Regular models of Fermat curves and applications to Arakelov theory

Dissertation
zur Erlangung des Doktorgrades
der Fakultät für Mathematik, Informatik
und Naturwissenschaften
der Universität Hamburg

vorgelegt
im Fachbereich Mathematik
von

Christian Curilla

aus Elmshorn

Hamburg
2010

Als Dissertation angenommen vom Fachbereich
Mathematik der Universität Hamburg

Auf Grund der Gutachten von Prof. Dr. Ulf Kühn
und Prof. Dr. Stefan Wewers

Hamburg, den 27.09.2010

Prof. Dr. Vicente Cortés
Leiter des Fachbereichs Mathematik

Contents

Introduction

History: One of the main concerns of number theory is the study of integral solutions of polynomial equations with integral coefficients. The Fermat curve plays a prominent role in this context. It is fascinating the people because of two properties which seem to be contrary to each other from a naive viewpoint. First, it is given by the very simple equation

$$X^n + Y^n = Z^n \,,$$

where n is a natural number, and second it is a very hard problem to prove the unsolvability by non-trivial integer solutions for $n > 2$. In fact, this problem, which is also known as "Fermat's Last Theorem", has challenged mathematics for more that three hundred years and has finally been proved by Wiles in 1993-1995. Even if this big problem is solved, the Fermat curve is still an interesting object because of its exemplary character.

In order to analyze the arithmetic properties of an algebraic curve X, which is defined over a number field E, one can try to construct a (minimal) arithmetic surface $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ which has X as generic fiber i.e. construct a (minimal) regular model $\mathcal{X}$ of this curve; here $\mathcal{O}_E$ denotes the ring of integers of E. Since $\mathcal{X}$ is a projective model of X the E-rational points $X(E)$ correspond bijectively to the set of sections $\mathcal{X}(\mathcal{O}_E)$. With the importance of the classical intersection theory of algebraic surfaces over algebraically closed fields in mind, one can ask how to construct a good intersection theory for arithmetic surfaces. This is not an easy problem since just adapting the classical definitions would give an intersection theory which is not well defined for divisor classes. Arakelov solved in his famous article [Ara] this problem by adding some analytic data in order to "compactify" the base scheme and to "complete" the arithmetic surface. He defined an intersection theory for arithmetic divisors[1] and he reformulated everything in the language of hermitian line bundles. Many other mathematicians as for example Deligne, Gillet and Soulé, et al. have made an advancement of this theory by extending it to other types of arithmetic divisors (hermitian line bundles resp.) and by generalizing it to higher dimensional arithmetic varieties.

The property that the Arakelov intersection theory is well defined for arithmetic divisor classes makes theoretically possible to compute arithmetic self-intersection numbers of all types of arithmetic divisors. Especially the arithmetic self-intersection number of the hermitian line bundle $\overline{\omega}^2_{\mathcal{X},\mathrm{Ar}}$, where $\overline{\omega}_{\mathcal{X},\mathrm{Ar}}$ is the line bundle $\omega_{\mathcal{X}/\operatorname{Spec}\mathbb{Z}} = \omega_{\mathcal{X}/\operatorname{Spec}\mathcal{O}_E} \otimes_{\mathcal{O}_\mathcal{X}}$

[1] In the literature often called *Arakelov divisors.*

$f^*\omega_{\operatorname{Spec}\mathcal{O}_E/\operatorname{Spec}\mathbb{Z}}$ equipped with the Arakelov metric, is a number of great importance (cf. [Sz],[Ul] and [Zh]). Unfortunately, its computation is a very difficult problem if the genus of the curve X is bigger or equal to two and therefore there is not much known about these numbers (cf. [BMMB], [AU] plus [MU] or [AU] plus [JK1]). Parshin showed that an upper bound for $\overline{\omega}^2_{\mathcal{X}_P,\mathrm{Ar}}$ for certain families of morphisms of arithmetic surfaces $\{\mathcal{X}_P \to \mathcal{Y}\}_{P\in Y(\overline{E})}$ would imply bounds for the height of rational points of the curve Y, hence it would yield an effective version of Mordell's conjecture (cf. [Vo], [Pa]). However, except for certain kinds of modular curves there are only a few results on such upper bounds. In [Kü1] Kühn extends the Arakelov intersection theory in order to obtain an intersection theory that works for hermitian line bundles equipped with metrics which have logarithmic singularities at a finite set of points. Provided that one can compute regular models that fulfill certain conditions, this generalized arithmetic intersection theory can be used in order to compute upper bounds for $\overline{\omega}^2_{\mathrm{Ar}}$ in case of modular curves and Fermat curves (cf. [Kü2]).

The main results: The main result of this thesis is the construction of (minimal) regular models $\mathfrak{F}_N$ of Fermat curves of squarefree exponent and the computation of upper bounds for $\overline{\omega}^2_{\mathfrak{F}_N,\mathrm{Ar}}$ using Kühn's results in [Kü1] and [Kü2]. Furthermore, we compute upper bounds for the regular model of the Fermat curves of prime exponent that was constructed by McCallum [Mc] and for certain types of regular models that appear often as models of modular curves.

Previous work: There are several works which deal with the construction of regular and minimal regular models $\mathfrak{F}_p$ of the Fermat curve F_p of prime exponent. The most prominent one is given by William G. McCallum which describes the minimal regular model over $\mathbb{Z}_p[\zeta_p]$ ($\mathbb{Z}[\zeta_p]$ resp.), where ζ_p is a primitive p-th root of unity (see [Mc]). Inspired by this work Haichau Chang [Cha] and Nguen Kkhak V'et [V$'$] constructed independently the minimal regular model over $\mathbb{Z}_p$ ($\mathbb{Z}$ resp.). In order to do this Chang started with the model which is given by the Fermat-equation and then - following the construction of McCallum - made a straight forward computation. Nguen Kkhak V'et considered the quotient scheme, which is given by McCallum's scheme and the group $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$, and resolved the singularities. The stable model of the Fermat curve of prime exponent was constructed by Hironobu Maeda [Mae1],[Mae2] and by Jeroen J. van Beele [vB].

In [Kü2] Kühn used McCallum's model and an "approximated" version of one of his formulae for upper bounds in order to compute an upper bound for $\overline{\omega}^2_{\mathfrak{F}_p,\mathrm{Ar}}$. In [CK] Kühn and the author made an improvement of this result using the original version of that formula.

Description of the contents: In Chapter 1 we review some of the necessary background material in order to work with arithmetic surfaces. We start summarizing methods which are needed for the construction of the arithmetic surface as for example blowing-ups and regularity criteria of schemes. Most of this material is not restricted to surfaces. Then we introduce the intersection theory for arithmetic surfaces which gives us an important tool for the study of these schemes. Finally we define the canonical sheaf (canonical divisor resp.). This invariant displays its significance in the adjunction formula (Theorem 1.4.9) which we will frequently use in later chapters. To illustrate the introduced results we already start in Proposition 1.1.13 and Proposition 1.4.11 applying them to the Fermat curve. The reader who is familiar with the basic concepts of arithmetic geometry may just take a look at these propositions which are related to the Fermat curve and skip the rest of this chapter.

Whereas the first chapter gives us the required tools, Chapter 2 explains the strategy to construct (minimal) regular models. In this context we present the resolution of surface-singularities like it was done by Lipman and the construction of minimal models done by Lichtenbaum. At the end we introduce a few facts about descent theory which explain that our constructions can be done fiber by fiber. Again, the reader who is familiar with these topics may skip the whole chapter.

In Chapter 3 we explain Arakelov's idea to extend the intersection theory of arithmetic surfaces by considering some analytic data in order to obtain an arithmetic intersection theory which is defined for divisor classes. In fact, we present the arithmetic intersection theory developed by Gillet and Soulé which is an advancement of Arakelov's theory. We show two approaches to this theory: The arithmetic intersection theory of hermitian line bundles and the one of arithmetic divisors. Since it is sometimes useful to switch between these languages we explain how results can be translated. The second section of Chapter 3 is devoted to a result of Kühn (Theorem 3.2.2) which gives us an upper bound for the arithmetic self-intersection number of the dualizing sheaf $\overline{\omega}^2_{\mathcal{X},\mathrm{Ar}}$ of an arithmetic surface $\mathcal{X}$ which fulfills certain conditions. This result is the starting point of our work. It enables us to compute $\overline{\omega}^2_{\mathcal{X},\mathrm{Ar}}$ just by some algebraic data which can be extracted from the arithmetic surface $\mathcal{X}$. Subsequent to this we describe how to approximate the numbers that can be computed with the algebraic data and we show that the Fermat curves (and certain modular curves) fulfill the conditions which are necessary in order to apply Kühn's result. The reader who is well versed in Arakelov theory may skip the first section of this chapter but should nevertheless read the second section since it is of fundamental importance for the rest of the work.

In Chapter 4 we start to apply Kühn's result we reviewed in the previous section. We explain the construction of a regular model $\mathfrak{F}_p$ of the Fermat curve of prime exponent F_p which was given by McCallum. This model is the first example of an arithmetic surface that fulfills the conditions of Kühn's theorem. Using the explicit description of the model, we compute certain vertical divisors which are necessary to calculate the upper bound of the arithmetic self-intersection number of the dualizing sheaf. In fact, we even compute a little bit more than that, namely a canonical divisor and a divisor which is associated with a pullback of the tautological sheaf. After that we calculate the upper bound (Theorem 4.2.6). McCallum describes the minimal regular model $\mathfrak{F}_p^{min}$ of F_p as well. Unfortunately, we cannot apply Kühn's result directly to that model since it does not satisfy the conditions needed. However, in Section 4.2.1 we use the result for McCallum's (non-minimal) model and obtain a relative result for the dualizing sheaf of the minimal regular model (Theorem 4.2.8).

After that we consider a different type of curves: The modular curves. Kühn used in [Kü2] his formula to compute upper bounds in case of the modular curve $X_0(N)$. He also used an "approximated" version of his formula to compute an upper bound for $X(N)$. In Chapter 5 we consider a situation which covers many cases of this kind of curves. Even if we have the modular curve situation in mind, we describe everything in an abstract setting which can be understood without any knowledge about the modular curves. Later we show that we can apply our results to specific cases of the curves $X_0(N)$ and $X(N)$, where we achieve the same results as Kühn in the first case and the better ("non-approximated") upper bound in the second case.

Chapter 6 is the main part of this thesis. It is divided into two sections. In the first section we construct the minimal regular model $\mathfrak{F}_N^{min}$ of the Fermat curve of squarefree odd exponent N over the ring of integers of the number field $\mathbb{Q}(\zeta_N)$; here ζ_N is a primitive N-th root of unity. In order to do this we start with an analyzation of the polynomial

$$\psi(X^m, Y^m) = \frac{(X^N + Y^N - Z^N) - (X^m + Y^m - Z^m)^p}{p},$$

where p is a prime with $p|N$ and $N = pm$. This is important for the study of the special fiber over the primes that lie above p. Then we construct a regular model of this curve and prove that this is in fact the minimal regular model. For the later applications it is important that we have made this construction over a number field that contains the primitive N-th roots of unity. In the second section we compute - similar to the prime exponent case in Chapter 4 - a canonical divisor and a divisor which is associated with the pullback of the tautological sheaf. We use this and apply Kühn's formula in order to compute an upper bound for $\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}}$.

In each of the Chapters 4, 5 and 6 we do not only compute upper bounds for $\overline{\omega}^2_{\mathrm{Ar}}$ but also give asymptotic formulae of these numbers and analyze which data in the bound - the analytic data or the algebraic data - is the dominating one. The asymptotic formulae intend to illustrate the significant part of the growth of the upper bounds for $\overline{\omega}^2_{\mathrm{Ar}}$ as the curves in question vary within a certain family of curves. However, the way the formulae are chosen is not uniform and differs for the families of curves.

In Chapter 7 we give a small discussion about subsequent work and open problems. Here we consider the case of the Fermat curve of squarefree even exponent. Furthermore, we describe a different approach to the results in Section 6.1 which was posed by Franz Király and which uses the theory of quotient singularities. At the end we illustrate the difficulties that appear in the case of Fermat curves of non-squarefree exponent.

Acknowledgement: I would like to thank the international research training group "Arithmetic and Geometry" at the Humboldt University of Berlin - and here especially professor Jürg Kramer and professor Ulf Kühn - for the opportunity of a temporary participation. This time has enhanced my mathematical background in Arithmetic Geometry. I would also like to thank the University of Hamburg for providing a good research-environment. During my work on this thesis there were many mathematicians who helped me by offering suggestions, encouragement and inspiring discussions. I would like to thank all of them and especially mention Fritz Hörmann and Franz Király. Furthermore I would like to thank Vincenz Busch for the reading of Section 6.1 and Inmaculada Pizán Molina for a careful reading regarding linguistic matters. Special thanks go to professor Stefan Wewers for his help with questions concerning the construction of models. Finally, and most importantly, I would like to thank professor Ulf Kühn for his encouragement and his motivating mentoring.

Terminology and Conventions

We assume that the reader is familiar with basic concepts of algebraic geometry. Even if we use most of the time standard terminology, as it is use for example in [Liu] or [Ha], we review at this point terminology and conventions which will be used frequently in this work.

We use the term *ring* to denote a commutative ring with a unit. A ring homomorphism is always assumed to take the unit element of one ring to the unit element of the other ring. If we have a ring A and an element $f \in A$, we will denote by A/f the factor ring $A/(f)$.

Given a polynomial ring $A[X_1, \ldots, X_r]$, we denote by $A[X_1, \ldots, \widehat{X_i}, \ldots, X_r]$ the same ring but after removing X_i. In other words, we have

$$A[X_1, \ldots, \widehat{X_i}, \ldots, X_r] = A[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_r]\,.$$

If S is a multiplicative subset of A, we denote by A_S the localization of A with respect to S. For a prime ideal $\mathfrak{p}$ of A we write $A_{\mathfrak{p}}$ for the localization A_S of A with $S = A \setminus \mathfrak{p}$. Given an integral ring A we denote its field of fractions by $\mathrm{Frac}(A)$ i.e. the localization of A with respect to the multiplicative subset A^*.

For an affine scheme $\operatorname{Spec} A$ and an ideal $I \subset A$ we denote by $V(I)$ the subset of $\operatorname{Spec} A$ which consists of the prime ideals of A that contain I. Similarly, we proceed with projective schemes $\operatorname{Proj} B = \bigoplus_{d\geq 0} B_d$; here B is a graded ring. We denote by $V_+(I)$ the set of homogenous prime ideals $\mathfrak{p} \in \operatorname{Proj} B$ that contain the homogenous ideal $I \subset B$. If there is no danger of confusion, we will use the same symbol $\mathfrak{p}$ to denote a prime ideal considered as an ideal of the ring $\mathfrak{p} \subset A$ ($\mathfrak{p} \subset B$ resp.) on the one hand and as an element of the scheme $\mathfrak{p} \in \operatorname{Spec} A$ ($\mathfrak{p} \in \operatorname{Proj} B$ resp.) on the other hand.

For a smooth projective curve C we denote by $g(C)$ the (geometric) genus of the curve. If there is no danger of confusion to which curve we are referring, we write g. We will denote the arithmetic genus of a curve by p_a. If the arithmetic genus and the geometric genus of a curve C coincide, we will just say genus and write $g(C)$ or g.

Chapter 1

Geometry of arithmetic surfaces

In this chapter we review some results of arithmetic geometry which are needed in order to work with arithmetic surfaces.

1.1 Regularity

Our aim is to define regularity for a scheme, to develop a couple of tools that help to show that a scheme or a ring is regular (or to show that it is non-regular), and to explain the geometric viewpoint of regularity.

Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue class field $k(\mathfrak{m}) = A/\mathfrak{m}$. We denote by $\dim A$ the Krull dimension which is defined to be the number of strict inclusions in a maximal chain of prime ideals. Since we just consider Noetherian rings, this dimension is finite. It can be shown that the Krull dimension of A is less or equal to the dimension of the $k(\mathfrak{m})$-vector space $\mathfrak{m}/\mathfrak{m}^2$ (see e.g. [Mat1], p.78). We are interested in rings where equality holds.

Definition 1.1.1. Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue class field $k(\mathfrak{m})$. We say that A is *regular* if $\dim A = \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$.

Given any system of generators of $\mathfrak{m}$, the number of generators is obviously bigger or equal to $\dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$. On the other hand there exists a system with exactly $\dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2$ generators. To see this we just have to consider any basis of $\mathfrak{m}/\mathfrak{m}^2$ and then choose for each element in this basis a preimage. Now, Nakayama's lemma tells us that these preimages already generate $\mathfrak{m}$ as an A-module (see e.g. [Ei], p.124: Corollary 4.8 (b)). This gives us another description of regularity:

Proposition 1.1.2. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue class field $k(\mathfrak{m})$. A is regular if and only if $\mathfrak{m}$ can be generated by $\dim A$ elements.*

Definition 1.1.3. Let A be a Noetherian ring and $\mathfrak{p} \subset A$ a prime ideal. We say that A is *regular at* $\mathfrak{p}$ if $A_{\mathfrak{p}}$ is a regular local ring. We say that A is *regular* if it is regular at each prime ideal.

Corollary 1.1.4. *Let A be a Noetherian ring and $\mathfrak{p} \subset A$ a prime ideal. Then A is regular at $\mathfrak{p}$ if and only if $\mathfrak{p}A_\mathfrak{p}$ is generated by $\operatorname{ht}(\mathfrak{p})$ elements.*

Proof: With Proposition 1.1.2 we have that A is regular at $\mathfrak{p}$ if and only if $\mathfrak{p}A_\mathfrak{p}$ is generated by $\dim A_\mathfrak{p}$ elements. Since $\operatorname{ht}(\mathfrak{p}) = \dim A_\mathfrak{p}$ (see e.g. [Liu], p.69: Proposition 5.8. (b)) the claim follows. $\square$

Proposition 1.1.5. *Let A be a regular Noetherian ring and S a muliplicative subset of A. Then A_S is regular.*

Proof: Let $\mathfrak{P}$ be a prime ideal of A_S. This ideal is of the form $\mathfrak{p}A_S$ with a prime ideal $\mathfrak{p}$ of A disjoint from S (see e.g. [Mat2], p.22: Theorem 4.1. (ii)). We have $(A_S)_{\mathfrak{p}A_S} = A_\mathfrak{p}$ (see e.g. [Mat2], p.24: Corollary 4.), hence the regularity of A_S at $\mathfrak{P}$ follows from the regularity of A at $\mathfrak{p}$. $\square$

Proposition 1.1.6. *Let A be a Noetherian ring. Then A is regular if and only if it is regular at its maximal ideals.*

Proof: Follows with [Mat2], p.24: Corollary 4. $\square$

In the following chapters we often have the situation that we have to check the regularity of a factor ring A/f, where A is a regular ring and f is an element of A. This ring comes with the canonical surjection $\operatorname{can} : A \to A/f$. Now, the preimage of a prime ideal of A/f gives us a prime ideal of A. We can use the following fact to check regularity:

Proposition 1.1.7. *Let A/f be a factor ring, where A is a regular ring and f is an element of A. Furthermore, let $\mathfrak{P}$ be a prime ideal of A/f and $\mathfrak{p} = \operatorname{can}^{-1}\mathfrak{P}$. Then A/f is regular at $\mathfrak{P}$ if and only if $f \notin (\mathfrak{p}A_\mathfrak{p})^2$.*

Proof: The proposition follows directly with [Liu], p.129: Corollary 2.12. and [Mat2], p.23: Theorem 4.2. $\square$

Definition 1.1.8. Let X be a locally Noetherian scheme and $x \in X$ a point. We say that X is *regular at x* if the stalk $\mathcal{O}_{X,x}$ at x of the structure sheaf $\mathcal{O}_X$ is a regular local ring. We say that X is *regular* if it is regular at all of its points. If x is a point of X which is not regular we call it a *singular point of X*. A scheme that is not regular is said to be *singular*.

In case our scheme comes together with a flat morphism we can use the following useful result:

Proposition 1.1.9. *Let X and Y be locally Noetherian schemes and $g : X \to Y$ a flat morphism. If Y is regular at $y \in g(X)$, and $X_y = X \times_Y \operatorname{Spec} k(y)$ is regular at a point x, then X is regular at x.*

Proof: See e.g. [Gr1], p.143: Corollaire 6.5.2. □

The proposition above is helpful if the studying of the points of Y and X_y is easy. Anyway, in the situations we consider later the scheme Y is already regular and we only need to take care of the scheme X_y. This scheme is a variety over the field $k(y)$. To analyze the points of this variety we can use the Jacobian criterion:

Theorem 1.1.10 (Jacobian criterion). *Let k be a field, $X = V(I)$ a closed subvariety of $\mathbb{A}^n_k = \operatorname{Spec} k[T_1, \ldots, T_n]$, and $F_1, \ldots, F_r$ a system of generators of I. For a rational point $x \in X(k)$ we consider the $r \times n$ matrix*

$$J_x = \left(\frac{\partial F_i}{\partial T_j}(x) \right)_{1 \leq i \leq r, 1 \leq j \leq n} .$$

Then X is regular at x if and only if $\operatorname{rank} J_x = n - \dim \mathcal{O}_{X,x}$.

Proof: See e.g. [Liu], p.130: Theorem 2.19. □

Remark 1.1.11. Let us assume the morphism g in Proposition 1.1.9 is *faithfully flat*, i.e. flat and surjective (see e.g. [Mi], p10: Proposition 2.7.). If Y and X_y are regular for all $y \in Y$ then X is regular. If X is regular then Y is regular (see e.g. [Gr1], p.143: Corollaire 6.5.2.). If Y is regular at y and X_y is singular at some x it may nevertheless happen that X is regular at x.

Definition 1.1.12. Let $N \in \mathbb{N}$ be a natural number with $N \geq 2$ and ζ_N a primitive N-th root of unity. We call the scheme

$$\mathcal{X} = \operatorname{Spec} \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1) . \tag{1.1.1}$$

the *(affine) Fermat scheme of exponent N.*

Proposition 1.1.13. *Let $\mathcal{X}$ be the Fermat scheme of exponent N (cf. Definition 1.1.12). Then $\mathcal{X}$ is regular at a prime ideal $\mathfrak{p} \in \mathcal{X}$, if $N \notin \mathfrak{p}$.*

Proof: We have a morphism $g : \mathcal{X} \to \mathcal{Y} = \operatorname{Spec} \mathbb{Z}[\zeta_N]$ which corresponds to the ring homomorphism

$$g^\sharp : \mathbb{Z}[\zeta_N] \to \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1)$$

where $g^\sharp$ is the composition of the inclusion $\mathbb{Z}[\zeta_N] \to \mathbb{Z}[\zeta_N][X, Y]$ and the canonical surjection $\mathbb{Z}[\zeta_N][X, Y] \to \mathbb{Z}[\zeta_N][X, Y]/(X^N + Y^N - 1)$. The scheme $\mathcal{X}$ is integral, $\mathcal{Y}$ is a Dedekind scheme, and g is non-constant, hence the morphism g is flat (see e.g. [Liu], p.137: Corollary 3.10.). We want to show that $\mathcal{X}$ is regular at a prime ideal $\mathfrak{p} \in \mathcal{X}$ if $N \notin \mathfrak{p}$. To see this we start with a prime ideal $\mathfrak{p}$ with $g(\mathfrak{p}) = 0$. Then this prime ideal is the image of an element of $\mathcal{X}_{\mathbb{Q}(\zeta_N)} = \operatorname{Spec} \mathbb{Q}(\zeta_N)[X, Y]/(X^N + Y^N - 1)$ with respect to the obvious morphism $\mathcal{X}_{\mathbb{Q}(\zeta_N)} \to \mathcal{X}$. Since this morphism is flat and $\mathcal{X}_{\mathbb{Q}(\zeta_N)}$ is regular it follows that $\mathcal{X}$ is regular at $\mathfrak{p}$ (see e.g. [Gr1], p.143: Corollaire 6.5.2.). Next, let $\mathfrak{p}$ be a prime ideal with $g(\mathfrak{p}) = \mathfrak{q}$, where $\mathfrak{q}$ is a prime in $\mathbb{Z}[\zeta_N]$. Since $\mathcal{Y}$ is regular, we only have to concentrate on the fiber $\mathcal{X}_\mathfrak{q} = \operatorname{Spec} k(\mathfrak{q})[X,Y]/(X^N+Y^N-1)$, where $k(\mathfrak{q})$ is the residue field of $\mathfrak{q}$ (Proposition 1.1.9). We use the Jacobian criterion to analyze the scheme $\mathcal{X}_\mathfrak{q}$. For simplicity we may change to the *geometric special fiber* $\overline{\mathcal{X}}_\mathfrak{q} = \mathcal{X}_\mathfrak{q} \times_{\operatorname{Spec} k(\mathfrak{q})} \operatorname{Spec} \overline{k(\mathfrak{q})} = \operatorname{Spec} \overline{k(\mathfrak{q})}[X,Y]/(X^N + Y^N - 1)$. Since the inclusion morphism $k(\mathfrak{q}) \hookrightarrow \overline{k(\mathfrak{q})}$ is faithfully flat, the projection morphism $p_2 : \overline{\mathcal{X}}_\mathfrak{q} \to \mathcal{X}_\mathfrak{q}$ is faithfully flat as well. Hence, if $\overline{\mathcal{X}}_\mathfrak{q}$ is regular, then $\mathcal{X}_\mathfrak{q}$ is regular. Now, let us assume that $N \notin \mathfrak{q}$. Then the rank of the Jacobian matrix $J = (NX^{N-1}, NY^{N-1})$ is 1 for all points of $\overline{\mathcal{X}}_\mathfrak{q}$ and so $\overline{\mathcal{X}}_\mathfrak{q}$ is regular (Theorem 1.1.10 and [Liu], p.130: Corollary 2.17.), hence $\mathcal{X}$ is regular in $\mathfrak{p}$ (Proposition 1.1.9). If $N \in \mathfrak{q}$ then the Jacobian matrix is zero and it follows that $\overline{\mathcal{X}}_\mathfrak{q}$ is singular at all points. In this situation Proposition 1.1.9 does not tell us, if $\mathcal{X}$ is regular at $\mathfrak{p}$. $\square$

Example 1.1.14. In Proposition 1.1.13 we saw that $\mathcal{X}$ given by (1.1.1) is regular at a prime ideal $\mathfrak{p}$, if $N \notin \mathfrak{p}$. Contrary to this, if $N \in \mathfrak{p}$ and $g(\mathfrak{p}) = \mathfrak{q}$, then the whole fiber above $\mathfrak{q}$ (considered as a $k(\mathfrak{q})$-variety) is singular, and we do not know anything about $\mathcal{X}$ at $\mathfrak{p}$. However, it may happen - like we mentioned before - that $\mathfrak{p}$ is a regular point of $\mathcal{X}$. We may illustrate this with the similar scheme

$$\mathcal{X} = \operatorname{Spec} \mathbb{Z}[X,Y]/(X^3 + Y^3 - 1)\,.$$

Consider the maximal ideal $\mathfrak{m} = (X-2, Y-2, 3) \in \mathcal{X}$. We can interpret this "closed point" as an element of $\mathcal{X}_{(3)}$. This is a singular point of $\mathcal{X}_{(3)}$ according to the Jacobian criterion. On the other hand we have

$$X^3 + Y^3 - 1 = (X + Y - 4)^3 + 3G(X,Y)$$

with $G(X,Y) = 21 - x^2y + 4x^2 - xy^2 + 8xy - 16x + 4y^2 - 16y$. If $G(X,Y) \in \mathfrak{m}$ we have $1 \in \mathfrak{m}$, a contradiction. It follows that $G(X,Y)$ becomes a unit in $(\mathbb{Z}[X,Y]/(X^3+Y^3-1))_\mathfrak{m}$. Now the claim follows with Corollary 1.1.4 because $\mathfrak{m}\,(\mathbb{Z}[X,Y]/(X^3+Y^3-1))_\mathfrak{m} = (X-2, Y-2)$.

In Remark 1.1.11 we just mentioned that if we have a surjective flat morphism $g : X \to Y$ with a regular scheme X, then Y is necessarily regular, too. It would be desirable to have a statement in the opposite direction. In other words, to have a certain kind of morphism with the property that if Y is regular then it follows that X is regular.

Definition 1.1.15. Let $g : X \to Y$ be a morphism that is locally of finite type. We say that g is *unramified at* $x \in X$ if $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x}$ is a finite separable field extension of $k(y)$, where $g(x) = y$ and $\mathfrak{m}_y$ is the maximal ideal of $\mathcal{O}_{Y,y}$. We say that g is *unramified* if it is unramified at all $x \in X$. The morphism g is called *étale* if it is flat and unramified.

Proposition 1.1.16. *Let $g : X \to Y$ be an étale morphism. The following properties are true.*

1. $\dim \mathcal{O}_{X,x} = \dim \mathcal{O}_{Y,g(y)}$ *for all* $x \in X$.

2. *If Y is normal, then X is normal.*

3. *If Y is regular, then X is regular.*

Proof: See e.g. [Mi], p.27: Proposition 3.17. $\square$

Now we are going to describe how we can use regularity to show normality.

Proposition 1.1.17. *Let R be a regular integral Noetherian ring and $f \in R \setminus R^*$. If R/f is regular in codimension 1 then R/f is normal.*

Proof: Since R is a regular ring it is a Cohen-Macaulay ring (see [Liu], p.337 for a definition and this statement). We want to show that R/f is a Cohen-Macaulay ring, too: Let $\mathfrak{m} \in \operatorname{Max}(R/f)$ and $\mathfrak{M} \in \operatorname{Max}(R)$ be the preimage of $\mathfrak{m}$. The ideal $\mathfrak{M}$ is indeed a maximal ideal because the canonical map $R \to R/f$ is a surjection. Since localization commutes with passing to quotients by ideals, we have

$$(R/f)_{\mathfrak{m}} = R_{\mathfrak{M}}/fR_{\mathfrak{M}}\,.$$

Now f is a regular element of $R_{\mathfrak{M}}$ and so $R_{\mathfrak{M}}/fR_{\mathfrak{M}}$ is a Cohen-Macaulay ring (see [Liu], p.337: Proposition 2.15. (a)). Since our computation is valid for all maximal ideal of R/f the ring R/f is Cohen-Macaulay (cf. [Ei], p.452: Proposition 18.8.). The statement follows now with Serre's criterion (see [Liu], p.339: Theorem 2.23.). $\square$

1.2 Blowing-ups

In the study of birational morphisms blowing-ups play an important role. In this section we will summarize the main facts we need about blowing-ups. Most of the material we introduce is standard and the proofs may be found in [Liu], [EH] and [Ha]. Later we will prove a result which deals with the concrete situation that will appear in the following chapters frequently. Apart from this we follow most of the time the book [Liu].

To start with, let A be a Noetherian ring and I an ideal of A. We denote by $\widetilde{A}$ the graded A-algebra

$$\widetilde{A} = \bigoplus_{d \geq 0} I^d, \text{ where } I^0 := A\,.$$

Definition 1.2.1. Let $X = \operatorname{Spec} A$ be an affine Noetherian scheme, I an ideal of A, and $\widetilde{X} = \operatorname{Proj} \widetilde{A}$. The scheme $\widetilde{X}$ together with the canonical morphism $\widetilde{X} \to X$ is called the *blowing-up of X along $V(I)$*.

The blowing-up has the following properties.

Lemma 1.2.2. *Let A be a Noetherian ring, and let I be an ideal of A.*

1. *The ring $\widetilde{A}$ is integral if and only if A is integral.*

2. *Let B be a flat A-algebra, and let $\widetilde{B}$ be the graded B-algebra associated to the ideal IB. Then we have a canonical isomorphism $\widetilde{B} \cong B \otimes_A \widetilde{A}$.*

Proof: See e.g. [Liu], p. 318: Lemma 1.2. (c) and (d). □

Now let $I = (a_1, \ldots, a_r)$. We denote by $t_i \in I = \widetilde{A}_1$ the element a_i considered as a homogeneous element of degree 1. We have a surjective homomorphism of graded A-algebras

$$\phi : A[X_1, \ldots, X_r] \to \widetilde{A}$$

defined by $\phi(X_i) = t_i$. It follows that $\widetilde{A}$ is isomorphic to a factor ring $A[X_1, \ldots, X_r]/J$; here J denotes an ideal of $A[X_1, \ldots, X_r]$. It may be desirable for certain applications to express the blowing-up in such a way. Unfortunately it is not always easy to describe the ideal J explicitly. However if the ideal I is generated by a regular sequence we have a nice description of J.

Lemma 1.2.3. *Let $I \subset A$ be an ideal which is generated by a regular sequence $a_1, \ldots, a_r$. Then $\widetilde{A} \cong A[X_1, \ldots, X_r]/J$ where the ideal J is generated by the elements of the form $X_i a_j - X_j a_i$ for $1 \leq i, j \leq r$.*

Proof: See e.g. [EH], p.172: Proposition IV-25. and p. 173: Exercise IV-26. □

Later on, we will often work with integral rings. Here we have the following situation:

Lemma 1.2.4. *Let A be a Noetherian integral ring and $I = (a_1, \ldots, a_r)$ an ideal of A, with $a_i \neq 0$ for all i. The blowing-up $\widetilde{X} \to X = \operatorname{Spec} A$ along $V(I)$ is the union of the affine open subschemes $\operatorname{Spec} A_i$, $1 \leq i \leq r$, where A_i is the sub-A-algebra*

$$A[\frac{a_1}{a_i}, \ldots, \frac{a_r}{a_i}]$$

of the field $\operatorname{Frac}(A)$ generated by the $\frac{a_j}{a_i} \in \operatorname{Frac}(A)$, $1 \leq j \leq r$.

