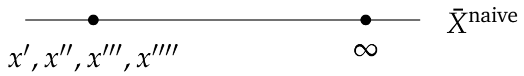


Figure 5.9: Coordinate x

We separate 1 from -1, i from $-i$, and 1 from $-i$, while fixing ∞. This corresponds to the following Möbius transformations $x_1 = (1 - x)/2$, $x_2 = (i - x)/(2i)$, $x_3 = (x + i)/(1 + i)$, which results in the situation depicted in Figure 5.10.

x	1	-1	i	$-i$	∞
$x \mod \mathfrak{P}_{L_0}$	1	1	1	1	∞
x_1	0	1	$\frac{1-i}{2}$	$\frac{1+i}{2}$	∞
$\bar{x}_1 \equiv x_1 \mod \mathfrak{P}_{L_0}$	0	1	∞	∞	∞,
x_2	$\frac{1+i}{2}$	$\frac{1-i}{2}$	0	1	∞
$\bar{x}_2 \equiv x_2 \mod \mathfrak{P}_{L_0}$	∞	∞	0	1	∞,
x_3	1	$\frac{-1+i}{1+i}$	$\frac{2i}{1+i}$	0	∞
$\bar{x}_3 \equiv x_3 \mod \mathfrak{P}_{L_0}$	1	1	0	0	∞,

Table 5.6: Coordinates x_1, x_2, x_3

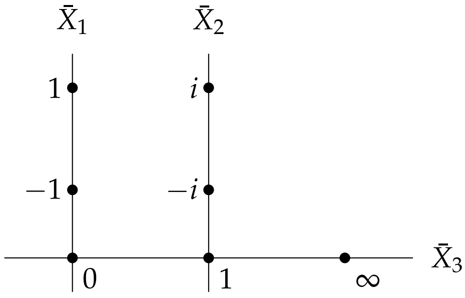


Figure 5.10: $\bar{X}$

Applying the change of variables leads to the following equation

$$\begin{aligned} y^3 &= x^4 - 1 \\ &= 8(2x_1^4 + 4x_1^3 + 3x_1^2 + x_1). \end{aligned}$$

We set $y^3 = 2^3 y_1^3$ and thus $y_1 = y/2$. The equation for the component $\bar{Y}_1$ of $\bar{Y}$ is

$$\bar{y}_1^3 \equiv \bar{x}_1^2 + \bar{x}_1,$$

an elliptic curve. Analogously, we set $y^3 = 2^3 i^3 y_2^3$ and thus $y_2 = y/(2i)$. The equation for $\bar{Y}_2$ is

$$\bar{y}_2^3 \equiv \bar{x}_2^2 + \bar{x}_2,$$

also an elliptic curve. For the third component $\bar{Y}_3$, we set $x = (1+i)x_3 - i$ and $y = \sqrt[3]{4}y_3$, hence we extend L_0 to $\mathbb{Q}_2(i, \sqrt[3]{2})$ and obtain

$$\bar{y}_3^3 = \bar{x}_3^4 + \bar{x}_3^2,$$

a third elliptic curve. Note that the Galois closure of $\mathbb{Q}_2(i, \sqrt[3]{2})$ is $L := \mathbb{Q}_2(i, \sqrt[3]{2}, \zeta_3)$. All field extensions used so far are (sorted from unramified to wildly ramified):

$$\begin{tikzcd}
L = \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}, i) \arrow[d, dash, "2"] & \mathfrak{P}_L \arrow[d, dash, "2"] & k(\mathfrak{P}_L) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "1"] \\
M := \mathbb{Q}_2(\zeta_3, \sqrt[3]{2}) \arrow[d, dash, "3"] & \mathfrak{P}_M = (\sqrt[3]{2}) = (\mathfrak{P}_L)^2 \arrow[d, dash, "3"] & k(\mathfrak{P}_M) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "1"] \\
K := \mathbb{Q}_2(\zeta_3) \arrow[d, dash, "2"] & \mathfrak{P}_K = (2) \arrow[d, dash, "1"] & k(\mathfrak{P}_K) = \mathbb{F}_2(\zeta_3) \arrow[d, dash, "2"] \\
K_0 = \mathbb{Q}_2 & \mathfrak{p} = (2) & k = \mathbb{F}_2
\end{tikzcd}$$

Galois group and inertia group

Using [Lan02, Cpt. VI, § 1, Thm. 1.14], we get

$$\Gamma = C_2 \times C_6 = \langle \alpha : i \mapsto -i, \beta : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}, \gamma : \zeta_3 \mapsto \zeta_3^2 \rangle.$$

The inertia subgroup is $I = C_3 \ltimes C_2 = C_6 = \langle \alpha : i \mapsto -i, \beta : \sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2} \rangle$.

Inertial reduction

We see that I acts trivially on $\bar{X}_1$,

$$\bar{X}_1/I = \bar{X}_1/\langle \alpha \rangle = \bar{X}_1.$$

This is not the case for $\bar{X}_2$:

$$\bar{X}_2/I = \bar{X}_2/\langle\alpha\rangle,$$

and the cover $\bar{Y}_2/I \to \bar{X}_2/I$ has only two ramification points, see Figure 5.11. So the component $\bar{Y}_2$ does not contribute to the L-factor.

The action of I on $\bar{Y}_1$ is

$$\bar{Y}_1/I = \bar{Y}_1.$$

So we have to consider the action of Γ/I on the cover $\bar{Y}_1 \to \bar{X}_1$. The group Γ/I is generated by $\gamma : \zeta_3 \mapsto \zeta_3^2$ and $y_1 = y/2$. So the component $\bar{Y}_1$ contributes to the L-factor as an elliptic curve.

On the third component, α exchanges the two pairs of double points on $\bar{X}_3$, and β exchanges the points of the fiber of $\bar{Y}_3 \to \bar{X}_3$: $\beta(y_3) = \zeta_3^2 y_3$. So the quotient by β has genus zero and it follows that this component does not contribute to L_2. But $\bar{Y}_3/\langle\alpha\rangle \to \bar{X}_3/\langle\alpha\rangle$ is still a genus one curve (Figure 5.11).

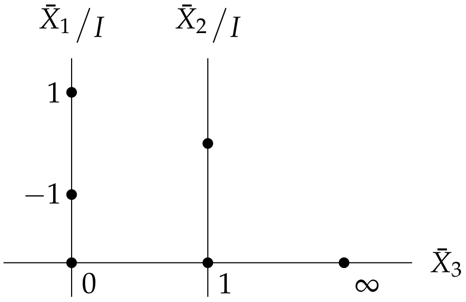


Figure 5.11: Action of I

As $|I| = C_3 \ltimes C_2$, we have $\Gamma_1 = C_2 = \langle\alpha : i \mapsto -i\rangle$. And since $(\mathfrak{P}_{L_0})^2 = (1+i)^2 = (2) = (\mathfrak{P}_L)^6$ we have $v_{\mathfrak{P}_L} = 3v_{\mathfrak{P}_{L_0}}$. So

$$v_{\mathfrak{P}_L}\left(\frac{\alpha(1+i)-(1+i)}{1+i}\right) = 3,$$

and $\langle\alpha\rangle = \Gamma_1 = \Gamma_2 = \Gamma_3 = C_2$. All further higher ramification groups $\Gamma_4, \Gamma_5, \ldots$ are trivial. We compute the conductor exponent at 2:

$$f_2 = \epsilon + \delta = 2g(Y) - 2g(\bar{Y}/\Gamma) + \sum_{i=1}^{3} \frac{|\Gamma_i|}{|\Gamma_0|} \cdot (2g(Y) - 2g(\bar{Y}/\Gamma_i)) = 6 - 2 + 3 \cdot \frac{2}{6} \cdot (6-4) = 6$$

Consequences

The local factor at $p = 2$ is the L-factor of the elliptic curve $\bar{Y}_1 \to \bar{X}_1$: $L_2 = 1 + 2T^2$, which results from $|\bar{Y}_1(\mathbb{F}_2)| = 3 = p + 1$. Moreover, the conductor exponent is $f_2 = 6$.

The case $p = 3$

We exchange x and y and adjust the equation to

$$y^4 = x^3 + 1 = (x+1)(x+\zeta_3)(x+\zeta_3^2)\,.$$

Hence we extend $\mathbb{Q}_3$ to the splitting field $L_0 = \mathbb{Q}_3(\zeta_3)$ of x^3+1 with prime ideal $\mathfrak{P}_{L_0} = (1-\zeta_3) \lhd \mathcal{O}_{L_0}$.

Separating points

Modulo $\mathfrak{P}_{L_0}$ we have the following situation. The cover $Y \to \mathbb{P}^1$ ramifies over the three zeros of x^3+1 and ∞. We choose the following Möbius transformation

$$x_1 = \frac{x+1}{1-\zeta_3},$$

which results in the situation of Figure 5.12:

x	-1	$-\zeta_3$	$-\zeta_3^2$	∞
$x \mod \mathfrak{P}_{L_0}$	-1	-1	-1	∞
x_1	0	1	$1+\zeta_3$	∞
$\bar{x}_1 \equiv x_1 \mod \mathfrak{P}_{L_0}$	0	1	2	∞ ,

Table 5.7: Coordinate x_1

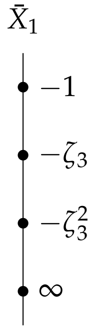


Figure 5.12: $\bar{X}$

New equation

Applying the change of variables leads to the following equation

$$\begin{aligned} y^4 &= x^3+1 \\ &= (1-\zeta_3)^3x_1^3 - 3(1-\zeta_3)^2x_1^2 + 3(1-\zeta_3)x_1 - 1 + 1 \\ &= (1-\zeta_3)^3(x_1^3 + (1-\zeta_3)\zeta_3^2x_1^2 - \zeta_3^2x_1)\,. \end{aligned}$$

We set $y^4 = (1-\zeta_3)^3y_1^4$ and note that $\bar{Y}$ has only one component $\bar{Y}_1$ and is semistable over the same field extension $L/\mathbb{Q}_3$ as in the $p = 3$ case of the first example. The equation for $\bar{Y}_1 \to \bar{X}_1$ is:

$$\bar{y}_1^4 \equiv \bar{x}_1^3 + \bar{x}_1,$$

with zeros at $0, 1, 2 \pmod{\mathfrak{P}_{L_0}}$.