Proof: See e.g. [Liu], p. 320: Lemma 1.4. □

Lemma 1.2.5. *Let A be an integral Noetherian ring, $a_1, \ldots, a_r$ a regular sequence, and $I = (a_1, \ldots, a_r)$. We have:*

1. *The ring*
$$R = A[X_1, \ldots, \widehat{X_i}, \ldots, X_r]/J\,,$$
where J is generated by the elements $a_j - X_j a_i$ with $1 \leq j \leq r$ and $j \neq i$, is integral.

2. *For an element $f \in A$ let $\overline{f}$ denote its image in R. We have*
$$f \in I^d \Leftrightarrow \overline{f} \in (\overline{a_i})^d\,.$$

Proof: Since A is integral $\widetilde{A}$ is integral, too (Lemma 1.2.2 (1)). We know that

$$\widetilde{A} \cong A[X_1, \ldots, X_r]/J$$

where J is generated by the elements $X_i a_j - X_j a_i$ for $1 \leq i, j, \leq r$ (Lemma 1.2.3). But then, $\operatorname{Spec} R$ is an affine open subset of $\operatorname{Proj} \widetilde{A}$ and therefore integral. This proves the first statement.
For simplicity we assume $i = 1$. Let $f \in I^d$. Then there exists a homogeneous polynomial $F(X) = F(X_1, \ldots, X_r) \in A[X_1, \ldots, X_r]$ of degree d with $f = F(a) = F(a_1, \ldots, a_r)$. If we set

$$f_0 = \frac{F(a_1, X_2 a_1, \ldots, X_r a_1)}{a_1^d} = F(1, X_2, \ldots, X_r)$$

we obviously have $\overline{f} = \overline{f_0}\overline{a_1}^d$ and therefore $\overline{f} \in (\overline{a_1})^d$.
Now let $\overline{f} \in (\overline{a_1})^d$. Furthermore, let n be the biggest integer with $f \in I^n$. Let us suppose $n < d$. Again, we have a homogeneous polynomial $F(X)$ of degree n with $F(a) = f$. If follows that not all coefficients of $F(X)$ are in I because otherwise we would have $f \in I^{n+1}$. Now $f_0 = \frac{F(a_1, X_2 a_1, \ldots, X_r a_1)}{a_1^n}$ is a polynomial in $X_2, \ldots, X_r$ where not all coefficients of f_0 are in I. Again, we have $\overline{f} = \overline{f_0}\overline{a_1}^n$ but, since R is integral, the element $\overline{a_1}$ must divide $\overline{f_0}$. Then $f_0 = a_1 G(X) + H(X)$ with ploynomials $G(X) \in A[X_2, \ldots, X_r]$ and $H(X) \in J$. It follows that all coefficients of f_0 are in I, a contradiction. In other words, we have $d \leq n$ and therefore $f \in I^d$. $\square$

So far we have seen, the most comfortable situations arise if we work with an integral scheme that we blow up along a subscheme associated to an ideal generated by a regular sequence. Unfortunately, sometimes we do not have these pleasant circumstances. However, in the situations that have to be considered later the following theorem will help us to overcome this problem.

Theorem 1.2.6. *Let A be an integral Noetherian ring, $a_1, \ldots, a_r$ a regular sequence, and $I = (a_1, \ldots, a_r)$ a prime ideal. Furthermore, let $f \in I$ and n be the biggest integer with $f \in I^n$. Then*

$$A[X_1, \ldots, \widehat{X_i}, \ldots, X_r]/J_0 \cong A/f[\frac{\boldsymbol{a}_1}{\boldsymbol{a}_i}, \ldots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_i}]$$

where J_0 is the ideal generated by the $a_j - X_j a_i$ (with $1 \leq j \leq r$ and $j \neq i$) and a polynomial f_0 with $f \equiv f_0 a_i^n \mod J$; here $\boldsymbol{a}_j$ denotes the residue class of a_j in A/f and J is the ideal from Lemma 1.2.5.

Proof: For simplicity we assume $i = 1$. The canonical surjection

$$\begin{aligned} \varphi : A[X_2, \ldots, X_r] &\longrightarrow A/f[\frac{\boldsymbol{a}_2}{\boldsymbol{a}_1}, \ldots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_1}] \\ F(X_2, \ldots, X_r) &\longmapsto \boldsymbol{F}(\frac{\boldsymbol{a}_2}{\boldsymbol{a}_1}, \ldots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_1}) \end{aligned}$$

(here the bold $\boldsymbol{F}$ indicates that we reduce the coefficients of the polynomial modulo f) induces, since $a_i - X_i a_1 \in \ker \varphi$, a surjection

$$\begin{aligned} \phi : A[X_2, \dots, X_r]/J &\longrightarrow A/f[\frac{\boldsymbol{a}_2}{\boldsymbol{a}_1}, \dots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_1}] \\ \overline{F}(\overline{X_2}, \dots \overline{X_r}) &\longmapsto \boldsymbol{F}(\frac{\boldsymbol{a}_2}{\boldsymbol{a}_1}, \dots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_1}) \end{aligned}$$

where J is the ideal from Lemma 1.2.5. We get the following commutative diagram

$$\begin{tikzcd} A[X_2, \dots, X_r]/J \arrow[r, two heads, "\phi"] & A/f[\frac{\boldsymbol{a}_2}{\boldsymbol{a}_1}, \dots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_1}] \\ A \arrow[u] \arrow[r, "\text{can}"] & A/f \arrow[u, hook] \end{tikzcd} \tag{1.2.1}$$

Next we want to investigate the kernel of the map ϕ. Let $x = \overline{F}(\overline{X_2}, \dots \overline{X_r})$ with a polynomial $F(X_2, \dots, X_r)$ of degree m and $\phi(x) = 0$. We have $a_1^m F(X_2, \dots, X_r) \equiv \mu \mod J$ with an element $\mu \in A$. Since diagram (1.2.1) is commutative and the right arrow in this diagram is injective we have $\text{can}(\mu) = 0$. It follows that $\mu = \lambda f$ with a $\lambda \in A$. Now let n (n_λ resp.) be the biggest integer with $f \in I^n$ ($\lambda \in I^{n_\lambda}$ resp.) and $f_0 \in A[X_2, \dots, X_r]$ ($\lambda_0 \in A[X_2, \dots, X_r]$ resp.) with $\overline{a_1}^n \overline{f_0} = \overline{f}$ ($\overline{a_1}^{n_\lambda} \overline{\lambda_0} = \overline{\lambda}$ resp.). We have

$$\overline{a_1}^m x = \overline{f\lambda} = \overline{a_1}^n \overline{f_0} \overline{a_1}^{n_\lambda} \overline{\lambda_0} \tag{1.2.2}$$

in $A[X_2, \dots, X_r]/J$. If we assume that $m \le n + n_\lambda$ we can cancel $\overline{a_1}^m$ in equation (1.2.2) (Lemma 1.2.5 (1)) and it follows that x is in the ideal $(\overline{f_0})$. So if we can show that $m > n + n_\lambda$ is impossible we have finished our proof. According to (1.2.2) we have $\lambda f \in I^m$ (Lemma 1.2.5 (2)). Now, $m > n + n_\lambda$ would implie that the associated graded algebra $\text{gr}_I(A)$ is not integral. But $a_1, \dots, a_r$ is a regular sequence and so we have an A/I-algebra isomorphism

$$\text{Sym}(I/I^2) \cong \text{gr}_I(A)$$

(see [Hu]) with $\text{Sym}(I/I^2)$ integral since I is a prime ideal. This gives us the contradiction. □

Remark 1.2.7. The schemes we have to consider later are of the form $\text{Spec}\, A/f$ (at least locally) with a ring A and a prime element $f \in A$. An ideal of A/f is of the form I/f with an ideal $I = (a_1, \dots, a_r) \subset A$. The blowing-up of A/f along $V(I/f)$ will be covered by the spectrum of the affine rings

$$A/f[\frac{\boldsymbol{a}_1}{\boldsymbol{a}_i}, \dots, \frac{\boldsymbol{a}_r}{\boldsymbol{a}_i}],$$

where $\boldsymbol{a}_j$ is the residue class of a_j in A/f (Lemma 1.2.4). According to Theorem 1.2.6 we can express these rings explicitly as factor rings. To do this, the only thing we need to know is the biggest integer n with $f \in I^n$ and polynomials $f_{0,i}$ with $f \equiv f_{0,i}a_i^n \mod J$. There is a strategy how one can find these quantities: One just needs to find a homogenous polynomial $F(X) \in A[X_1, \dots, X_r]$ where not all coefficients are in I and with $F(a) = f$. Obviously $f \in I^n$ where n is the degree of $F(X)$. Because $a_1, \dots, a_r$ is a regular sequence it is a quasi-regular sequence as well (see [Mat2], p.125: Theorem 16.2.). It follows that if $f \in I^{n+1}$ then all coefficients are in I, a contradiction. So n is the biggest integer with $f \in I^n$. The $f_{0,i}$ we get now in the same way like in the proof of Lemma 1.2.5. More explicit, we have

$$f_{0,i} = f(X_1, \dots, X_{i-1}, 1, X_{i+1}, \dots, X_r)\,.$$

It is possible to extend the construction of blowing-up affine scheme to arbitrary schemes. In this situation we need to use a coherent sheaf of ideals to construct the blowing-up.

Definition 1.2.8. Let X be a Noetherian scheme, and $\mathcal{I}$ be a coherent sheaf of ideals on X. Consider the sheaf of graded algebras $\bigoplus_{d\geq 0} \mathcal{I}^d$, where $\mathcal{I}^d$ is the d-th power of the ideal $\mathcal{I}$, and we set $\mathcal{I}^0 = \mathcal{O}_X$. Then $\widetilde{X} = \operatorname{Proj} \bigoplus_{d\geq 0} \mathcal{I}^d$ is the blowing-up of X with respect to the coherent sheaf of ideals $\mathcal{I}$. If Y is the closed subscheme of X corresponding to $\mathcal{I}$, then we also call $\widetilde{X}$ the blowing-up of X along Y.

Proposition 1.2.9. *Let X be a locally Noetherian scheme, and let $\mathcal{I}$ be a coherent sheaf of ideals on X. Let $\pi : \widetilde{X} \to X$ be the blowing-up of X along $Y = V(\mathcal{I})$. Then the following properties are true:*

1. *The morphism π is proper.*

2. *Let $Z \to X$ be a flat morphism with Z locally Noetherian. Let $\widetilde{Z} \to Z$ be the blowing-up of Z along $\mathcal{I}\mathcal{O}_Z$; then $\widetilde{Z} \cong \widetilde{X} \times_X Z$.*

3. *The morphism π induces an isomorphism $\pi^{-1}(X \setminus V(\mathcal{I})) \to X \setminus V(\mathcal{I})$. If X is integral, and if $\mathcal{I} \neq 0$, then $\widetilde{X}$ is integral, and π is a birational morphism.*

Proof: See e.g. [Liu], p.322: Proposition 1.12. □

Now let us assume, that X is a locally Noetherian scheme that comes together with a closed immersion $f : X \to Z$ to a locally Noetherian scheme Z. Let $\mathcal{J}$ be a quasi-coherent sheaf of ideals on Z with the property that $f(X)$ is not contained in the center $V(\mathcal{J})$. Then the blowing-up $\widetilde{X}$ of X along $\mathcal{I}$, where $\mathcal{I} = (f^{-1}\mathcal{J})\mathcal{O}_X$, is a closed immersion of the blowing-up $\widetilde{Z}$ of Z along $\mathcal{J}$ (see e.g. [Liu], p.324: Corollary 1.16.). The closed subscheme $\widetilde{X} \subseteq \widetilde{Z}$ is called the *strict transform* of X. Later, the situation just described will appear very often. In our case the scheme X will be a singular scheme which is a subscheme of a regular scheme Z. We will use a sequence of blowing-ups of X to get a desingularization of this scheme[1]. Each of these blowing-ups comes from a blowing-up of the scheme Z. The blowing-ups of Z will be regular again:

Theorem 1.2.10. *Let Z be a regular locally Noetherian scheme, and $\pi : \widetilde{Z} \to Z$ be the blowing-up of Z along a regular closed subscheme $Y = V(\mathcal{J})$. Then the scheme $\widetilde{Z}$ is regular.*

Proof: See e.g. [Liu], p.325: Theorem 1.19. □

1.3 Intersection theory for arithmetic surfaces

Definition 1.3.1. An *arithmetic surface* $\mathcal{X}$ is a regular integral scheme of dimension 2 together with a projective flat morphism $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$, where $\mathcal{O}_E$ is the ring of integers of a number field E or a localization of such a ring. Moreover we assume that the *generic fiber*

$$X_E = \mathcal{X} \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} E$$

of f is geometrically irreducible[2]. For each $s \in \operatorname{Spec} \mathcal{O}_E$ we define the fiber above s as $\mathcal{X}_s := \mathcal{X} \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} k(s)$. We have $\mathcal{X}_{(0)} = X_E$. Any point $s \neq (0)$ will be called a *closed point* and the corresponding fiber $\mathcal{X}_s$ a *special fiber*.

Definition 1.3.2. Let C be a smooth projective geometrically irreducible curve over a number field E, and $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ an arithmetic surface. We say that $\mathcal{X}$ is a *regular model* of C, if there is an E-isomorphism between the curves C and X_E.

Assumption 1.3.3. For the rest of this subsection we make the assumption that $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ is an arithmetic surface in the sense of Definition 1.3.1.

Remark 1.3.4. Due to the fact that $\operatorname{Spec} \mathcal{O}_E$ is Noetherian and that f is of finite type it follows that $\mathcal{X}$ is Noetherian as well.

Definition 1.3.5. We denote by $Z^1(\mathcal{X})$ the *group of Weil divisors of* $\mathcal{X}$, by $\operatorname{Cl}(\mathcal{X})$ the *divisor class group of* $\mathcal{X}$ i.e. the group of Weil divisors divided by the subgroup of principal divisors $R^1(\mathcal{X})$, and by $\operatorname{Pic}(\mathcal{X})$ the *Picard group of* $\mathcal{X}$. Instead of saying “a Weil divisor” we will just say “a divisor”.[3]

[1]We will describe later that a desingularization of an arithmetic surface always exists. To get it, one has to perform a finite sequence of modifications, where a modification is the normalization of the blowing-up of the singular locus. However, in the following chapters, whenever we construct regular models of the Fermat curve of squarefree exponent, we just need to work with blowing-ups and never need to normalize explicitly.

[2]That X_E is geometrically irreducible is equivalent to the property that E is algebraically closed in the function field $K(X_E)$ (see e.g. [Liu], p.91: Corollary 2.14. (d)).

[3]The names and symbols for these groups differ in the literatur. For example the group of Weil divisors is sometimes denoted by $\operatorname{Div}(\mathcal{X})$ (see e.g. [Ha]) or the divisor class group is called *Chow group* (see e.g. [La]).

Remark 1.3.6. Since $\mathcal{X}$ is a regular Noetherian integral scheme, the divisor class group $\mathrm{Cl}(\mathcal{X})$ of $\mathcal{X}$ is isomorphic to the Picard group $\mathrm{Pic}(\mathcal{X})$ (see [Liu], p.257: Corollary 1.19 and p.271: Proposition 2.16). Let us denote by f the canonical surjection $f : Z^1(\mathcal{X}) \to \mathrm{Cl}(\mathcal{X})$ and by g the isomorphism $g : \mathrm{Cl}(\mathcal{X}) \to \mathrm{Pic}(\mathcal{X})$. For any divisor $\mathcal{D} \in Z^1(\mathcal{X})$ we denote the corresponding invertible sheaf $(g \circ f)(\mathcal{D})$ by $\mathcal{O}_{\mathcal{X}}(\mathcal{D})$.

Remark 1.3.7. Since $\mathcal{X}$ is a regular Noetherian integral scheme, the group of Weil divisors $Z^1(\mathcal{X})$ of $\mathcal{X}$ is isomorphic to its group of Cartier divisors $\mathrm{Div}(\mathcal{X})$ (see e.g. [Liu], p. 271: Proposition 2.16.). A Cartier divisor can by represented by a system $\{(U_i, f_i)_i\}$, where the U_i are open subsets of $\mathcal{X}$ that form a covering of $\mathcal{X}$, f_i is the quotient of two regular elements of $\mathcal{O}_{\mathcal{X}}(U_i)$, and $f_i|_{U_i \cap U_j} \in f_j|_{U_i \cap U_j} \mathcal{O}_{\mathcal{X}}(U_i \cap U_j)^*$ for every i, j.

Definition 1.3.8. Let $\mathcal{D}$ be a divisor and $\{(U_i, f_i)_i\}$ its corresponding Cartier divisor (Remark 1.3.7). We say that f_i is a *local equation* of $\mathcal{D}$ in U_i. Let $x \in \mathcal{X}$ be a closed point and U_i one of the open sets with $x \in U_i$. We denote the image of f_i in $K(\mathcal{X})$ - which is induced by the map $\mathcal{O}_{\mathcal{X}}(U_i) \to \mathcal{O}_{\mathcal{X},x}$ - by f_x and call it a *local equation of* $\mathcal{D}$ *in* x.

Remark 1.3.9. A local equation f_x of a divisor $\mathcal{D}$ in a closed point x is not unique, since it depends on the system $\{(U_i, f_i)_i\}$, which represents the Cartier divisor. However, if $\{(V_j, g_j)_j\}$ is a different system that represents the same divisor, then on $U_i \cap V_j$ the elements f_i and g_j differ by an element of $\mathcal{O}_{\mathcal{X}}(U_i \cap V_j)^*$, hence g_x differs from f_x just by a unit of $\mathcal{O}_{\mathcal{X},x}$.

Remark 1.3.10. If $\mathcal{D}$ is effective, then $f_i \in \mathcal{O}_{\mathcal{X}}(U_i)$ for all i (see e.g. [Ue], p. 45: PROBLEM 13.), hence $f_x \in \mathcal{O}_{\mathcal{X},x}$ for all $x \in \mathcal{X}$.

Definition 1.3.11. Let $\mathcal{D}$, $\mathcal{E}$ be effective divisors without common component, $x \in \mathcal{X}$ a closed point and f_x, g_x local equations of $\mathcal{D}$, $\mathcal{E}$ in the local ring $\mathcal{O}_{\mathcal{X},x}$. Then we define the *intersection number* $i_x(\mathcal{D}, \mathcal{E})$ *in* x as the length of $\mathcal{O}_{\mathcal{X},x}/(f_x, g_x)$ as an $\mathcal{O}_{\mathcal{X},x}$-module. We say that $\mathcal{D}$ *intersects* $\mathcal{E}$ if $\mathrm{Supp}\,\mathcal{D} \cap \mathrm{Supp}\,\mathcal{E} \neq \emptyset$. This is equivalent to the existence of closed points $x \in \mathcal{X}$ with $i_x(\mathcal{D}, \mathcal{E}) \neq 0$. We say that the intersection of $\mathcal{D}$ and $\mathcal{E}$ is *transverse* in x if $i_x(\mathcal{D}, \mathcal{E}) = 1$. The symbol $i_x(\mathcal{D}, \mathcal{E})$ is bilinear and so we may extend the intersection number to all pairs of divisors of $\mathcal{X}$ (just write $\mathcal{D}$ as $\mathcal{D}_+ - \mathcal{D}_-$ with $\mathcal{D}_+$ and $\mathcal{D}_-$ effective and then define $i_x(\mathcal{D}, \mathcal{E}) := i_x(\mathcal{D}_+, \mathcal{E}) - i_x(\mathcal{D}_-, \mathcal{E})$) that have no common components. Now let $s \in \mathrm{Spec}\,\mathcal{O}_E$ be a closed point. The *intersection number of* $\mathcal{D}$ *and* $\mathcal{E}$ *above* s is then defined as

$$i_s(\mathcal{D}, \mathcal{E}) := \sum_{x \in \mathcal{X}_s^{(1)}} i_x(\mathcal{D}, \mathcal{E})[k(x) : k(s)]\,,$$

where $\mathcal{X}_s^{(1)}$ denotes the set of closed points of $\mathcal{X}_s$ and $k(x)$ ($k(s)$ resp.) denotes the residue class field of x (s resp.). If one of the divisors has support in a special fiber $\mathcal{X}_s$ then $i_{s'}(\mathcal{D}, \mathcal{E}) = 0$ for all $s' \neq s$. If it is clear which s is considered we just write $\mathcal{D} \cdot \mathcal{E}$ (instead of $i_s(\mathcal{D}, \mathcal{E})$).

Definition 1.3.12. Let $s \in \operatorname{Spec} \mathcal{O}_E$ be a closed point and $\mathcal{E}$ a vertical divisor contained in the special fiber $\mathcal{X}_s$. According to the moving lemma (see e.g. [Liu], p.379: Corollary 1.10) there exists a principal divisor (f) so that $\mathcal{D} := \mathcal{E} + (f)$ and $\mathcal{E}$ have no common component. Since $(f) \cdot \mathcal{E} = 0$ (see. e.g. [La], p.58: Theorem 3.1.) we may define the *self-intersection* of $\mathcal{E}$ as

$$\mathcal{E}^2 := \mathcal{D} \cdot \mathcal{E}\,.$$

Remark 1.3.13. Another possible way to define $\mathcal{E}^2$ can be done by Serre's Tor-formula via cohomological methods (see e.g. [De] or [SABK], p.11.).

Definition 1.3.14. We set $\mathrm{Cl}(\mathcal{X})_{\mathbb{Q}} = \mathrm{Cl}(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Obviously $\mathrm{Cl}(\mathcal{X})_{\mathbb{Q}}$ is a group again. The difference is that we are now allowed to work with divisors with rational coefficients. We will use $Z^1(\mathcal{X})_{\mathbb{Q}}$ and $\mathrm{Pic}(\mathcal{X})_{\mathbb{Q}}$ for the analog construction for the group of Weil divisors and the Picard group. The morphisms f, g of Remark 1.3.6 extend to morphisms $f_{\mathbb{Q}} := f \otimes \mathrm{id}_{\mathbb{Q}}, g_{\mathbb{Q}} := g \otimes \mathrm{id}_{\mathbb{Q}}$ of the groups $Z^1(\mathcal{X})_{\mathbb{Q}}, \mathrm{Cl}(\mathcal{X})_{\mathbb{Q}}$ and $\mathrm{Pic}(\mathcal{X})_{\mathbb{Q}}$. Again, for $\mathcal{D} \in Z^1(\mathcal{X})_{\mathbb{Q}}$ we will denote by $\mathcal{O}_{\mathcal{X}}(\mathcal{D})$ its image with respect to $g_{\mathbb{Q}} \circ f_{\mathbb{Q}}$ in $\mathrm{Pic}(\mathcal{X})_{\mathbb{Q}}$.

Remark 1.3.15. We extend the intersection numbers of Definition 1.3.11 to elements of $Z^1(\mathcal{X})_{\mathbb{Q}}$. We will illustrate this with divisors $\frac{r}{s}\mathcal{D}, \frac{r'}{s'}\mathcal{E} \in Z^1(\mathcal{X})_{\mathbb{Q}}$, where $\mathcal{D}$ and $\mathcal{E}$ are pairwise different prime divisors of $\mathcal{X}$. In this case we set

$$i_x(\frac{r}{s}\mathcal{D}, \frac{r'}{s'}\mathcal{E}) := \frac{r}{s}\frac{r'}{s'} i_x(\mathcal{D}, \mathcal{E})\,.$$

Now, the intersection of arbitrary elements of $Z^1(\mathcal{X})_{\mathbb{Q}}$ will be defined by using the bilinearity of the intersection products of Definition 1.3.11.

Lemma 1.3.16. *Let $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ be an arithmetic surface and $s \in \operatorname{Spec} \mathcal{O}_E$ a closed point. Then*

$$\mathcal{X}_s = \frac{1}{m}\,\mathrm{div}(h)$$

in $Z^1(\mathcal{X})_{\mathbb{Q}}$, where $\mathcal{X}_s = f^*s$, $h \in K(\mathcal{X})$ and $m \in \mathbb{Z}$.

Proof: We know that the divisor class group $\mathrm{Cl}(\operatorname{Spec} \mathcal{O}_E)$ is finite and so we can find a positive integer m and a rational function $g \in E = K(\operatorname{Spec} \mathcal{O}_E)$ with the property that $m \cdot s = \mathrm{div}(g)$. Since $\mathcal{X}$ is regular it follows that $f^*s = \mathcal{X}_s$ (see [Liu], p.351: Lemma 3.9) and so $f^*(m \cdot s) = m \cdot \mathcal{X}_s = \mathrm{div}(h)$ for a $h \in K(\mathcal{X})$. Now, in $Z^1(\mathcal{X})_{\mathbb{Q}}$ we may divide this equation by m and the lemma is proven. $\square$

1.4 Canonical divisors on an arithmetic surface

Let $f : X \to Y$ be a quasi-projective local complete intersection of Noetherian schemes. Since f is quasi-projective there exists a scheme Z together with a regular immersion $g : X \to Z$ and a smooth morphism $h : Z \to Y$ so that $f = h \circ g$. Since h is smooth and Y is Noetherian $\Omega^1_{Z/Y}$ is locally free (see [Liu], p.222: Proposition 2.5.); here $\Omega^1_{Z/Y}$ denotes the sheaf of relative differentials of degree 1. Now, because g is an immersion it decomposes into a closed immersion $\iota : X \to V$ and an open immersion $V \to Z$, where V is an open subscheme of Z. Let $\mathcal{J}$ be the ideal sheaf of V that is associated to the morphism ι. The sheaf $\mathscr{C}_{X/Z} := \iota^*(\mathcal{J}/\mathcal{J}^2)$ is called the *conormal sheaf of X in Z*. It is a locally free sheaf of X (see e.g. [Liu], p.229: Corollary 3.8.) which is independent of V.

Definition 1.4.1. We use the notation from above. The invertible sheaf

$$\omega_{X/Y} := \det(\mathscr{C}_{X/Z})^\vee \otimes_{\mathcal{O}_X} h^*(\det \Omega^1_{Z/Y})$$

is called the *canonical sheaf of $X \to Y$*; here det denotes the top exterior product $\wedge^{\mathrm{top}}$ and $\det(\mathscr{C}_{X/Z})^\vee := \mathrm{Hom}_{\mathcal{O}_X}(\det(\mathscr{C}_{X/Z}), \mathcal{O}_X)$. It is independent of the decomposition $X \to Z \to Y$ (see e.g. [Liu], p.238: Lemma 4.5.).

Remark 1.4.2. Let $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ be an arithmetic surface in the sense of Definition 1.3.1. Then f is a quasi-projective local complete intersection (see [Liu], p.232: Example 3.18.).

Remark 1.4.3. Since the scheme $\operatorname{Spec} \mathcal{O}_E$ is a locally Noetherian scheme and f is a flat projective local complete intersection of relative dimension 1, the canonical sheaf is isomorphic to the 1-dualizing sheaf (see [Liu], p.247: Theorem 4.32.).

Definition 1.4.4. Let $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ be an arithmetic surface in the sense of Definition 1.3.1. We have $\omega_{\mathcal{X}/\operatorname{Spec}\mathbb{Z}} = \omega_{\mathcal{X}/\operatorname{Spec}\mathcal{O}_E} \otimes_{\mathcal{O}_{\mathcal{X}}} f^*\omega_{\operatorname{Spec}\mathcal{O}_E/\operatorname{Spec}\mathbb{Z}}$ (see [Liu], p.239: Theorem 4.9. (a)). For simplicity we just write $\omega_{\mathcal{X}}$ for $\omega_{\mathcal{X}/\operatorname{Spec}\mathbb{Z}}$ (here we follow the notation of [MB], p.75).

Definition 1.4.5. We call any divisor $\mathcal{K}$ of $\mathcal{X}$ with $\mathcal{O}_{\mathcal{X}}(\mathcal{K}) \cong \omega_{\mathcal{X}/\operatorname{Spec}\mathcal{O}_E}$ a *canonical divisor*. This divisor exists because of Remark 1.3.6.

Remark 1.4.6. By abuse of language we call a divisor $\mathcal{K} \in Z^1(\mathcal{X})_{\mathbb{Q}}$ with $\mathcal{O}_{\mathcal{X}}(\mathcal{K}) = \omega_{\mathcal{X}/\operatorname{Spec}\mathcal{O}_E}$ in $\mathrm{Pic}(\mathcal{X})_{\mathbb{Q}}$ a canonical divisor as well. Given another canonical divisor $\mathcal{K}'$ it follows that $\mathcal{K} - \mathcal{K}' = \frac{1}{s}\operatorname{div}(f)$ with a $s \in \mathbb{Z}$, and $f \in K(\mathcal{X})$ an element of the field of functions[4].

Definition 1.4.7. Let $f : \mathcal{X} \to \mathcal{Y}$ be a morphism of Noetherian schemes and f^* the induced group homomorphism $f^* : \mathrm{Pic}(\mathcal{Y}) \to \mathrm{Pic}(\mathcal{X})$. For $\mathcal{F} \in \mathrm{Pic}(\mathcal{Y})$ we denote by $\mathcal{F}|_{\mathcal{X}}$ the pullback $f^*\mathcal{F} \in \mathrm{Pic}(\mathcal{X})$ and call it the *restriction of $\mathcal{F}$ to $\mathcal{X}$*. Let us now assume in addition that $\mathcal{X}$ and $\mathcal{Y}$ are regular and integral, and that f is flat or dominant. In this case we have a group homomorphism $f^* : Z^1(\mathcal{Y}) \to Z^1(\mathcal{X})$ (see [Liu], p.261: Lemma 1.33.). Again, for a divisor $\mathcal{D} \in Z^1(\mathcal{Y})$ we denote by $\mathcal{D}|_{\mathcal{X}}$ its pullback $f^*\mathcal{D} \in Z^1(\mathcal{X})$ and call it the *restriction of $\mathcal{D}$ to $\mathcal{X}$*. Notice that we have $\mathcal{O}_{\mathcal{X}}(\mathcal{D}|_{\mathcal{X}}) \cong \mathcal{O}_{\mathcal{Y}}(\mathcal{D})|_{\mathcal{X}}$ (see [Liu], p. 262: Remark 1.35.). The morphism f^* induces a morphism $f^*_{\mathbb{Q}} : \mathrm{Pic}(\mathcal{Y})_{\mathbb{Q}} \to \mathrm{Pic}(\mathcal{X})_{\mathbb{Q}}$ ($f^*_{\mathbb{Q}} : Z^1(\mathcal{Y})_{\mathbb{Q}} \to Z^1(\mathcal{X})_{\mathbb{Q}}$ resp.). We set $\mathcal{F}|_{\mathcal{X}} := f^*_{\mathbb{Q}}\mathcal{F}$ ($\mathcal{D}|_{\mathcal{X}} := f^*_{\mathbb{Q}}\mathcal{D}$ resp.) for a line bundle $\mathcal{F} \in \mathrm{Pic}(\mathcal{Y})_{\mathbb{Q}}$ (a divisor $\mathcal{D} \in Z^1(\mathcal{Y})_{\mathbb{Q}}$ resp.).

[4]Notice that $\mathrm{Cl}(\mathcal{X})_{\mathbb{Q}}$ is canonically isomorphic to $Z^1(\mathcal{X})_{\mathbb{Q}}/(R^1(\mathcal{X}) \otimes_{\mathbb{Z}} \mathbb{Q})$ since $\mathbb{Q}$ is flat over $\mathbb{Z}$.

Remark 1.4.8. Let $s \in \operatorname{Spec} \mathcal{O}_E$ (we do not postulate that s is a closed point). For each fiber $\mathcal{X}_s \to \operatorname{Spec} k(s)$ we get a canonical sheaf $\omega_{\mathcal{X}_s/\operatorname{Spec} k(s)}$, and we have the relation $\omega_{\mathcal{X}_s/\operatorname{Spec} k(s)} \cong \omega_{\mathcal{X}/\operatorname{Spec} \mathcal{O}_E}|_{\mathcal{X}_s}$ (see [Liu], p.350: Corollary 3.6. (d)). If s is the generic point we define a canonical divisor $K \in Z^1(X)_{\mathbb{Q}}$ of $X := \mathcal{X} \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} E$ in the same way we did with the arithmetic surface i.e. K is a divisor that fulfills $\mathcal{O}_X(K) \cong \omega_{X/\operatorname{Spec} E}$. For a canonical divisor $\mathcal{K}$ of $\mathcal{X}$ it follows that $\mathcal{K}|_X$ is a canonical divisor of X, hence $\mathcal{K}|_X$ and K represent the same class in $\operatorname{Cl}(X)_{\mathbb{Q}}$.

Now let $\mathcal{E} \in Z^1(\mathcal{X})$ be a vertical divisor contained in a special fiber $\mathcal{X}_s$ and $\mathcal{K}$ a canonical divisor on $\mathcal{X}$. Since any other canonical divisor is rationally equivalent to $\mathcal{K}$ the intersection number $\mathcal{K} \cdot \mathcal{E}$ depends uniquely on $\omega_{\mathcal{X}/\mathcal{O}_{\operatorname{Spec} E}}$ and not on the choice of a representative $\mathcal{K}$. We have the following important theorem:

Theorem 1.4.9 (Adjunction formula)**.** *Let $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ be an arithmetic surface, $s \in \operatorname{Spec} \mathcal{O}_E$ a closed point and $\mathcal{E} \in Z^1(\mathcal{X})$ a vertical divisor contained in the special fiber $\mathcal{X}_s$. Then we have*

$$2p_a(\mathcal{E}) - 2 = \mathcal{E}^2 + \mathcal{K} \cdot \mathcal{E}\,, \tag{1.4.1}$$

where $p_a(\mathcal{E})$ is the arithmetic genus of $\mathcal{E}$.

Proof: See [Li] Theorem 3.2. in case $\mathcal{K} \in Z^1(\mathcal{X})$. If $\mathcal{K} \in Z^1(\mathcal{X})_{\mathbb{Q}}$ then there exists a canonical divisor $\mathcal{K}' \in Z^1(\mathcal{X})$ with $\mathcal{K} - \mathcal{K}' = \frac{1}{s}\operatorname{div}(f)$ (cf. Remark 1.4.6), hence $\mathcal{K}$ fulfills (1.4.1). □

Definition 1.4.10. Let S be a Dedekind scheme of dimension 1. We say that $\mathcal{X}$ is a *fibered surface*, if $\mathcal{X}$ is an integral scheme of dimension 2 together with a projective flat morphism $f : \mathcal{X} \to S$. If $\mathcal{X}$ is normal we say that it is a *normal fibered surface*. For a closed point $s \in S$ let $\mathcal{X}_s := \mathcal{X} \times_S \operatorname{Spec} k(s)$. Furthermore, let $\mathcal{C}$ be an irreducible component of $\mathcal{X}_s$ and $\xi \in \mathcal{X}_s$ the generic point of $\mathcal{C}$. Then we define the *multiplicity of $\mathcal{C}$ in $\mathcal{X}_s$* to be the length of $\mathcal{O}_{\mathcal{X}_s,\xi}$ as $\mathcal{O}_{\mathcal{X}_s,\xi}$-module.

Proposition 1.4.11. *Let N be a squarefree natural number with $N \geq 2$ and $\mathcal{X}$ the Fermat scheme* (1.1.1) *of exponent N. Each fiber above a prime ideal of $\mathbb{Z}[\zeta_N]$ has just one component. If $\mathfrak{p} \subset \mathbb{Z}[\zeta_N]$ is a prime ideal with $N \in \mathfrak{p}$, then this component has multiplicity p, where $\mathfrak{p} \cap \mathbb{Z} = (p)$. Else, it has multiplicity one.*

Proof: If $\mathfrak{q}$ is a prime ideal of $\mathbb{Z}[\zeta_N]$ with $N \notin \mathfrak{q}$, then

$$\mathcal{X}_{\mathfrak{q}} = \operatorname{Spec} k(\mathfrak{q})[X,Y]/(X^N + Y^N - 1)\,,$$

where $(X^N + Y^N - 1)$ is irreducible in $k(\mathfrak{q})[X,Y]$ (Eisenstein criterion). It is obvious, that $\mathcal{X}_{\mathfrak{q}}$ has just one component, namely $\mathcal{C} = V(X^N + Y^N - 1)$. Let us set $R = k(\mathfrak{q})[X,Y]$ and $I = (X^N + Y^N - 1)$. Let ξ be the generic point of $\mathcal{X}_{\mathfrak{q}}$. Then we have

$$\mathcal{O}_{\mathcal{X}_{\mathfrak{q}},\xi} = (R/I)_{(0)} = R_I/IR_I\,.$$

It follows

$$\text{length}_{R_I/IR_I} R_I/IR_I = \text{length}_{R_I} R_I/IR_I = 1\,,$$

hence the multiplicity of $\mathcal{C}$ is one. If $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[\zeta_N]$ with $N \in \mathfrak{p}$, then

$$\mathcal{X}_{\mathfrak{p}} = \operatorname{Spec} k(\mathfrak{p})[X,Y]/(X^{N/p} + Y^{N/p} - 1)^p\,,$$

where $(X^{N/p} + Y^{N/p} - 1)$ is irreducible in $k(\mathfrak{p})[X,Y]$ and $\mathfrak{p} \cap \mathbb{Z} = (p)$. Similar to the previous case, we see, that $\mathcal{C} = V(X^{N/p} + Y^{N/p} - 1)$ is the only component of $\mathcal{X}_{\mathfrak{p}}$. We set $R = k(\mathfrak{p})[X,Y]$ and $I = (X^{N/p} + Y^{N/p} - 1)$. In this situation $\xi = (X^{N/p} + Y^{N/p} - 1)$ is the generic point of $\mathcal{X}_{\mathfrak{q}}$. Here we have

$$\mathcal{O}_{\mathcal{X}_{\mathfrak{q}},\xi} = (R/I^p)_I = R_I/I^p R_I = R_I/(IR_I)^p\,.$$

It follows

$$\text{length}_{R_I/(IR_I)^p} R_I/(IR_I)^p = \text{length}_{R_I} R_I/(IR_I)^p = p\,,$$

hence the multiplicity of $\mathcal{C}$ is p.

□

Definition 1.4.12. Let $\mathcal{X}$ be a normal scheme and $\mathcal{C}$ a prime divisor i.e. an irreducible subscheme of codimension 1. The ring $\mathcal{O}_{\mathcal{X},\xi}$, where ξ is the generic point of $\mathcal{C}$, is a discrete valuation ring. We denote the valuation by $\nu_{\mathcal{C}}$ and an uniformizing parameter by $t_{\mathcal{C}}$, i.e. an element $t_{\mathcal{C}} \in \mathcal{O}_{\mathcal{X},\xi}$ with $\nu_{\mathcal{C}}(t_{\mathcal{C}}) = 1$.

Remark 1.4.13. Let $\mathcal{X}$ be a normal fibered surface in the sence of Definition 1.4.10. Another way of computing the multiplicity of $\mathcal{C}$ in $\mathcal{X}_s$ is the following: Let ξ be the generic point of $\mathcal{C}$ *in* $\mathcal{X}$. Then the multiplicity of $\mathcal{C}$ is $\nu_{\mathcal{C}}(t_s)$ where t_s is a uniformizing parameter of $\mathcal{O}_{\operatorname{Spec}\mathcal{O}_E,s}$ (cf. [LL], p.63).

Remark 1.4.14. Let $f : \mathcal{X} \to \operatorname{Spec}\mathcal{O}_E$ and $s \in \operatorname{Spec}\mathcal{O}_E$ be as in Theorem 1.4.9. Let $\mathcal{C}_1, \ldots, \mathcal{C}_r$ be the irreducible components of $\mathcal{X}_s$, with respective multiplicities $d_1, \ldots, d_r$. Then we have the following equality of Weil divisors in $\mathcal{X}$:

$$\mathcal{X}_s = \sum_{1 \le i \le r} d_i \mathcal{C}_i\,,$$

where $\mathcal{X}_s = f^* s$ (see. [Liu], p.351: Lemma 3.9. (a)). Furthermore, since the generic fiber X_E is geometrically irreducible it is geometrically connected. Hence, $\mathcal{X}_s$ is geometrically connected (see e.g. [Liu], p.350: Corollary 3.6. (b).

Proposition 1.4.15. *Let $f : \mathcal{X} \to \operatorname{Spec}\mathcal{O}_E$ be an arithmetic surface, $s \in \operatorname{Spec}\mathcal{O}_E$ a closed point and $\mathcal{C}_1, \ldots, \mathcal{C}_r$ the irreducible components of $\mathcal{X}_s$, with respective multiplicities $d_1, \ldots, d_r$. Then the following properties are true:*

1. *For all $\mathcal{C}_i$ we have $\mathcal{X}_s \cdot \mathcal{C}_i = 0$.*

2. *For all $\mathcal{C}_i$ we have*
$$\mathcal{C}_i^2 = -\frac{1}{d_i}\sum_{j\neq i} d_j\mathcal{C}_j \cdot \mathcal{C}_i\,.$$

3. *Furthermore, let $\mathcal{K}$ be a canonical divisor of $\mathcal{X}$. We have $2p_a(X_E)-2 = \mathcal{K}\cdot\mathcal{X}_s$, where X_E is the generic fiber of $\mathcal{X}$.*

Proof: See [Liu], p.384: Proposition 1.21. and p.389: Proposition 1.35. Statement 3. is true for $\mathcal{K} \in Z^1(\mathcal{X})_{\mathbb{Q}}$ as well. This follows by the same arguments as in Theorem 1.4.9. $\square$

Later on it will be important to construct the canonical divisor explicitly. The following proposition will help us with that.

Proposition 1.4.16. *Let $f : \mathcal{X} \to \operatorname{Spec}\mathcal{O}_E$ be an arithmetic surface and $\mathcal{K} \in Z^1(\mathcal{X})_{\mathbb{Q}}$ a divisor on $\mathcal{X}$ which satisfies the adjunction formula* (1.4.1) *and whose restriction to the generic fiber X is a canonical divisor of X. Then $\mathcal{K}$ is a canonical divisor on $\mathcal{X}$.*

Proof: Let $\widetilde{\mathcal{K}}$ be a canonical divisor on $\mathcal{X}$ (we already know that it exists). We want to show that $\widetilde{\mathcal{K}} \sim \mathcal{K}$ and so that $\mathcal{K}$ is a canonical divisor as well. We denote the horizontal part of the divisors by $\widetilde{\mathcal{K}}_h$ and $\mathcal{K}_h$. Since the restriction to the generic fiber of both divisors is a canonical divisor of X we have $\widetilde{\mathcal{K}}|_X = \widetilde{\mathcal{K}}_h|_X \sim \mathcal{K}_h|_X = \mathcal{K}|_X$ and so there exists a rational element $g \in K(X)$ and a $s \in \mathbb{Z}$ with $\widetilde{\mathcal{K}}|_X - \frac{1}{s}\operatorname{div}(g) = \mathcal{K}|_X$. Because we have $K(X) \cong K(\mathcal{X})$, we can interpret g as an element of $K(\mathcal{X})$ and so obtain a principal divisor whose restriction to X is $\operatorname{div}(g)$. We denote this principal divisor by $\operatorname{div}(g)$ as well. If we now set $\mathcal{K}' := \mathcal{K} + \frac{1}{s}\operatorname{div}(g)$ we get a divisor with the properties $\mathcal{K}' \sim \mathcal{K}$ and $\mathcal{K}'_h = \widetilde{\mathcal{K}}_h$. Since we are just interested in $\mathcal{K}$ up to rational equivalence we may assume from now on that the horizontal part of $\mathcal{K}$ is the same as the one of $\widetilde{\mathcal{K}}$.
Let $s \in \operatorname{Spec}\mathcal{O}_E$ be a closed point with $s \in f(\operatorname{Supp}\widetilde{\mathcal{K}}_v \cup \operatorname{Supp}\mathcal{K}_v)$ and $\mathcal{X}_s$ the fiber above it; here $\widetilde{\mathcal{K}}_v$ ($\mathcal{K}_v$ resp.) denotes the vertical part of $\widetilde{\mathcal{K}}$ ($\mathcal{K}$ resp.). Let $\widetilde{\mathcal{K}}_s$ ($\mathcal{K}_s$ resp.) be the part of $\widetilde{\mathcal{K}}$ ($\mathcal{K}$ resp.) which has support in $\mathcal{X}_s$. Since $\widetilde{\mathcal{K}}$ and $\mathcal{K}$ fulfill the adjunction formula and have the same horizontal part we have
$$0 = (\widetilde{\mathcal{K}}_s - \mathcal{K}_s)\cdot(\widetilde{\mathcal{K}} - \mathcal{K}) = (\widetilde{\mathcal{K}}_s - \mathcal{K}_s)\cdot(\widetilde{\mathcal{K}}_s - \mathcal{K}_s)\,.$$
and so $\widetilde{\mathcal{K}}_s - \mathcal{K}_s = q\mathcal{X}_s$, where q is a rational number (see [La], p.61: Proposition 3.5.). Now, according to Lemma 1.3.16, we find $m \in \mathbb{Z}$ and $h \in K(\mathcal{X})$ so that $\widetilde{\mathcal{K}}_s - \mathcal{K}_s = q\mathcal{X}_s = \frac{q}{m}\operatorname{div}(h)$ and so we have $\widetilde{\mathcal{K}}_s = \mathcal{K}_s$ in $\operatorname{Cl}(\mathcal{X})_{\mathbb{Q}}$. If we set $\mathcal{K}' := \mathcal{K} + \frac{q}{m}\operatorname{div}(h)$ we have just changed the part of $\mathcal{K}$ with support in $\mathcal{X}_s$. Again, we have $\mathcal{K}' \sim \mathcal{K}$ and now $\widetilde{\mathcal{K}}_h + \widetilde{\mathcal{K}}_s = \mathcal{K}'_h + \mathcal{K}'_s$. Continuing successively with the other (finitely many) closed points of $f(\operatorname{Supp}\widetilde{\mathcal{K}}_v \cup \operatorname{Supp}\mathcal{K}_v)$ we arrive at a divisor $\mathcal{K}''$ with $\mathcal{K}'' = \widetilde{\mathcal{K}}$ and $\mathcal{K}'' \sim \mathcal{K}$ as we claimed at the beginning. $\square$

Remark 1.4.17. The Proposition 1.4.16 uses the fact that in $Z^1(\mathcal{X})_{\mathbb{Q}}$ the special fibers are divisors coming from functions (see Lemma 1.3.16). In other words, the canonical divisor in the sense of Remark 1.4.6 is only defined up to rational multiples of principal divisors and therefore in particular defined only up to special fibers (in $Z^1(\mathcal{X})_{\mathbb{Q}}$).

Chapter 2

Regular and minimal regular models of curves

Assumption 2.0.18. Unless otherwise specified, we denote by C a smooth projective geometrically irreducible curve over a number field E. Furthermore, we denote by $\mathcal{O}_E$ the ring of integers of E.

In this chapter we explain how we can construct a (minimal) regular model for C. Explicitly, we can use the results of the subsequent sections in the following way: Since C is projective there exists a natural number n and a closed embedding $C \hookrightarrow \mathbb{P}^n_E$. Let $\mathcal{X}$ be the normalization of the closure of C in $\mathbb{P}^n_{\mathcal{O}_E}$ with respect to the morphism

$$C \hookrightarrow \mathbb{P}^n_E \to \mathbb{P}^n_{\mathcal{O}_E}\,.$$

Then $\mathcal{X}$ is a normal scheme over $\operatorname{Spec}\mathcal{O}_E$ and its generic fiber is E-isomorphic to C. Now, in Section 2.1 we describe how we can desingularize $\mathcal{X}$. Then, in Section 2.2 we show that we can construct a minimal regular model out of the regular model we obtained in the previous section in case the genus of the curve is greater than 0. Finally, in Section 2.3 we demonstrate that all this work can be done fiber by fiber.

2.1 Resolution of singularities for surfaces

Let C be as in Assumption 2.0.18. Regarding the nice properties of arithmetic surfaces it is desirable to find a regular model of this curve. We have seen before that it is easy to construct a normal fibered surface over $\operatorname{Spec}\mathcal{O}_E$ that has a generic fiber isomorphic to C. Next, we could ask ourselves if we can use this normal fibered surface as a starting point of a construction that yields us a regular model of this curve. Lipman gave in [Lip1],[Lip2] a positive answer to this question[1]. In this section we will review shortly the basic ideas of his proof. We follow the presentation given by Artin in [Ar1].

[1]In fact, the idea of his proof can be applied to arbitrary excellent two-dimensional schemes.

Definition 2.1.1. Let $\mathcal{X}$ be a normal fibered surface. We call a proper birational morphism $f : \mathcal{X}' \to \mathcal{X}$ with $\mathcal{X}'$ regular a *desingularization* (or a *resolution of singularities*) of $\mathcal{X}$.

Remark 2.1.2. The scheme $\mathcal{X}$ is excellent (see e.g. [Liu], p.343: Theorem 2.39. (c) and Corollary 2.40. (c)). This, together with the fact that $\mathcal{X}$ is normal, yield that the *singular locus* $\mathrm{Sing}(\mathcal{X})$, i.e. the set of points $x \in \mathcal{X}$ at which $\mathcal{X}$ is singular, is a closed subset of codimension 2 (see [Gr1], (7.8.6) (iii)).

Theorem 2.1.3. *Let $\mathcal{X}$ be a normal fibered surface. We construct a sequence of surfaces and proper birational morphisms*

$$\ldots \to \mathcal{X}_{n+1} \to \mathcal{X}_n \to \ldots \to \mathcal{X}_1 \to \mathcal{X}_0 = \mathcal{X}\,, \tag{2.1.1}$$

where $\mathcal{X}_{i+1}$ is the normalization of the blowing-up of $\mathcal{X}_i$ along $\mathrm{Sing}(\mathcal{X}_i)$. *Then the sequence* (2.1.1) *is finite, hence a desingularization of $\mathcal{X}$ exists.*

Proof: See [Lip1],[Lip2] of alternatively [Ar1]. □

Remark 2.1.4. The proof of the Theorem 2.1.3 (as it is described in [Ar1]) can be done in three steps: In the first it is shown that we can reduce everything to the situation that $\mathcal{X}$ just has rational singularities. A point $x \in \mathcal{X}$ is called a *rational singularity*, if for every proper birational morphism $f : \mathcal{X}' \to \mathcal{X}$ the stalk $R^1 f_* \mathcal{O}_{\mathcal{X}'}$ at x is zero[2]: here $R^1 f_*$ denotes the first right derived functor of f_* and $\mathcal{O}_{\mathcal{X}'}$ the structure sheaf of $\mathcal{X}'$. In the second step it is shown that everything can be reduced to the situation of a surface with rational singularities of multiplicity 2, so called *rational double points*. The multiplicity of a rational singularity x is defined as the multiplicity of the local ring $\mathcal{O}_{\mathcal{X},x}$ (cf. [ZS], p. 294). The third step deals with the desingularization of these singularities.

2.2 The minimal regular model

Again, let C be as in Assumption 2.0.18. Furthermore, let us set $S = \operatorname{Spec} \mathcal{O}_E$. We have seen in Section 2.1 that there exists a regular model $\mathcal{X} \to S$ of C, i.e. $\mathcal{X}$ is an arithmetic surface over S and its generic fiber X_E is isomorphic to C. For another arithmetic surface $\mathcal{X}'$ which is S-birational equivalent to $\mathcal{X}$ its generic fiber is isomorphic to C as well, hence it is a regular model too. In this section we discuss under which conditions there exists a minimal regular model in a birational equivalence class. Before we do this we must define what we mean by a minimal regular model. First of all we make the following observation: If we have a (S-) birational morphism $f : \mathcal{X} \to \mathcal{X}'$ of regular models, then f is surjective

[2] Normally one defines a rational singularity x as a point $x \in \mathcal{X}$ where for each desingularization $f : V' \to \operatorname{Spec} \mathcal{O}_{\mathcal{X},x}$ we have $R^1 f_* \mathcal{O}_{V'} = 0$ (cf. [La], p. 125). However, since this definition needs the existence of a desingularization Lipman uses the term *pseudo-rational singularity* in his proof. Once it is shown that the desingularization exists it turns out that every rational sigularity is a pseudo-rational singularity and vice versa (cf. [Lip2], p. 157: Remark).

(it is closed, since it is proper, and it is dominant, since it is a birational map of integral schemes). Hence, it would make sense to postulate, that, if there exists a minimal regular model, then any birational morphism to any other regular model should be an isomorphism. On the other hand, a minimal regular model should be unique. However, there could be several non-isomorphic models that have the above property, hence we have to postulate a little bit more.

Definition 2.2.1. We call a regular model $\mathcal{X}$ of the curve C a *relatively minimal model* if every S-birational morphism $f : \mathcal{X} \to \mathcal{X}'$ to another regular model $\mathcal{X}'$ is necessarily an isomorphism. If all relatively minimal models in the birational equivalence class of $\mathcal{X}$ are isomorphic, we say that $\mathcal{X}$ is a *minimal (regular) model* of C.

Now, we want to analyze S-birational morphisms of regular models in more detail. It turns out, that a specific kind of blowing-up-morphisms play an important role in the study of these morphisms:

Definition 2.2.2. Let $\mathcal{X}$ be an arithmetic surface. We call the blowing-up $\pi : \widetilde{\mathcal{X}} \to \mathcal{X}$ of $\mathcal{X}$ along a closed point x a *monoidal transformation*.

As a blowing-up a monoidal transformation is a birational morphism. It induces an isomorphism $\widetilde{\mathcal{X}} \setminus \pi^{-1}(x) \cong \mathcal{X} \setminus \{x\}$ (Proposition 1.2.9 (3.)), and the preimage of x is isomorphic to $\mathbb{P}^1_{k(x)}$ (see e.g. [Liu], p.325: Theorem 1.19. (b)). Now, the Factorization Theorem states that we can express any birational morphism of regular models in terms of monoidal transformations:

Theorem 2.2.3 (Factorization Theorem)**.** *Let $f : \mathcal{X} \to \mathcal{X}'$ be a S-birational morphism of regular models. Then $\mathcal{X}$ is isomorphic to a scheme obtained from $\mathcal{X}'$ by a finite number of successive monoidal transformations.*

Proof: See e.g. [Chi], p.311: Theorem 2.1 or [Li], p.392: Theorem 1.15. resp. $\square$

Definition 2.2.4. Let $\mathcal{X}$ be a regular model. A prime divisor $\mathcal{E}$ on $\mathcal{X}$ is called an *exceptional divisor* if there exists a regular model $\mathcal{X}'$ and a S-birational morphism $f : \mathcal{X} \to \mathcal{X}'$ such that $f(\mathcal{E})$ is reduced to a point, and that $f : \mathcal{X} \setminus \mathcal{E} \to \mathcal{X}' \setminus f(\mathcal{E})$ is an isomorphism.

Given a regular model $\mathcal{X}$ of C the Factorization Theorem tells us that $\mathcal{X}$ is a relatively minimal model if and only if it does not contain any exceptional divisors. It is obvious now that it is very useful to identify the exceptional divisors of the given model. Even if our model $\mathcal{X}$ is not relatively minimal, the knowledge of the exceptional divisors describes to us the appearance of a relatively minimal model that is in the same birational equivalence class. Another famous theorem helps us to identify the exceptional divisors.

Theorem 2.2.5 (Castelnuovo's criterion)**.** *Let $\mathcal{X} \to S$ be a regular model of C. Let $\mathcal{E} \subset \mathcal{X}$ be a vertical prime divisor in the fiber above $s \in S$, and $k' = H^0(\mathcal{E}, \mathcal{O}_{\mathcal{E}})$. Then $\mathcal{E}$ is an exceptional divisor if and only if $\mathcal{E} \cong \mathbb{P}^1_{k'}$ and $\mathcal{E}^2 = -|k' : k(s)|$.*

Proof: See e.g. [Chi], p.315: Theorem 3.1 or [Li], p.399: Theorem 3.9. resp. □

Now we are ready to prove that there exists a relatively minimal model.

Lemma 2.2.6. *Let $\mathcal{X} \to S$ be a regular model of C. Then there exists a relatively minimal model $\mathcal{X}^{rel}$ and a S-birational morphism $f : \mathcal{X} \to \mathcal{X}^{rel}$.*

Proof: This proof is a composition of proofs in [Ar1] and [Liu]. Since an irreducible fiber has self-intersection 0 (Proposition 1.4.15 (1.)), the exceptional divisors lie in reducible fibers. The set of points $s \in S$ where the fiber of $\mathcal{X}$ over s is irreducible is a dense open subset of S because the generic fiber is geometrically irreducible (see e.g. [Gr2], Proposition (9.7.8)). Since $\mathcal{O}_E$ is a Dedekind ring, every closed set of S is finite, hence there are only finitely many reducible fibers. Let us denote by $\delta(\mathcal{X})$ the number of irreducible components which lie in reducible fibers of $\mathcal{X}$. According to our previous observations $\delta(\mathcal{X})$ is finite. If we now blow down an exceptional divisor $\mathcal{E}$ of $\mathcal{X}$, the resulting model $\mathcal{X}'$ will have less irreducible components that lie in reducible fiber, hence $\delta(\mathcal{X}') < \delta(\mathcal{X})$. We continue this process of blowing down exceptional divisors and obtain a chain $\mathcal{X} \to \mathcal{X}' \to \mathcal{X}'' \to \mathcal{X}''' \to \ldots$ of regular models. We have $\delta(\mathcal{X}) < \delta(\mathcal{X}') < \delta(\mathcal{X}'') < \delta(\mathcal{X}''') < \ldots$, and since $\delta(\mathcal{X})$ was finite the chain of regular models must stop after finitely many steps with a regular model $\mathcal{X}^{rel}$ that has not exceptional divisors. According to the Factorization Theorem this must be a relatively minimal model. □

Theorem 2.2.7 (Minimal Models Theorem)**.** *Let E be a number field, $\mathcal{O}_E$ its ring of integers, and $S = \operatorname{Spec} \mathcal{O}_E$. Furthermore, let C be a smooth projective geometrically irreducible curve over E with $g(C) \geq 1$ and $\mathcal{X} \to S$ a regular model of C. Then there exists a minimal regular model $\mathcal{X}^{min}$ and a S-birational morphism $f : \mathcal{X} \to \mathcal{X}^{min}$.*

Proof: See e.g. [Chi], p.313 or [Liu], p.422: Theorem 3.21. □

Remark 2.2.8. In the Minimal Model Theorem the property that $g(C) \geq 1$ is used to show that any two different exceptional divisors of $\mathcal{X}$ are disjoint (cf. [Chi], p.324: Lemma 7.2). This and the Minimal Model Theorem itself is false without the $g(C) \geq 1$ hypothesis (see [Liu], p.422: Remark 3.23.)

Corollary 2.2.9. *If in the situation of Theorem 2.2.7 the scheme $\mathcal{X}$ does not contain any exceptional divisor, then it is a minimal regular model of C.*

Proof: Since $\mathcal{X}$ does not have any exceptional divisor it is a relative minimal model. According to Theorem 2.2.7 this is already a minimal regular model. □

2.3 Descent

In this section we sketch some aspects of descent theory which will be useful in our context. For more background material and details the reader may take a look at [BLR], [Mur][Mi] and [FGI$^+$]. The application of the theory we have in mind is the glueing of schemes. Especially the situation of glueing schemes along subsets which are not open with respect to the Zariski-topology will be of interest. At this point the author would like to thank professor Stefan Wewers for the useful discussions regarding the content of this section.

We consider the following problem: given a morphism of schemes $p : S' \to S$ and a S'-scheme X'. Under which conditions does X' "descent" to a S-scheme X i.e. is of the form $X' = p^*X = X \times_S S'$? It turns out that there are a few necessary conditions that have to be fulfilled. Let $S'' = S' \times_S S'$ and $S''' = S' \times_S S' \times_S S'$. Furthermore let p_1 and p_2 be the first and second projection of S'' onto S' and $p_{i,j}$ the projections $p_{i,j} : S''' \to S''$ onto the factor with indices i and j for $i, j \in \{1, 2, 3\}$ with $i < j$. A *covering datum* of X' is a S''-isomorphism $\varphi : p_1^*X' \to p_2^*X'$. We say that this covering datum is a *descent datum* if the *cocycle condition*

$$p_{1,3}^* \varphi = p_{2,3}^* \varphi \circ p_{1,2}^* \varphi$$

is fulfilled. Given a S-scheme X it can be easily verified that we get a canonical decent datum $\psi : p_1^*X_{S'} \to p_2^*X_{S'}$ on the scheme $X_{S'} := X \times_S S'$. Now, a decent datum φ for X' is called *effective* if it is isomorphic to such a canonical one i.e. there exist a S-scheme X and an isomorphism $f : X' \to X_{S'}$, so that the diagram

$$\begin{tikzcd} p_1^*X' \arrow[r, "\varphi"] \arrow[d, "p_1^*f"'] & p_2^*X' \arrow[d, "p_2^*f"] \\ p_1^*X_{S'} \arrow[r, "\psi"] & p_2^*X_{S'} \end{tikzcd}$$

is commutative. In order to solve the problem from the beginning it seems to be obvious that we have to find a descent datum and a criterion that helps us to decide whether this descent datum is effective. Before we explain how one can do this we will take a look at our setting from a different viewpoint.

Since we are working with objects which are (at least locally) affine, we want to explain what the formalism above means if we interpret it in the language of rings and modules[3]. So, let $p : R \to R'$ be a morphism of rings and M' an R'-module. A covering datum for M' corresponds to a $R' \otimes_R R'$-isomorphism

$$\varphi : M' \otimes_R R' \to R' \otimes_R M' .$$

[3]In fact, since we have the glueing of schemes in mind it would be sufficient to work just with rings. However, descent theory can be used to glue quasi-coherent modules as well and therefore we consider the more general (but not much more difficult) situation with modules.

This covering datum fulfills the cocycle condition if the $R' \otimes_R R' \otimes_R R'$-isomorphisms

$$\begin{aligned}\varphi_1 &: R' \otimes_R M' \otimes_R R' \to R' \otimes_R R' \otimes_R M' ,\\ \varphi_2 &: M' \otimes_R R' \otimes_R R' \to R' \otimes_R R' \otimes_R M' ,\\ \varphi_3 &: M' \otimes_R R' \otimes_R R' \to R' \otimes_R M' \otimes_R R' ,\end{aligned}$$

fulfill $\varphi_2 = \varphi_1\varphi_3$; here φ_1,φ_2 and φ_3 are obtained by tensoring φ with $\mathrm{id}_{R'}$ in the first, second and third position. In this situation φ is a descent datum, and it is effective if there exists a R-module M and an isomorphism $f : M' \to M \otimes_R R'$ so that the diagram

$$\begin{tikzcd} M' \otimes_R R' \arrow[r, "\varphi"] \arrow[d, "f\otimes \mathrm{id}_{R'}"'] & R' \otimes_R M' \arrow[d, "\mathrm{id}_{R'}\otimes f"] \\ (M \otimes_R R') \otimes_R R' \arrow[r, "\psi"] & R' \otimes_R (M \otimes_R R') \end{tikzcd}$$

commutes; here the $R' \otimes_R R'$-isomorphism ψ is given by $(m \otimes r) \otimes r' \mapsto r \otimes (m \otimes r')$. In this situation one can show the following result.

Proposition 2.3.1. *Let $p : R \to R'$ be a faithfully flat ring-homomorphism, M' a R'-module and φ a descent datum for M'. Then φ is an effective descent datum.*

Proof: See [Mur], p.124: Proposition 7.1.1. □

Let us return now to the situation of the beginning of the S'-scheme X' and the morphism $p : S' \to S$. To postulate that p is faithfully flat and that the base-schemes are affine is not enough in order to obtain a similar result to the proposition above (cf. [BLR], Section 6.7.). Hence, in this situation a descent datum φ for X' is not necessarily an effective descent datum. However, if X' can be covered by affine open subschemes U' which are stable under φ (an open subscheme U' is *stable under* φ if φ restricts to an isomorphism $p_1^*U' \to p_2^*U'$) we have the following.

Theorem 2.3.2. *Let $p : S' \to S$ be a faithfully flat and quasi-compact morphism of affine schemes. A descent datum φ on an S'-scheme X' is effective if and only if X' can be covered by affine open subschemes which are stable under φ.*

Proof: See [BLR] p.135-136: Theorem 6. (b). □

We consider the situation described in Assumption 2.0.18. We explain now how we can use the descent theory in order to glue schemes. In fact we are especially interested in the situation which is relevant for the construction of regular models of C over $\mathcal{O}_E$. For this reason, let us assume we have constructed regular models over a finite number of localizations of $\mathcal{O}_E$ with respect to prime ideals. Furthermore we assume that we have constructed a regular model over the open subset which is given by the complement of the finite set of prime ideals. We want to glue these models to a regular model over $\mathcal{O}_E$. In order to use Theorem 2.3.2 we need to explain how our situation fits into the setting of the theorem. It seems to be clear that S will be the spectrum of the ring of integers of E. Next, we need to discover the role of its localizations and the open subset.

Remark 2.3.3. Let E be a number field and $R = \mathcal{O}_E$ its ring of integers. For an element $f \in R$ we let $R_0 = \mathcal{O}_E[f^{-1}]$ be the localization of R with respect to the set $\{1, f, f^2, \ldots\}$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of R with $f \in \mathfrak{p}_i$. We denote by R_i the localization of R with respect to the prime ideal $\mathfrak{p}_i$ for $1 \leq i \leq s$. Then the ring

$$R' = R_0 \times \ldots \times R_s$$

is faithfully flat over the ring R with respect to the obvious morphism $a \mapsto (a, \ldots, a)$. In fact the affine scheme $S' = \operatorname{Spec} R'$ is the disjoint union of the schemes $S_i = \operatorname{Spec} R_i$, and the scheme-morphism $p : S' \to S = \operatorname{Spec} R$ is faithfully flat and quasi-compact.