Inertia group

With the same arguments as in the $p = 3$ case of $y^3 = x^4 + 1$, we see that $\bar{Y}_1/I \to \bar{X}_1/I$ is ramified over at most three distinct points, hence has genus zero by Riemann–Hurwitz.

Consequences

The local factor at $p = 3$ is $L_3 = 1$. With a calculation as in the $p = 3$ case of $y^3 = x^4 + 1$, we get $f_3 = 6$.

Recall that the two curves discussed so far are twists of each other, isomorphic over a degree-8 extension of $\mathbb{Q}$. Since $p = 3$ does not divide this degree, the Swan conductor δ in the conductor exponent f_3 is equal for both curves.

Numerical verification

We can verify the results of the two examples with a very high probability numerically, cf. Section 3.6. Recall that we assume (FEq) to be verified if the result of `check_functional_equation()` is smaller than 10^{-14} in absolute value.

We give an excerpt of a *Sage* session which verifies (FEq) for both curves. Note that the coefficients a_n (`coeff`) were computed beforehand. The parameter `gammaV` represents the genus of the curve, `weight=2` is from the symmetry of (FEq): $\Lambda(s) = \Lambda(\mathbf{2} - s)$, and `mu` is the sign of (FEq), see Conjecture 3.5.1.

Curve $y^3 = x^4 + 1$:

```
sage: L=Dokchitser(conductor=2^16*3^6,gammaV=[0,0,0,1,1,1],weight=2,mu=1)
sage: L.init_coeffs(coeff)  # initialization
sage: L.check_functional_equation()
-1.30104260698261e-18
```

Curve $y^3 = x^4 - 1$:

```
sage: L=Dokchitser(conductor=2^6*3^6,gammaV=[0,0,0,1,1,1],weight=2,mu=1)
sage: L.init_coeffs(coeff)
sage: L.check_functional_equation()
-6.38378239159465e-16
```

We conclude that our results verify the conjectured functional equation (FEq) for these two curves, up to the described precision.

5.2 L-functions of Picard curves over $\mathbb{Q}$ good away from S

5.2.1 Picard curves

Definition 5.2.1 (Picard curve)

Let K be a field of characteristic $\neq 3$. Let Y be a smooth absolutely irreducible projective curve of genus 3 over K given by the following equation (in the sense of Def. 2.1.5)

$$y^3 = f(x) \;\text{ with }\; f \in K[x] \;,\; \deg(f) = 4,$$

where f has no multiple roots over K^{alg}. Then we call Y a *Picard curve* over K. ◁

Remark 5.2.2 (Properties)

i) The polynomial f in Definition 5.2.1 may be replaced by

$$\tilde{f}(x) = f(ax+b) \;\text{ with }\; a \in K^{\times}\,,\, b \in K$$

without changing the curve Y.

ii) If one fixes an equation $y^3 = f(x)$ for Y, then Y has a unique point at infinity, denoted ∞ (Lemma 2.1.7).

We now assume that $K = K_{\mathfrak{p}}$ is a $\mathfrak{p}$-adic number field with residue characteristic $\neq 3$.

iii) For a fixed equation $y^3 = f(x)$ for Y, the following holds.
- If $\bar{f} = f \pmod{\mathfrak{p}}$ is separable, the special fiber at $\mathfrak{p}$ of the naive model (cf. Section 4.4.1) is given by

$$y^3 = \bar{f}(x),$$

cf. Theorem 2.2.6. In particular, Y has good reduction at $\mathfrak{p}$.
- The specialization of the point at infinity is smooth (Corollary 2.2.7).

We now consider Picard curves over $K = \mathbb{Q}$, resp. $\mathbb{Q}_p$.

Lemma 5.2.3

A Picard curve Y over $\mathbb{Q}$ has bad reduction at $p = 3$.

Proof: Let Y be given by a fixed equation $y^3 = f(x)$. Assume there is a smooth model $\mathcal{Y}$ of Y over $\mathbb{Z}_3$. Let $\bar{Y}$ be the special fiber of $\mathcal{Y}$. This is a smooth curve over $\mathbb{F}_3$ by assumption. Let $\mathcal{O}_L := \mathbb{Z}_3[\zeta_3]$ and $\mathcal{Y}' := \mathcal{Y} \otimes_{\mathbb{Z}_3} \mathcal{O}_L$. Then $\mathcal{Y}'$ is a smooth model over $\mathcal{O}_L$ with special fiber $\bar{Y}$. Let τ be the automorphism of $\mathcal{Y}'$ induced by the automorphism $\tilde{\tau}$ of $\mathcal{O}_L$ with $\tilde{\tau}(\zeta_3) = \zeta_3^2$. We observe that the restriction of τ to $\bar{Y}$ is trivial.

Now let σ be the $\mathcal{O}_L$-linear automorphism of $\mathcal{Y}'$ with $\sigma(y) = \zeta_3 y$. A simple calculation shows that $\tau \circ \sigma \circ \tau = \sigma^2$. Since Y has genus $3 \geq 2$, $\mathcal{Y}'$ is a stable model over $\mathcal{O}_L$. Therefore the homomorphism

$$\mathrm{Aut}(\mathcal{Y}'/\mathcal{O}_L) \to \mathrm{Aut}(\bar{Y}/\mathbb{F}_3)$$

is injective by [DM69, Thm. I.11]. Particularly we have

$$\sigma \neq \sigma^2. \tag{5.2.1}$$

However, if we restrict Equation (5.2.1) to $\bar{Y}$, we get

$$\sigma_{|\bar{Y}} = (\sigma^2)_{|\bar{Y}}.$$

This is a contradiction and proves the lemma. □

Lemma 5.2.4

Let Y be a Picard curve over $\mathbb{Q}$ given by $y^3 = f(x)$. Denote by $K_0/\mathbb{Q}$ the splitting field of f and let $p \neq 3$ be a prime.

If Y has good reduction at p, then p is unramified in the extension $K_0/\mathbb{Q}$.

Proof: Assume Y has good reduction at p. Then the ramification points, i.e. the roots of f and ∞, specialize to pairwise distinct points. Or in terms of Section 5.1.1, $(\bar{X}, \bar{D})$ consists of one projective line with all ramification points on it. This means that w.l.o.g. Y may be given by a polynomial f with $\bar{f} \in \mathbb{F}_p[x]$ separable. Hence p is unramified in $K_0/\mathbb{Q}$. □

Corollary 5.2.5

A Picard curve Y over $\mathbb{Q}$ has good reduction at $p \neq 3$ if and only if there is an equation $y^3 = f(x)$ for Y such that $p \nmid \Delta(f)$. ◁

Computing L-factors and conductor

We now describe how to compute all bad factors and the conductor of a Picard curve over $\mathbb{Q}$. For all primes in $S \setminus \{3\}$ (the *tame case*), we can proceed as in Section 5.1. However, in general we cannot circumvent the case that p divides the degree of the cover, as with the two examples given by $y^3 = x^4 \pm 1$ resp. $y^4 = x^3 \pm 1$. So if $p = 3$ (the *wild case*), we apply an algorithm which is described in [Arz12] and [AW12]. Some improvements and a *Sage* implementation of many of the necessary steps can be found in [Rüt14] and [RW].

5.2.2 Tame case: $p \neq 3$

If $p \neq 3$, there are typical cases for the reduction behavior of the polynomial f that occur with almost all examples. We now list these cases and describe the structure of their bad L-factors and conductor exponents.

All examples given in this section have been successfully checked to fulfill the functional equation (FEq) with the procedure from Section 3.6. The complete lists of all Picard curves over $\mathbb{Q}$ where we successfully verified (FEq) can be found in Sections A.1 and A.2.

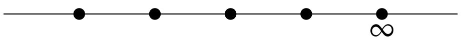
Remark 5.2.6 (Typical cases)

We have seen in Sections 5.1.2 and 5.1.3 that the structure of the special fiber $\bar{X}$ of the stably marked model is important for the semistable model of Y (for details, consider [BW16, § 4.1]). More precisely, we look at the stably marked tree $(\bar{X}, \bar{D})$ of components of $\bar{X}$ together with the divisor $\bar{D}$ of the ramification points.

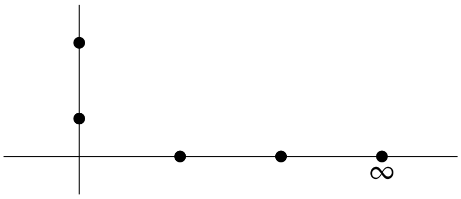
A Picard curve Y has one distinguished point — the point at infinity. The other ramification points are the roots of f in the splitting field K_0.

All possible stably marked trees in this situation are:

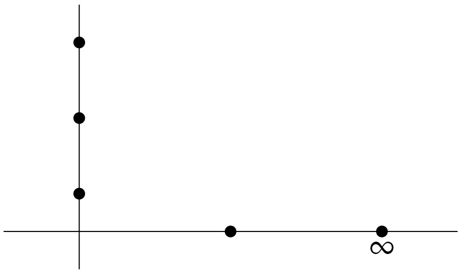
[1111]



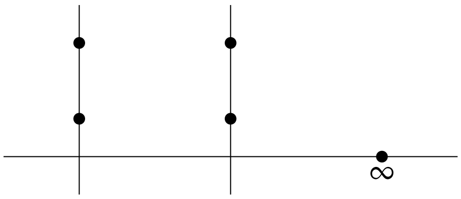
[112]



[13]



[22]



For a given Picard curve Y, we may choose f such that f has degree 4. Moreover, in the following cases for the reduction behavior of f modulo p we may directly read off the according case from the configuration of roots of $\bar{f}$:

- $\bar{f} = (x-a)(x-b)(x-c)(x-d)$ for pairwise distinct $a, b, c, d \in \mathbb{F}_p$ (case `[1111]`).
- $\bar{f} = (x-a)(x-b)(x-c)^2$ for pairwise distinct $a, b, c \in \mathbb{F}_p$ (case `[112]`).
- $\bar{f} = (x-a)(x-b)^3$ for pairwise distinct $a, b \in \mathbb{F}_p$ (case `[13]`).
- $\bar{f} = (x-a)^2(x-b)^2$ for pairwise distinct $a, b \in \mathbb{F}_p$ (case `[22]`). ◁

There are special cases that do not fall within this list, e.g. `[112]`a) and `[22]`c) (see below). There one identifies the structure of $\bar{X}$ with the methods from Section 5.1. Moreover, case `[1111]` may be acquired only after a ramified extension $K_0/\mathbb{Q}_p$. This is the case of potentially good reduction (Definition 2.3.1). ◁

We now discuss the cases `[112]`, `[22]`, and `[13]` in more detail. All of the examples of Picard curves good away from S where we verified (FEq) (Section A.2) can be matched to one of those three cases. We give a sketch of the computations necessary to compute all bad factors and the conductor N. For details, consider the detailed examples in Sections 5.1.2 and 5.1.3. We emphasize that in principle, we can find examples for all of the cases discussed in Remark 5.2.6. However, we found computable examples (i.e. with N small enough to verify (FEq)) only for the cases `[112]`, `[22]`, and `[13]`.

Case `[112]`

The polynomial f reduces to $(x-a)^2 \cdot g(x)$ in $\mathbb{F}_p[x]$ where $g(a) \neq 0$ and g is squarefree. We apply the algorithm from Section 5.1. One finds that $\bar{X}$ looks as follows (Figure 5.13).

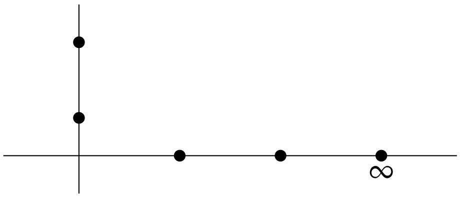


Figure 5.13: Case `[112]`

The inertial reduction $\bar{Y}/\Gamma$ has genus two and the contribution of the graph of components to the local L-factor is trivial. In this situation L_p is of degree 4 and can be computed by point counting on the normalization of the special fiber of the naive model. The conductor exponent is $f_p = 2 \cdot (3-2) + \delta = 2 + \delta$ (cf. Conjecture 3.5.1 or [BW16, Thm. 2.9]). The contribution of δ to f_p is trivial if and only if the extension $L/\mathbb{Q}_p$ where Y acquires semistable reduction is at most tamely ramified [BW16, Cor. 2.6].

Examples:

a) f splits over a degree-two extension of $\mathbb{Q}_2$.

$$f = x^4 + 3x^3 + 3x^2 + 2x = x(x+2)(x^2+x+1) \equiv_2 x^2(x^2+x+1)$$
$$L_2 = 1 + T^2 + 4T^4$$
$$N = 2^2 \cdot 3^{13}$$

b) $\mathbb{Q}_5$ is the splitting field of f, but Y acquires semistable reduction only after a tamely ramified extension of $\mathbb{Q}_5$.

$$f = x^4 - 8x^3 + 17x^2 - 10x = x(x-1)(x-2)(x-5) \equiv_5 x^2(x-1)(x-2)$$
$$L_5 = 1 + T^2 + 25T^4$$
$$N = 2^4 \cdot 3^{11} \cdot 5^2$$

Case [22]

The polynomial f reduces to $(x-a)^2(x-b)^2$ with $a \neq b$ in $\mathbb{F}_p$. One finds that $\bar{X}$ looks as follows (Figure 5.14).

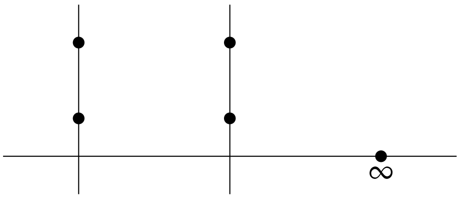


Figure 5.14: Case [22]

The contribution of the graph of components is trivial. The L-factor is either trivial (as with the example given by $y^3 = x^4 + 1$ in Section 5.1.2) or can be derived by point counting on the genus-one components of $\bar{Y}/\Gamma$.
The conductor exponent is $f_p = 2 \cdot (3 - g(\bar{Y}/\Gamma)) + \delta$.

Examples:

a) The polynomial f splits already over $\mathbb{Q}_5$. We acquire semistable reduction over a tamely ramified extension $L/\mathbb{Q}_5$.

$$f = x^4 - 12x^3 + 41x^2 - 30x = x(x-1)(x-5)(x-6) \equiv_5 x^2(x-1)^2$$
$$L_5 = 1 + 5T^2$$
$$N = 2^4 \cdot 3^{11} \cdot 5^4$$

b) The polynomial f splits over a degree-two extension of $\mathbb{Q}_2$, resp. $\mathbb{Q}_7$.

$$\begin{aligned} f &= x^4+3x^2+4 = (x^2+x+2)(x^2-x+2) \equiv_2 x^2(x-1)^2 \equiv_7 (x-3)^2(x-4)^2 \\ L_2 &= 1+2T^2 \\ L_7 &= 1+T+7T^2 \\ N &= 2^4\cdot 3^9\cdot 7^4 \end{aligned}$$

c) Here f splits over a degree-three extension of $\mathbb{Q}_7$.

$$\begin{aligned} f &= x^4+31x^3+195x^2-144x-83 = (x-1)(x^3+32x^2+227x+83) \equiv (x-1)^4 \\ L_7 &= 1+4T+7T^2 \\ N &= 3^9\cdot 7^4 \end{aligned}$$

The two curves given by $y^3 = x^4 \pm 1$ (Sec. 5.1.2 and 5.1.3) also fall within case [22].

Case [13]

The polynomial f reduces to $(x-a)(x-b)^3$ and $\bar{X}$ looks as follows.

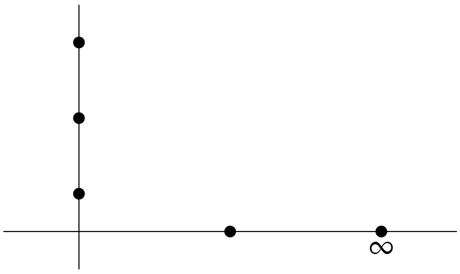


Figure 5.15: Case [13]

The cover $\bar{Y} \to \bar{X}$ consists of a genus-one curve and a genus-zero curve, intersecting in the three points above the specializations of the three roots of f.

We can classify all L-factors that occur within this case. The necessary theory is developed in the following.

Lemma 5.2.7 (Cubes in finite fields)
In a prime field $\mathbb{F}_p$ the endomorphism

$$a \mapsto a^3 \quad , \quad a \in \mathbb{F}_p$$

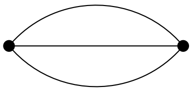
is bijective if and only if $\frac{p-1}{3}$ is not an integer.
If the map is not bijective, then there are $\frac{p-1}{3}$ cubes in $\mathbb{F}_p^\times$ with 3 cube roots each.

Proof: This follows from the fact that $(\mathbb{F}_p^\times, \cdot)$ is a cyclic group. □

The following lemma describes the graph of components of $\bar{Y} \to \bar{X}$. Recall that in the graph, edges correspond to intersection points and vertices to components.

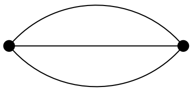
Lemma 5.2.8

Consider the following graph of components which represents two irreducible curves intersecting in three points.

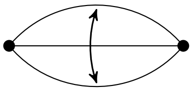


We give a list of all possible permutations of the edges, together with a representation of the action on the cohomology of the graph and the characteristic polynomials.

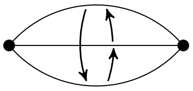
i) Fixed edges

 , $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $(1-T)^2$

ii) Transposition of two edges

 , $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, $(1-T)(1+T)$

iii) Permutation of all three edges

 , $\begin{pmatrix}\zeta_3 & 0\\ 0 & \zeta_3^2\end{pmatrix}$, $1+T+T^2$

Proof: The statement follows from cohomology and representation theory. □

We claim that the L-factors occurring in case `[13]` are exactly the characteristic polynomials stated in Lemma 5.2.8, and that they can be characterized with the criterion in Lemma 5.2.7.

Proposition 5.2.9

Let Y be a Picard curve over $\mathbb{Q}$ given by f, good away from the set S. Let $p \in S$ be a prime different from 3. Let $f \pmod{p}$ have reduction type `[13]`, i.e. modulo p the polynomial f reduces to

$$\bar{f} = (x-a)\cdot(x-b)^3 \text{ with } a \neq b \pmod{p}.$$

Then the local L-factor at p is

i) $(1-T)^2$ if and only if $\frac{p-1}{3} \in \mathbb{Z}$ and $b-a$ is a cube in $\mathbb{F}_p$,

ii) $(1-T^2)$ if and only if $\frac{p-1}{3} \notin \mathbb{Z}$,

iii) $1+T+T^2$ if and only if $b-a$ is not a cube in $\mathbb{F}_p$.