Theorem 2.3.4. *In the situation of Remark 2.3.3 let C be a $\operatorname{Spec} E$-scheme and for each i let $\mathcal{Y}_i = \operatorname{Spec} A_i$ be an affine S_i-scheme, where $\mathcal{Y}_i \times_{S_i} \operatorname{Spec} E$ is $\operatorname{Spec} E$-isomorphic to C. Then there exists a S-scheme $\mathcal{Y}$ with $\mathcal{Y} \times_S S_i \cong \mathcal{Y}_i$ for $0 \leq i \leq s$.*

Proof: Let $\mathcal{Y}' = \coprod_{i=0}^{s} \mathcal{Y}_i$ be the disjoint union of the $\mathcal{Y}_i$, hence $\mathcal{Y}' = \operatorname{Spec}(A_0 \times \ldots \times A_s)$. Since $\mathcal{Y}'$ is affine and the morphism $p : S' \to S$ is faithfully flat and quasi-compact (Remark 2.3.3) a descent datum φ for $\mathcal{Y}'$ is effective (Theorem 2.3.2). We will construct this descent datum. By assumption the rings $A_i \otimes_{R_i} E$ are pairwise E-isomorphic to each other. Let us denote by $\phi_{i,i+1}$ the isomorphism from $A_i \otimes_{R_i} E$ to $A_{i+1} \otimes_{R_{i+1}} E$ for $0 \leq i \leq s-1$ and by $\phi_{i,i}$ the identity morphism of the corresponding ring $A_i \otimes_{R_i} E$ for $0 \leq i \leq s$. Then we define for arbitrary $i \neq j$ with $|i - j| > 1$ morphisms $\phi_{i,j} = \phi_{j-1,j} \circ \phi_{j-2,j-1} \circ \ldots \circ \phi_{i,i+1}$ if $i < j$ and $\phi_{i,j} = (\phi_{i-1,i} \circ \phi_{i-2,i-1} \circ \ldots \circ \phi_{j,j+1})^{-1}$ if $i > j$. Hence, we have defined E-isomorphisms

$$\phi_{i,j} : A_i \otimes_{R_i} E \to A_j \otimes_{R_j} E$$

for all $0 \leq i, j \leq s$ with

$$\phi_{j,k} \circ \phi_{i,j} = \phi_{i,k} \,. \tag{2.3.1}$$

Next, we are going to construct a covering datum. Such a covering datum corresponds to a family of $R_i \otimes_R R_j$-isomorphisms

$$\varphi_{i,j} : A_i \otimes_R R_j \to R_i \otimes_R A_j \,.$$

If $i = j$ we can define $\varphi_{i,i}$ by $a \otimes r \mapsto r \otimes a$. More interesting is the case $i \neq j$. Before we define these isomorphisms we need to make more preparative work. We define ring homomorphisms

$$\iota_{i,j} : R_i \otimes_R R_j \to E$$

by $r_i \otimes r_j \mapsto r_i \cdot r_j$. Notice, for $i \neq j$ this homomorphism is actually an isomorphism. Furthermore we define E-isomorphisms $\widetilde{\phi}_{i,j} := t_j \circ \phi_{i,j}$, where

$$t_j : A_j \otimes_{R_j} E \to E \otimes_{R_j} A_j$$

is given by $a \otimes l \mapsto l \otimes a$. Now, for $i \neq j$ we obtain an $R_i \otimes_R R_j$-isomorphism from $A_i \otimes_{R_i} (R_i \otimes_R R_j)$ to $(R_i \otimes_R R_j) \otimes_{R_j} A_j$ by the composition

$$(\iota_{i,j}^{-1} \otimes \mathrm{id}_{A_j}) \circ \widetilde{\phi}_{i,j} \circ (\mathrm{id}_{A_i} \otimes \iota_{i,j}) \,. \tag{2.3.2}$$

Since $A_i \otimes_{R_i} (R_i \otimes_R R_j)$ is $R_i \otimes_R R_j$-isomorphic to $A_i \otimes_R R_j$ and $(R_i \otimes_R R_j) \otimes_{R_j} A_j$ is $R_i \otimes_R R_j$-isomorphic to $R_i \otimes_R A_j$ we obtain the remaining $\varphi_{i,j}$ by composing the morphism (2.3.2) with these isomorphisms, and therefore obtain a covering datum. In order to show that this covering datum is a descent datum we have to prove that it fulfills the cocycle condition. To be more precise, we have to show that for any i, j, k the morphism

$$\Phi^{(1)}_{i,j,k} \circ \Phi^{(3)}_{i,j,k} : A_i \otimes_R R_j \otimes_R R_k \to R_i \otimes_R R_j \otimes_R A_k$$

coincides with the morphism $\Phi^{(2)}_{i,j,k}$, where $\Phi^{(1)}_{i,j,k} = (\mathrm{id}_{R_i} \otimes \varphi_{j,k})$, $\Phi^{(3)}_{i,j,k} = (\varphi_{i,j} \otimes \mathrm{id}_{R_k})$ and $\Phi^{(2)}_{i,j,k}$ is obtained by tensoring $\varphi_{i,k}$ with id_{R_j} in the second position. Let us show the equality

$$\Phi^{(2)}_{i,j,k} = \Phi^{(1)}_{i,j,k} \circ \Phi^{(3)}_{i,j,k} \tag{2.3.3}$$

for pairwise different i, j, k. Since $\Phi^{(l)}_{i,j,k}$ $(l = \{1, 2, 3\})$ is a $R_i \otimes_R R_j \otimes_R R_k$-isomorphism it is enough to show the equality for

$$a_i \otimes 1 \otimes 1 \in A_i \otimes_R R_j \otimes_R R_k\,,$$

where $a_i \in A_i$ is an arbitrary element. Now, let $\phi_{i,j}(a_i \otimes 1) = a_j \otimes b$ and $\phi_{j,k}(a_j \otimes 1) = a_k \otimes c$, hence $\phi_{i,k}(a_i \otimes 1) = a_k \otimes bc$ according to (2.3.1). Furthermore let $\iota^{-1}_{i,j}(b) = r_i \otimes r_j$, $\iota^{-1}_{j,k}(c) = r'_j \otimes r'_k$, $\iota^{-1}_{i,k}(b) = r''_i \otimes r''_k$ and $\iota^{-1}_{i,k}(c) = r'''_i \otimes r'''_k$. Then we have

$$\Phi^{(3)}_{i,j,k}(a_i \otimes 1 \otimes 1) = r_i \otimes r_j a_j \otimes 1$$

and

$$\Phi^{(1)}_{i,j,k}(1 \otimes a_j \otimes 1) = 1 \otimes r'_j \otimes r'_k a_k\,,$$

hence

$$\Phi^{(1)}_{i,j,k} \circ \Phi^{(3)}_{i,j,k}(a_i \otimes 1 \otimes 1) = r_i \otimes r_j r'_j \otimes r'_k a_k\,.$$

On the other hand

$$\Phi^{(2)}_{i,j,k}(a_i \otimes 1 \otimes 1) = r''_i r'''_i \otimes 1 \otimes r''_k r'''_k a_k\,.$$

Now, since $r_i \cdot r_j = r''_i \cdot r''_k$ and $r'_j \cdot r'_k = r'''_i \cdot r'''_k$ we have $r_i \otimes r_j r'_j \otimes r'_k = r''_i r'''_i \otimes 1 \otimes r''_k r'''_k$ and therefore the equality (2.3.3). The remaining cases follow similar (but even easier). One has just to remember the basic properties of the tensor as for example $r_i \otimes a_i = 1 \otimes r_i a_i$ for an element $r_i \otimes a_i \in R_i \otimes_R A_i$ and the basic properties of the morphisms involved as for example $\phi^{-1}_{i,j} = \phi_{j,i}$. We leave the remaining verifications to the reader. □

Corollary 2.3.5. *In the situation of Remark 2.3.3 let C be a curve which is defined over the number field E and for each i let $\mathcal{X}_i$ be a regular model of C over the scheme $S_i = \operatorname{Spec} R_i$. Then there exists a regular model $\mathcal{X}$ over R with $\mathcal{X} \times_S S_i \cong \mathcal{X}_i$ for $0 \leq i \leq s$.*

Sketch of the proof: It is enough to show that there exist affine open coverings

$$\bigcup_{j=1}^{n} C_j = C\,, \tag{2.3.4}$$

and for each $\mathcal{X}_i$

$$\bigcup_{j=1}^{n} U_{i,j} = \mathcal{X}_i \tag{2.3.5}$$

so that $U_{i,j}$ restricts to C_j on the generic fiber i.e. $U_{i,j} \times_{S_i} \operatorname{Spec} E \cong C_j$. Indeed, if we have such coverings then we can follow the proof of Theorem 2.3.4 and construct for each j an effective descent datum φ_j of

$$U'_j := \coprod_{i=0}^{s} U_{i,j}\,.$$

This descent data give us a descent datum φ for

$$\mathcal{X}' := \coprod_{i=0}^{s} \mathcal{X}_i\,,$$

and moreover the U'_j form an affine open cover of $\mathcal{X}'$ which is stable under φ. Therefore 2.3.2 will yield the claim.

Let us construct the C_j and the $U_{i,j}$. We choose for each $\mathcal{X}_i$ a finite affine open covering

$$\bigcup_{k=1}^{m_i} U_i^{(k)} = \mathcal{X}_i\,. \tag{2.3.6}$$

This covering induces by restriction an affine open covering $\cup_{k=1}^{m_i} C_i^{(k)}$ of C. Now we set

$$C_j := C_0^{(j)} \text{ for } 1 \leq j \leq m_0\,,$$

$$C_{m_0+j} := C_1^{(j)} \text{ for } 1 \leq j \leq m_1\,,$$

$$C_{m_0+m_1+j} := C_2^{(j)} \text{ for } 1 \leq j \leq m_2\,,$$

etc.

In this way we obtain $n = m_0 + \ldots + m_s$ affine open subsets $C_1, \ldots, C_n$. Obviously $\cup_{j=1}^{n} C_j = C$, hence (2.3.4) is fulfilled. Next, we want to define the $U_{i,j}$. Let $\mathcal{X}_i$ be one of the arithmetic surfaces and C_j one of the affine open subsets in the covering of C. If j is of the form

$$j = m_0 + \ldots + m_{i-1} + k \tag{2.3.7}$$

with $1 \leq k \leq m_i$ (in case $i = 0$ equation (2.3.7) has to be replaced by $j = k$) then we just set $U_{i,j} := U_i^{(k)}$, where $U_i^{(k)}$ is the affine open subset in the covering (2.3.6). If this is not the case, it is not automatically clear that there exists an affine open subset of $\mathcal{X}_i$ whose restriction equals C_j. We know that C_j is just the curve C after removing finitely many points $P_1, \dots, P_l$. Let $\mathcal{P}_1, \dots, \mathcal{P}_l$ be the Zariski-closure of $P_1, \dots, P_l$ in $\mathcal{X}_i$. If we remove $\mathcal{P}_1, \dots, \mathcal{P}_l$ from $\mathcal{X}_i$ the resulting scheme will be open. Unfortunately it will not be affine in general. However, one can show that if we remove in addition the (finitely many) vertical components of $\mathcal{X}_i$ which do not intersect any of the $\mathcal{P}_1, \dots, \mathcal{P}_l$ then we obtain a scheme $U_j \subset \mathcal{X}_i$ which is affine and whose restriction to C will be C_j. In this case we set $U_{i,j} := U_j$. Obviously the $U_{i,j}$ chosen in this way fulfill (2.3.5) since each $U_i^{(k)}$ in (2.3.6) is one of the $U_{i,j}$. Finally, because of the construction we have $U_{i,j} \times_{S_i} \operatorname{Spec} E \cong C_j$. $\square$

Chapter 3

Arakelov Intersection Theory

In Section 1.3 we have introduced a local intersection theory for arithmetic surfaces. Unfortunately, the theory does not extend to a global intersection theory which is well defined for divisor classes. To see this, let us consider for example an arithmetic surface $\mathcal{X}$ over $\operatorname{Spec}\mathbb{Z}$. Then every special fiber is a principal divisor but the intersection of a horizontal prime divisor with the fiber is strictly positive (see [Liu], p.388: Proposition 1.30.). The problem is that the scheme $\mathcal{X}$ is not "complete". This means that it is possible to move an intersection point of two divisors "out to infinity" (where it then disappears) by choosing other divisors in the divisor classes[1]. Arakelov overcame this problem by adding some analytic data which "compactify" the base scheme and which "complete" the arithmetic surface.

3.1 Arithmetic intersection numbers for hermitian line bundles

Let E be a number field, $\mathcal{O}_E$ its ring of integers and $f : \mathcal{X} \to \operatorname{Spec}\mathcal{O}_E$ an arithmetic surface in the sense of Definition 1.3.1. We denote the complex valued points $\mathcal{X}(\mathbb{C})$ by $\mathcal{X}_\infty$; this is a compact, 1-dimensional, complex manifold, which may have several connected components. Actually we have the decomposition

$$\mathcal{X}_\infty = \coprod_{\sigma : E \hookrightarrow \mathbb{C}} \mathcal{X}_\sigma(\mathbb{C}),$$

where $\mathcal{X}_\sigma(\mathbb{C})$ denotes the set of complex valued points of the curve $\mathcal{X}_\sigma = \mathcal{X} \times_{\operatorname{Spec} E, \sigma} \operatorname{Spec}\mathbb{C}$ coming from the embedding $\sigma : E \hookrightarrow \mathbb{C}$.

[1] Let $\mathcal{X} = \operatorname{Proj} B$, with a graded ring $B = \oplus_{d \geq 0} B_d$. Furthermore let $\mathcal{D}_1 = V_+(\mathfrak{p}_1)$ and $\mathcal{D}_2 = V_+(\mathfrak{p}_2)$ be divisors, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are homogenous prime ideals of B. An intersection point P corresponds to a maximal ideal $\mathfrak{m}$ with $\mathfrak{p}_i \subset \mathfrak{m}$ $(i = 1, 2)$. It may be possible to find a divisor $\mathcal{D}_3 = V_+(\mathfrak{p}_3)$ which is linear equivalent to $\mathcal{D}_2$ and where the maximal ideal $\mathfrak{m}'$ with $\mathfrak{p}_i \subset \mathfrak{m}'$ $(i = 1, 3)$ fulfills $\oplus_{d>0} B_d \subset \mathfrak{m}'$. This means the intersection point has moved to infinity (cf. [Si], p.340: Example 7.1.).

Definition 3.1.1. A *hermitian line bundle* $\overline{\mathcal{L}} = (\mathcal{L}, h)$ is a line bundle $\mathcal{L}$ on $\mathcal{X}$ together with a smooth, hermitian metric h on the induced holomorphic line bundle $\mathcal{L}_\infty = \mathcal{L} \otimes_{\mathbb{Z}} \mathbb{C}$ on $\mathcal{X}_\infty$. We denote the norm associated with h by $||\cdot||$. Two hermitian line bundles $\overline{\mathcal{L}}$, $\overline{\mathcal{M}}$ on $\mathcal{X}$ are *isomorphic*, if

$$\overline{\mathcal{L}} \otimes \overline{\mathcal{M}}^{-1} \cong (\mathcal{O}_\mathcal{X}, |\cdot|)\,,$$

where $|\cdot|$ denotes the usual absolute value. The *arithmetic Picard group* $\widehat{\mathrm{Pic}}(\mathcal{X})$ is the group of isomorphy classes of hermitian line bundles $\overline{\mathcal{L}}$ on $\mathcal{X}$, the group structure being given by the tensor product (cf. e.g. [BG], p.58: 2.7.3.).

Definition 3.1.2. Let $\mathcal{L}$ be a line bundle on $\mathcal{X}$ that has a non-trivial global section l. By definition there exists an open covering $\bigcup U_i = \mathcal{X}$ and $\mathcal{O}_\mathcal{X}$-isomorphism

$$\varphi_i : \mathcal{L}|_{U_i} \to \mathcal{O}_\mathcal{X}|_{U_i}\,.$$

Furthermore, let $x \in \mathcal{X}$ and U_i an open subset with $x \in U_i$. We denote the image of $\varphi_i(l)$ in $\mathcal{O}_{\mathcal{X},x}$ (with respect to the map $\mathcal{O}_\mathcal{X}(U_i) \to \mathcal{O}_{\mathcal{X},x}$) by l_x and call it a *local equation of* l *in* x.

Remark 3.1.3. We use the notation from Definition 3.1.2. According to Remark 1.3.6 we can associate a divisor class to the line bundle $\mathcal{L}$. The property, that $\mathcal{L}$ has a non-trivial global section l is equivalent to the assertion that there exists an effective divisor in this class (see e.g. [Ue], p. 48: Lemma 7.43.). In fact, the system $\{(U_i, \varphi_i(l))_i\}$ defines such an effective Cartier divisor (Weil divisor). We denote this divisor by $\mathrm{div}(l)$. It follows, that a local equation l_x for l in x is nothing but a local equation of $\mathrm{div}(l)$ in x in the sense of Definition 1.3.8.

Definition 3.1.4. Let $\overline{\mathcal{L}}$, $\overline{\mathcal{M}}$ be two hermitian line bundles on $\mathcal{X}$ and l, m non-trivial, global sections, whose induced divisors $\mathrm{div}(l)$ and $\mathrm{div}(m)$ on $\mathcal{X}$ have no common components. Then we define the *intersection number at the finite places* $(l.m)_{\mathrm{fin}}$ of l and m by the formula

$$\begin{aligned}(l.m)_{\mathrm{fin}} &:= \sum_{x \in \mathcal{X}^{(2)}} \log \sharp\left(\mathcal{O}_{\mathcal{X},x}/(l_x, m_x)\right) = \sum_{x \in \mathcal{X}^{(2)}} i_x(\mathrm{div}(l), \mathrm{div}(m)) \log |k(x)| \\ &= \sum_{s \in \mathrm{Spec}\,\mathcal{O}_E} \left(\sum_{x \in \mathcal{X}_s^{(1)}} i_x(\mathrm{div}(l), \mathrm{div}(m))[k(x) : k(s)] \right) \log |k(s)|\,,\end{aligned}$$

where l_x and m_x are local equations of l and m at the point $x \in \mathcal{X}$; here $\mathcal{X}^{(2)}$ denotes the set of closed points of $\mathcal{X}$ ($\mathcal{X}_s^{(1)}$ denotes the set of closed points of $\mathcal{X}_s$ respectively). The sections l and m induce global sections on $\mathcal{L}_\infty$ and $\mathcal{M}_\infty$, which we denote by abuse of notation again by l and m. We assume that the associated divisors $\mathrm{div}(l)$ and $\mathrm{div}(m)$ on $\mathcal{X}_\infty$ have no points in common. Writing $\mathrm{div}(l) = \sum_\alpha p_\alpha P_\alpha$ with $p_\alpha \in \mathbb{Z}$ and $P_\alpha \in \mathcal{X}_\infty$, we set

$$(\log ||m||)[\mathrm{div}(l)] := \sum_\alpha p_\alpha \log ||m(P_\alpha)||\,, \tag{3.1.1}$$

where $||\cdot||$ is the norm which is associated to the metric of $\mathcal{M}_\infty$. The *intersection number at the infinite places* $(l.m)_\infty$ of l and m is now given by the formula

$$(l.m)_\infty := -(\log ||m||)[\mathrm{div}(l)] - \int_{\mathcal{X}_\infty} \log ||l|| \cdot c_1(\overline{\mathcal{M}}) , \tag{3.1.2}$$

where the first Chern form $c_1(\overline{\mathcal{M}}) \in H^{1,1}(\mathcal{X}_\infty, \mathbb{R})$ of $\overline{\mathcal{M}}$ is given, away from the divisor $\mathrm{div}(m)$ on $\mathcal{X}_\infty$, by

$$c_1(\overline{\mathcal{M}}) = \mathrm{dd^c}(-\log ||m(\cdot)||^2) ;$$

the integral in (3.1.2) has to be understood as integrating with respect to the extension of $c_1(\overline{\mathcal{M}})$ to all of $\mathcal{X}_\infty$. We define the *arithmetic intersection number* $\overline{\mathcal{L}}.\overline{\mathcal{M}}$ of $\overline{\mathcal{L}}$ and $\overline{\mathcal{M}}$ by

$$\overline{\mathcal{L}}.\overline{\mathcal{M}} := (l.m)_{\mathrm{fin}} + (l.m)_\infty . \tag{3.1.3}$$

For general $\overline{\mathcal{L}}$ and $\overline{\mathcal{M}}$ we can choose line bundles $\mathcal{L}_i$ and $\mathcal{M}_j$ $(i, j = 1, 2)$ for which non-trivial global sections exist, such that $\mathcal{L}_i$ has disjoint global sections with $\mathcal{M}_j$ for $i, j = 1, 2$ and

$$\mathcal{L} \cong \mathcal{L}_1 \otimes \mathcal{L}_2^{\otimes -1}, \mathcal{M} \cong \mathcal{M}_1 \otimes \mathcal{M}_2^{\otimes -1} . \tag{3.1.4}$$

We provide $\mathcal{L}_{i\infty}$ and $\mathcal{M}_{j\infty}$ with metrics in such a way that the by (3.1.4) induced equivalences are isometries. Then we define $\overline{\mathcal{L}}.\overline{\mathcal{M}}$ by linearity. The *arithmetic self-intersection number* of $\overline{\mathcal{L}}$ is given by $\overline{\mathcal{L}}.\overline{\mathcal{L}}$.

Theorem 3.1.5 (Arakelov, Deligne et al.)**.** *Formula* (3.1.3) *induces a bilinear, symmetric pairing*

$$\widehat{\mathrm{Pic}}(\mathcal{X}) \times \widehat{\mathrm{Pic}}(\mathcal{X}) \to \mathbb{R} .$$

Proof: See for example [So]. □

Remark 3.1.6. Theorem 3.1.5 is a generalisation, essentially due to Deligne, of the arithmetic intersection pairing, invented by Arakelov, where only hermitian line bundles, whose Chern forms are multiples of a fixed volume form, were considered.

Definition 3.1.7. We have $\mathcal{X}_\infty = \coprod_{\sigma: E \hookrightarrow \mathbb{C}} \mathcal{X}_\sigma(\mathbb{C})$. By abuse of notation we call a (1,1)-form ν on $\mathcal{X}_\infty$ such that $\nu = \prod_{\sigma: E \hookrightarrow \mathbb{C}} \nu_\sigma$, where each ν_σ is a volume form, i.e. a positive, normalized, real (1,1)-form, on $\mathcal{X}_\sigma(\mathbb{C})$, also a volume form on $\mathcal{X}_\infty$. A hermitian line bundel $\overline{\mathcal{L}}$ is called ν*-admissible*, if $c_1(\overline{\mathcal{L}}) = \deg(\mathcal{L})\nu$. If the genus of $\mathcal{X}$ is greater than one, then for each σ we have on $\mathcal{X}_\sigma(\mathbb{C})$ the *canonical volume form*

$$\nu^\sigma_{\mathrm{can}}(z) = \frac{i}{2g} \sum_j |f^\sigma_j|^2 \mathrm{d}z \wedge \mathrm{d}\overline{z},$$

where $f^\sigma_1(z)\mathrm{d}z, \ldots, f^\sigma_g(z)\mathrm{d}z$ is an orthonormal basis of $H^0(\mathcal{X}_\sigma(\mathbb{C}), \Omega^1)$ equipped with the natural scalar product. We write ν_{can} for the induced volume form on $\mathcal{X}_\infty$.

Definition 3.1.8. Let $\mathcal{D}$ be an effective divisor on $\mathcal{X}$. Furthermore let $\mathcal{O}(\mathcal{D})$ be the associated invertible line bundle (Remark 1.3.6). We can endow $\mathcal{O}(\mathcal{D})_\infty$ with the unique ν_{can}-admissible metric $||\cdot||$ such that

$$\int_{\mathcal{X}_\infty} \log ||1_{\mathcal{D}}||\nu_{\mathrm{can}} = 0$$

where $1_{\mathcal{D}}$ is the canonical section of $\mathcal{O}(\mathcal{D})_\infty$. We denote by $\overline{\mathcal{O}}(\mathcal{D})$ the line bundle $\mathcal{O}(\mathcal{D})$ together with this metric.

Remark 3.1.9. Due to Arakelov is the observation that there is a unique metric $\|\cdot\|_{\mathrm{Ar}}$ on $\omega_{\mathcal{X}}$ (cf. Definition 1.4.4) such that for all sections $\mathcal{P}$ of $f : \mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ (i.e. $\mathcal{P}$ comes from an E-rational point of the geometric fiber) it holds the adjunction formula

$$\overline{\omega}_{\mathcal{X},\mathrm{Ar}}.\overline{\mathcal{O}}(\mathcal{P}) + \overline{\mathcal{O}}(\mathcal{P})^2 = \log |\Delta_{E|\mathbb{Q}}|, \tag{3.1.5}$$

where $\overline{\omega}_{\mathcal{X},\mathrm{Ar}} = (\omega_{\mathcal{X}}, \|\cdot\|_{\mathrm{Ar}})$. Moreover $\overline{\omega}_{\mathcal{X},\mathrm{Ar}}$ is a ν_{can}-admissible line bundle (see [La] or [Ara], § 4.).

Remark 3.1.10. In Remark 1.4.17 we saw that a canonical divisor is in particular only defined up to rational multiples of the special fibers. Because of formula (3.1.5) this indeterminacy will be deleted by the norm of the section.

We may reformulate the intersection pairing of Theorem 3.1.5, which was defined for elements of the arithmetic Picard group, as an intersection pairing of elements of the so called arithmetic Chow group of codimension 1. This is useful because it enables us to switch between these both points of view and allows us to choose the one which is more adequate in the given situation. In order to explain this in more detail we start by defining Green's functions.

Definition 3.1.11. Let D be a divisor of $\mathcal{X}_\infty$. By a *Green's function* for D we mean a function

$$g : \mathcal{X}_\infty \setminus \operatorname{Supp}(D) \to \mathbb{R}$$

which satisfies the following condition: If D is represented by a rational function f on an open set U, then there exists a smooth function α on U such that for $P \notin \operatorname{Supp}(D)$,

$$g(P) = -\log |f(P)|^2 + \alpha(P)\,.$$

Now, let $\mathcal{D}$ be a divisor on $\mathcal{X}$. By a *Green's function* for $\mathcal{D}$ we mean a Greens's function for $\mathcal{D}|_{\mathcal{X}_\infty}$.

Remark 3.1.12. Observe, as a current a green function for $\mathcal{D}$ satisfies

$$\mathrm{dd^c}\, g_D + \delta_D = \nu \tag{3.1.6}$$

for some smooth volume form ν; here $D = \mathcal{D}|_{\mathcal{X}_\infty}$. In the original setup of Arakelov only Green's functions g_{Ar} which satisfy (3.1.6) for a fixed volume form ν_{Ar} had been considered. Also in addition $g_{\mathcal{D},\mathrm{Ar}} = g_{\mathrm{Ar}}(\mathcal{D}, \cdot)$ had to be normalized by

$$\int_{\mathcal{X}_\infty} g_{\mathrm{Ar}}(\mathcal{D}, z)\nu_{\mathrm{Ar}}(z) = 0\,.$$

Definition 3.1.13. An *arithmetic divisor* $\widehat{\mathcal{D}} = (\mathcal{D}, g)$ is a divisor $\mathcal{D} \in Z^1(\mathcal{X})$ together with a Green's function g for $\mathcal{D}$. The set of arithmetic divisors forms a group with respect to the obvious addition

$$(\mathcal{D}, g) + (\mathcal{D}', g') = (\mathcal{D} + \mathcal{D}', g + g')\,,$$

called *the group of arithmetic divisors* $\widehat{Z}^1(\mathcal{X})$. For a rational function $f \in K(\mathcal{X})$ we denote its restriction to $K(\mathcal{X}_\infty)$ by f_∞. The function

$$-\log|f_\infty|^2\,,$$

where $|\cdot|$ is the usual absolute value, is a Green's function for the principal divisor $\mathrm{div}(f)$. The subgroup of $\widehat{Z}^1(\mathcal{X})$ which consists of the arithmetic divisors

$$\widehat{\mathrm{div}}(f) = (\mathrm{div}(f), -\log|f_\infty|^2)$$

will be denoted by $\widehat{R}^1(\mathcal{X})$. Finally, the *arithmetic Chow group of codimension 1* is defined to be the quotient

$$\widehat{\mathrm{CH}}^1(\mathcal{X}) = \widehat{Z}^1(\mathcal{X})/\widehat{R}^1(\mathcal{X})\,.$$

For $\widehat{\mathcal{D}} \in \mathcal{D} \in Z^1(\mathcal{X})$ we denote the corresponding element in $\widehat{\mathrm{CH}}^1(\mathcal{X})$ by $[\widehat{\mathcal{D}}]$.

Remark 3.1.14. An arithmetic divisor $\mathcal{D} + \alpha\mathcal{X}_\infty$ (with $\alpha\mathcal{X}_\infty = \sum_\sigma \alpha_\sigma \mathcal{X}_\sigma$) in the sense of Arakelov corresponds in the setup of Definition 3.1.13 to the arithmetic divisor $(\mathcal{D}, g_{\mathcal{D},\mathrm{Ar}} + \sum_\sigma \alpha_\sigma)$; this correspondence is compatible with rational equivalence and the product structure described below in Definition 3.1.15.

Definition 3.1.15. Let $Z = \sum_{x \in \mathcal{X}^{(2)}} n_x\, x$ be a 2-cycle[2] on $\mathcal{X}$ with integral coefficients i.e. the x are closed points of $\mathcal{X}$ and the n_x belong to $\mathbb{Z}$, where only finitely many n_x are different from 0. We define its *Arakelov degree* by

$$\widehat{\deg} Z := \sum_{x \in \mathcal{X}^{(2)}} n_x \log|k(x)|\,.$$

[2]Here we follow the definition of [SABK] which defines a 2-cycle as an element of the free abelian group generated by the points of codimension 2 (cf. [SABK], p.11). The are several books where they define cycles not by codimension but by dimension. In these books this element would be called a 0-cycle (cf. e.g. [La], p.52).

Given two Weil divisors $\mathcal{D}_1, \mathcal{D}_2$ of $\mathcal{X}$ which have no common components we define their intersection 2-cycle (which we denote by abuse of notation by $\mathcal{D}_1 \cdot \mathcal{D}_2$) as

$$\mathcal{D}_1 \cdot \mathcal{D}_2 := \sum_{x \in \mathcal{X}^{(2)}} i_x(\mathcal{D}_1, \mathcal{D}_2)\, x\,,$$

where $i_x(\mathcal{D}_1, \mathcal{D}_2)$ is the intersection of $\mathcal{D}_1$ and $\mathcal{D}_2$ in x (cf. Definition 1.3.11). Now, let $\widehat{\mathcal{D}}_1 = (\mathcal{D}_1, g_1)$ and $\widehat{\mathcal{D}}_2 = (\mathcal{D}_2, g_2)$ be arithmetic divisors, where $\mathcal{D}_1$ and $\mathcal{D}_2$ have no common components. On $\mathcal{X}_\infty \setminus \mathrm{Supp}(\mathcal{D}_1|_{\mathcal{X}_\infty})$ we have the (1,1)-form $\mathrm{dd}^{\mathrm{c}}\, g_i$. We can extend this to a form of $\mathcal{X}_\infty$, and we will denote this extension by ω_i. The *arithmetic intersection number* of $\widehat{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_2$ is defined as

$$\widehat{\mathcal{D}_1} \cdot \widehat{\mathcal{D}}_2 := \widehat{\deg}\,(\mathcal{D}_1 \cdot \mathcal{D}_2) + \frac{1}{2}\left(\int_{\mathcal{X}_\infty} g_2\omega_1 + \sum_\alpha p_\alpha g_1(P_\alpha)\right)\,, \tag{3.1.7}$$

where $\mathcal{D}_2|_{\mathcal{X}_\infty} = \sum_\alpha p_\alpha P_\alpha$ (cf. e.g. [Bo], p.274: (5.8) or [GS], p. 152: (v)). Now, for any elements $z_1, z_2 \in \widehat{\mathrm{CH}}^1(\mathcal{X})$ we can find $\widehat{\mathcal{D}}_1$ and $\widehat{\mathcal{D}}_2$ with $z_1 = [\widehat{\mathcal{D}}_1]$ and $z_2 = [\widehat{\mathcal{D}}_2]$ so that $\mathcal{D}_1$ and $\mathcal{D}_2$ have no common components. We obtain therefore the following result:

Theorem 3.1.16 (Gillet, Soule et al.)**.** *The formula 3.1.7 induces a bilinear, symmetric pairing*

$$\widehat{\mathrm{CH}}^1(\mathcal{X}) \times \widehat{\mathrm{CH}}^1(\mathcal{X}) \to \mathbb{R}\,.$$

Proof: See for example [GS] or [SABK]. □

Proposition 3.1.17. *There is an isomorphism*

$$\widehat{c}_1 : \widehat{\mathrm{Pic}}(\mathcal{X}) \to \widehat{\mathrm{CH}}^1(\mathcal{X})$$

mapping the class of $\overline{\mathcal{L}}$ *to the class of* $(\mathrm{div}(s), -\log||s||^2)$*, for any rational section* s *of* $\mathcal{L}$*; here* $||\cdot||$ *is the norm associated with the hermitian metric of* $\mathcal{L}_\infty$*. The isomorphism is compatible with the intersection pairings* (3.1.3) *and* (3.1.7).

Proof: For the first statement see e.g. [SABK], p. 67: Proposition 1. The second statement follows directly by the definitions. □

Convention 3.1.18. Analog to Section 1.3 and Section 1.4 we will allow rational coefficients for the groups $\widehat{\mathrm{Pic}}(\mathcal{X})$ and $\widehat{\mathrm{CH}}^1(\mathcal{X})$. The corresponding groups will be denoted by $\widehat{\mathrm{Pic}}(\mathcal{X})_\mathbb{Q}$ and $\widehat{\mathrm{CH}}^1(\mathcal{X})_\mathbb{Q}$. Furthermore, we will extend the arithmetic intersection numbers to these groups. Unless otherwise specified, we will always assume in the following to work with these groups i.e. assume to work with rational coefficients.

3.2 Kühn's formula for $\overline{\omega}^2_{\mathbf{Ar}}$

3.2.1 The formula

Assumption 3.2.1. Let E be a number field and $\mathcal{O}_E$ its ring of integers. Furthermore, let $\mathcal{Y} \to \operatorname{Spec} \mathcal{O}_E$ be an arithmetic surface and write Y for its generic fiber. We fix $\infty, P_1, ..., P_r \in Y(E)$ such that $Y \setminus \{\infty, P_1, ..., P_r\}$ is hyperbolic. Then we consider an arithmetic surface $\mathcal{X} \to \operatorname{Spec} \mathcal{O}_E$ equipped with a dominant morphism of arithmetic $\operatorname{Spec} \mathcal{O}_E$-surfaces $\boldsymbol{\beta} : \mathcal{X} \to \mathcal{Y}$ such that the induced morphism $\boldsymbol{\beta} : X \to Y$ of algebraic curves defined over E is unramified above $Y(E) \setminus \{\infty, P_1, ..., P_r\}$[3]. Let $g \geq 2$ be the genus of X and $d = \deg(\boldsymbol{\beta})$. We write $\boldsymbol{\beta}^*\infty = \sum b_j S_j$ and the points S_j will be called *labeled*. Set $b_{\max} = \max_j\{b_j\}$. Divisors on X with support in the labeled points are called *labeled*. Finally, a prime $\mathfrak{p}$ is said to be *bad* if the fiber of $\mathcal{X}$ above $\mathfrak{p}$ is reducible[4].