Proof: With the same methods as in Section 5.1 one shows that the special fiber of the semistable model $\bar{Y} \to \bar{X}$ consists of two irreducible curves of genus one resp. zero that intersect in three points. Again by the method in Section 5.1, the only contribution to L_p comes from the Galois action on the graph of components of $\bar{Y}$.

The three intersection points are (in reduction) determined by the solutions to the equation $\bar{y}^3 = b - a$ over $\mathbb{F}_p$. By Lemma 5.2.7 the cases *i), ii),* and *iii)* correspond to $3, 1$, and 0 solutions of $\bar{y}^3 = b - a$ over $\mathbb{F}_p$, respectively. So 0, 2, and 3 solutions are permuted by the Galois action, in the respective cases. The statement follows with Lemma 5.2.8. □

Examples:

a) $\frac{p-1}{3} \in \mathbb{Z}$ and $(a-b)$ is a cube in $\mathbb{F}_p$. Example for $p = 7$:

$$f = x^4 - 10x^3 + 24x^2 + 18x - 65 = (x-5)(x^3 - 5x^2 - x + 13) \equiv_7 (x-5)(x-4)^3$$
$$L_7 = (1-T)^2$$
$$N = 2^6 \cdot 3^9 \cdot 7^4$$

This corresponds to case *i)* in Proposition 5.2.9.

b) $\frac{p-1}{3} \notin \mathbb{Z}$, so all elements of $\mathbb{F}_p$ are cubes by Lemma 5.2.7. Example for $p = 5$:

$$f = x^4 - 2x^3 - 2x^2 + 5x - 2 = (x-1)(x-2)(x^2 + x - 1) \equiv_5 (x-1)(x-2)^3$$
$$L_5 = 1 - T^2$$
$$N = 3^9 \cdot 5^4$$

This corresponds to case *ii)* in Proposition 5.2.9.

c) $\frac{p-1}{3} \in \mathbb{Z}$ and $(a-b)$ is not a cube in $\mathbb{F}_p$. Example for $p = 7$:

$$f = x^4 + 5x^3 + 6x^2 + x = x(x^3 + 5x^2 + 6x + 1) \equiv_7 x(x-3)^3$$
$$L_7 = 1 + T + T^2$$
$$N = 3^7 \cdot 7^4$$

It corresponds to case *iii)* in Proposition 5.2.9. It is a twist of the curve c) in case [22] with $f_{[22]\mathrm{c})} = f_{[13]\mathrm{c})}(x/7 - 1/7) \cdot 7^4$.

5.2.3 Wild case: $p = 3$

The main idea of the algorithm developed in [Arz12] is to identify the components of the semistable model with a finite set of discrete valuations on $K[x]$. For an example, see e.g. [Rüt14, Cpt. 2].

We illustrate the main steps of this algorithm with one of the Picard curves good away from 3, which can be found in Table A.1.

Example 5.2.10 ($y^3 = x^4 + 2x^3 + 2x^2 + x$)
Using the algorithm in [Arz12, Sec. 3.2], we obtain semistable reduction over the field

$$L = \mathbb{Q}_3(i, \sqrt[4]{3}, \sqrt[3]{3}, \sqrt[3]{2}).$$

Note that the extension $\mathbb{Q}_3(i)/\mathbb{Q}_3$ is unramified, $K := \mathbb{Q}_3(i, \sqrt[4]{3})/\mathbb{Q}_3$ is tamely ramified, and $K(\sqrt[3]{3})/K$ as well as $L/K(\sqrt[3]{2})$ are wildly ramified. The inertia group of the extension $L/\mathbb{Q}_3$ is defined by the subextension $L/\mathbb{Q}_3(i)$ and it has the form

$$I = C_4 \ltimes P_3,$$

where P_3 is the Sylow 3-subgroup. Here P_3 is isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/3$. More precisely, the extension L/K looks as follows:

$$\begin{tikzcd}
 & L \arrow[dl, dash, "H=\langle\gamma\rangle"'] \arrow[dr, dash, "\langle\beta\rangle"] & \\
M_1 = L^H = K(\sqrt[3]{3}) \arrow[dr, dash, "\langle\beta\rangle"'] & & M_2 = K(\sqrt[3]{2}) \arrow[dl, dash, "\langle\gamma\rangle"] \\
 & K = \mathbb{Q}_3(i, \sqrt[4]{3}) &
\end{tikzcd}$$

Where $\beta(\sqrt[3]{3}) = \zeta_3\sqrt[3]{3}$ and $\gamma(\sqrt[3]{2}) = \zeta_3\sqrt[3]{2}$.

As in the $p = 2$ case of Section 5.1.2, one computes uniformizers for each intermediate field and obtains exactly the following two jumps $h_1 = 2, h_2 = 14$ as defined in Definition 3.1.2. For details, see [BW12, § 2.2].

One shows analogously to Sections 5.1.2 and 5.1.3 that the local L-factor is $L_3 = 1$ and $g(\bar{Y}/\langle\beta\rangle) = 2$, $g(\bar{Y}/\langle\gamma\rangle) = 0$. Note that we found $L_3 = 1$ with all our examples, cf. also Sections A.1 and A.2.

The conductor exponent is (with the numbers $h_1 = 2$ and $h_2 - h_1 = 12$ in bold):

$$\begin{aligned} f_3 &= 2g(Y) - 2g(\bar{Y}/\Gamma) + \sum_{i=1}^{\infty} \frac{|\Gamma_i|}{|\Gamma_0|} \big(2g(Y) - 2g(\bar{Y}/\Gamma_i)\big) \\ &= 6 - 0 + \mathbf{2} \cdot \frac{9}{36} \cdot 2 \cdot (3 - 0) + \mathbf{12} \cdot \frac{3}{36} \cdot 2 \cdot (3 - 2) \\ &= 11 \end{aligned}$$

◁

5.3 Construction of Picard curves with low conductor

We introduce Malmskog and Rasmussen's algorithm for the construction of all Picard curves over $\mathbb{Q}$ with good reduction away from $S = 3$ in Section 5.3.1. Then we discuss a generalization to Picard curves over $\mathbb{Q}$ with good reduction outside a finite set S of small primes. A detailed discussion of how to find the minimal conductor N of a Picard curve over $\mathbb{Q}$ can be found in Section 5.3.2.

5.3.1 Malmskog and Rasmussen's algorithm

Let K be a number field. We consider Picard curves Y/K good away from a finite set S, as defined in Definition 5.2.1. Without going into details, we state some more properties of Picard curves necessary for the constructions later in the following remark. For a more detailed description, we refer to [MR14, Sec. 3].

Remark 5.3.1

Let Y be a Picard curve given by a polynomial

$$f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \text{ with } a_4 \neq 0,\, a_i \in K.$$

The curve Y has a smooth projective model with equation $zy^3 = F(x)$ where

$$F(x,z) = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \ ,\, a_i \in K.$$

Denote by $\mathcal{O}_S$ the ring of S-integers of K, i.e.

$$\mathcal{O}_S := \{a \in K \mid v_{\mathfrak{p}}(a) \geq 0 \ \forall\, \mathfrak{p} \notin S\}.$$

For $S = \{3\}$ and $K = \mathbb{Q}$, we have $\mathcal{O}_S = \mathbb{Z}[\frac{1}{3}]$. Define the *discriminant* of $F(x,z)$ as

$$\operatorname{disc}(F) := \prod_{i<j}(\alpha_i\beta_j - \alpha_j\beta_i)^2.$$

Up to twists of the form $dy^3 = F(x,z)$ with an S-unit $d \in \mathcal{O}_S^\times$, every Picard curve with good reduction away from a finite set of primes S in $\mathcal{O}_K$ admits a model given by

$$y^3z = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 =: F(x,z),$$

where $a_i \in \mathcal{O}_S$, $\operatorname{disc}(F) \in \mathcal{O}_S^\times$, and $a_4 = 1$. This model is called *normal form*. We remark that twists are not discussed at this point in [MR14]. In the case $K = \mathbb{Q}$, the twists are defined by d with $d = \prod_{p \in S} p^{k_p}$ with $k_p \in \{0,1,2\}$. For more details about the role of twists, see the discussion after Lemma 5.3.3. ◁

We use the term *Picard curve given by* f (Definition 5.2.1) also for the model $F(x,z)$. For the constructions below, we introduce an equivalence relation on Picard curves over K good away from a fixed finite set of places S of K.

Definition 5.3.2 (Equivalence relation)

Two Picard curves Y_1, Y_2 over a number field K given by $F_1(x,z), F_2(x,z)$ are *equivalent* if there are $a, b, d \in \mathcal{O}_S$ with $a \cdot d \in \mathcal{O}_S^\times$ and $\lambda \in \mathcal{O}_S^\times$ such that

$$F_2(x,z) = \lambda F_1(ax + bz, dz).$$

Write $Y_1 \sim Y_2$ or $F_1 \sim F_2$. ◁

We now only consider Picard curves good away from 3 and present an algorithm by Malmskog and Rasmussen for the construction of all $\mathbb{Q}$-isomorphism classes of Picard curves over $\mathbb{Q}$ with good reduction away from 3 [MR14].

Lemma 5.3.3 (Splitting fields)

Let Y be a Picard curve over $\mathbb{Q}$, good away from 3. The possible splitting fields of the polynomial f defining Y are the number fields given by

$$x^3 - 3\,,\; x^3 - 3x + 1\,,\; \textit{and}\; x^2 + x + 1\,.$$

Proof: By Corollary 5.2.5, the only candidates for f are irreducible polynomials of degree ≤ 4 that generate a number field unramified at 3. The lemma follows from an exhaustive search of the *Database for Number Fields* [KM16]. See also [MR14, Table 1]. □

For the classification of all Picard curves over $\mathbb{Q}$, good away from 3 into a finite number of $\mathbb{Q}$-isomorphism classes, Malmskog and Rasmussen use an idea of Smart [Sma97]. He shows that the equivalence classes of a suitable equivalence relation are in one-to-one correspondence to the $\mathbb{Q}$-isomorphism classes of hyperelliptic curves good away from 2, up to a finite number of twists.

In the case of Picard curves over $\mathbb{Q}$ good away from 3, the twists in question are

$$dy^3 = f(x),$$

with $d \in \{1, 3, 9\}$. Malmskog and Rasmussen adapt Smart's idea to the situation of Picard curves and prove the following:

- If $Y_1 \cong_{\mathbb{Q}} Y_2$ then $Y_1 \sim Y_2$.
- If $Y_2 \sim Y_2$ then Y_1 is $\mathbb{Q}$-isomorphic to one of the three twists of Y_2 by $d \in \{1, 3, 9\}$.

Together with Faltings' Theorem (Shafarevich conjecture) [Fal83], this implies that there are only finitely many equivalence classes of $\sim$. Malmskog and Rasmussen obtain the following theorem.

Theorem 5.3.4 (Construction of Picard curves)

There is a one-to-one correspondence between equivalence classes of $\sim$ and $\mathbb{Q}$-isomorphism classes of Picard curves good away from 3*, up to twists by* $d \in \{1, 3, 9\}$*.*

Proof: This follows from the statements above. □

Recall that every Picard curve admits a normal form given by $F(x,z) \in \mathcal{O}_S[x,z]$ (Remark 5.3.1). Over some extension L of $\mathbb{Q}$, the polynomial F factors as

$$F(x,z) = \prod_{i=1}^{r} (\alpha_i x - \beta_i z) \text{ , with } \alpha_i, \beta_i \in L.$$

We define

$$\Delta_{ij} := \alpha_i \beta_j - \alpha_j \beta_i$$

and the *cross ratio*

$$[i,j,k,\ell] := \frac{\Delta_{ij}\Delta_{k\ell}}{\Delta_{ik}\Delta_{j\ell}} \text{ , for pairwise distinct indices } i,j,k,\ell.$$

Denote by T the set of places in L that lie above the places in S. If F has coefficients in $\mathcal{O}_S$ and

$$\operatorname{disc}(F) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2$$

is in $\mathcal{O}_S^{\times}$, then Δ_{ij} is in $\mathcal{O}_T^{\times}$ for $i \neq j$. The same holds for the cross ratio: $[i,j,k,\ell] \in \mathcal{O}_T^{\times}$. The definition of the cross ratio implies that $[i,j,k,\ell]$ satisfies an equation of the form

$$[i,j,k,\ell] + [k,j,i,\ell] = 1. \tag{5.3.1}$$

The solutions to these equations are a key point in the construction of all Picard curves over $\mathbb{Q}$ good away from 3. More precisely, Equation (5.3.1) is an *S-unit equation* over the field L. Note that we use the standard term S-units although we are actually looking for T-units. There are only finitely many solutions to an S-unit equation [Sil09, Thm. IX.4.1]. Starting with L, we obtain a finite number of equivalence classes of $\sim$. We illustrate the problem of finding solutions of an S-unit equation with an example.

Example 5.3.5 (S-unit equation)

Let $K = \mathbb{Q}(\zeta_3)$. In $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ we have $(3) = (\zeta_3 - 1)^2 := \mathfrak{p}^2$. Set $S := \{\mathfrak{p}, \infty\}$, then

$$\mathcal{O}_S = S^{-1}\mathcal{O}_K = \mathcal{O}_K\big[1/(\zeta_3 - 1)\big].$$

And $\mathcal{O}_S^{\times} = \langle -1, \zeta_3, \zeta_3 - 1 \rangle$.

The solutions of $x + y = 1$ in $\mathcal{O}_S^\times$ are:

$$1 = (\zeta_3 + 1) + (-\zeta_3) = (\zeta_3 + 2) + (-\zeta_3 - 1) = (-\zeta_3 + 1) + \zeta_3 = (\tfrac{1}{3}\zeta_3 + \tfrac{2}{3}) + (-\tfrac{1}{3}\zeta_3 + \tfrac{1}{3}).$$

With these solutions, one finds 9 Picard curves over $\mathbb{Q}$ good away from 3, see Table A.1, (splitting field $x^2 + x + 1$). ◁

In [MR14], Malmskog and Rasmussen found 45 isomorphism classes of Picard curves with good reduction away from 3 over $\mathbb{Q}$ [MR14, Tbl. 5]. These findings have been independently verified by the author of this thesis. During this process, 18 additional equivalence classes were found. We discussed this with Malmskog and Rasmussen. As a result, they found an error in their implementation and published a reviewed version of their paper [MR16], now listing all 63 Picard curves over $\mathbb{Q}$ good away from 3. A list of those curves can be found in Section A.1.

Based on this list, we computed all bad factors and the conductor at the bad prime 3 and verified (FEq) for all 63 curves (Tables A.3 and A.4). For details abound these computations see Section 5.2.3.

5.3.2 Generalization of the Malmskog–Rasmussen construction

We now consider Picard curves over $\mathbb{Q}$ good away from a finite set of primes S of $\mathbb{Q}$. As the computational cost of verifying (FEq) is $\mathcal{O}(N)$, it is natural to discuss lower bounds on N. We sketch a generalization of the Malmskog–Rasmussen-algorithm to describe the search for a minimal conductor.

Proposition 5.3.6 (Mestre bound)

Assuming some well-verified conjectures on L-functions, the conductor N of the L-function of a genus g_Y curve fulfills the following inequality

$$N > 10.323^{g_Y}.$$

Proof: See [Mes86]. □

Note that 10.323^3 is approximately 1100.06. Further improvements for special types of curves have been made by D. Farmer et al., see [Far15]. Note that in the list of Picard curves over $\mathbb{Q}$ with good reduction away from 3 (Tables A.3 and A.4) the smallest conductor is $N = 3^{10} = 59049$.

We now prove some lower bounds on the conductor exponents.

Lemma 5.3.7 (Minimal exponent at $p \neq 3$)

Let $p \neq 3$ be a bad prime. For a Picard curve over $\mathbb{Q}$ the minimal conductor exponent is $f_p = 2$, and there is a Picard curve with this exponent.

Proof: First, note that $x^2 + x + 1$ has discriminant -3. Thus the only prime field $\mathbb{F}_p$ where $x^2 + x + 1$ has a double root is $\mathbb{F}_3$. Now let $p \neq 3$ be a bad prime. Then f_p is at least 1. With the same methods as in Section 5.1, we find that the curve given by

$$y^3 = x^4 + (p+1)x^3 + (p+1)x^2 + px = x \cdot (x+p) \cdot (x^2 + x + 1)$$

has conductor exponent $f_p = 2$. Secondly, assume that $f_p = 1$ and use the notation of Section 5.1. Recall the definition of the conductor exponent from [BW16, Thm. 2.9], with $\epsilon = 2g(Y) - 2g(\bar{Y}/\Gamma)$:

$$f_p = \epsilon + \delta = 2g(Y) - 2g(\bar{Y}/\Gamma) + \sum_{i=1}^{\infty} \frac{|\Gamma_i|}{|\Gamma_0|} \left(2g(Y) - 2g(\bar{Y}/\Gamma_i)\right).$$

All terms are nonnegative integers. So $f_p = 1$ implies $\epsilon = 0$. Thus Γ does not affect the genus of $\bar{Y}$. So $g(\bar{Y}/\Gamma_i) = g(Y)$ for all $i \geq 1$. Hence $\delta = 0$, which is a contradiction. □

Construction of Picard curves good away from S

Take S to be a finite set of prime numbers, containing the prime 3. By using the *Database for Number Fields* [KM16] it is (for the primes listed in the database) in principle possible to find all number fields $K_1, \ldots, K_r$ ramified at a fixed prime $p \in S$. If one can compute a complete list of solutions of the S-unit equation $x + y = 1$ over $K_1, \ldots, K_r$, the algorithm given in [MR14] can be adapted to the case $S = \{3, p, \ldots\}$. For the computation of S-unit equation solutions over number field, see Koutsianas' article [Kou15].

We have used Koutsianas' S-unit equation solutions to find all Picard curves good away from $\{3, 5\}$ where the defining polynomial f splits over the number field given by $x^2 - 5$.

Example 5.3.8

There are exactly three Picard curves, up to twists by a number d of the form $d = 3^k 5^\ell$, $0 \leq k, \ell \leq 2$ [MR14, Lem. 3.1 for $S = \{3, 5\}$] which have good reduction away from $\{3, 5\}$ and whose defining polynomial f splits over $\mathbb{Q}[x]/(x^2 - 5)$. These Picard curves are given by

$$y^3 = x^4 - 2x^2 + x$$
$$y^3 = -x^4 + 2x^3 - x$$
$$y^3 = x^4 + 6x^3 + 10x^2 + 5x. \qquad \triangleleft$$

This is not a complete list of all Picard curves good away from $\{3, 5\}$, as there are several more number fields ramified only at the primes 3 or 5.

Remark 5.3.9

With the same tools it may be possible to prove the following hypothesis (Hypothesis 5.3.10 ii)). It is based on two arguments. First, in the classification of Picard curves good away from 3 (Section A.1) the smallest conductor is $N = 3^{10}$. Within our examples of Picard curves good away from S (Section A.2), there is only one Picard curve with conductor in this range. The Picard curve given by $y^3 = x^4 - 1$ (Section 5.1.3) has $N = 2^6 \cdot 3^6 = 46656$, which is smaller than $3^{10} = 59049$.