Theorem 3.2.2. *Let $\boldsymbol{\beta} : \mathcal{X} \to \mathcal{Y}$ be a morphism of arithmetic surfaces as in Assumption 3.2.1. Assume that all labeled points are E-rational points and that all labeled divisors of degree zero are torsion, then the arithmetic self-intersection number of the dualizing sheaf $\overline{\omega}_{\mathcal{X},\mathrm{Ar}}$ (cf. Remark 3.1.9) on $\mathcal{X}$ satisfies the inequality*

$$\overline{\omega}^2_{\mathcal{X},\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{E|\mathbb{Q}}|^2 + [E:\mathbb{Q}]\,(\kappa_1 \log b_{\max} + \kappa_2) + \sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p})\right), \quad (3.2.1)$$

where $\kappa_1, \kappa_2 \in \mathbb{R}^*_+$ are positive constants that depend only on Y and the points $\infty, P_1, ..., P_r$. The coefficients $a_{\mathfrak{p}} \in \mathbb{Q}$ are determined by certain local intersection numbers (see formula (3.2.4) *below).*

Proof: See [Kü2] Theorem I. □

Remark 3.2.3. The proof of Theorem 3.2.2 uses classical Arakelov theory, as well as *generalized arithmetic intersection theory* (see [Kü1]), which allows to use results of Jorgenson and Kramer [JK2]. The generalized arithmetic intersection theory is an extension of the intersection theory for hermitian line bundles we introduced in Section 3.1. The difference is that we are now allowed to work with *hermitian, logarithmically singular line bundles* i.e. pairs $(\mathcal{L}, h)$, where $\mathcal{L}$ is a line bundle on $\mathcal{X}$ and h is a *hermitian logarithmically singular metric* on $\mathcal{L}_\infty$ with respect to a finite subset $\mathcal{S} \subset \mathcal{X}_\infty$ (cf. [Kü1] Definition 3.1). The isomorphism classes of these line bundles form the *generalized arithmetic Picard group* $\widehat{\mathrm{Pic}}(\mathcal{X}, \mathcal{S})$, and we have a canonical inclusion of $\widehat{\mathrm{Pic}}(\mathcal{X})$ in $\widehat{\mathrm{Pic}}(\mathcal{X}, \mathcal{S})$. It is shown in [Kü1] how to extend the intersection at the infinite places (3.1.2) in order to work for

[3]That the morphism β is dominant means that the generic point of $\mathcal{X}$ will be mapped to the generic point of $\mathcal{Y}$. This assures that the induced morphism of the generic fibers gives us a non-constant morphism of algebraic curves. Since β is projective (see e.g. [Liu], p.108: Corollary 3.32. (e)), the morphism β is closed. In this situation the property "dominant" is equivalent to "surjective".

[4]Notice, that a prime of bad reduction does not need to be a bad prime.

the hermitian, logarithmically singular line bundles. This induces a bilinear, symmetric pairing

$$\widehat{\mathrm{Pic}}(\mathcal{X},\mathcal{S}) \times \widehat{\mathrm{Pic}}(\mathcal{X},\mathcal{S}) \to \mathbb{R}$$

extending the pairing of Arakelov. In fact, if $\mathcal{S} = \emptyset$ then the definitions coincide with the definitions of Section 3.1.

Definition 3.2.4. To keep the notation simple, we write $\mathcal{S}_j$ for the Zariski closure in $\mathcal{X}$ of a labeled point S_j. Let $\mathcal{K}$ be a canonical divisor of $\mathcal{X}$, then for each labeled point S_j we can find a divisor $\mathcal{F}_j$ such that

$$\left(\mathcal{S}_j + \mathcal{F}_j - \frac{1}{2g-2}\mathcal{K}\right) \cdot \mathcal{C} = 0 \tag{3.2.2}$$

for all vertical irreducible components $\mathcal{C}$ of $\mathcal{X}$. Similarly we find for each labeled point S_j a divisor $\mathcal{G}_j$ such that also for all $\mathcal{C}$ as before

$$\left(\mathcal{S}_j + \mathcal{G}_j - \frac{1}{d}\boldsymbol{\beta}^*\overline{\infty}\right) \cdot \mathcal{C} = 0\,. \tag{3.2.3}$$

Notice that we can choose $\mathcal{F}_j$ and $\mathcal{G}_j$ to have support in the fiber above the bad primes (Lemma 1.3.16). The rational numbers $a_{\mathfrak{p}}$ in Theorem 3.2.2 are determined by the following arithmetic intersection numbers of trivially metrised hermitian line bundles

$$\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) = -\frac{2g}{d}\sum_j b_j\, \overline{\mathcal{O}}(\mathcal{G}_j)^2 + \frac{2g-2}{d}\sum_j b_j\, \overline{\mathcal{O}}(\mathcal{F}_j)^2. \tag{3.2.4}$$

The number $\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p})$ is called the *geometric contribution*. The number

$$[E:\mathbb{Q}]\,(\kappa_1 \log b_{\max} + \kappa_2)$$

the *analytic contribution* (cf. [Kü2]).

Remark 3.2.5. Notice that pullbacks of divisors are always defined in our situation, since the morphism is dominant (see e.g. [Liu], p.261: Lemma 1.33.).

Remark 3.2.6. Here we briefly explain why the divisors $\mathcal{F}_j$ and $\mathcal{G}_j$ exist and how one can construct them. We illustrate everything with the divisors $\mathcal{G}_j$. If we assume for the moment that we know already that the divisor $\mathcal{G}_j$ as defined in (3.2.3) exists, it is obvious that it can even be chosen to have support in the fibers above the bad primes, hence in this situation we get

$$\mathcal{G}_j = \sum_{\mathfrak{p}\text{ bad}} \mathcal{G}_{j,\mathfrak{p}}\,,$$

where $\mathcal{G}_{j,\mathfrak{p}}$ is a vertical divisor with support in the fiber above $\mathfrak{p}$. Then

$$\left(\mathcal{S}_j + \mathcal{G}_{j,\mathfrak{p}} - \frac{1}{d}\boldsymbol{\beta}^*\overline{\infty}\right) \cdot \mathcal{C} = 0 \tag{3.2.5}$$

for all vertical components $\mathcal{C}$ in the fiber above $\mathfrak{p}$. On the other hand, if we can choose for each bad prime $\mathfrak{p}$ a vertical divisor $\mathcal{G}_{j,\mathfrak{p}}$ with support in the fiber above $\mathfrak{p}$ which satisfies (3.2.5) for all vertical components in the fiber above $\mathfrak{p}$, then $\sum_{\mathfrak{p}\text{ bad}} \mathcal{G}_{j,\mathfrak{p}}$ fulfills (3.2.3). If follows that the existence of $\mathcal{G}_j$ is equivalent to the existence of the $\mathcal{G}_{j,\mathfrak{p}}$, and that the computation of $\mathcal{G}_j$ can be done fiber by fiber once we have shown the existence. Now let

$$\mathcal{X}_{\mathfrak{p}} = \mathcal{X} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec}\overline{k(\mathfrak{p})} = \sum_{j=1}^{r_{\mathfrak{p}}} d_j \mathcal{C}_j$$

be the special fiber above $\mathfrak{p}$. The rank of the *intersection matrix* $C_{\mathfrak{p}} = (d_i\mathcal{C}_i \cdot d_j\mathcal{C}_j)_{1\leq i,j\leq r_{\mathfrak{p}}}$ is $r_{\mathfrak{p}} - 1$ (see. [La], p. 60: Proposition 3.3. and p. 61: Lemma 3.4.). We define the vector $B_{\mathfrak{p}} := (B_1, \ldots, B_{r_{\mathfrak{p}}})^t$, where

$$B_i := \left(\mathcal{S}_j - \frac{1}{d}\boldsymbol{\beta}^*\overline{\infty}\right) \cdot \mathcal{C}_i\,.$$

It follows easily that $\mathcal{G}_{j,\mathfrak{p}}$ as defined in (3.2.5) exists if and only if $B_{\mathfrak{p}} = C_{\mathfrak{p}}x$ is solvable, where $x \in \mathbb{Q}^{r_{\mathfrak{p}}}$ is a column vector. Now since $(\mathcal{S}_j - d^{-1}\boldsymbol{\beta}^*\overline{\infty}) \cdot \mathcal{X}_{\mathfrak{p}} = 0$ and $\mathcal{C}_i \cdot \mathcal{X}_{\mathfrak{p}} = 0$ for all i we can eliminate one row in the augmented matrix $(C_{\mathfrak{p}}|B_{\mathfrak{p}})$ by elementary row operations. We will denote the resulting matrix by $(C_{\mathfrak{p}}|B_{\mathfrak{p}})'$. We have $r_{\mathfrak{p}} - 1 = \operatorname{rank} C_{\mathfrak{p}} \leq \operatorname{rank}(C_{\mathfrak{p}}|B_{\mathfrak{p}}) = \operatorname{rank}(C_{\mathfrak{p}}|B_{\mathfrak{p}})' \leq r_{\mathfrak{p}} - 1$, hence $\operatorname{rank} C_{\mathfrak{p}} = \operatorname{rank}(C_{\mathfrak{p}}|B_{\mathfrak{p}})$ which shows that $B_{\mathfrak{p}} = C_{\mathfrak{p}}x$ is solvable. In a completely analog way we can show that the divisors $\mathcal{F}_j$ exists and that we can make our computation fiber by fiber i.e. that we can compute the $\mathcal{F}_{j,\mathfrak{p}}$ in order to get $\mathcal{F}_j$, where $\mathcal{F}_{j,\mathfrak{p}}$ is the part of $\mathcal{F}_j$ which has support in the fiber above $\mathfrak{p}$.

Remark 3.2.7. Since the divisors $\mathcal{G}_j$ and $\mathcal{F}_j$ are vertical the hermitian line bundles $\overline{\mathcal{O}}(\mathcal{G}_j)$ and $\overline{\mathcal{O}}(\mathcal{F}_j)$ have a trivial metric[5]. Hence, the intersection number at the infinite places of $\overline{\mathcal{O}}(\mathcal{G}_j)^2$ and $\overline{\mathcal{O}}(\mathcal{F}_j)^2$ is zero, and so the computation of (3.2.4) becomes a pure algebraic problem.

Remark 3.2.8. With equation (3.2.3) we have to be careful. In general we do not have $\boldsymbol{\beta}^*\overline{\infty} = \overline{\boldsymbol{\beta}^*\infty}$. However, we can show the following: Let $P \in Y$ be a E-rational point and $\overline{P}$ the horizontal divisor obtained by taking the Zariski-closure of P in $\mathcal{Y}$. Since $\overline{P}|_Y = P$ we have $(\boldsymbol{\beta}^*\overline{P})|_X = \boldsymbol{\beta}^*P$ (see e.g. [Gr3] (21.4.4)) and therefore $\boldsymbol{\beta}^*\overline{P} - \overline{\boldsymbol{\beta}^*P}$ is a vertical divisor.

3.2.2 A first analysis of the geometric contribution

In [Kü2] a general bound for the quantity (3.2.4) is given. We will give a short review of the facts related to this bound and discuss whether or not this is a good bound in a given situation.

Let $\mathfrak{p}$ be a bad prime and

$$\mathcal{X} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec}\overline{k(\mathfrak{p})} = \sum_{j=1}^{r_{\mathfrak{p}}} d_j \mathcal{C}_j$$

[5]Some authors write $\mathcal{O}(\mathcal{G}_j)$ and $\mathcal{O}(\mathcal{F}_j)$ instead of $\overline{\mathcal{O}}(\mathcal{G}_j)$ and $\overline{\mathcal{O}}(\mathcal{F}_j)$ to indicate this circumstance.

be the decomposition into irreducible components. We set

$$u_{\mathfrak{p}} = \max_{i,j} |\mathcal{C}_i \cdot \mathcal{C}_j|, \qquad l_{\mathfrak{p}} = \min_{\mathcal{C}_i \cdot \mathcal{C}_j \neq 0} |\mathcal{C}_i \cdot \mathcal{C}_j| \,.$$

Since $\mathcal{X} \times_{\operatorname{Spec} \mathcal{O}_E} \operatorname{Spec} \overline{\mathbb{F}}_{\mathfrak{p}}$ is connected (Remark 1.4.14), there is a minimal number of intersection points needed to connect any two irreducible components of $\mathcal{X}_s$; we denote this number by $c_{\mathfrak{p}}$. We set

$$b_{\mathfrak{p}} = \left(\sum_{k=1}^{c_{\mathfrak{p}}} \left(\sum_{l=1}^{k} \left(\frac{u_{\mathfrak{p}}}{l_{\mathfrak{p}}} \right)^{l-1} \right)^2 + (r_{\mathfrak{p}} - c_{\mathfrak{p}} - 1) \left(\sum_{l=1}^{c_{\mathfrak{p}}} \left(\frac{u_{\mathfrak{p}}}{l_{\mathfrak{p}}} \right)^{l-1} \right)^2 \right) \frac{u_{\mathfrak{p}}}{l_{\mathfrak{p}}^2} \,.$$

Proposition 3.2.9. *Let $\mathcal{G}_j$ be as in (3.2.3) and $\mathcal{G}_{j,\mathfrak{p}}$ be the part of $\mathcal{G}_j$ which lies in the special fiber above $\mathfrak{p}$, where $\mathfrak{p}$ is a bad prime. Then we have*

$$-\left(\mathcal{G}_{j,\mathfrak{p}}\right)^2 \leq b_{\mathfrak{p}} \,.$$

In order to discuss the quality of the bound given in Proposition 3.2.9 we need to review in short the proof of the proposition:

Sketch of the proof: After possibly renumbering the irreducible components and adding rational multiples of full fibers, we may assume $0 \neq \mathcal{G}_{j,\mathfrak{p}} = \sum_{k=2}^{r_{\mathfrak{p}}} n_k \mathcal{C}_k$ with all $n_k \geq 0$ and $n_1 = 0$. Now, let

$$W = \{ \mathcal{C}_j \} \tag{3.2.6}$$

be the set of all irreducible components of the fiber above $\mathfrak{p}$ and set

$$\begin{aligned} U_0 &= \{ \mathcal{C}_j \in W \mid n_j = 0 \} \\ V_0 &= W \setminus U_0. \end{aligned}$$

Then we define recursively

$$\begin{aligned} U_{k+1} &= \{ \mathcal{C}_j \in V_k \mid \exists \mathcal{C}_i \in U_k \,\text{with}\, \mathcal{C}_j \cdot \mathcal{C}_i > 0 \} \\ V_{k+1} &= V_k \setminus U_{k+1}. \end{aligned}$$

Since the fiber above $\mathfrak{p}$ is connected, the subsets $U_k \subset W$ determine a disjoint decomposition of W. In fact this decomposition has at most $c_{\mathfrak{p}} + 1$ disjoint sets. It can be shown that for each coefficient n_j with component $\mathcal{C}_j \in U_k$ there exists the upper bound

$$n_j \leq \frac{1}{l_{\mathfrak{p}}} \sum_{l=1}^{k} \left(\frac{u_{\mathfrak{p}}}{l_{\mathfrak{p}}} \right)^{l-1} \tag{3.2.7}$$

(see proof of Proposition 6.1. in [Kü2]). These bounds can be used to obtain

$$
\begin{aligned}
-\left(\mathcal{G}_{j,\mathfrak{p}}\right)^2 &= -\sum_{j,k=2}^{r_\mathfrak{p}} n_j n_k (\mathcal{C}_j \cdot \mathcal{C}_k) && (3.2.8)\\
&\leq -\sum_{j=2}^{r_\mathfrak{p}} n_j^2 (\mathcal{C}_j \cdot \mathcal{C}_j) \leq \sum_{j=2}^{r_\mathfrak{p}} n_j^2 u_\mathfrak{p} && (3.2.9)\\
&\leq \sum_{\substack{U_k \subset W \\ U_k \neq U_0}} \#U_k \cdot \left(\sum_{l=1}^{k} \left(\frac{u_\mathfrak{p}}{l_\mathfrak{p}} \right)^{l-1} \right)^2 \frac{u_\mathfrak{p}}{l_\mathfrak{p}^2} && (3.2.10)\\
&\leq \left(\sum_{k=1}^{c_\mathfrak{p}-1} \left(\sum_{l=1}^{k} \left(\frac{u_\mathfrak{p}}{l_\mathfrak{p}} \right)^{l-1} \right)^2 + (r_\mathfrak{p} - c_\mathfrak{p}) \left(\sum_{l=1}^{c_\mathfrak{p}} \left(\frac{u_\mathfrak{p}}{l_\mathfrak{p}} \right)^{l-1} \right)^2 \right) \frac{u_\mathfrak{p}}{l_\mathfrak{p}^2} . && (3.2.11)
\end{aligned}
$$

Hence, the proposition is proved. □

In case that $\mathcal{Y} = \mathbb{P}^1$ and $\beta : \mathcal{X} \to \mathbb{P}^1$ is a *Galois cover*[6], i.e. the extension of the function fields $K(\mathcal{Y}) \to K(\mathcal{X})$ is Galois with group G and $\mathcal{Y}$ is isomorphic to $\mathcal{X}/G$, then we have

$$\mathcal{G}_j^2 = \mathcal{F}_j^2 \,,$$

where $\mathcal{F}_j$ is the vertical divisor in (3.2.2) (see [Kü2], p.22: Proposition 6.2.). Hence, in this situation we have

$$\sum_{\mathfrak{p} \text{ bad}} a_\mathfrak{p} \log \mathrm{Nm}(\mathfrak{p}) = -\frac{2}{d} \sum_j b_j\, \overline{\mathcal{O}}(\mathcal{G}_j)^2 \,,$$

and we can use the $b_\mathfrak{p}$ to get a bound for the $a_\mathfrak{p}$. In general the situation is not that easy. However, since $\mathcal{F}_j^2 \leq 0$, we can find at least a "rough" bound for the $a_\mathfrak{p}$. We summarize this in the following theorem:

Theorem 3.2.10. *With the notation from above we have*

$$a_\mathfrak{p} \leq 2g b_\mathfrak{p} \,.$$

If in addition $\mathcal{Y} = \mathbb{P}^1$ and $\beta : \mathcal{X} \to \mathbb{P}^1$ is a Galois cover, then we have the stronger inequality

$$a_\mathfrak{p} \leq 2 b_\mathfrak{p} \,.$$

Proof: See [Kü2], p.25: Theorem 6.3. □

---

[6]Since β is surjective it is always a *cover* (cf. [LL], p.63).

Remark 3.2.11. If we want to discuss whether or not this is a good bound for (3.2.4) we need to analyze which input the computation of the bound needs, and we have to compare this with the necessary input one would need to compute the exact quantity. The given numbers are $r_\mathfrak{p}, u_\mathfrak{p}, l_\mathfrak{p}$ and $c_\mathfrak{p}$.
We start with an analyzation of Proposition 3.2.9. According to equation (3.2.8) the exact computation of the $(\mathcal{G}_{j,\mathfrak{p}})^2$ would imply the knowledge of the coefficients n_i and the knowledge of the intersection matrix of the special fiber. Even if it is likely that we know the intersection matrix (otherwise it would have been difficult to compute $u_\mathfrak{p}$ and $i_\mathfrak{p}$) the proposition does not use this information. Hence the intersection numbers $-\mathcal{C}_i \cdot \mathcal{C}_j$ for $i \neq j$ will be approximated by zero and the intersection numbers $-\mathcal{C}_i \cdot \mathcal{C}_i$ by $u_\mathfrak{p}$. This gives the step from (3.2.8) to (3.2.9). Now, the approximation of the n_i will be done dependent on a specific choice of a disjoint decomposition of the set W (3.2.6). In general we cannot expect that this approximation gives us the correct values of the n_i since neither the intersection matrix nor the intersection of the horizontal divisor $\mathcal{S}_j$ (cf. (3.2.3)) with the special fiber are used (cf. [Kü2], proof of Proposition 6.1.). However, if we could include the knowledge of the dual graph and the identification of the n_i which are zero we could improve the proposition since we would know the "best decomposition". In this case we would take (3.2.10) as the bound of the $-(\mathcal{G}_{j,\mathfrak{p}})^2$. Without this we have to assume the "worst decomposition", and so we end up with (3.2.11). In order to get the "worst decomposition" we have to assume that $n_i \neq 0$ for $i \neq 1$. Furthermore, it is important to assume that the configuration of the special fiber looks like a chain of length $c_\mathfrak{p}$ that starts with component $\mathcal{C}_1$ and ends with a component, say $\mathcal{C}_{c_\mathfrak{p}}$, where all the remaining $r_\mathfrak{p} - c_\mathfrak{p}$ components intersect just the component $\mathcal{C}_{c_\mathfrak{p}}$ of the chain. Notice that just the configuration of the special fiber does not give us the "worst decomposition" but the position of the component $\mathcal{C}_1$ in it. It follows that the quality of the approximation done in the step from (3.2.10) to (3.2.11) depends basically on three things: the difference between the real configuration and the configuration described above, the number of the n_i which are zero, and the position of the corresponding components in the special fiber.
Finally, let us discuss the bound of the $a_\mathfrak{p}$ given in Theorem 3.2.10. For sure the quality of the theorem has to be considered relative to Proposition 3.2.9. However, if we assume that the proposition gave us a good approximation of the numbers $-(\mathcal{G}_{j,\mathfrak{p}})^2$ the significance of the theorem depends strongly on the morphism $\beta : \mathcal{X} \to \mathcal{Y}$. If the morphism is a Galois cover, we have (relative to Proposition 3.2.9) the best approximation. If it is not a Galois cover, it is difficult to say something about the significance of the results because we do not know the numbers $\mathcal{F}_{j,\mathfrak{p}}^2$. In this case the theorem would just give a good result if the numbers $\mathcal{F}_{j,\mathfrak{p}}^2$ are small in comparison to the numbers $\mathcal{G}_{j,\mathfrak{p}}^2$.

3.2.3 Application to Fermat curves and modular curves

In Subsection 3.1 we saw how the Arakelov Intersection Theory extends the regular arithmetic intersection theory which was introduced in Subsection 1.3, and we explained how to equip the canonical sheaf with a unique metric in order to fulfill an adjunction formula in this new setting. The hermitian line bundle we obtained in this way was denoted by $\overline{\omega}_{\mathrm{Ar}}$.

Considering all the aspects which are involved in the computation of the self-intersection number of $\overline{\omega}_{\mathrm{Ar}}$ it seems to be clear that this cannot be a simple problem. In [Kü2] Kühn computed upper bounds for the number $\overline{\omega}^2_{\mathrm{Ar}}$ where he used his extension of the intersection theory. Theorem 3.2.2 was taken from this article and is the starting point of our work. The advantage of Theorem 3.2.2 is that it reduces the computation of the upper bound for $\overline{\omega}^2_{\mathrm{Ar}}$ to a pure algebraic problem i.e. the analytic data of the intersection is already contained in the analytic contribution $[E:\mathbb{Q}]\,(\kappa_1 \log b_{\max} + \kappa_2)$ in (3.2.1).
Now, in order to apply the Theorem we proceed as follows: We have to consider curves X, Y that are defined over a number field E (where we know how to compute $\Delta_{E/\mathbb{Q}}$ and $|E:\mathbb{Q}|$), and a morphism $\beta : X \to Y$ which fulfills the conditions of the theorem, hence all labeled points are E-rational and all labeled divisors of degree zero are torsion. Then we use the theory developed in Chapter 1 and 2 in order to construct regular models $\mathcal{X}$, $\mathcal{Y}$ and a morphism $\beta : \mathcal{X} \to \mathcal{Y}$ that extends the morphism of the curves. Once we have done this we determine the vertical divisors as defined in (3.2.2) and (3.2.3). Finally, we compute the geometric contribution (3.2.4).

In this work we will consider two types of curves, where we can show that there exists a morphism to $\mathbb{P}^1$ which fulfills the conditions of the theorem: the Fermat curves and the modular curves. We start with the first type. Let N be a squarefree integer. We consider the Fermat curve

$$F_N : X^N + Y^N = Z^N,$$

together with the natural morphism

$$\beta : F_N \to \mathbb{P}^1 \tag{3.2.12}$$

given by $(x:y:z) \mapsto (x^N : y^N)$. Since the morphism β is defined over $\mathbb{Q}$, it is defined over any number field. It is a Galois covering of degree N^2 and, since there are only the three branch points $0, 1, \infty$, it is a Belyi morphism. All the ramification orders equal N. In [MR] Murty and Ramakrishnan give the associated Belyi uniformisation $F_N(\mathbb{C}) \setminus \boldsymbol{\beta}^{-1}\{0,1,\infty\} \cong \Gamma_N \setminus \mathbb{H}$. The subgroup Γ_N of $\Gamma(2)$ is given by $\Gamma_N = \ker \psi$ where $\psi : \Gamma(2) \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ maps the generators of $\Gamma(2)$ to the elements $(1,0)$ and $(0,1)$.

Definition 3.2.12. Let $f : X \to Y$ be a morphism of curves. A ramified point, i.e. an element $S \in X$ that maps to one of the branch points of Y, will be called a *cusp*. Divisors with support in the cusps having degree zero are called *cuspidal divisor*.

Convention 3.2.13. Let us consider the situation of Assumption 3.2.1. The cusps are contained in the preimage of the set $\{\infty, P_1, \ldots, P_r\}$. We make for the rest of this work the convention that the point ∞ has been chosen so that the labeled points are contained in the cusps.

Theorem 3.2.14 (Rohrlich)**.** *Let F_N be the Fermat curve of exponent N and $\beta : F_N \to \mathbb{P}^1$ the morphism in* (3.2.12)*. Then the group of cuspidal divisors modulo the group of principal cuspidal divisors is a torsion subgroup of* $\mathrm{Cl}(F_N)$*.*

Proof: The statement follows from [Ro], p. 101: Theorem 1. □

Corollary 3.2.15. *Let F_N be the Fermat curve of exponent N and $\beta : F_N \to \mathbb{P}^1$ the morphism in* (3.2.12). *Furthermore, let $S \in F_N$ be a cusp. Then $(2g-2)S$ is a canonical divisor.*

Proof: By the Hurwitz formula there exists a canonical divisor with support in the cusps. Then by Theorem 3.2.14 the claim follows. □

If we now construct a regular model of F_N over the ring of integers of a cyclotomic field we can find a canonical divisor of the following form:

Lemma 3.2.16. *Let N be a squarefree odd integer, ζ_N a primitive N-th root of unity and F_N the Fermat curve of exponent N. Furthermore let $\mathfrak{F}$ be a regular model of F_N over* $\operatorname{Spec}\mathbb{Z}[\zeta_N]$. *Then there exists a canonical divisor $\mathcal{K} \in Z^1(\mathfrak{F})_{\mathbb{Q}} = Z^1(\mathfrak{F}) \otimes_{\mathbb{Z}} \mathbb{Q}$ on $\mathfrak{F}$ of the form*

$$\mathcal{K} = (2g-2)\mathcal{S} + \mathcal{V}\,,$$

where $\mathcal{S}$ is a horizontal divisor coming from an arbitrary cusp, $g = g(F_N)$ is the genus of F_N and $\mathcal{V}$ denotes a vertical divisor having support in the special fibers, that lie above the bad prime ideals.

Proof: It follows from Corollary 3.2.15 that

$$(2g-2)S$$

is a canonical divisor in $Z^1(F_N)_{\mathbb{Q}}$, where S is any cusp. If we now set

$$\mathcal{K}_0 := (2g-2)\mathcal{S} + \mathcal{V}_0\,,$$

where $\mathcal{S}$ is the Zariski closure of S and $\mathcal{V}_0$ is a sum of divisors, having support in the closed fibers, so that $\mathcal{K}_0$ fulfills the adjunction formula, then $\mathcal{K}_0$ is a canonical divisor of $\mathfrak{F}$ (see Proposition 1.4.16). Note that similar arguments, as in the proof of Proposition 1.4.16, assure that $\mathcal{V}_0$ exists. For all primes $\mathfrak{q} \in \operatorname{Spec}\mathcal{O}_E$ not dividing N - in fact these are the good primes - the special fiber $\mathfrak{F} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec} k(\mathfrak{q})$ is smooth and so it consists of a single irreducible component. Since the self-intersection of this fiber is zero (see [La]: p.61: Proposition 3.5.) we can add any multiple of it to $\mathcal{K}_0$ and the resulting divisor still fulfills the adjunction formula. Using this fact we can transform $\mathcal{K}_0$ into a divisor $\mathcal{K} = (2g-2)\mathcal{S} + \mathcal{V}$, where $\mathcal{V}$ is a vertical divisor having support in the special fibers above the bad primes. Again, by Proposition 1.4.16, this is a canonical divisor. □

Next, we want to analyze the situation in case of the modular curves. A *modular curve* $Y(\Gamma)$ is a curve constructed as the quotient of the complex upper half-plane by the action of a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. The compactification of $Y(\Gamma)$ is a *(compact) modular curve* denoted by $X(\Gamma)$. For an introduction to the subject of modular curves the reader may take a look at the books [DS], [Sh] or [Si] CHAPTER 1. For a modular curve $X(\Gamma)$ there exists a natural morphism $X(\Gamma) \to X(1) \cong \mathbb{P}^1$, where the cusps of this morphism are exactly the cusps of the modular curve, i.e. the points $X(\Gamma) \setminus Y(\Gamma)$. We have the following important theorem.

Theorem 3.2.17 (Manin-Drinfeld)**.** *Let Γ be a congruent subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $X(\Gamma)$ the corresponding modular curve. Then the divisors of $X(\Gamma)$ of degree 0 and with support in the cusps are torsion divisors.*

Proof: See [El], p. 59: Théorème. □

Remark 3.2.18. We have seen in Theorem 3.2.14 and Theorem 3.2.17 that the Fermat curve F_N together with the morphism $\beta : F_N \to \mathbb{P}^1$ (3.2.12) and the modular curves $X(\Gamma)$ with their natural morphisms $X(\Gamma) \to \mathbb{P}^1$ fulfill the condition that the cuspidal divisors (labeled divisor of degree zero resp.) are torsion. Since the Fermat curve and the morphism β are defined over $\mathbb{Q}$ they are defined over any number field. The cusps of β are $\mathbb{Q}(\zeta_N)$-rational, hence the regular models and the morphism between them, which extend the curves and their morphism, must be $\operatorname{Spec}\mathcal{O}_E$-schemes and a $\operatorname{Spec}\mathcal{O}_E$-morphism, where $\mathcal{O}_E$ is the ring of integer of a number field E with $\mathbb{Q}(\zeta_N) \subseteq E$. In that case the cusps will be E-rational and the conditions of Theorem 3.2.2 will be fulfilled. In case of the modular curve we will find number fields as well. Since these number fields depend on the specific type of modular curve we will not discuss the several situations by now but we will do this for each case separately the first time they appear.

In Chapter 4 and Chapter 6 we will work with Fermat curves over cyclotomic fields. In several situations it will be important to distinguish between the cusps.

Notation 3.2.19. Let N be an odd squarefree integer and F_N the Fermat curve of exponent N. Furthermore we assume that we have fixed a primitive N-th root of unity ζ_N. Then we denote by S_{x_i} (S_{y_i}, S_{z_i} resp.) the cusp $(0 : \zeta_N^i : 1)$ ($(\zeta_N^i : 0 : 1)$, $(\zeta_N^i : -1 : 0)$ resp.). If the properties of the cusp, which are relevant for our consideration, do not depend on the exponent i we will drop the subscript and just write S_x (S_y, S_z resp.). For a normal model of the Fermat curve the Zariski-closure of a cusp gives us a horizontal prime divisor. If there is no danger of confusion which normal model we consider we will denote by $\mathcal{S}_{x_i}, \mathcal{S}_x, \mathcal{S}_{y_i}$, etc. the Zariski-closure of S_{x_i}, S_x, S_{y_i}, etc.

Chapter 4

Fermat curves of prime exponent

In this chapter we apply Theorem 3.2.2 to the regular model whose construction was given by McCallum. The results of this chapter build the basis for the preprint [CK].