Second, we conducted a search for polynomials

$$f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \quad \text{with} \quad a_i \in \{-200, \ldots, 200\}$$

with conductors consisting of primes smaller than 14. Note that by Remark 5.3.1, we may assume f to be monic.

In order to find a Picard curve with conductor smaller than $2^6 \cdot 3^6$, one has to exclude polynomials f where too many (or too large) primes divide the discriminant of f. This is the case e.g. if both 2 and 5 divide the discriminant of f, since $2^2 \cdot 5^2 > 2^6$. Note that here we use Lemma 5.3.7 and Hypothesis 5.3.10 i) (the minimal conductor exponent at 3 is 6).

During our search, none of the polynomials defined a Picard curve that could in principle have a conductor smaller than $2^6 \cdot 3^6$. $\triangleleft$

Hypothesis 5.3.10 (Conductor)

i) The minimal conductor exponent for a Picard curve over $\mathbb{Q}$ at $p = 3$ is $f_3 = 6$.

ii) There are no Picard curves over $\mathbb{Q}$ with the following conductors.

$2^2 \cdot 3^6 = 2916$

$2^3 \cdot 3^6 = 5832$

$2^4 \cdot 3^6 = 11664$

$2^5 \cdot 3^6 = 23328$

$2^2 \cdot 3^7 = 8748$

$2^3 \cdot 3^7 = 17496$

$2^4 \cdot 3^7 = 34992$

$2^2 \cdot 3^8 = 26244$

$5^2 \cdot 3^6 = 18225$

$7^2 \cdot 3^6 = 35721$

Suggested approach for Hypothesis 5.3.10 i)

The statement should follow from an analysis of the stable reduction of Y at $p = 3$, using the methods of [RW].

Suggested approach for Hypothesis 5.3.10 ii)

Consider all Picard curves good away from $\{2, 3\}$, $\{3, 5\}$, and $\{3, 7\}$. For this we need a list of number fields of degree ≤ 4, ramified only in the (pairs of) primes occurring in the conductors above. This is a list of about 70 number fields according to [KM16]. Then obtain the necessary S-units to classify the Picard curves in these cases. Finally, compute the conductor exponents for these curves as explained in Section 5.1.

Remark 5.3.11

Small conductors are obviously achieved with curves having large automorphism groups. If those curves acquire semistable reduction already over a relatively small and tame field extension of $\mathbb{Q}_p$, the functional equation may be verified in reasonable time. The curve given by $y^3 = x^4 - 1$ has an automorphism group of order 48 [KS96] and the splitting field of $x^4 - 1$ is $\mathbb{Q}(i)$. Hence for a Picard curve with a conductor in the range of $2^6 \cdot 3^6$, one expects a large automorphism group. $\triangleleft$

Theorem 5.3.12 (Lowest conductor)

Assume Hypothesis 5.3.10 holds. The lowest possible conductor for a Picard curve over $\mathbb{Q}$ *is* $N = 2^6 \cdot 3^6 = 46656$*, and there is a curve with this conductor.*

Proof: First, the curve given by

$$y^3 = x^4 - 1$$

has conductor $N = 2^6 \cdot 3^6$ (Section 5.1.3). We emphasize that $N = 3^{10}$ is the smallest conductor among the Picard curves over $\mathbb{Q}$ good away from $S = \{3\}$, see Section A.1. Therefore Hypothesis 5.3.10 ii) covers all possible conductors of Picard curves over $\mathbb{Q}$ up to $2^6 \cdot 3^6$ by Lemma 5.3.7 and Hypothesis 5.3.10 i). $\square$

Appendix A

Computational results

A.1 All Picard curves over $\mathbb{Q}$ good away from 3

A.1.1 Completed list

In [MR14], Malmskog and Rasmussen published a list of 45 $\mathbb{Q}$-isomorphism classes of Picard curves over $\mathbb{Q}$ good away from 3. These curves and the 18 additional ones found by the author are listed in the following tables (see also [MR16, Tables 5, 6, and 7]).

Splitting field: $x^3 - 3$	Splitting field: $x^2 + x + 1$
$x^4 + 3x$	$x^4 + 6x^3 + 12x^2 + 9x$
$x^4 + 81x$	$x^4 + 18x^3 + 108x^2 + 243x$
$x^4 + 2187x$	$x^4 + 54x^3 + 972x^2 + 6561x$
$x^4 + 12x^3 - 6x^2 + x$	$x^4 + x$
$x^4 + 36x^3 - 54x^2 + 27x$	$x^4 + 27x$
$x^4 + 108x^3 - 486x^2 + 729x$	$x^4 + 729x$
$x^4 - 6x^3 + 12x^2 + x$	$x^4 + 2x^3 + 2x^2 + x$
$x^4 - 18x^3 + 108x^2 + 27x$	$x^4 + 6x^3 + 18x^2 + 27x$
$x^4 - 54x^3 + 972x^2 + 729x$	$x^4 + 18x^3 + 162x^2 + 729x$
$x^4 + 9x$	
$x^4 + 243x$	
$x^4 + 6561x$	

Table A.1: Picard curves over $\mathbb{Q}$ good away from 3, part 1 of 2

Splitting field: $x^3 - 3x + 1$	
$x^4 + 9x^3 + 18x^2 - 9x$	$x^4 + 6x^3 + 9x^2 + 3x$
$x^4 + 27x^3 + 162x^2 - 243x$	$x^4 + 18x^3 + 81x^2 + 81x$
$x^4 + 81x^3 + 1458x^2 - 6561x$	$x^4 + 54x^3 + 729x^2 + 2187x$
$x^4 - 6x^3 - 9x^2 - 3x$	$x^4 + 9x^3 + 18x^2 + 9x$
$x^4 - 18x^3 - 81x^2 - 81x$	$x^4 + 27x^3 + 162x^2 + 243x$
$x^4 - 54x^3 - 729x^2 - 2187x$	$x^4 + 81x^3 + 1458x^2 + 6561x$
$x^4 + 3x^3 - 3x$	$x^4 + 6x^3 + 3x^2 - x$
$x^4 + 9x^3 - 81x$	$x^4 + 18x^3 + 27x^2 - 27x$
$x^4 + 27x^3 - 2187x$	$x^4 + 54x^3 + 243x^2 - 729x$
$x^4 - 9x^2 + 9x$	$x^4 + 3x^3 - 6x^2 + x$
$x^4 - 81x^2 + 243x$	$x^4 + 9x^3 - 54x^2 + 27x$
$x^4 - 729x^2 + 6561x$	$x^4 + 27x^3 - 486x^2 + 729x$
Additional curves	
$x^4 - 3x^2 - x$	$x^4 + 9x^3 + 6x^2 + x$
$x^4 - 27x^2 - 27x$	$x^4 + 27x^3 + 54x^2 + 27x$
$x^4 - 243x^2 - 729x$	$x^4 + 81x^3 + 486x^2 + 729x$
$x^4 + 3x^3 - x$	$x^4 - 6x^3 + 9x^2 - x$
$x^4 + 9x^3 - 27x$	$x^4 - 18x^3 + 81x^2 - 27x$
$x^4 + 27x^3 - 729x$	$x^4 - 54x^3 + 729x^2 - 729x$
$x^4 - 24x^3 + 3x^2 + x$	$x^4 - 3x^3 - 24x^2 - x$
$x^4 - 72x^3 + 27x^2 + 27x$	$x^4 - 9x^3 - 216x^2 - 27x$
$x^4 - 216x^3 + 243x^2 + 729x$	$x^4 - 27x^3 - 1944x^2 - 729x$

Table A.2: Picard curves over $\mathbb{Q}$ good away from 3, part 2 of 2

A.1.2 *L*-factors and conductor for all Picard curves good away from 3

In this section, we give bad factors, conductor exponents, and signs μ for all $\mathbb{Q}$-isomorphism classes of Picard curves over $\mathbb{Q}$ good away from 3. This list has some interesting properties:

- $L_3 = 1$ for all 63 $\mathbb{Q}$-isomorphism classes
- $N = 3^{f_3}$ ranges from 3^{10} to 3^{21}
- 42 curves have the same conductor exponent f_3 and sign μ as their twists
- 21 curves have f_3 and/or μ different from their twists, e.g.:

$$\begin{array}{rll} x^4 - 3x^3 - 24x^2 - x & N = 3^{10} & \mu = 1 \\ x^4 - 9x^3 - 216x^2 - 27x & N = 3^{15} & \mu = -1 \\ x^4 - 27x^3 - 1944x^2 - 729x & N = 3^{12} & \mu = 1 \end{array}$$

All calculations were made using the methods in Sections 5.2.2 and 5.2.3. The functional equation (FEq) was verified for all those curves as described in Section 3.6. All L-series (up to the bound M) are available online, see Section A.2.