4.1 Regular and minimal regular models of the Fermat curve of prime exponent

Let p be an odd prime number. In this section we are going to sketch the construction done by McCallum [Mc] of a regular model and the minimal model of the curve $F_p : X^p + Y^p = Z^p$ over $S = \operatorname{Spec} R$, where R is the localization of $\mathbb{Z}[\zeta_p]$ with respect to the prime ideal (π); here $\pi = 1 - \zeta_p$, where ζ_p is a primitive p-th root of unity. The prime ideal (π) lies above p; in fact since p is totally ramified in $\mathbb{Q}(\zeta_p)$ we have $p = u\pi^{p-1}$ with an element $u \in \mathbb{Z}[\zeta_p]^*$. Let us start with the model which is given by the normalization of the projective completion of the curve

$$X^p + Y^p = 1 \tag{4.1.1}$$

in $\mathbb{A}^2_S$. Reduction modulo π gives us $(X+Y-1)^p = 0$, hence the special fiber is non-regular and consists of one line which has multiplicity p. Moving this line to the X-axis[1], equation (4.1.1) becomes

$$-u\pi^{p-1}\phi(X, -Y-1) + u\pi^{p-1}\phi(Y) + Y^p = 0\,,$$

where

$$\phi(X, Y) := \frac{(X+Y)^p - X^p - Y^p}{p}$$

and $\phi(X) := \phi(X, 1)$. Now, by blowing up the line $\pi = Y = 0$, one obtains a model which is covered by two affine open sets U_1 and U_2 which will be described in the following. We introduce new variables W and Z. Setting $Z = \frac{Y}{\pi}$, we have

$$U_1 = \operatorname{Spec}\left(R[X, Y, Z]/(Z\pi - Y, f_1(X, Y))\right) \tag{4.1.2}$$

[1] To be more precise, we make the coordinate change given by $X' = X$ and $Y' = Y + X - 1$. After that we redefine $X := X'$ and $Y := Y'$.

where

$$f_1(X,Y) = -u\phi(X,-Y-1) + u\phi(Y) + \pi Z^p\,;$$

setting $W = \frac{\pi}{Y}$ the second affine open set is $U_2 = \mathrm{Spec}\,(R[X,Y,W]/(WY-\pi, f_2(X,Y)))$ where

$$f_2(X,Y) = -uW^{p-1}\phi(X,-Y-1) + uW^{p-1}\phi(Y) + Y\,.$$

The geometric special fiber $U_1 \times_S \mathrm{Spec}\,\overline{k(\pi)} \cup U_2 \times_S \mathrm{Spec}\,\overline{k(\pi)}$ of this model consists of a component L (which is located just in U_2 and associated to the ideal of $R[X,Y,W]/(WY-\pi, f_2(X,Y))$ which is generated by the images of Y and W with respect to the canonical surjection) and components $L_x, L_y, L_{\alpha_1}, \ldots, L_{\alpha_r}, L_{\beta_1}, \ldots, L_{\beta_s}$ which intersect L and correspond to the different roots of the polynomial

$$\phi(X,-1) = -X(X-1)\prod_{i=1}^{r}(X-\alpha_i)^2\prod_{j=1}^{s}(X-\beta_j)\,;$$

we have $\alpha \in k(\pi)$, $\alpha \neq 0,1$ and $\beta \notin k(\pi)$. The L_{α_i} appear with multiplicity 2 whereas all other components with multiplicity 1. There is also a line L_z crossing the point at infinity on L, which we cannot see in this affine model. There are just singularities left on the double lines L_{α_i}. Blowing up these singularities we achieve new components $L_{\alpha_{i,j}}$ crossing L_{α_i}. All components have genus 0. For later applications we define the index set

$$I := \{x, y, z, \beta_j, \alpha_i, \alpha_{i,j}, \ldots\}\,. \tag{4.1.3}$$

Let us denote the model we achived by $\mathfrak{F}_p$. The scheme $\mathfrak{F}_p$ is a regular model and its geometric special fiber $\mathfrak{F}_p \times_{\mathrm{Spec}\,R} \mathrm{Spec}\,\overline{k(\pi)}$ corresponding to (π) has the configuration as in Figure 4.1; the pair (n,m) indicates the multiplicity n and the self-intersection m of the component ([Mc], Theorem 3.).

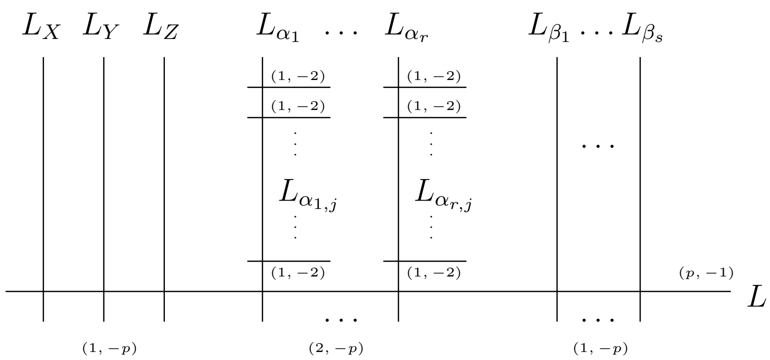

Figure 4.1: The configuration of the geometric special fiber $\mathfrak{F}_p \times_{\mathrm{Spec}\,R} \mathrm{Spec}\,\overline{k(\pi)}$. All components have genus 0. The only component with self-intersection number -1 is L.

Remark 4.1.1. If we now blow down the curve L (which is the only one with self-intersection -1), we get the minimal regular model $\mathfrak{F}_p^{min}$ (cf. Section 2.2).

Remark 4.1.2. A regular model over $\mathbb{Z}[\zeta_p]$ can be obtained by glueing the model $\mathfrak{F}_p$ over S and the smooth model of F_p over $\operatorname{Spec}\mathbb{Z}[\zeta_p] \setminus \{(\pi)\}$. We will denote this model as well by $\mathfrak{F}_p$ (cf. Section 2.3).

Remark 4.1.3. The morphism $\beta : F_p \to \mathbb{P}^1$ in (3.2.12) induces a morphism $\beta : \mathfrak{F}_p^0 \to \mathbb{P}^1_{\mathbb{Z}[\zeta_p]}$ of surfaces: here $\mathfrak{F}_p^0$ is the surface over $\operatorname{Spec}\mathbb{Z}[\zeta_p]$ that is given by the same equation as F_p. Since $\mathfrak{F}_p$ was obtained as a sequence of blowing-ups of $\mathfrak{F}_p^0$ the morphism (3.2.12) extends to a morphism of arithmetic surfaces

$$\beta : \mathfrak{F}_p \to \mathbb{P}^1_{\mathbb{Z}[\zeta_p]}\,. \tag{4.1.4}$$

4.2 Explicit geometric contributions to Kühn's formula for $\overline{\omega}^2_{\mathbf{Ar}}$ in the prime exponent case

Let p be a prime number with $p > 3$ and $\mathfrak{F}_p$ the regular model described in Section 4.1.

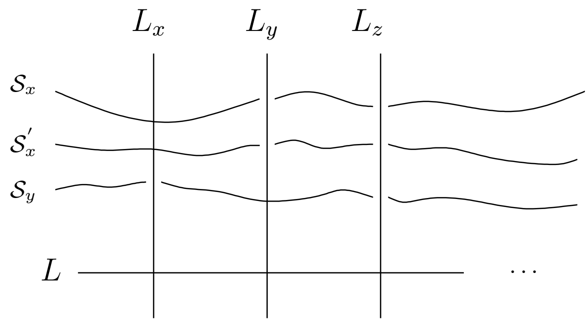

Figure 4.2: The divisors $\mathcal{S}_x, \mathcal{S}_x'$ and $\mathcal{S}_y$, where $\mathcal{S}_x'$ is coming from another cusp of the form $(0 : \zeta_p^j : 1)$.

Proposition 4.2.1. *To distinguish between the cusp of F_p we use Notation 3.2.19. Let $\mathcal{S}$ and $\mathcal{S}'$ be horizontal divisors of $\mathfrak{F}_p$ coming from different cusps S and S' on F_p. Then the following properties are true:*

1. *$\mathcal{S}$ does not intersect $\mathcal{S}'$.*

2. *If $\mathcal{S} = \mathcal{S}_x$ ($\mathcal{S}_y, \mathcal{S}_z$ resp.), then $\mathcal{S}$ only intersects the component L_x (L_y, L_z resp.) in the special fiber $\mathfrak{F}_p \times_{\operatorname{Spec}\mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\pi)$ (see figure 4.2).*

Proof: If we talk about a cusp in the following, we will mean a point of the form $(0 : \zeta_p^i - 1 : 1)$ ($(\zeta_p^i : \zeta_p^i - 1 : 1)$ resp.) which is just S_x (S_y resp.) after the transformation of the line $X + Y = 1$ to the X-axis (cf. Section 4.1).
Now let $\mathcal{S}, \mathcal{S}'$ be two horizontal divisors on $\mathfrak{F}_p$ associated with cusps S, S' and let $Q \in \operatorname{Supp} \mathcal{S} \cap \operatorname{Supp} \mathcal{S}'$ be a point. We will denote by $\mathfrak{m}$ the maximal ideal corresponding to Q in an open affine neighborhood of Q. For each element (ideal resp.) in a ring that corresponds to an open affine subset of a fiber we will denote by the same symbol the image of this element (ideal resp.) in the ring that corresponds to the neighborhood of Q.
Let us analyze the different situations that may arise. If the cusps lie above different branch points, for example $S = (0 : \zeta_p^i - 1 : 1)$ and $S' = (\zeta_p^j : \zeta_p^j - 1 : 1)$, we have $X, X - \zeta_p^j \in \mathfrak{m}$. But then $\zeta_p^j \in \mathfrak{m}$ which is impossible since ζ_p^j is a unit. So let S and S' lie above the same branch point. Without loss of generality we may assume $S = (\zeta_p^i : \zeta_p^i - 1 : 1)$ and $S' = (\zeta_p^j : \zeta_p^j - 1 : 1)$. It is a basic result from number theory that $(\zeta_p^l - 1)/\pi$ is a unit in $\mathbb{Z}[\zeta_p]$ if $l \not\equiv 0 \mod p$. We will denote this unit by ϵ_l. If Q is a point in the fiber $\mathfrak{F}_p \times_{\operatorname{Spec} \mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\mathfrak{q})$, where $\mathfrak{q} \in \operatorname{Spec} \mathbb{Z}[\zeta_p]$, then $\mathfrak{q} \subseteq \mathfrak{m}$. On the other hand since $X - \zeta_p^i, X - \zeta_p^j \in \mathfrak{m}$ we have $\zeta_p^i - \zeta_p^j = \zeta_p^i(1 - \zeta_p^{j-i}) = \zeta_p^i \epsilon_{j-i} \pi$ and so $(\pi) \subseteq \mathfrak{m}$. Now if $\mathfrak{q}$ is different from (π) and so in particular coprime to (π) we have $1 \in \mathfrak{m}$ which gives us a contradiction again. It follows that the only possibility for Q to be in a special fiber is to be in the fiber of bad reduction $\mathfrak{F}_p \times_{\operatorname{Spec} \mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\pi)$. It follows that we can reduce our analyzation to the scheme $\mathfrak{F}_p \to \operatorname{Spec} R$ that was constructed at the beginning of the previous section. Now since S and S' are $\mathbb{Q}(\zeta_p)$-rational points $\mathcal{S}$ and $\mathcal{S}'$ are reduced to single points P and P' in this fiber. A direct computation shows that

$$M = \left(X - \zeta_p^i, \pi, Z - \epsilon_i\right)$$

and

$$M' = \left(X - \zeta_p^j, \pi, Z - \epsilon_j\right)$$

are the ideals corresponding to these points in the open affine subset U_1 (cf. Equation (4.1.2)). If we take a look at the affine open set U_1 we can easily verify that M and M' are indeed maximal ideals and that $\mathcal{S}$ and $\mathcal{S}'$ are reduced to these points in the fiber of bad reduction since

$$\pi \left(Z - \epsilon_i\right) = Y - \zeta_p^i + 1$$

and $\pi \left(Z - \epsilon_j\right) = Y - \zeta_p^j + 1$. Now if $P = P' = Q$ we have

$$\epsilon_i - \epsilon_j = \frac{\zeta_p^i - 1}{\pi} - \frac{\zeta_p^j - 1}{\pi} = \frac{\zeta_p^i - \zeta_p^j}{\pi} = \frac{\zeta_p^i(1 - \zeta_p^{j-i})}{\pi} = \zeta_p^i \epsilon_{j-i} \,.$$

and so $\zeta_p^i \epsilon_{j-i} \in \mathfrak{m}$. But since $\zeta_p^i \epsilon_{j-i} \in \mathbb{Z}[\zeta_p]^*$, this gives us a contradiction and we have completed the proof of (i).
Now let $S = (0 : \zeta_p^i - 1 : 1)$, so S is S_x after the transformation described in Section 4.1. Again $\mathcal{S} \cap \mathfrak{F}_p \times_{\operatorname{Spec} \mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\pi)$ is reduced to a single point P. Let M be the corresponding maximal ideal, so $M = (X, \pi, Z - \epsilon_i)$. The irreducible component L_x corresponds (in U_1) to the prime ideal $I = (\pi, X)$. Obviously $I \subset M$ and so P is in the component L_x in the

fiber of bad reduction (remember that the component L does not lie in U_1). Since $\mathcal{S}$ is only reduced to P it only intersects L_x. Similar computations for S_y and S_z yield (ii). $\square$

Now we are ready to compute the canonical divisor for the model $\mathfrak{F}_p$. In the Lemma 3.2.16 we saw that such a divisor can be constructed with a horizontal divisor $\mathcal{S}$ coming from a cusp and vertical divisors having support in the fibers above the bad primes. Now let S_x be a cusp (cf. Notation 3.2.19),

$$\mathcal{V}_x = \lambda_x L_x + \lambda_y L_y + \lambda_z L_z \tag{4.2.1}$$

and

$$\mathcal{V}_\Sigma = \sum_{i=1}^{r}\left(\sum_{j=1}^{p}\lambda_{\alpha_{i,j}}L_{\alpha_{i,j}} + \lambda_{\alpha_i}L_{\alpha_i}\right) + \sum_{j=1}^{s}\lambda_{\beta_j}L_{\beta_j}\,, \tag{4.2.2}$$

where

$$\lambda_x = \frac{2g-p}{p}\,, \tag{4.2.3}$$

$$\lambda_y = \lambda_z = \lambda_{\beta_j} = \lambda_{\alpha_{i,k}} = -\frac{p-2}{p} \text{ for all } i = 1,\dots,r \text{ and } j = 1,\dots,s\,, \tag{4.2.4}$$

$$\lambda_{\alpha_i} = -2\left(\frac{p-2}{p}\right) \text{ for all } i = 1,\dots,r\,. \tag{4.2.5}$$

Lemma 4.2.2. *The divisor*

$$\mathcal{K}_x = (2g-2)\mathcal{S}_x + \mathcal{V}_x + \mathcal{V}_\Sigma \tag{4.2.6}$$

is a canonical divisor. In particular $\mathcal{S}_x + \mathcal{F}_x$ with $\mathcal{F}_x = \frac{1}{(2g-2)}(\mathcal{V}_x + \mathcal{V}_\Sigma)$ satisfies (3.2.2) *(notice that $\mathcal{S}_x$ ($\mathcal{F}_x$ resp.) is one of the $\mathcal{S}_j$ ($\mathcal{F}_j$ resp.) in the notation of Theorem 3.2.2).*

Proof: First of all notice that L is not included in $\mathcal{K}_x$, since it is modulo the full fiber just a linear combination of the other components. From Lemma 3.2.16 we know that there exists a canonical divisor of the form (4.2.6) with (4.2.1) and (4.2.2) for some coefficients λ. Now, the whole idea of the proof is the repeating use of the adjunction formula (Theorem 1.4.9) combined with the fact that the genus of the components of the special fiber is zero (see [Mc], p.59: Theorem 3) in order to approve the choice of the coefficients λ we made in (4.2.3), (4.2.4) and (4.2.5). We start with the observation

$$2\lambda_{\alpha_{i,j}} = \lambda_{\alpha_i}\,. \tag{4.2.7}$$

Indeed, according to the adjunction formula $L_{\alpha_{i,j}}^2 + \mathcal{K}_x \cdot L_{\alpha_{i,j}} = 2g(L_{\alpha_{i,j}}) - 2$ and $L_{\alpha_{i,j}}^2 = -2$ (see previous section) we have

$$0 = L_{\alpha_{i,j}} \cdot \mathcal{K}_x = L_{\alpha_{i,j}} \cdot \left(\sum_{l=1}^{p}\lambda_{\alpha_{i,j}}L_{\alpha_{i,j}} + \lambda_{\alpha_i}L_{\alpha_i}\right) = \lambda_{\alpha_{i,j}}(-2) + \lambda_{\alpha_i}\,.$$

Now using (4.2.7) and the adjunction formula for L_{α_i}, we get

$$p-2 = L_{\alpha_i}\cdot\mathcal{K}_x = \sum_{j=1}^{p}\lambda_{\alpha_{i,j}} + \lambda_{\alpha_i}(-p) = \frac{p}{2}\lambda_{\alpha_i} - p\lambda_{\alpha_i} = -\frac{p}{2}\lambda_{\alpha_i}\,.$$

Similar computations yield λ_y, λ_z and the λ_{β_j}. Finally, one observes that

$$p-2 = \mathcal{K}_x\cdot L_x = (2g-2)\mathcal{S}_x\cdot L_x + \lambda_x L_x^2 = (2g-2)+\lambda_x(-p)$$

and with this we finish the first part of our proof. To show that $\mathcal{S}_x + \frac{1}{(2g-2)}\left(\mathcal{V}_x+\mathcal{V}_\Sigma\right)$ fulfills (3.2.2) is now a simple verification. □

With a view to this lemma we see that the vertical part of two divisors coming from cusps that lie over different branch points, say $\mathcal{K}_x$ and $\mathcal{K}_y$, just differs in the parts $\mathcal{V}_x$ and $\mathcal{V}_y$.

We now calculate certain intersection numbers, which will be used later to complete the computations of the coefficient $a_\mathfrak{p}$ in (3.2.4).

Lemma 4.2.3. *Let $\mathcal{V}_x$ and $\mathcal{V}_\Sigma$ be the divisor defined in* (4.2.1) *and* (4.2.2)*. Then we have*

$$\mathcal{V}_\Sigma\cdot\mathcal{V}_\Sigma = (p-3)(-p)\left(\frac{p-2}{p}\right)^2\,, \tag{4.2.8}$$

$$\mathcal{V}_x\cdot\mathcal{V}_x = (-p)\left(\frac{2g-p}{p}\right)^2 + (-2p)\left(\frac{p-2}{p}\right)^2 \tag{4.2.9}$$

and

$$\mathcal{V}_x\cdot\mathcal{V}_\Sigma = 0\,. \tag{4.2.10}$$

Proof: In all the computations in this proof we have to remember the coefficients we calculated in Lemma 4.2.2. Let us start by showing the equation (4.2.8). If we write $\mathcal{V}_\Sigma = \mathcal{V}_{\Sigma_\alpha} + \mathcal{V}_{\Sigma_\beta}$, where $\mathcal{V}_{\Sigma_\alpha}$ denotes the part with support in the L_α and $\mathcal{V}_{\Sigma_\beta}$ the part with support in the L_β, we have

$$\mathcal{V}_\Sigma\cdot\mathcal{V}_\Sigma = \mathcal{V}_{\Sigma_\alpha}\cdot\mathcal{V}_{\Sigma_\alpha} + \mathcal{V}_{\Sigma_\beta}\cdot\mathcal{V}_{\Sigma_\beta}\,,$$

since each of the components of $\mathcal{V}_{\Sigma_\alpha}$ does not intersect any component of $\mathcal{V}_{\Sigma_\beta}$ and vice versa. From Figure 4.1 we see that each L_{β_i} just intersects itself and that the number of self-intersection is $-p$. Since there are s lines L_{β_i}, we have

$$\mathcal{V}_{\Sigma_\beta}\cdot\mathcal{V}_{\Sigma_\beta} = s(-p)\left(\frac{p-2}{p}\right)^2\,.$$

Now let $\mathcal{K}$ be a canonical divisor. According to the adjunction formula, we have $\mathcal{K}\cdot L_{\alpha_{i,j}} = 0$ and, since each $L_{\alpha_{i,j}}$ just intersects the $\mathcal{V}_{\Sigma_\alpha}$ part of $\mathcal{K}$, the equation $0 = \mathcal{K}\cdot L_{\alpha_{i,j}} = \mathcal{V}_{\Sigma_\alpha}\cdot L_{\alpha_{i,j}}$. This yields

$$\mathcal{V}_{\Sigma_\alpha}\cdot\mathcal{V}_{\Sigma_\alpha} = \mathcal{V}_{\Sigma_\alpha}\cdot\sum_{i=1}^{r}\lambda_{\alpha_i}L_{\alpha_i} = \sum_{i=1}^{r}\lambda_{\alpha_i}\left(\mathcal{V}_{\Sigma_\alpha}\cdot L_{\alpha_i}\right)\,,$$

where each addend is

$$\lambda_{\alpha_i}\left(\mathcal{V}_{\Sigma_\alpha}\cdot L_{\alpha_i}\right)=\lambda_{\alpha_i}\left(\left(\sum_{i=1}^{p}\lambda_{\alpha_{i,j}}L_{\alpha_{i,j}}+\lambda_{\alpha_i}L_{\alpha_i}\right)\cdot L_{\alpha_i}\right)$$
$$=\lambda_{\alpha_i}\left(\frac{p}{2}\lambda_{\alpha_i}+\lambda_{\alpha_i}(-p)\right)$$
$$=-\frac{p}{2}\lambda_{\alpha_i}^2=2(-p)\left(\frac{p-2}{p}\right)^2 .$$

Since there are r lines L_{α_i}, we have

$$\mathcal{V}_\Sigma\cdot\mathcal{V}_\Sigma=(2r+s)(-p)\left(\frac{p-2}{p}\right)^2=(p-3)(-p)\left(\frac{p-2}{p}\right)^2$$

Next we show (4.2.9). The lines L_x,L_y and L_z only intersect themselves and each self-intersection number is $-p$. Now everything follows from the equations (4.2.3) and (4.2.4).

Finally, equation (4.2.10) follows since $\operatorname{Supp}\mathcal{V}_x\cap\operatorname{Supp}\mathcal{V}_\Sigma=\emptyset$. □

Lemma 4.2.4. *Let*

$$\mathcal{D}_x=\mathcal{S}_x+\mathcal{G}_x\,, \tag{4.2.11}$$

where $\mathcal{G}_x=\frac{1}{p}L_x$. Then the divisor $\mathcal{D}_x$ is associated with $\left(\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}}(1)\right)^{\otimes\frac{1}{p^2}}$, or in other words

$$\mathcal{O}(\mathcal{D}_x)^{\otimes p^2}\cong\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}}(1)\,;$$

here β is the extension of the morphism $\beta:F_N\to\mathbb{P}^1$ (cf. Remark 4.1.3). In particular $\mathcal{S}_x+\mathcal{G}_x$ satisfies (3.2.3) *since the Zariski-closure $\overline{\infty}$ of ∞ in $\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}$ is associated with $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}}(1)$ (notice that $\mathcal{S}_x$ ($\mathcal{G}_x$ resp.) is one of the $\mathcal{S}_j$ ($\mathcal{G}_j$ resp.) in the notation of Theorem 3.2.2).*

Proof: Let S_x be a cusp and $Q\in\mathbb{P}^1_{\mathbb{Q}(\zeta_p)}$ the corresponding branch point. Since $\operatorname{Pic}(\mathbb{P}^1_{\mathbb{Q}(\zeta_p)})\cong\mathbb{Z}$ and $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Q}(\zeta_p)}}(1)$ is a generator of $\operatorname{Pic}(\mathbb{P}^1_{\mathbb{Q}(\zeta_p)})$ any divisor of degree 1 is associated with $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Q}(\zeta_p)}}(1)$. We choose Q to be this associated divisor. Now

$$\beta^*Q=\sum_{i=1}^{p}pS_i\,,$$

where S_i runs through the cusps lying above Q (we may assume without loss of generality $S_1=S_x$). If follows from Theorem 3.2.14 that $\beta^*Q=p^2S_x$ in $\operatorname{Cl}(F_p)_{\mathbb{Q}}$ and so p^2S_x is associated with $\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Q}(\zeta_p)}}(1)$. Since $\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}}(1)|_{F_p}\cong\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Q}(\zeta_p)}}(1)$ it is clear that we can find $\mathcal{D}_x$ with $\mathcal{O}(\mathcal{D}_x)^{\otimes p^2}\cong\beta^*\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_p]}}(1)$ and $\mathcal{D}_x=\mathcal{S}_x+\mathcal{G}_x$ where $\mathcal{G}_x$ is a vertical divisor having support in the special fiber $\mathfrak{F}_p \times_{\operatorname{Spec}\mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\pi)$ (Lemma 1.3.16). Now let I be the index set defined in (4.1.3). Since each component of the special fiber which is different from L is mapped to a single point by β, we have

$$(p^2\mathcal{D}_x) \cdot L_i = 0 \qquad (\forall i \in I) \tag{4.2.12}$$

(see [Liu], p. 398: Theorem 2.12 (a)). On the other hand we have

$$p^2 = p^2\mathcal{D}_x \cdot \mathfrak{F}_p \times_{\operatorname{Spec}\mathbb{Z}[\zeta_p]} \operatorname{Spec} k(\pi) = p^2\mathcal{D}_x \cdot pL \tag{4.2.13}$$

(see [Liu], p. 388: Remark 1.31.). Solving (4.2.12) and (4.2.13) we get $\mathcal{G}_x = \frac{1}{p}L_x$. $\square$

Theorem 4.2.5. *Let* $\mathcal{K}_x = (2g-2)(\mathcal{S}_x + \mathcal{F}_x)$ *be a canonical divisor as in* (4.2.6) *and* $\mathcal{D}_x = \mathcal{S}_x + \mathcal{G}_x$ *a divisor as in* (4.2.11), *where* x *indicates that this divisor belongs to a cusp* S_x. *Then*

$$\mathcal{F}_x \cdot \mathcal{F}_x = -\frac{p^3 - 7p^2 + 15p - 8}{p^2(p-3)^2},$$

and

$$\mathcal{G}_x \cdot \mathcal{G}_x = -\frac{1}{p}.$$

Proof: We have $\mathcal{F}_x^2 = \frac{1}{(2g-2)^2}\left(\mathcal{V}_x^2 + \mathcal{V}_\Sigma^2\right)$ by Lemma 4.2.2 and Lemma 4.2.3. Now again Lemma 4.2.3 together with $g = \frac{(p-1)(p-2)}{2}$ yield (after simplifying equations) our first claim. Since $\mathcal{G}_x = \frac{1}{p}L_x$ the second claim follows. $\square$

Now, we successfully prepared all the ingredients to calculate some intersection numbers for the Fermat curves.

Theorem 4.2.6. *Let* $\mathfrak{F}_p$ *be the regular model of the fermat curve* F_p *over* $\operatorname{Spec}\mathbb{Z}[\zeta_p]$ *which was constructed in Section 4.1. Then the arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$\overline{\omega}^2_{\mathfrak{F}_p,\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_p):\mathbb{Q}]\,(\kappa_1\log p + \kappa_2) + \frac{p^2-4p+2}{p(p-3)}\log p\right),$$

where $\kappa_1, \kappa_2 \in \mathbb{R}_+^*$ *are positive constants independent of* p.

Proof: In Remark 4.1.3 and Remark 3.2.18 we saw that the morphism $\beta : \mathfrak{F}_p \to \mathbb{P}^1_{\mathbb{Z}[\zeta_p]}$ is a morphism of arithmetic surfaces as in Assumption 3.2.1 and that the induced morphism $\beta : F_p \to \mathbb{P}^1$ fulfills the requirements of Theorem 3.2.2. Since $\beta^*\infty = \sum_{i=1}^{p} pS_i$ we have $b_j = b_{\max} = p$. The morphism β is of degree p^2. It follows with Theorem 4.2.5, Lemma

4.2.2 and Lemma 4.2.4 that in our case the formula (3.2.4) of Theorem 3.2.2 becomes

$$\begin{aligned}\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) = a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) &= -2g\overline{\mathcal{O}}(\mathcal{G}_j)^2 + (2g-2)\overline{\mathcal{O}}(\mathcal{F}_j)^2 \\ &= -2g{\mathcal{G}_j}^2 \log p + (2g-2){\mathcal{F}_j}^2 \log p \\ &= \frac{2g}{p} \log p - (2g-2)\frac{p^3 - 7p^2 + 15p - 8}{p^2(p-3)^2} \log p \\ &= \frac{p^2 - 4p + 2}{p(p-3)} \log p.\end{aligned}$$

□

4.2.1 $\overline{\omega}^2_{\mathbf{Ar}}$ for the minimal regular model of F_p

In Section 4.1 we have seen that we get a minimal regular model $\mathfrak{F}_p^{min}$ of F_p if we blow down the component L of the special fiber. Let $\pi : \mathfrak{F}_p \to \mathfrak{F}_p^{min}$ denote this blowing-down. Then there exists a vertical divisor $\mathcal{W}$ on $\mathfrak{F}_p$ (with support in the special fiber above the bad prime) such that $\pi^*\omega_{\mathfrak{F}_p^{min}} = \omega_{\mathfrak{F}_p} \otimes \mathcal{O}(\mathcal{W})$. We have

$$\overline{\omega}^2_{\mathfrak{F}_p^{min},\mathrm{Ar}} = \pi^*\overline{\omega}^2_{\mathfrak{F}_p^{min},\mathrm{Ar}} = \overline{\omega}^2_{\mathfrak{F}_p,\mathrm{Ar}} + 2\overline{\omega}_{\mathfrak{F}_p} \cdot \overline{\mathcal{O}}(\mathcal{W}) + \overline{\mathcal{O}}(\mathcal{W})^2 .$$

Proposition 4.2.7. *With the notation from above we have*

$$2\overline{\omega}_{\mathfrak{F}_p} \cdot \overline{\mathcal{O}}(\mathcal{W}) + \overline{\mathcal{O}}(\mathcal{W})^2 = (2p^2 - 10p + 13) \log p.$$

Proof: We start by computing the canonical divisor $\mathcal{K}_x^{min}$ of $\mathfrak{F}_p^{min}$, so the divisor with $\mathcal{O}(\mathcal{K}_x^{min}) \cong \omega_{\mathfrak{F}_p^{min}}$. Let $\widetilde{L}_u := \pi L_u$, where $u \in I$ and I is the index set (4.1.3). In order to compute intersections of the $\widetilde{L}_u$ we need to find their pullback and then compute everything on $\mathfrak{F}_p$. We have $\pi^*\widetilde{L}_u = L_u$ for $u = \alpha_{i,j}$ and

$$\pi^*\widetilde{L}_u = L_u + L$$

for all other u. Indeed, let for instance $u = x$. Then we have $\pi^*\widetilde{L}_x = L_x + \mu_x L$, where μ_x is a rational number. It follows that $0 = L \cdot \pi^*\widetilde{L}_x = 1 - \mu_x$ (see [Liu], p.398: Theorem 2.12. (a)).
The canonical divisor on $\mathfrak{F}_p^{min}$ is given by

$$\mathcal{K}_x^{min} = (2g-2)(\mathcal{S}_x + \frac{1}{p}\widetilde{L}_x) .$$

To verify this we just need to prove that $\mathcal{K}_x^{min}$ satisfies the adjunction formula and restricts to the canonical divisor K_x of the generic fiber F_p (see Proposition 1.4.16). The second property is obviously fulfilled. In order to verify the adjunction formula one has to check that it is valid for each irreducible component of the special fiber. We will illustrate this for the component $\widetilde{L}_x$ and leave the rest to the reader since the computations are very similar. We have

$$\begin{aligned}
\mathcal{K}_x^{min} \cdot \widetilde{L}_x &= (2g-2)(\mathcal{S}_x \cdot \widetilde{L}_x + \frac{1}{p}\widetilde{L}_x^2) \\
&= (2g-2)(1 + \frac{1}{p}(L_x + L)^2) \\
&= p(p-3)(1 - \frac{1}{p}(p-1)) = (p-3)
\end{aligned}$$

(see [Liu], p.398: Theorem 2.12. (c) for the second equality). On the other hand

$$2p_a(\widetilde{L}_x) - 2 - \widetilde{L}_x^2 = -2 - (L_x + L)^2 = (p-3)$$

and so the formula is valid for $\widetilde{L}_x$. The pullback of the canonical divisor is

$$\pi^*\mathcal{K}_x^{min} = (2g-2)(\mathcal{S}_x + \frac{1}{p}L_x + \frac{1}{p}L)$$

and an easy computation shows that

$$\mathcal{W} = -\lambda_y L_y - \lambda_z L_z - \frac{(2-p)}{p}L_x - \mathcal{V}_\Sigma + \frac{2g-2}{p}L$$

fulfills $\pi^*\mathcal{K}_x^{min} = \mathcal{K}_x + \mathcal{W}$. It follows that we have to compute $(2\mathcal{K}_x \cdot \mathcal{W} + \mathcal{W}^2)\log p$ in order to get $2\overline{\omega}_{\mathfrak{F}_p} \cdot \overline{\mathcal{O}}(\mathcal{W}) + \overline{\mathcal{O}}(\mathcal{W})^2$. Since we have $\mathcal{W} \cdot (2\mathcal{K}_x + \mathcal{W}) = \mathcal{W} \cdot (\mathcal{K}_x + \pi^*\mathcal{K}_x^{min})$ we may compute $\mathcal{W} \cdot \mathcal{K}_x$ and $\mathcal{W} \cdot \pi^*\mathcal{K}_x^{min}$. Using the adjunction formula and linearity we get

$$\begin{aligned}
\mathcal{W} \cdot \mathcal{K}_x &= (p-2)\left(-\lambda_y - \lambda_z - \left(\frac{2-p}{p}\right)\right) - \mathcal{V}_\Sigma \cdot \mathcal{K}_x - \left(\frac{2g-2}{p}\right) \\
&= 3\left(\frac{(p-2)^2}{p}\right) - \mathcal{V}_\Sigma^2 - \left(\frac{p(p-3)}{p}\right) \\
&= (p-2)^2 - (p-3)\,.
\end{aligned}$$

On the other hand we have

$$\begin{aligned}
\mathcal{W} \cdot \pi^*\mathcal{K}_x^{min} &= \mathcal{W} \cdot (p(p-3)\mathcal{S}_x + (p-3)L_x + (p-3)L) \\
&= (p-2)(p-3) - (p-2)(p-3) + (p-3)^2 + (p-3)\mathcal{W} \cdot L \\
&= (p-3)^2 + (p-3)\left(-\lambda_y - \lambda_z - \frac{2-p}{p} + \frac{p-2}{p}(p-3) - (p-3)\right) \\
&= (p-3)^2 + (p-3)(p-2) - (p-3)^2 = (p-2)(p-3)
\end{aligned}$$

and so $2\overline{\omega}_{\mathfrak{F}_p} \cdot \overline{\mathcal{O}}(\mathcal{W}) + \overline{\mathcal{O}}(\mathcal{W})^2 = (2p^2 - 10p + 13)\log p$. □

Theorem 4.2.8. *Let $\mathfrak{F}_p^{min}$ be the minimal regular model of the fermat curve F_p over* $\operatorname{Spec}\mathbb{Z}[\zeta_p]$ *from Section 4.1. Then the arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$\overline{\omega}^2_{\mathfrak{F}_p^{min},\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_p):\mathbb{Q}]\,(\kappa_1\log p+\kappa_2) + \frac{3p^2-14p+15}{p(p-3)}\log p\right),$$

where $\kappa_1,\kappa_2\in\mathbb{R}_+^*$ are positive constants independent of p.