Splitting field	$f(x)$	f_3	sign μ
x^3-3	x^4+3x	21	1
	x^4+81x	21	1
	$x^4+2187x$	21	1
	$x^4+12x^3-6x^2+x$	17	1
	$x^4+36x^3-54x^2+27x$	17	1
	$x^4+108x^3-486x^2+729x$	17	1
	$x^4-6x^3+12x^2+x$	17	-1
	$x^4-18x^3+108x^2+27x$	17	-1
	$x^4-54x^3+972x^2+729x$	17	-1
	x^4+9x	21	-1
	x^4+243x	21	-1
	$x^4+6561x$	21	-1
x^2+x+1	$x^4+6x^3+12x^2+9x$	13	1
	$x^4+18x^3+108x^2+243x$	11	1
	$x^4+54x^3+972x^2+6561x$	15	-1
	x^4+x	13	1
	x^4+27x	15	1
	x^4+729x	15	-1
	$x^4+2x^3+2x^2+x$	11	1
	$x^4+6x^3+18x^2+27x$	15	-1
	$x^4+18x^3+162x^2+729x$	13	1

Table A.3: Bad data for Picard curves over $\mathbb{Q}$ good away from 3, part 1 of 2

Splitting field	$f(x)$	f_3	sign μ
$x^3 - 3x + 1$	$x^4 + 9x^3 + 18x^2 - 9x$	19	1
	$x^4 + 27x^3 + 162x^2 - 243x$	19	1
	$x^4 + 81x^3 + 1458x^2 - 6561x$	19	1
	$x^4 - 6x^3 - 9x^2 - 3x$	19	-1
	$x^4 - 18x^3 - 81x^2 - 81x$	19	-1
	$x^4 - 54x^3 - 729x^2 - 2187x$	19	-1
	$x^4 + 3x^3 - 3x$	19	-1
	$x^4 + 9x^3 - 81x$	19	-1
	$x^4 + 27x^3 - 2187x$	19	-1
	$x^4 - 9x^2 + 9x$	19	1
	$x^4 - 81x^2 + 243x$	19	1
	$x^4 - 729x^2 + 6561x$	19	1
	$x^4 + 6x^3 + 9x^2 + 3x$	19	-1
	$x^4 + 18x^3 + 81x^2 + 81x$	19	-1
	$x^4 + 54x^3 + 729x^2 + 2187x$	19	-1
	$x^4 + 9x^3 + 18x^2 + 9x$	19	1
	$x^4 + 27x^3 + 162x^2 + 243x$	19	1
	$x^4 + 81x^3 + 1458x^2 + 6561x$	19	1
	$x^4 + 6x^3 + 3x^2 - x$	15	-1
	$x^4 + 18x^3 + 27x^2 - 27x$	13	1
	$x^4 + 54x^3 + 243x^2 - 729x$	15	1
	$x^4 + 3x^3 - 6x^2 + x$	15	1
	$x^4 + 9x^3 - 54x^2 + 27x$	15	-1
	$x^4 + 27x^3 - 486x^2 + 729x$	11	1
	$x^4 - 3x^2 - x$	17	-1
	$x^4 - 27x^2 - 27x$	17	-1
	$x^4 - 243x^2 - 729x$	17	-1
	$x^4 + 3x^3 - x$	17	1
	$x^4 + 9x^3 - 27x$	17	1
	$x^4 + 27x^3 - 729x$	17	1
	$x^4 - 24x^3 + 3x^2 + x$	11	1
	$x^4 - 72x^3 + 27x^2 + 27x$	15	-1
	$x^4 - 216x^3 + 243x^2 + 729x$	13	1
	$x^4 + 9x^3 + 6x^2 + x$	17	-1
	$x^4 + 27x^3 + 54x^2 + 27x$	17	-1
	$x^4 + 81x^3 + 486x^2 + 729x$	17	-1
	$x^4 - 6x^3 + 9x^2 - x$	17	1
	$x^4 - 18x^3 + 81x^2 - 27x$	17	1
	$x^4 - 54x^3 + 729x^2 - 729x$	17	1
	$x^4 - 3x^3 - 24x^2 - x$	10	1
	$x^4 - 9x^3 - 216x^2 - 27x$	15	-1
	$x^4 - 27x^3 - 1944x^2 - 729x$	12	1

Table A.4: Bad data for Picard curves over $\mathbb{Q}$ good away from 3, part 2 of 2

A.2 Examples for Picard curves good away from S

The L-series of all Picard curves good away from 3 and other primes can be retrieved from `https://www.uni-ulm.de/index.php?id=79073`.

Bibliography

AP96 Y. Aubry and M. Perret, *A Weil theorem for singular curves*, In: Arithmetic geometry and coding theory, de Gruyter, Berlin, 1996, pp. 1–7.

Arz12 K. Arzdorf, *Semistable reduction of cyclic covers of prime power degree*, Ph.D. thesis, Leibniz Universität Hannover, 2012, `http://edok01.tib.uni-hannover.de/edoks/e01dh12/71609648.pdf`.

AW12 K. Arzdorf and S. Wewers, *Another proof of the semistable reduction theorem*, Preprint, arXiv:1211.4624, 2012.

BBW16 M. Börner, I.I. Bouw, and S. Wewers, *The functional equation for L-functions of hyperelliptic curves*, Experimental Mathematics, to appear (2016), arXiv:1504.00508.

BCDT01 C. Breuil, B. Conrad, F. Diamond, and 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.

BCG$^+$04 D. Bump, J.W. Cogdell, D. Gaitsgory, E. de Shalit, E. Kowalski, and S.S. Kudla, *An Introduction to the Langlands Program*, Birkhäuser, Boston, 2004.

Boo03 A. Booker, *Numerical tests of modularity*, Ph.D. thesis, Princeton University, 2003.

Boo05 ______, *Numerical tests of modularity*, J. Ramanujan Math. Soc. **20** (2005), no. 4, 283–339.

Bra10 R.W. Bradshaw, *Provable computation of motivic L-functions*, Ph.D. thesis, University of Washington, 2010.

BW12 I.I. Bouw and S. Wewers, *Group actions on curves and the lifting problem*, Course notes, avaliable at `http://math.arizona.edu/~swc/aws/2012/`, 2012.

BW15 I.I. Bouw and S. Wewers, *Semistable reduction of curves and computation of bad Euler factors of L-functions*, Course notes, avaliable at `http://www.uni-ulm.de/mawi/rmath/mitarbeiter/wewers.html`, 2015.

BW16 I.I. Bouw and S. Wewers, *Computing L-functions and semistable reduction of superelliptic curves*, Glasgow Math. J., to appear (2016), arXiv:1211.4459.

Chê04 G. Chênevert, *Some remarks on Frobenius and Lefschetz in étale coho-*

mology, Seminar notes, available at `http://www.math.mcgill.ca/goren/SeminarOnCohomology/Frobenius.pdf`, 2004.

DdJZ06 T. Dokchitser, R. de Jeu, and D. Zagier, *Numerical verification of Beilison's conjecture for K_2 of hyperelliptic curves*, Compositio Math. **142** (2006), 339–373.

Del74 P. Deligne, *La conjecture de Weil I*, Publications mathématiques de l'IHÉS **43** (1974), 273–307.

DM69 P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Publications mathématiques de l'IHÉS **36** (1969), no. 1, 75–109.

Dok04 T. Dokchitser, *Computing special values of motivic L-functions*, Experimental Mathematics **13** (2004), no. 2, 137–149.

Dok06 ______, *The computeL package in pari*, `http://www.maths.bris.ac.uk/~matyd/computel/files/computel.zip`, 2006.

dS04 E. de Shalit, *L-functions of Elliptic Curves an Modular Forms*, In: An Introduction to the Langlands Program (J. Bernstein and S. Gelbart, eds.), Birkhäuser, Boston, 2004.

Fal83 G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

Far15 D. Farmer, *The structure of L-functions*, 'Computational aspects of L-functions' workshop at ICERM, `https://icerm.brown.edu/materials/Slides/sp-f15-w3/The_Structure_of_L-functions_]_David_Farmer,_AIM.pdf`, 2015.

FHS07 X. Faber, B. Hutz, and S. Stoll, *On the number of rational iterated preimages of the origin under quadratic dynamical systems*, Int. J. Number Theory **7** (2007), no. 7.

Fon85 J.-M. Fontaine, *Il n'y a pas de variété abélienne sur $\mathbb{Z}$*, Invent. Math. **81** (1985), 515–538.

Gel84 S. Gelbart, *An elementary introduction to the Langlands Program*, Bull. Amer. Math. Soc. **10** (1984), no. 2, 177–219.

GH00 P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, In: Algorithmic number theory (New York) (W. Bosma, ed.), Lecture Notes in Computer Science, no. 1838, Springer, 2000, pp. 313–332.

Har77 R. Hartshorne, *Algebraic Geometry*, Springer, New York, 1977.

Har14a M. Harris, *Galois representations, automorphic forms, and the Sato-Tate conjecture*, Indian J. Pure Appl. Math. **45** (2014), no. 5, 707–746.

Har14b D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. **179** (2014), no. 2, 783–803.

HS00 M. Hindry and J. H. Silverman, *Diophantine Geometry*, Springer, New York, 2000.

Hus04 D. Husemöller, *Elliptic Curves*, Springer, New York, 2004.

IS00 H. Iwaniec and P. Sarnak, *Perspectives on the analytic theory of L-functions*, vol. 705-741, GAFA, 2000.

Kat89 K. Kato, *Swan conductor for characters of degree one in the imperfect residue field case*, ContempoInvent. M. **83** (1989), 101–131.

Ked01 K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338.

KM16 J. Klüners and G. Malle, *A Database for Number Fields*, `galoisdb.math.upb.de`, 2016.

Kou15 A. Koutsianas, *Computing all elliptic curves over an arbitrary number field with prescribed primes of bad reduction*, arXiv:1511.05108 (2015).

KS96 M.J. Klassen and E.F. Schaefer, *Arithmetic and geometry of the curve* $y^3 + 1 = x^4$, Acta Arith. **74** (1996), 241–257.

KS08 K.S. Kedlaya and A. Sutherland, *Computing L-series of hyperelliptic curves*, In: Algorithmic Number Theory (Berlin) (A. J. van der Poorten and A. Stein, eds.), Lecture Notes in Computer Science, no. 5011, Springer, 2008, pp. 312–326.