Proof: This follows directly from Theorem 4.2.6 and Proposition 4.2.7. □

Remark 4.2.9. Since $|\mathbb{Q}(\zeta_p):\mathbb{Q}| = \varphi(p) = p-1$ it is obvious that - independent of κ_1 and κ_2 - the analytic contribution $[\mathbb{Q}(\zeta_p):\mathbb{Q}]\,(\kappa_1\log p+\kappa_2)$ will dominate the geometric contribution $\frac{3p^2-14p+15}{p(p-3)}\log p$ for big prime numbers p.

Corollary 4.2.10. *With the notation from the Theorem 4.2.8 we have:*

$$\overline{\omega}^2_{\mathfrak{F}_p^{min},\mathrm{Ar}} \leq (2g-2)\varphi(p)\left((2+\kappa_1)\log p+\kappa_2\right) + \mathcal{O}(g\log p) \tag{4.2.14}$$

Proof: It is a well known fact that $\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}} = (-1)^{\frac{\varphi(p)}{2}}\left(\frac{p^{\varphi(p)}}{p}\right)$ and $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = \varphi(p)$ and so Theorem 4.2.8 yields

$$\begin{aligned}\overline{\omega}^2_{\mathfrak{F}_p,\mathrm{Ar}} &\leq (2g-2)\left(2\log\frac{p^{\varphi(p)}}{p} + \varphi(p)\,(\kappa_1\log p+\kappa_2) + \frac{3p^2-14p+15}{p(p-3)}\log p\right)\\ &= (2g-2)\left(\varphi(p)\left((2+\kappa_1)\log p+\kappa_2\right) + \frac{p-5}{p}\log p\right),\end{aligned}$$

hence we obtain the asymptotic bound we claimed. □

Chapter 5

Some modular curves

In this chapter we describe how to compute the quantities $\mathcal{G}_j$ and $\mathcal{F}_j$ defined in (3.2.3) and (3.2.2) in a situation that covers many cases of the modular curves $X_0(N)$ and $X(N)$. Regular models of these curves have been determined by Deligne and Rapoport [DR]; the latter one as well by Katz and Mazur via moduli interpretation [KM]. We will give a short review of the models we are interested in, similar to the review given in [Kü2] Chapter 6 and Chapter 9. Furthermore, we will use our computation in order to apply Theorem 3.2.2 to specific cases (see as well footnote below).

5.1 The general situation

Assumption 5.1.1. We consider the following situation: Let E be a number field with ring of integers $\mathcal{O}_E$ and $\beta : \mathcal{X} \to \mathcal{Y}$ a morphism of arithmetic $\operatorname{Spec}\mathcal{O}_E$-surfaces as it is described in Assumption 3.2.1; we denote by β the induced morphism of the algebraic curves X and Y that are given by the generic fibers of $\mathcal{X}$ and $\mathcal{Y}$. Furthermore, we assume $\mathcal{Y}$ to be smooth. Let us assume for simplicity that there is just one bad prime ideal $\mathfrak{p} \subset \mathcal{O}_E$, and that the special fiber of $\mathcal{X}$ above $\mathfrak{p}$ consists of $r_{\mathfrak{p}} = n + 1$ components $\mathcal{C}_0, \dots \mathcal{C}_n$ of multiplicity one[1] with $\beta(\mathcal{C}_i) = \mathcal{D}$, where $\mathcal{D}$ is the special fiber of $\mathcal{Y}$ above $\mathfrak{p}$; all components intersect each other in a set of points which we will call the supersingular points (Figure 5.1). The intersections are transverse and we denote the number of supersingular points by s. We set

$$d = \deg \beta \tag{5.1.1}$$

and

$$d_i = \deg \beta|_{\mathcal{C}_i} = |K(\mathcal{C}_i) : K(\mathcal{D})| \, . \tag{5.1.2}$$

Notice that we have

$$d = \sum_{i=0}^{n} d_i \, ,$$

[1] The cases with multiplicity greater than one can be handled with a little extra work with the same strategy.

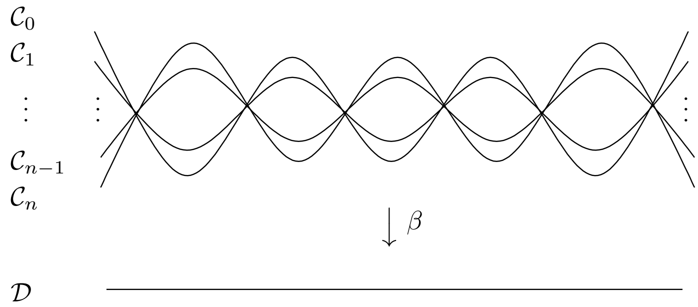

Figure 5.1: The special fibers above $\mathfrak{p}$ of the arithmetic surfaces. All components $\mathcal{C}_0, \dots, \mathcal{C}_n$ are mapped to the component $\mathcal{D}$ and intersect each other in the supersingular points.

since the multiplicity of the $\mathcal{C}_i$ is one. Let $\infty \in Y$ be a E-rational ramified point and

$$\beta^* \infty = \sum_j b_j S_j \, . \tag{5.1.3}$$

We assume that the S_j are E-rational and that any divisor of degree zero with support in them is torsion. For a S_j we denote by $\mathcal{S}_j$ the Zariski-closure of S_i in $\mathcal{X}$. It follows that in this situation the Theorem 3.2.2 is applicable.

Remark 5.1.2. Notice that we have now all the information we need to apply Proposition 3.2.9 and Theorem 3.2.10 to get an approximation of the geometric contribution. In this subsection we are going to compute the geometric contribution explicitly (Theorem 5.1.6 and Theorem 5.1.9).

In order to compute the geometric contribution exactly we start by determining the vertical divisor $\mathcal{G}_j$ defined in (3.2.3). The divisor $\mathcal{G}_j$ has to satisfy

$$d(\mathcal{S}_j + \mathcal{G}_j) \cdot \mathcal{C}_i = \beta^* \overline{\infty} \cdot \mathcal{C}_i$$

for $0 \leq i \leq n$. On the other hand, we have

$$\beta^* \overline{\infty} \cdot \mathcal{C}_i = \overline{\infty} \cdot d_i \mathcal{D} = d_i$$

for $0 \leq i \leq n$ (see e.g. [Liu], p.398: Theorem 2.12. (b)). Hence, we are searching for a vertical divisor $\mathcal{G}_j$, which satisfies

$$d(\mathcal{S}_j + \mathcal{G}_j) \cdot \mathcal{C}_i = d_j \tag{5.1.4}$$

for all $0 \leq i \leq n$.

Given a column vector $\lambda = (\lambda_1, \ldots, \lambda_n)^t \in \mathbb{Q}^n$, we set

$$\mathcal{C}\lambda := \lambda_1 \mathcal{C}_1 + \ldots + \lambda_n \mathcal{C}_n \,.$$

Since the adding of a rational multiple of the whole fiber gives us another divisor which satisfies this equation, we can make the ansatz

$$\mathcal{G}_j = \mathcal{C}\lambda\,; \tag{5.1.5}$$

hence, we do not require $\mathcal{C}_0$. We know, that $\mathcal{S}_j$ just intersects one of the $\mathcal{C}_i$ and that this intersection is transverse (see e.g. [Liu], p.388: Remark 1.31. and Corollary 1.32.). Let us assume that $\mathcal{C}_k$ is this component. To indicate this dependence we will introduce a second subscript and write $\mathcal{G}_{j,k}$. Equation (5.1.4) becomes now

$$d(\mathcal{S}_j + \mathcal{G}_{j,k}) \cdot \mathcal{C}_i = d_j \tag{5.1.6}$$

for all $0 \le i \le n$. Solving this equation is nothing more than solving

$$C\lambda = D_k\,, \tag{5.1.7}$$

where $C \in \mathbb{Q}^{n\times n}$ is given by

$$C = \begin{pmatrix} -ns & & s \\ & \ddots & \\ s & & -ns \end{pmatrix},$$

and $D_k = D - e_k \in \mathbb{Q}^n$, where

$$D = \begin{pmatrix} \frac{d_1}{d} \\ \vdots \\ \frac{d_n}{d} \end{pmatrix},$$

e_0 is the zero vector, and e_k (for $k \neq 0$) is the column vector which has a 1 in the k-th position and zeros everywhere else (notice that C is just the intersection matrix). If we add all the rows of the augmented matrix $(C|D_k)$ it can be easily seen that

$$-s\lambda_1 - \ldots - s\lambda_n = \frac{\sum_{i=1}^n d_i}{d} - 1 = -\frac{d_0}{d}\,,$$

hence a solution λ of (5.1.7) solves (5.1.6) for $j = 0$ as well and is therefore indeed a solution of (5.1.4) for all j.

Notation 5.1.3. Analog to our way of redefining the vertical divisor $\mathcal{G}_{j,k}$ we have to redefine the ramification indices of the S_j: We will write $b_{j,k}$ if $\mathcal{S}_j$ intersects $\mathcal{C}_k$ (this notation is well defined, since each $\mathcal{S}_j$ just intersects one of the components $\mathcal{C}_i$).

Lemma 5.1.4. *We have* $\det C = (n+1)^{(n-1)}(-s)^n$*, hence* (5.1.7) *is uniquely solvable. Let us set*

$$W = \sum_{i=1}^{n} \frac{d_i}{d}\,, \tag{5.1.8}$$

$$a_k = -\frac{1}{(n+1)s}\left(We - e + D_k\right)\,,$$

for $k \neq 0$*, and*

$$a_0 = -\frac{1}{(n+1)s}\left(We + D\right)\,,$$

where $e \in \mathbb{Q}^n$ *is the column vector which has everywhere* 1 *as entry. Then a solution of* (5.1.6) *is given by* $\mathcal{G}_{j,k} = \mathcal{C}a_k$*.*

Proof: The formula for $\det C$ is a simple linear algebra exercise. That (5.1.7) is uniquely solvable follows since $\det C \neq 0$ or for example by Remark 3.2.6. We verify the second statement: Let $k \neq 0$. Then

$$\begin{aligned}
Ca_k &= -\frac{1}{(n+1)}\begin{pmatrix} -n & & 1 \\ & \ddots & \\ 1 & & -n \end{pmatrix}((W-1)e + D_k) \\
&= -\frac{1}{(n+1)}((1-W)e + \begin{pmatrix} -n & & 1 \\ & \ddots & \\ 1 & & -n \end{pmatrix} D_k) \\
&= -\frac{1}{(n+1)}\begin{pmatrix} -(n+1) & & 0 \\ & \ddots & \\ 0 & & -(n+1) \end{pmatrix} D_k = D_k\,,
\end{aligned}$$

which proves that our choice of a_k is in fact the solution. The verification for $k = 0$ follows in a similar manner. □

Corollary 5.1.5. *We have*

$$\mathcal{G}_{j,k}^2 = a_k^t C a_k = -\frac{1}{(n+1)s}\left(W^2 + \sum_{i=1}^{n}\left(\frac{d_i}{d}\right)^2\right) + \frac{2}{(n+1)s}\left(W + \frac{d_k}{d} - 1\right)\,,$$

for $k \neq 0$ *and*

$$\mathcal{G}_{j,0}^2 = a_0^t C a_0 = -\frac{1}{(n+1)s}\left(W^2 + \sum_{i=1}^{n}\left(\frac{d_i}{d}\right)^2\right)\,;$$

the row vector a_k^t *denotes the transpose of* a_k*, and* W *is defined by* (5.1.8)*.*

Proof: The first equality follows with (5.1.5) and the fact that C is the intersection matrix. Let $k \neq 0$. Then the second equality follows, because

$$\begin{aligned} a_k^t C a_k &= a_k^t D_k \\ &= -\frac{1}{(n+1)s}\left(\sum_{\substack{i=1\\ i\neq k}}^{n}\left((W-1)\frac{d_j}{d}+\left(\frac{d_j}{d}\right)^2\right)+(W-1)\frac{d_k}{d}-2\frac{d_k}{d}+\left(\frac{d_k}{d}\right)^2-W+2\right) \\ &= -\frac{1}{(n+1)s}\left(W^2-W+\sum_{i=1}^{n}\left(\frac{d_i}{d}\right)^2-2\frac{d_k}{d}-W+2\right). \end{aligned}$$

Again, a similar computation gives us the result for the $k=0$ case. □

The special fiber $\mathcal{X} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec} k(\mathfrak{p})$ is not smooth over $\operatorname{Spec} k(\mathfrak{p})$. Hence we cannot assume that the Cartier divisors are the Weil divisors in this situation. However the curves $\mathcal{C}_i$ are smooth and we have the following diagram of regular schemes

$$\begin{array}{ccc} \mathcal{C}_i & \xrightarrow{\ p|_{\mathcal{C}_i}\ } & \mathcal{X} \\ {\scriptstyle \beta|_{\mathcal{C}_i}}\downarrow & & \downarrow{\scriptstyle \beta} \\ \mathcal{Y} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec} k(\mathfrak{p}) & \xrightarrow[\ p_1\ ]{} & \mathcal{Y} \end{array} \tag{5.1.9}$$

where $\beta|_{\mathcal{C}_i}$ is the restriction of β to the component $\mathcal{C}_i$, p_1 is the first projection, and $p|_{\mathcal{C}_i}$ is the composition $p|_{\mathcal{C}_i} = p_1 \circ \iota$ of the closed immersion $\iota : \mathcal{C}_i \to \mathcal{X} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec} k(\mathfrak{p})$ followed by the first projection $p_1 : \mathcal{X} \times_{\operatorname{Spec}\mathcal{O}_E} \operatorname{Spec} k(\mathfrak{p}) \to \mathcal{X}$. Pullbacks with respect to $\beta|_{\mathcal{C}_i}$ exist (see e.g. [Liu], p.261: Lemma 1.33. (2)). The pullback $p_1^*\overline{\infty}$ ($(p|_{\mathcal{C}_i})^*\overline{\beta^*\infty}$ resp.) exists, because $\overline{\infty}$ ($\overline{\beta^*\infty}$ resp.) does not contain any irreducible component of the special fiber of $\mathcal{X}$ (cf. [Liu], p.260: Lemma 1.29 and p.261: Remark 1.30.). Since there are no vertical divisors in the special fiber of $\mathcal{X}$ which are mapped to a closed point of $\mathcal{Y}$ we have $\overline{\beta^*\infty} = \beta^*\overline{\infty}$ (cf. Remark 3.2.8). It follows that $(p|_{\mathcal{C}_i})^*\beta^*\overline{\infty}$ exists an we have

$$(\beta|_{\mathcal{C}_i})^* p_1^*\overline{\infty} = (p|_{\mathcal{C}_i})^*\beta^*\overline{\infty} \tag{5.1.10}$$

(see e.g. [Gr3] (21.4.4)). The pullback with respect to p_1 ($p|_{\mathcal{C}_i}$ resp.) of a horizontal divisor that came from an E-rational point is just a point of the special fiber with ramification index one (see e.g. [Liu], p.381: Theorem 1.12. (d) and p.388: Corollary 1.32.). Let $x = p_1^*\overline{\infty}$ be this point. Then it follows by (5.1.10) that

$$(\beta|_{\mathcal{C}_i})^* x = \sum_{\substack{j\\ \mathcal{S}_j\cdot\mathcal{C}_i=1}} b_{j,i}\mathcal{S}_j\,,$$

where $s_j = (p|_{\mathcal{C}_i})^* \mathcal{S}_j$. Combining this with (5.1.2) we get

$$d_i = \sum_{\substack{j \\ \mathcal{S}_j \cdot \mathcal{C}_i = 1}} b_{j,i} \,. \tag{5.1.11}$$

Theorem 5.1.6. *In the situation of Assumption 5.1.1 we have*

$$\sum_j b_j \mathcal{G}_j^2 = \frac{d}{(n+1)s} \left(\sum_{i=0}^{n} \left(\frac{d_i}{d} \right)^2 - 1 \right) ,$$

where the b_j *are given by* (5.1.3) *and the* $\mathcal{G}_j$ *are the vertical divisor of the special fiber above the bad prime* $\mathfrak{p}$ *which are defined by* (5.1.4) *(*(3.2.3) *resp.).*

Proof: We have

$$\sum_j b_j \mathcal{G}_j^2 = \sum_{i=0}^{n} \sum_{\substack{j \\ \mathcal{S}_j \cdot \mathcal{C}_i = 1}} b_{j,i} \mathcal{G}_{j,i}^2$$

(Notation 5.1.3). It follows by Corollary 5.1.5 and (5.1.11) that

$$\begin{aligned}
\sum_{i=0}^{n} \sum_{\substack{j \\ \mathcal{S}_j \cdot \mathcal{C}_i = 1}} b_{j,i} \mathcal{G}_{j,i}^2 &= \sum_{i=0}^{n} -\frac{d_i}{(n+1)s} \left(W^2 + \sum_{i=1}^{n} \left(\frac{d_i}{d} \right)^2 \right) + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} \left(W + \frac{d_i}{d} - 1 \right) \\
&= -\frac{d}{(n+1)s} \left(W^2 + \sum_{i=1}^{n} \left(\frac{d_i}{d} \right)^2 \right) + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} \left(W + \frac{d_i}{d} - 1 \right) \\
&= -\frac{d}{(n+1)s} \sum_{i=0}^{n} \left(\frac{d_i}{d} \right)^2 + \frac{d}{(n+1)s} \left(\frac{2d_0}{d} - 1 \right) + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} \left(\frac{d_i - d_0}{d} \right) \\
&= \frac{d}{(n+1)s} \sum_{i=0}^{n} \left(\frac{d_i}{d} \right)^2 - \frac{d}{(n+1)s} \,,
\end{aligned}$$

where we used a few times $W = 1 - \frac{d_0}{d}$ (which is equivalent to $\sum_{i=0}^{n} d_i = d$). □

Next we want to compute the $\mathcal{F}_j$ defined in (3.2.2). The vertical divisor we are looking for has to fulfill

$$(2g-2)(\mathcal{S}_j + \mathcal{F}_j) \cdot \mathcal{C}_i = \mathcal{K} \cdot \mathcal{C}_i \tag{5.1.12}$$

for $0 \le i \le n$, where $\mathcal{K}$ is a canonical divisor of $\mathcal{X}$ and g is the genus of the curve X. Let us assume that the horizontal divisor $\mathcal{S}_j$ intersects the component $\mathcal{C}_k$. Analog to the previous situation we make the ansatz

$$\mathcal{F}_{j,k} = \mathcal{C}\lambda \,, \tag{5.1.13}$$

where we changed - as we did in the case of the $\mathcal{G}_{j,k}$ - the notation of the $\mathcal{F}_j$ to $\mathcal{F}_{j,k}$ (now our notation indicates the cusp S_j we used and the vertical divisor $\mathcal{C}_k$ which is intersected by $\mathcal{S}_j$). Let us set

$$\mathcal{K}_i = \frac{\mathcal{K} \cdot \mathcal{C}_i}{(2g-2)} \,. \tag{5.1.14}$$

Notice that $\sum_{i=0}^{n} \mathcal{K}_i = 1$, since $\mathcal{K} \cdot (\mathcal{C}_0 + \ldots + \mathcal{C}_n) = 2g-2$. Then the problem of solving

$$(2g-2)(\mathcal{S}_j + \mathcal{F}_{j,k}) \cdot \mathcal{C}_i = \mathcal{K} \cdot \mathcal{C}_i \tag{5.1.15}$$

for $0 \leq i \leq n$ may be reformulated as finding the vector

$$\lambda = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

which satisfies

$$K - e_k = C\lambda \,,$$

where C and e_k are defined as before and $K = (\mathcal{K}_1, \ldots, \mathcal{K}_n)^t$. We denote by K_k the column vector $K - e_k$.

Lemma 5.1.7. *Let us set*

$$V = \sum_{i=1}^{n} \mathcal{K}_i \,, \tag{5.1.16}$$

and

$$a_k = -\frac{1}{(n+1)s} \left(Ve - e + K_k \right) \,,$$

for $k \neq 0$, and

$$a_0 = -\frac{1}{(n+1)s} \left(Ve + K \right) \,,$$

where $e \in \mathbb{Q}^n$ is the column vector which has everywhere 1 as entry, and the $\mathcal{K}_i$ are defined by (5.1.14). Then a solution of (5.1.15) is given by $\mathcal{F}_{j,k} = \mathcal{C}a_k$.

Proof: The proof is totally analog to the one of Lemma 5.1.4. $\square$

Corollary 5.1.8. *We have*

$$\mathcal{F}_{j,k}^2 = a_k^t C a_k = -\frac{1}{(n+1)s} \left(V^2 + \sum_{i=1}^{n} \mathcal{K}_i^2 \right) + \frac{2}{(n+1)s} \left(V + \mathcal{K}_k - 1 \right) \,,$$

for $k \neq 0$ and

$$\mathcal{F}_{j,0}^2 = a_0^t C a_0 = -\frac{1}{(n+1)s} \left(V^2 + \sum_{i=1}^{n} \mathcal{K}_i^2 \right) \,;$$

the row vector a_k^t denotes the transpose of a_k, V and $\mathcal{K}_i$ are given by (5.1.16) and (5.1.14).

Proof: The proof is the same as in Corollary 5.1.5, one just has to interchange the symbols. $\square$

Theorem 5.1.9. *In the situation of Assumption 5.1.1 we have*

$$\sum_j b_j \mathcal{F}_j^2 = -\frac{d}{(n+1)s} \sum_{i=0}^{n} \mathcal{K}_i^2 + \frac{2}{(n+1)s} \sum_{i=0}^{n} d_i \mathcal{K}_i - \frac{d}{(n+1)s},$$

where the b_j are given by (5.1.3) *and the $\mathcal{F}_j$ are the vertical divisor of the special fiber above the bad prime $\mathfrak{p}$ which are defined by* (5.1.12) *(*(3.2.2) *resp.).*

Proof: It follows by Corollary 5.1.8 and equation (5.1.11) that

$$\begin{aligned}
\sum_j b_j \mathcal{F}_j^2 &= \sum_{i=0}^{n} \sum_{\substack{j \\ \mathcal{S}_j \cdot \mathcal{C}_i = 1}} b_{j,i} \mathcal{F}_{j,i}^2 \\
&= -\frac{d}{(n+1)s} \left(V^2 + \sum_{i=1}^{n} \mathcal{K}_i^2 \right) + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} (V + \mathcal{K}_i - 1) \\
&= -\frac{d}{(n+1)s} \sum_{i=0}^{n} \mathcal{K}_i^2 + \frac{d}{(n+1)s} (2\mathcal{K}_0 - 1) + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} (\mathcal{K}_i - \mathcal{K}_0) \\
&= -\frac{d}{(n+1)s} \sum_{i=0}^{n} \mathcal{K}_i^2 + \frac{2d}{(n+1)s} \mathcal{K}_0 - \frac{d}{(n+1)s} + \sum_{i=1}^{n} \frac{2d_i}{(n+1)s} \mathcal{K}_i + \frac{2(d_0 - d)}{(n+1)s} \mathcal{K}_0,
\end{aligned}$$

where we used $V = 1 - \mathcal{K}_0$. $\square$

Corollary 5.1.10. *If all the genera of the $\mathcal{C}_i$ are the same, then*

$$\sum_j b_j \mathcal{F}_j^2 = -\frac{dn}{(n+1)^2 s},$$

where the b_j are given by (5.1.3) *and the $\mathcal{F}_j$ are the vertical divisor of the special fiber above the bad prime $\mathfrak{p}$ which are defined by* (5.1.12) *(*(3.2.2) *resp.).*

Proof: Let us set $g_{\mathcal{C}} := g(\mathcal{C}_i)$. By the adjunction formula 1.4.9 we have

$$2g - 2 = \mathcal{K} \cdot (\mathcal{C}_0 + \ldots + \mathcal{C}_n) = (n+1)(2g_{\mathcal{C}} - 2 + ns),$$

hence

$$\mathcal{K}_i = \frac{2g_{\mathcal{C}} - 2 + ns}{(n+1)(2g_{\mathcal{C}} - 2 + ns)} = \frac{1}{n+1}.$$

Substitution of this into the equation of Theorem 5.1.9 gives the claim. $\square$

Remark 5.1.11. Since the computation of $\overline{\mathcal{O}}(\mathcal{G}_j)^2$ and $\overline{\mathcal{O}}(\mathcal{F}_j)^2$ in (3.2.4) can be done fiber by fiber (cf. Remark 3.2.6) we can easily extend the situation of Assumption 5.1.1 and its associated results (Theorem 5.1.6 and Theorem 5.1.9) to situations with more than one bad prime.

5.2 The minimal regular model of $X_0(N)$

Now we are going to apply the results of the previous subsection to the modular cuver $X_0(N)$ for certain values of N.

Remark 5.2.1. Let N be a squarefree natural number coprime to 6 which has at least two prime factors, and whose prime factors p fulfill $p \equiv 1, 3$ or $9 \mod 12$. Then it is shown in [Kü2] Chapter 7 that the minimal regular model $\mathcal{X}_0(N)$ of $X_0(N)$ together with the natural morphism $\beta : \mathcal{X}_0(N) \to \mathcal{X}(1)$ fulfills the requirement of Assumption 5.1.1 (see also Remark 5.1.11). In fact, with the notation from Assumption 5.1.1 we have $d = \prod_{p|N}(p+1)$, $s = d\frac{p-1}{12(p+1)}$, $n = 1$, $d_0 = \frac{pd}{p+1}$ and $d_1 = \frac{d}{p+1}$.

Lemma 5.2.2. *In the situation of Remark 5.2.1 we have*

$$\sum_j b_j \overline{\mathcal{O}}(\mathcal{G}_j)^2 = -12 \sum_{p|N} \frac{p}{p^2-1} \log p$$

and

$$\sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_j)^2 = -3 \log N - \sum_{p|N} \frac{6}{p-1} \log p\,,$$

where $\mathcal{G}_j$ and $\mathcal{F}_j$ are the vertical divisors defined in (3.2.3) *and* (3.2.2)*.*

Proof: The morphism β fulfills the conditions of Theorem 3.2.2 by the discussion above. We have

$$\overline{\mathcal{O}}(\mathcal{G}_j)^2 = \sum_{p|N} \overline{\mathcal{O}}(\mathcal{G}_{j,p})^2,\ \overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{p|N} \overline{\mathcal{O}}(\mathcal{F}_{j,p})^2\,, \tag{5.2.1}$$

where $\mathcal{G}_{j,p}$ ($\mathcal{F}_{j,p}$ resp.) denotes the part of the vertical divisor $\mathcal{G}_j$ ($\mathcal{F}_j$ resp.) which has support in the special fiber above p. Let us fix a bad prime p. Then by Theorem 5.1.6 it follows

$$\begin{aligned}\sum_j b_j \overline{\mathcal{O}}(\mathcal{G}_{j,p})^2 &= \frac{6(p+1)}{p-1}\left(\left(\frac{p}{p+1}\right)^2 + \left(\frac{1}{p+1}\right)^2 - 1\right)\log p \\ &= \frac{-12p}{p^2-1}\log p\,.\end{aligned}$$

Since $\mathcal{C}_0$ and $\mathcal{C}_\infty$ are copies of the same curve, their genus is the same. Hence, we can apply Corollary 5.1.10 and get

$$\begin{aligned}\sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_{j,p})^2 &= -\frac{12(p+1)}{2^2(p-1)}\log p \\ &= -\frac{3(p+1)}{p-1}\log p\,.\end{aligned}$$

Now, we use equation (5.2.1) and sum up over the bad primes. Simplifying the derived equations yields our claim. □

Remark 5.2.3. The results of Lemma 5.2.2 are not new. They have been computed already by U. Kühn in [Kü2] (Lemma 7.3. and Lemma 7.4). In his paper U. Kühn computes the quantities $\sum_j b_j \overline{\mathcal{O}}(\mathcal{G}_j)^2$ and $\sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_j)^2$ for more values of N (in this case vertical components can appear which are mapped to a point by β). Unfortunately our approach does not attack these cases. Our approach is a generalization of the computation of the other cases. The advantage is that it can be applied to other modular curves whose special fiber of the (minimal) regular models looks similar to the one of $\mathcal{X}_0(N)$ for the values of N in Remark 5.2.1.

Remark 5.2.4. In [Kü2] the results are used to compute an upper bound for $\overline{\omega}^2_{\mathcal{X}_0(N),\mathrm{Ar}}$. It leads to the bound

$$\overline{\omega}^2_{\mathcal{X}_0(N),\mathrm{Ar}} \leq (16\pi\kappa_\circ - 1)g\log(N) + \mathcal{O}(g)\,,$$

where $\kappa_\circ \in \mathbb{R}^*_+$ is an absolute constant independent of N and g is the genus of $X_0(N)$.

5.3 A regular model of $X(N)$

Let $N = p^k m$, where $p > 3$ is a prime and $m \neq 1$ is a natural number coprime to $6p$. The modular curve $X(N)$ is defined over the number field $\mathbb{Q}(\zeta_N)$; again, ζ_N denotes a primitive N-th root of unity. Its complex valued points correspond to the compact Riemann surface $\Gamma(N)\backslash(\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$, where

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

The regular model $\mathcal{X}(N)$ over $\operatorname{Spec}\mathbb{Z}[\zeta_N]$ determined by Katz and Mazur can be described as follows: The scheme $\mathcal{X}(N)$ is smooth over $\mathbb{Z}[\zeta_N, 1/N]$. For a prime ideal $\mathfrak{p} \subset \mathbb{Z}[\zeta_N]$ with $\mathfrak{p} \cap \mathbb{Z} = (p)$ the special fiber $\mathcal{X}(N) \times_{\operatorname{Spec}\mathbb{Z}[\zeta_N]} \operatorname{Spec}\mathbb{F}_p$ is the union of

$$r_\mathfrak{p} = p^k + p^{k-1} \tag{5.3.1}$$

irreducible components crossing in

$$s_\mathfrak{p} = \frac{p-1}{24} m^2 \varphi(m) \prod_{q|m} \left(1 + \frac{1}{q}\right) \tag{5.3.2}$$

supersingular points; here φ is Euler's function. We assume that all intersections are transverse[2]. The natural morphism $\beta : X(N) \to X(1)$ extends to a morphism of the arithmetic surfaces $\beta : \mathcal{X}(N) \to \mathcal{X}(1)$. It is a Galois cover, and its degree equals

$$d = \deg\beta = \frac{N^3}{2} \prod_{p|N} \left(1 - \frac{1}{p^2}\right). \tag{5.3.3}$$

[2]The transversality condition is not easy to verify. One could possibly use Corollary 13.8.5, p.431 in [KM] in order to decide whether or not the condition is fulfilled.

For $\mathfrak{p}$ the components $\mathcal{C}_0, \ldots, \mathcal{C}_{p^k+p^{k-1}-1}$ are mapped to the smooth component $\mathcal{D}$ of the special fiber of $\mathcal{X}(1)$. They all have the same local degree and since their multiplicity is one, this local degree is given by

$$\frac{d}{p^k + p^{k-1}} .$$

Remark 5.3.1. Let N be a natural number coprime to 6 that has at least two different prime factors, let $\mathcal{X}(N)$ be the regular model of the modular curve $X(N)$ over $\operatorname{Spec} \mathbb{Z}[\zeta_N]$ which was constructed by Katz and Mazur, and let $\beta : \mathcal{X}(N) \to \mathcal{X}(1)$ be the natural morphism that was obtained as the extension of the morphism $\beta : X(N) \to X(1)$. For an $\mathbb{Q}(\zeta_N)$-rational ramified point $\infty \in X(1)$ let $\beta^*\infty = \sum_j b_j S_j$. Then the S_j are $\mathbb{Q}(\zeta_N)$-rational and any divisor of degree zero with support in them is torsion (cf. [Og] and Theorem 3.2.17); we have $b_j = N$ for all j (cf. [Sh]). It follows that $\mathcal{X}(N)$ together with its morphism $\beta : \mathcal{X}(N) \to \mathcal{X}(1)$ fulfills the requirements of Assumption 5.1.1.