Lan02 S. Lang, *Algebra*, Springer, New York, 2002.

Lef37 S. Lefschetz, *On the fixed point formula*, Ann. of Math. **2** (1937), no. 38, 819–822.

Liu96 Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), 4577–4610.

Liu06 Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, Oxford, 2006.

LMF16 LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2013-2016, `http://www.lmfdb.org`.

Mes86 J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), no. 2, 209–232.

Mil80 J.S. Milne, *Étale cohomology*, Princeton Univ. Press, Princeton, 1980.

Min10 M. Minzlaff, *Computing zeta functions of superelliptic curves in larger char-*

acteristic, Math. Comput. Sci. **3** (2010), 209–224.

MP05 Y.I. Manin and A.A. Panchishkin, *Introduction to Modern Number Theory*, Springer, Heidelberg, 2005.

MR14 B. Malmskog and C. Rasmussen, *Picard curves over* $\mathbb{Q}$ *with good reduction away from 3*, arXiv:1407.7892v1 (2014).

MR16 ———, *Picard curves over* $\mathbb{Q}$ *with good reduction away from 3*, arXiv:1407.7892v2 (2016).

Neu92 J. Neukirch, *Algebraische Zahlentheorie*, Springer, Berlin, Heidelberg, 1992.

Rüt14 J. Rüth, *Models of curves and valuations*, Ph.D. thesis, Ulm University, 2014.

RW J. Rüth and S. Wewers, *Semistable reduction of superelliptic curves of degree* p, in preparation.

Sar04 P. Sarnak, *Problems of the Millennium: The Riemann Hypothesis*, In: The Proceedings of the Clay Mathematics Institute, Budapest, 2004.

Sau03 M. Sautoy, *Groups St. Andrews 2001 in Oxford*, Cambridge University Press, 2003.

Ser70 J.-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou (Théorie des Nombres), no. 19, 1970, pp. 1–15.

Ser79 ———, *Local Fields*, Springer, Berlin, New York, 1979.

Sil09 J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 2009.

Sma97 N. Smart, *S-unit equations, binary forms and curves of genus 2.*, Proc. London Math. **(3)** (1997), no. 75(2), 271–307.

St16 W. Stein and the Sage developers, *Sagemath, the Sage Mathematics Software System (Version 6.4)*, 2014-2016, `http://www.sagemath.org`.

Sto08 M. Stoll, *Rational* 6*-cycles under iteration of quadratic polynomials*, London Math. Soc. J. Comput. Math. **11** (2008), 367–380.

Voi16 J. Voight, *Researchers announce new way to explore mathematical universe*, Press release Dartmouth College, `www.dartmouth.edu/press-releases/mathematical-universe-051016.html` (2016).

Wil95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

Wil06 ———, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/sites/default/files/birchswin.pdf` (2006).

Acknowledgments

First and foremost, I thank Irene Bouw for the trust she placed in me already well before I realized I'd want to do my Ph.D. here. My two supervisors, Stefan Wewers and Irene Bouw, have always guided and supported me during those three years. They always had the 'big plan' in mind and without them I wouldn't have finished by now.

My colleagues have always provided help and fruitful discussions when I needed it. Perhaps I learned the most from Julian Rüth, who was always patient with my Sage questions and whose little pieces of software made life easier every day.

Angelos Koutsianas thankfully computed the solutions to the S-unit equations for Example 5.3.8 and confirmed my calculations on S-units in the case of Picard curves good away from 3.

Special thanks is due to Andreas Borchert who provided the necessary hardware for my computations.

And last but not least, I thank Jeroen Sijsling for being my second referee and for many interesting discussions.

This work has been funded by the DFG Priority Project SPP 1489 on *Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory*. I am very grateful for the opportunity to dedicate large parts of my working hours to this project.

Zusammenfassung

In der vorliegenden Arbeit betrachten wir superelliptische Kurven Y vom Geschlecht g über einem Zahlkörper K. Als superelliptische Kurven bezeichnen wir glatte projektive zusammenhängende Kurven gegeben durch eine Gleichung der Form

$$y^n = f(x) \quad \text{für} \quad f \in K[x] \quad \text{und} \quad n \in \mathbb{N}.$$

Wir untersuchen die L-Funktion einer solchen Kurve. Die L-Funktion ist als Euler-Produkt lokaler Faktoren $L_\mathfrak{p}$ definiert

$$L(Y,s) = \prod_\mathfrak{p} L_\mathfrak{p}(Y,s),$$

wobei das Produkt über die Primideale des Ganzheitsrings von K läuft. Für die Berechnung der L-Funktion einer Kurve können fast alle lokalen Faktoren durch Punkte zählen auf Kurven über endlichen Körpern gefunden werden. Es ist jedoch im allgemeinen nicht bekannt, wie die lokalen Faktoren an den endlich vielen Primstellen $\mathfrak{p}$ schlechter Reduktion berechnet werden. Wir beschreiben die Berechnung der schlechten lokalen Faktoren $L_\mathfrak{p}$ und des Führers N für zwei Klassen superelliptischer Kurven. Diese Ergebnisse nutzen wir, um die vermutete Funktionalgleichung

$$\Lambda(Y,s) = \pm\Lambda(Y,2-s), \tag{FEq}$$

mit $\Lambda(Y,s) := \sqrt{N}^s \cdot (2\pi)^{-gs} \cdot \Gamma(s)^g \cdot L(Y,s)$ numerisch zu verifizieren.

Teilt die Restklassencharakteristik von $\mathfrak{p}$ den Grad n nicht, beschreibt [BW16] eine Methode zur Berechnung der schlechten Faktoren $L_\mathfrak{p}$ und des Führers N. Die beiden betrachteten Klassen sind hyperelliptische Kurven (vom Geschlecht $g \geq 2$) und Picard-Kurven (vom Geschlecht $g = 3$) über $\mathbb{Q}$. Wir haben Voraussetzungen an die Kurven festgelegt, so dass die Berechnung von $L_\mathfrak{p}$ und N als Algorithmus von einem Computer praktisch umsetzbar ist.

Insbesondere klären wir zunächst, unter welchen Voraussetzungen die Reduktion der Kurve Y an der Stelle $\mathfrak{p}$ durch die reduzierte Gleichung $\bar{y}^n = \bar{f}(\bar{x}) \pmod{\mathfrak{p}}$ gegeben ist. Danach geben wir Bedingungen an f an, unter denen die betrachteten Kurven semistabile Reduktion erreichen können. Das heißt über einer (möglichst einfachen) endlichen Erweiterung von $\mathbb{Q}$ hat die reduzierte Kurve nur gewöhnliche Doppelpunkte als Singularitäten.

Die betrachtete Unterklasse hyperelliptischer Kurven hat bereits über $\mathbb{Q}$ semistabile Reduktion. Wir geben einen Algorithmus an, der (nur limitiert durch die verfügbare Rechenzeit fürs Punkte zählen) prinzipiell alle lokalen L-Faktoren und den Führer N einer gegebenen hyperelliptischen Kurve aus dieser Klasse berechnet.

Mit Hilfe der Ergebnisse von Dokchitser [Dok04] können wir für eine wählbare numerische Genauigkeit die Anzahl der für die Funktionalgleichung (FEq) benötigten L-Faktoren a priori auf eine Konstante in der Größenordnung des Führers einschränken. Nach diesem Vorgehen haben wir für einige hundert Beispiele und für Geschlecht bis zu 6 die Funktionalgleichung (FEq) numerisch verifiziert, d.h. innerhalb der geforderten Genauigkeit ist die Gleichung erfüllt. Unter Zuhilfenahme größerer Rechenleistung kann man innerhalb der betrachteten Klasse hyperelliptischer Kurven die Funktionalgleichung für Kurven beliebig hohen Geschlechts verifizieren.

Ein weiterer Aspekt dieser Arbeit ist die Suche nach Kurven mit vorgegebenen Parametern. Insbesondere suchen wir untere Schranken für den Führer N. Hierfür betrachten wir Picard-Kurven, eine Klasse superelliptischer Kurven vom Geschlecht 3. Malmskog und Rasmussen haben in [MR14] beschrieben, wie man eine Liste aller Picard-Kurven über $\mathbb{Q}$ mit schlechter Reduktion nur bei $p = 3$ erstellt. Jedoch ist die Liste aufgrund eines Implementierungsfehlers nicht vollständig. Wir geben eine vollständige Liste an und diskutieren Erweiterungen des Algorithmus' auf Picard-Kurven mit schlechter Reduktion an endlich vielen Stellen $\{3, p, \ldots\}$. Für alle Picard-Kurven mit schlechter Reduktion bei 3 sowie einige Beispiele mit schlechter Reduktion bei $\{3, p, \ldots\}$ haben wir die lokalen Faktoren an den schlechten Stellen und den Führer berechnet und mit diesen Daten (FEq) verifiziert. Abschließend diskutieren wir untere Schranken für den Führer N. Dies ist hilfreich für eine mögliche Klassifikation von Kurven festen Geschlechts nach allen vorkommenden Führern.

Ehrenwörtliche Erklärung

Hiermit bestätige ich, dass ich die vorliegende Dissertation mit dem Thema

L-functions of curves of genus ≥ 3

selbstständig angefertigt habe und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt sowie die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht habe.

Ulm, den

Michel Börner

Lebenslauf aus Gründen des Datenschutzes entfernt.

Teile dieser Dissertation wurden bereits in folgendem Fachartikel veröffentlicht:

M. Börner, I.I. Bouw, und S. Wewers, *The functional equation for L-functions of hyperelliptic curves*, erscheint in: Experimental Mathematics,
DOI: 10.1080/10586458.2016.1189860.