Lemma 5.3.2. *In the situation of Remark 5.3.1 we have*

$$\sum_j b_j \overline{\mathcal{O}}(\mathcal{G}_j)^2 = \sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_j)^2 = -\varphi(N) 12 \sum_{p|N} \frac{p(p^k + p^{k-1} - 1)}{p^2 - 1} \log p \,, \tag{5.3.4}$$

where $\mathcal{G}_j$ and $\mathcal{F}_j$ are the vertical divisors defined in (3.2.3) *and* (3.2.2)*.*

Proof: Let us first show the second equality in (5.3.4). We have

$$\overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{\mathfrak{p} \text{ bad}} \overline{\mathcal{O}}(\mathcal{F}_{j,\mathfrak{p}})^2 ,$$

where $\mathcal{F}_{j,\mathfrak{p}}$ denotes the part of the vertical divisor $\mathcal{F}_j$ which has support in the special fiber above $\mathfrak{p}$. We fix a bad prime ideal $\mathfrak{p}$. The equations (5.3.1), (5.3.2) and (5.3.3) together with Corollary 5.1.10 yield

$$\begin{aligned} \sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_{j,\mathfrak{p}})^2 &= -\frac{12}{p-1} p^{3k} \left(1 - \frac{1}{p^2}\right) \frac{p^k + p^{k-1} - 1}{(p^k + p^{k-1})^2} \log \operatorname{Nm}(\mathfrak{p}) \\ &= -\frac{12 p^k (p^k + p^{k-1} - 1)}{p+1} \log \operatorname{Nm}(\mathfrak{p}) . \end{aligned}$$

Now, let f be the inertial degree of $\mathfrak{p}$ over p i.e. the natural number with $\operatorname{Nm}(\mathfrak{p}) = p^f$, and e the ramification index of $\mathfrak{p}$ over p. Since $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is a Galois extension, all the inertial degrees and ramification indices of the prime ideals over p are the same, and we get the equation $|\mathbb{Q}(\zeta_N) : \mathbb{Q}| = efr$, where r denotes the number of prime ideals over p. We have $e = \varphi(p^k)$ (see. [Ne], p. 61: (10.3)). Now, let us set

$$\mathcal{F}_{j,p} := \sum_{\substack{\mathfrak{p} \text{ bad} \\ \mathfrak{p} \cap \mathbb{Z} = (p)}} \mathcal{F}_{j,\mathfrak{p}} .$$

Since $|\mathbb{Q}(\zeta_N):\mathbb{Q}| = \varphi(N)$, we have $fr = \varphi(m)$, hence

$$
\begin{aligned}
\sum_j b_j \overline{\mathcal{O}}(\mathcal{F}_{j,p})^2 &= -r\frac{12p^k(p^k+p^{k-1}-1)}{p+1}\log p^f \\
&= -\varphi(m)\frac{12p^k(p^k+p^{k-1}-1)}{p+1}\log p \\
&= -\varphi(N)\frac{12p(p^k+p^{k-1}-1)}{p^2-1}\log p\,.
\end{aligned}
$$

Now, summing up along all primes p with $p|N$ gives the claim. The first equality in (5.3.4) follows either by direct computations as above (but now with Theorem 5.1.6) or by the fact that $\beta : \mathcal{X}(N) \to \mathcal{X}(1)$ is a Galois cover. □

Theorem 5.3.3. *Let N be a natural number coprime to 6 that has at least two different prime factors, and let $\mathcal{X}(N)$ be the regular model of the modular curve $X(N)$ over* $\operatorname{Spec}\mathbb{Z}[\zeta_N]$ *which was constructed by Katz and Mazur. We assume that all intersections are transverse*[3]*. Then the arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$
\begin{aligned}
\overline{\omega}^2_{\mathcal{X}(N),\mathrm{Ar}} \le{}& (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_N):\mathbb{Q}](\kappa_1\log N+\kappa_2)\right) \\
&+ \frac{(2g-2)48}{N^2\prod_{p|N}(1+\frac{1}{p})}\sum_{p|N}\frac{p(p^k+p^{k-1}-1)}{p^2-1}\log p\,,
\end{aligned}
$$

where $\kappa_1,\kappa_2 \in \mathbb{R}^*_+$ are positive constants independent of N.

Proof: By Remark 5.3.1 the requirements of Assumption 5.1.1 are fulfilled, hence Theorem 3.2.2 is applicable. Since $b_{\max} = N$ (cf. Remark 5.3.1) we only have to compute the geometric contribution. By Lemma 5.3.2 we have

$$
\begin{aligned}
\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}}\log\mathrm{Nm}(\mathfrak{p}) &= -\frac{2g}{d}\sum_j b_j\,\overline{\mathcal{O}}(\mathcal{G}_j)^2 + \frac{2g-2}{d}\sum_j b_j\,\overline{\mathcal{O}}(\mathcal{F}_j)^2 \\
&= -\frac{2}{d}\sum_j b_j\,\overline{\mathcal{O}}(\mathcal{F}_j)^2 \\
&= \frac{48}{N^2\prod_{p|N}(1+\frac{1}{p})}\sum_{p|N}\frac{p(p^k+p^{k-1}-1)}{p^2-1}\log p\,,
\end{aligned}
$$

which completes the prove. □

[3]The transversality condition is not easy to verify. One could possibly use Corollary 13.8.5, p.431 in [KM] in order to decide whether or not the condition is fulfilled.

Remark 5.3.4. In [Kü2] Kühn uses Proposition 3.2.9 and Theorem 3.2.10 (Proposition 6.1. and Theorem 6.3 in [Kü2]) to approximate the geometric contribution. This leads to the upper bound

$$\begin{aligned}\overline{\omega}^2_{\mathcal{X}(N),\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_N):\mathbb{Q}](\kappa_1\log N + \kappa_2)\right) \\ + 2(2g-2)\sum_{\mathfrak{p}\supset(N)} \frac{(r_\mathfrak{p}-1)^2}{s_\mathfrak{p}} \log \mathrm{Nm}\,\mathfrak{p}\,,\end{aligned}$$

where $r_\mathfrak{p}$ is the number of components and $s_\mathfrak{p}$ the number of supersingular points; the rest of the notation is the same as in Theorem 5.3.3 (cf. Theorem 9.1. [Kü2]). However, our computation gives us the exact value of the geometric contribution, hence Theorem 5.3.3 is an improvement of Theorem 9.1. in [Kü2].

Theorem 5.3.5. *With the notation of Theorem 5.3.3 we have the asymptotic bound*

$$\overline{\omega}^2_{\mathcal{X}(N),\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_N):\mathbb{Q}](\kappa_1\log N + \kappa_2)\right) + \mathcal{O}\left(g\right)\,.$$

Proof: According to Theorem 5.3.3 we have

$$\begin{aligned}\sum_{\mathfrak{p}\text{ bad}} a_\mathfrak{p}\log\mathrm{Nm}(\mathfrak{p}) &= \frac{48}{N^2\prod_{p|N}(1+\frac{1}{p})}\sum_{p|N}\frac{p(p^k+p^{k-1}-1)}{p^2-1}\log p \\ &< \frac{48}{N^2}\sum_{p|N}p^k\log p \\ &< \frac{48}{N}\sum_{p|N}\log p \\ &\leq \frac{48}{N}\log N \in \mathcal{O}(1)\,,\end{aligned}$$

and this yields the claim. □

Remark 5.3.6. Since $\sum_{\mathfrak{p}\text{ bad}} a_\mathfrak{p}\log\mathrm{Nm}(\mathfrak{p}) \in \mathcal{O}(1)$ it is obvious that the analytic contribution dominates the geometric contribution.

Chapter 6

Fermat curves of squarefree exponent

In the previous two chapters we applied Kühn's formula (Theorem 3.2.2) to regular models of curves. In case of the Fermat curves we used the model constructed by McCallum and in case of the modular curves we used the model of Deligne and Rapoport (Katz and Mazur resp.). In this chapter we extend the results about the Fermat curve of prime exponent to Fermat curves of squarefree odd exponent. In order to do this we construct a regular model of this curve. Later we will show that this model is in fact the minimal regular model of this curve, and we will apply Kühn's formula.

6.1 The minimal regular model of the Fermat curve of squarefree exponent

Let N be a squarefree odd natural number which has at least two prime factors, and ζ_N a primitive N-th root of unity. In this section we construct the minimal regular model of the Fermat curve

$$F_N : X^N + Y^N = Z^N$$

over $\operatorname{Spec} \mathbb{Z}[\zeta_N]$. Let p be a prime number with $N = pm$. Since N is squarefree, we have $\gcd(p, m) = 1$. We fix a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\zeta_N]$ that divides p, or in other words that lies above it[1]. We denote by R the localization of $\mathbb{Z}[\zeta_N]$ with respect to $\mathfrak{p}$, and by R^{sh} the strict henselization of R. Let π be the prime element of R. We can and will interpret this element as the prime element of R^{sh} too. We start with the model

$$\mathfrak{F}^0_{N,\mathfrak{p}} = \operatorname{Proj} R[X, Y, Z]/(X^N + Y^N - Z^N)\,. \tag{6.1.1}$$

To construct the minimal regular model we will work with affine open subschemes of this model. Later we just have to glue the constructed parts together to get the intended

[1] Contrary to the prime exponent case it may happen that there is more than just one prime ideal above the prime. For example if $N = 3 \cdot 5 \cdot 11$, then there are 4 prime ideals lying above 11 (see e.g. [Ne] p. 61 (10.3)).

projective model. We may illustrate everything with the affine open subscheme[2]

$$\mathcal{X} := \operatorname{Spec} R[X,Y]/(X^N + Y^N - 1)\,. \tag{6.1.2}$$

The Noetherian scheme $\mathcal{X}$ is integral because $R[X,Y]$ is a unique factorization domain and $X^N + Y^N - 1$ is an irreducible element according to the Eisenstein criterion. For a natural number n we will use (by abuse of notation) F_n to denote the polynomial $X^n + Y^n - 1$. It will be clear from the context if we refer to the Fermat curve or to the polynomial. For the following computations it will be useful to write the equation (6.1.2) as

$$F_m^p + p\psi(X^m, Y^m) \tag{6.1.3}$$

where

$$\psi(a,b) = \frac{a^p + b^p - 1 - (a+b-1)^p}{p}\,. \tag{6.1.4}$$

According to [Ne] p. 61 (10.3) we have $p = \mu\pi^{p-1}$ with a unit $\mu \in R^*$. Using equation (6.1.3), it can be easily seen that the special fiber of $\mathcal{X}$ is of the form

$$\operatorname{Spec}(R[X,Y]/(F_m^p + p\psi(X^m, Y^m)) \otimes_R k(\pi)) = \operatorname{Spec}(k(\pi)[X,Y]/F_m^p)\,,$$

where $k(\pi)$ is a finite field extension of $\mathbb{F}_p$, the field with p elements [3]. The special fiber consists of one component $\mathcal{C}$ which has multiplicity p (Proposition 1.4.11). The component - considered as a subset of $\mathcal{X}$ - is the closure of the ideal $I = (\pi, F_m)/(X^N + Y^N - 1) \subset R[X,Y]/(X^N + Y^N - 1)$, so $V(I) = \mathcal{C}$. The ideal I is a prime ideal since the ring

$$R[X,Y]/I \cong k(\pi)[X,Y]/(X^m + Y^m - 1) \tag{6.1.5}$$

is integral. Because of the regularity of this ring, the closed subscheme $\mathcal{C}$ is regular by definition. However since $F_N \in I^{p-1}$ and $p \neq 2$ the scheme $\mathcal{X}$ is singular. In fact, it is not even normal because it is not regular in codimension 1 (Proposition 1.1.17)[4].

Notation 6.1.1. In the following computations we have to work very often with factor rings of the form

$$R[X_1, \ldots, X_r]/J\,,$$

with an ideal J. If there is no danger of confusion, we will use for an element $f \in R[X_1 \ldots, X_r]$ the same symbol to denote the residue class of it in $R[X_1 \ldots, X_r]/J$. For example in the situation described above we will write $(\pi, F_m) \subset R[X,Y]/(X^N + Y^N - 1)$ to denote the ideal $(\pi, F_m)/(X^N + Y^N - 1)$.

---

[2] In fact, if we want to make everything totally accurate we should introduce new variables $X_0 := \frac{X}{Z}$ and $Y_0 := \frac{Y}{Z}$ to get the subscheme $R[X_0, Y_0]/(X_0^N + Y_0^N - 1)$ as the set of elements of degree 0 in the localization of the ring with respect to the multiplicative subset $\{1, Z, Z^2, Z^3, \ldots\}$. Instead of this, we will use - for simpicity - the symbols X and Y for these new variables.

[3] Strictly speaking we have $|k(\pi) : \mathbb{F}_p| = f_p$, where f_p denotes the smallest number with $p^{f_p} \equiv 1 \mod m$ (see [Ne] p.61 (10.3)).

[4] It can be shown that the scheme $\operatorname{Spec} A[X,Y]/(X^N + Y^N - 1)$, where A is the ring of integers of a number field, is normal if and only if all prime numbers $p|N$ are unramified in A (see [KW], p.106: Theorem 3.3.).

Notation 6.1.2. We can interpret $k(\pi)$ as a subfield of $\overline{\mathbb{F}}_p$, where $\overline{\mathbb{F}}_p$ is an algebraic closure of $\mathbb{F}_p$. The algebraic closure of $k(\pi)$ (in $\overline{\mathbb{F}}_p$) is just $\overline{\mathbb{F}}_p$. For this reason we choose $\overline{\mathbb{F}}_p$ as the fixed algebraic closure of $k(\pi)$.

6.1.1 The polynomial $\psi(X^m, Y^m)$

In this subsection we are going to study the polynomial $\psi(X^m, Y^m)$. In order to do this we take a close look at the polynomial $\psi(a, b)$ and then later we just have to insert X^m and Y^m. We have the following:

$$\begin{aligned}\psi(a,b) - \psi(a, 1-a) &= \frac{a^p + b^p - 1 - (a+b-1)^p}{p} - \frac{a^p + (1-a)^p - 1}{p} \\ &= \frac{b^p - (a+b-1)^p + (a-1)^p}{p} = \sum_{k=1}^{p-1} \frac{\binom{p}{k}}{p} (a+b-1))^{p-k} b^k (-1)^k \,.\end{aligned}$$

Substituting X^m for a and Y^m for b we get

$$\psi(X^m, Y^m) = \psi(X^m, 1 - X^m) + \sum_{k=1}^{p-1} \frac{\binom{p}{k}}{p} {F_m}^{p-k} Y^{mk} (-1)^k \tag{6.1.6}$$

For later computations it will be important to know the factorization of $\psi(X^m, Y^m)$. We will review a result of McCallum [Mc]:

Lemma 6.1.3. *Let $p \geq 3$. We have the decomposition*

$$\psi(a, 1-a) = a(a-1)\Psi(a)\,, \tag{6.1.7}$$

with a polynomial $\Psi(a) \in R[a]$. In the factorization of $\Psi(a)$ over $\overline{\mathbb{F}}_p$, factors occur with multiplicity 1 if not rational over $\mathbb{F}_p$, and with multiplicity 2 otherwise.

Proof: The proof is an elaboration of the proof given in [Mc] p.59. We have $(\psi(a, 1-a))' = a^{p-1} - (1-a)^{p-1} \equiv -(a-2) \cdot \ldots \cdot (a-p+1) \mod (\pi)$. The only roots of $\psi(a, 1-a) \mod (\pi)$ with multiplicity higher than 1 are of the form $\overline{\alpha} \in \{\overline{2}, \ldots, \overline{p-1}\}$ with an $\alpha \in R$. If we assume that the multiplicity of $\overline{\alpha}$ is greater than two the second derivative would vanish in $\overline{\alpha}$, too. But from $(p-1)\alpha^{p-2} + (p-1)(1-\alpha)^{p-2} \equiv 0 \mod (\pi)$ it follows $\alpha^{p-2} \equiv (\alpha-1)^{p-2} \mod (\pi)$ and so by multiplication with $\alpha(\alpha-1)$ we obtain $\alpha - 1 \equiv \alpha \mod (\pi)$ and this is obviously impossible. Let us denote the root of multiplicity 2 by $\overline{\alpha}_1, \ldots, \overline{\alpha}_s$ (they are pairwise distinct, because otherwise we would have a root of higher multiplicity).
Together with the fact that 0 and 1 are simple roots of $\psi(a, 1-a)$ (and $\overline{\psi}(a, 1-a)$) we get the decomposition

$$\overline{\psi}(a, 1-a) = a(a-1)(a-\overline{\beta}_1) \cdot \ldots \cdot (a-\overline{\beta}_r)(a-\overline{\alpha}_1)^2 \cdot \ldots \cdot (a-\overline{\alpha}_s)^2\,, \tag{6.1.8}$$

over $\overline{\mathbb{F}}_p$, where $\overline{\beta}_i \notin \mathbb{F}_p$. $\square$

Corollary 6.1.4. *Let $p \geq 3$. We have the decomposition*

$$\psi(X^m, 1 - X^m) = X^m \prod_{i=0}^{m-1} (X - \zeta_m^i)\Psi(X^m)\,. \tag{6.1.9}$$

In the factorization of $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$, factors $(X - \overline{\delta})$ occur with multiplicity 1 if $\overline{\delta}^m$ is not rational over $\mathbb{F}_p$, and with multiplicity 2 otherwise.

Proof: If we replace in (6.1.7) a by X^m it is obvious that we get (6.1.9), since $\zeta_m^i \in R$. A decomposition as in (6.1.8) becomes

$$\overline{\psi}(X^m, 1 - X^m) = X^m \prod_{i=0}^{m-1} (X - \overline{\zeta}_m^i)(X - \overline{\delta}_1) \cdot \ldots \cdot (X - \overline{\delta}_{rm})(X - \overline{\gamma}_1)^2 \cdot \ldots \cdot (X - \overline{\delta}_{sm})^2$$

after this replacement; here $\overline{\delta}^m = \overline{\beta}$ and $\overline{\gamma}^m = \overline{\alpha}$. Since the $\overline{\alpha}_i$ and $\overline{\beta}_j$ from Lemma 6.1.3 are not zero the polynomials $X^m - \overline{\alpha}_i$ ($X^m - \overline{\beta}_j$ resp.) split into coprime linear factors over $\overline{\mathbb{F}}_p$. The linear polynomials $(X - \overline{\gamma}_k)$ are the only factors of multiplicity 2 in $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$. $\square$

Definition 6.1.5. Let us denote by ϱ the number of factors $(X - \overline{\gamma}_k)^2$ of $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$.

Remark 6.1.6. Since $\psi(a, 1-a)$ is a polynomial of degree $p-1$ the polynomial $\psi(X^m, 1-X^m)$ is of degree $m(p-1)$. Corollary 6.1.4 tells us that there are

$$\deg \Psi(X^m) - 2\varrho = m(p-3) - 2\varrho$$

linear factors of multiplicity one in $\Psi(X^m)$. However, for different prime numbers p the corresponding number ϱ_p may vary strongly. For example let $p = 5$. Then $\Psi_5(a) \equiv a^2 - a + 1 \mod 5$, where $a^2 - a + 1$ is an irreducible element of $\mathbb{F}_5[a]$. It follows that in this case $\varrho_5 = 0$. On the other hand, consider the case $p = 7$. Here we have $\Psi_7(a) \equiv (a+2)^2(a+4)^2 \mod 7$, hence $\varrho_7 = \frac{1}{2} \deg \Psi_7(X^m) = 2m$.

6.1.2 The blowing-up of $\mathcal{X}$ along $V(I)$

We start by giving an explicit description of the blowing-up.

Proposition 6.1.7. *The blowing-up $\widetilde{\mathcal{X}}$ of the scheme $\mathcal{X}$ in* (6.1.2) *along $V(I)$, where $I = (\pi, F_m) \subset R[X, Y]/F_N$, is given by the affine open subsets $U_1 = \operatorname{Spec} S_1$ and $U_2 = \operatorname{Spec} S_2$, where*

$$S_1 := R[X, Y, Z]/(F_m - Z\pi, \pi Z^p + \mu\psi(X^m, Y^m)) \tag{6.1.10}$$

and

$$S_2 := R[X, Y, W]/(WF_m - \pi, F_m + \mu W^{p-1}\psi(X^m, Y^m))\,. \tag{6.1.11}$$

In other words, we have $\widetilde{\mathcal{X}} = U_1 \cup U_2$.

Proof: The generators of the ideal I obviously form a regular sequence in $R[X,Y]$, since $R[X,Y]$ and $R[X,Y]/\pi$ ($R[X,Y]/F_m$ resp.) are integral. It follows that we can apply Theorem 1.2.6. The polynomial

$$F_m Z^{p-1} + \mu W^{p-1} \psi(X^m, Y^m) \in (R[X,Y])\,[W,Z]$$

is homogenous (in W and Z) and the coefficient $\mu\psi(X^m, Y^m)$ is not in the ideal I. The statement follows now with Remark 1.2.7. $\square$

Remark 6.1.8. The scheme $\widetilde{\mathcal{X}}$ can be considered as a subscheme of the scheme $\widetilde{\mathcal{Z}} = V_1 \cup V_2$, where

$$V_1 := \operatorname{Spec} R[X,Y,Z]/(F_m - Z\pi)$$

and

$$V_2 := \operatorname{Spec} R[X,Y,W]/(WF_m - \pi)\,.$$

Since $\widetilde{\mathcal{Z}}$ is just the blowing-up of the regular scheme $\mathcal{Z} = \operatorname{Spec} R[X,Y]$ along (π, F_m), it is regular as well (Lemma 1.2.4 and Theorem 1.2.10). The scheme $\widetilde{\mathcal{X}}$ is the strict transform of $\mathcal{X}$ in $\widetilde{\mathcal{Z}}$.

Proposition 6.1.9. *The scheme $\widetilde{\mathcal{X}}$ from Proposition 6.1.7 is normal. Let $\overline{F}_m, \overline{\psi}(X^m, 1 - X^m) \in \overline{\mathbb{F}}_p[X,Y]$ be the reductions of F_m and $\psi(X^m, 1-X^m)$ with respect to the canonical morphism $R[X,Y] \to \overline{\mathbb{F}}_p[X,Y]$. The geometric special fiber $\widetilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{\mathbb{F}}_p$ has configuration as in Figure 6.1, where the components $L_{(x,y)}$ are of genus 0 and parameterized by the pairs $(x,y) \in \overline{\mathbb{F}}_p^2$ with*

$$x^m + y^m - 1 = \overline{\psi}(x^m, 1 - x^m) = 0\,.$$

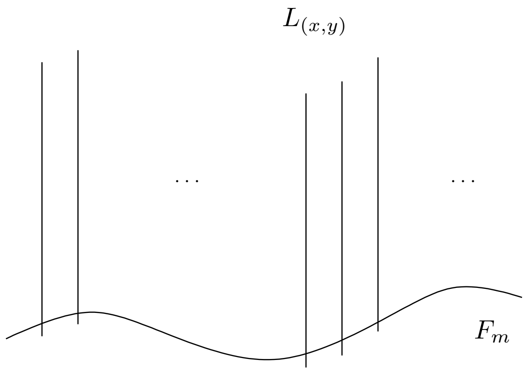

Figure 6.1: The configuration of the geometric special fiber $\widetilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{\mathbb{F}}_p$.

Proof: We consider the scheme

$$\widetilde{\mathcal{X}}^{sh} = \widetilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} R^{sh} \tag{6.1.12}$$

i.e. the scheme $\widetilde{\mathcal{X}}$ after the base change $\operatorname{Spec} R^{sh} \to \operatorname{Spec} R$. Since this base change is faithfully flat, normality of $\widetilde{\mathcal{X}}^{sh}$ implies normality of $\widetilde{\mathcal{X}}$ (the advantage is that the special fiber of $\widetilde{\mathcal{X}}^{sh}$ is a variety over the algebraically closed field $\overline{\mathbb{F}}_p$). We will start our computation with the affine open subscheme $U_1^{sh} = \operatorname{Spec} S_1^{sh}$, where $S_1^{sh} = S_1 \otimes_R R^{sh}$. The special fiber of this scheme is

$$\begin{aligned} U_1^{sh} \times_{\operatorname{Spec} R^{sh}} \operatorname{Spec} \overline{\mathbb{F}}_p &= \operatorname{Spec} \left(\overline{\mathbb{F}}_p[X,Y,Z]/(F_m, \psi(X^m, Y^m))\right) \\ &= \operatorname{Spec} \left(\overline{\mathbb{F}}_p[X,Y,Z]/(F_m, \psi(X^m, 1-X^m))\right) . \end{aligned} \tag{6.1.13}$$

This variety consists of lines $L_{x,y} = V(X-x, Y-y)$, where x is a root of $\overline{\psi}(X^m, 1-X^m)$ and y is a root of $Y^m + x^m - 1 \in \overline{\mathbb{F}}_p[Y]$. These lines correspond to prime divisors $V(\mathfrak{P})$ of U_1^{sh}, where $\mathfrak{P} = (X - X', Y - Y', \pi)$ is a prime ideal of height 1 and $X' \equiv x \mod \pi$ ($Y' \equiv y \mod \pi$ resp.). Because of Remark 6.1.8 and Proposition 1.1.17, the only thing to do is to show that S_1^{sh} is regular at $\mathfrak{P}$ (since the generic fiber of $\widetilde{\mathcal{X}}^{sh}$ (U_1^{sh} resp.) is regular S_1^{sh} is regular at every prime ideal which does not contain π). Notice that π cannot be a divisor of X' and of Y', since $x^m + y^m = 1$. Because of symmetry we may assume $\pi \nmid Y'$ without loss of generality. We have $\psi(X'^m, 1 - X'^m) = \lambda\pi$ with an element $\lambda \in R^{sh}$. Now,

$$\psi(X^m, 1 - X^m) = \lambda\pi + (X - X')G(X)$$

with a polynomial $G(X) \in R^{sh}[X]$. It follows from Proposition 6.1.7 and equation (6.1.6), that

$$-(X - X')G(X) = \pi \left(Z^p\mu^{-1} + ZY^{m(p-1)} + \lambda + \pi H(Y,Z)\right)$$

in S_1^{sh}, where $H(Y,Z)$ is a polynomial in Y and Z. Let us suppose that $Z^p\mu^{-1} + ZY^{m(p-1)} + \lambda + \pi H(Y,Z) \in \mathfrak{P}$. Then $Z^p\mu^{-1} + ZY'^{m(p-1)} + \lambda \in \mathfrak{P}$ and - using Hensel's lemma - $(Z - Z') \in \mathfrak{P}$, where Z' is a root of $Z^p\mu^{-1} + ZY'^{m(p-1)} + \lambda =: f(Z) \in R^{sh}[Z]$. Indeed, since $\overline{f'}(Z) = y^{m(p-1)} \neq 0$ the polynomial $\overline{f}(Z)$ splits into coprime linear factors in $\overline{\mathbb{F}}_p$, and this decomposition "lifts" to R^{sh}. But if this linear factor is in $\mathfrak{P}$ then $\mathfrak{P}$ is a maximal ideal, a contradiction since $\mathfrak{P}$ was assumed to be of height 1. If follows that $Z^p\mu^{-1} + ZY^{m(p-1)} + \lambda + \pi H(Y,Z) \notin \mathfrak{P}$ and so this element becomes a unit in $(S_1^{sh})_{\mathfrak{P}}$. We will denote this unit by ϵ.

Now, since $\pi | X'^m + Y'^m - 1$ we have $X'^m + Y'^m - 1 = \tau\pi$ with an element $\tau \in R^{sh}$. It follows again with Proposition 6.1.7 that

$$\begin{aligned} \pi Z &= X^m + Y^m - 1 \\ &= X^m - X'^m + Y^m - Y'^m + X'^m + Y'^m - 1 \\ &= (X - X') \prod_{i=1}^{m-1} (X - X'\zeta_m^i) + (Y - Y') \prod_{i=1}^{m-1} (Y - Y'\zeta_m^i) + \tau\pi \end{aligned}$$

in S_1^{sh}. Now, $\prod_{i=1}^{m-1}(Y - Y'\zeta_m^i) \notin \mathfrak{P}$ because otherwise $Y' \in \mathfrak{P}$ or $(1 - \zeta_m^i) \in \mathfrak{P}$ and this is impossible, since these elements are units in R^{sh}. To see this, remember that $\pi \nmid Y'$, and that $(1 - \zeta_m^i)$ is a divisor of m and m is coprime to p. It follows that $\prod_{i=1}^{m-1}(Y - Y'\zeta_m^i)$ is a unit in $(S_1^{sh})_{\mathfrak{P}}$. We will denote this unit by ϵ'. In the localization $(S_1^{sh})_{\mathfrak{P}}$ we have

$$-(X - X')G(X)\frac{1}{\epsilon} = \pi$$

and

$$-(X - X')\left(\prod_{i=1}^{m-1}(X - X'\zeta_m^i) + G(X)\frac{1}{\epsilon}(Z - \tau)\right)\frac{1}{\epsilon'} = (Y - Y')\,.$$

It follows $\mathfrak{P}(S_1^{sh})_{\mathfrak{P}} = (X - X')$ and so S_1^{sh} is regular at $\mathfrak{P}$ (Corollary 1.1.4).
In the second affine open subscheme $U_2^{sh} = \operatorname{Spec} S_2^{sh}$, where $S_2^{sh} = S_2 \otimes_R R^{sh}$, the only thing left to do is to check the regularity of S_2^{sh} at the prime ideal

$$\mathfrak{P} = (W, F_m, \pi) \tag{6.1.14}$$

which corresponds to the component F_m in Figure 6.1. But in S_2^{sh} we even have $\mathfrak{P} = (W)$ (Proposition 6.1.7) and so this ring is obviously regular at $\mathfrak{P}$. □

6.1.3 The minimal regular model

The next thing we want to do is to find the singular closed points of $\widetilde{\mathcal{X}}$ and then resolve these singularities (remember that there are no other (non-closed) singular points, since $\widetilde{\mathcal{X}}$ is normal). These singular points are elements of irreducible closed subsets of codimension 1, i.e. prime divisors of $\widetilde{\mathcal{X}}$. Since we can identify vertical prime divisors with the components of the special fiber, we will say that "a singular point P lies on a component L" when we want to indicate that P is an element of the corresponding prime divisor. The resolution we have in mind can be done by blowing up the lines that have singular points lying on them. Since blowing up commutes with flat morphisms (Proposition 1.2.9 (2.)) we can work the whole time with $\widetilde{\mathcal{X}}^{sh}$ instead of $\widetilde{\mathcal{X}}$, as long as we just blow up along ideal sheaves $\mathcal{J}$ of $\widetilde{\mathcal{X}}^{sh}$ which are of the form $\mathcal{I}\mathcal{O}_{\widetilde{\mathcal{X}}^{sh}}$ with an ideal sheaf $\mathcal{I}$ of $\widetilde{\mathcal{X}}$. Before we come to the main result of this section we need to introduce some more terminology:

Definition 6.1.10. We use the notation from Proposition 6.1.9. We call a component $L_{(x,y)}$ of $\widetilde{\mathcal{X}}^{sh} = \widetilde{\mathcal{X}} \times_{\operatorname{Spec} R} \operatorname{Spec} R^{sh}$ *a component of type* A, if $x = 0$ or $x^m = 1$, and *a component of type* B, if x is a multiple root of $\overline{\psi}(X^m, 1 - X^m)$ different from 0.

Theorem 6.1.11. *Let $\widetilde{\mathcal{X}}^{sh}$ be the normal scheme given by* (6.1.12)*. If we blow up* $(m-1)$*-times along the components of type A, we get p chains consisting of* $(m-1)$ *lines (Figure 6.2), blowing up along the components of type B gives p chains consisting of one line (Figure 6.3); we use the word line to indicate that it is a component of genus* 0*. The resulting scheme is regular.*

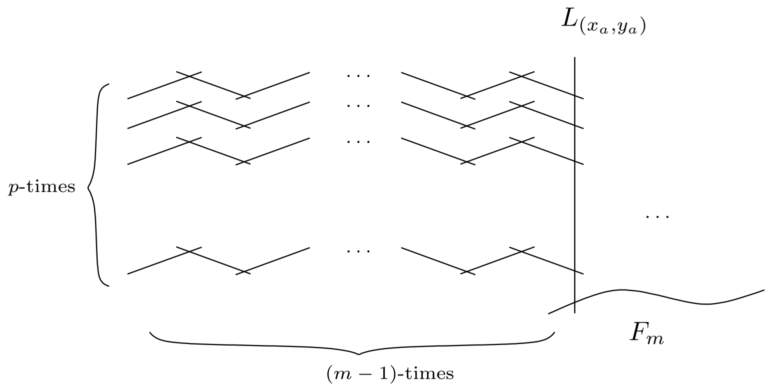

Figure 6.2: The configuration of the components after $(m-1)$-times blowing up a component $L_{(x_a,y_a)}$ of type A.

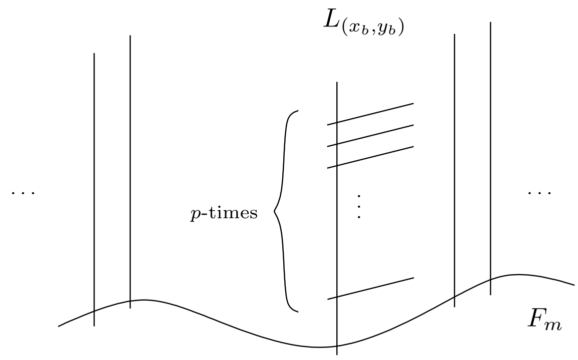

Figure 6.3: The configuration of the components after blowing up a component $L_{(x_b,y_b)}$ of type B.

Before we proof the theorem we will show three preparative lemmata.

Lemma 6.1.12. *We use the notation from Proposition 6.1.9. The only singular closed points of $\widetilde{\mathcal{X}}^{sh}$ lie on the components $L_{(x,y)}$ of type A and of type B (Figure 6.4).*

Proof: In order to find the singular closed points we analyze the special fiber of $\widetilde{\mathcal{X}}^{sh}$. For simplicity we will use, for the rest of the proof, the word point if we refer to a closed point. We start our analyzation with the affine open subset

$$U_1^{sh} \times_{\operatorname{Spec} R^{sh}} \operatorname{Spec} \overline{\mathbb{F}}_p = \operatorname{Spec}\left(\overline{\mathbb{F}}_p[X,Y,Z]/(F_m, \psi(X^m, 1-X^m))\right)$$

(from Equation (6.1.13)). The Jacobian criterion (Theorem 1.1.10) helps us to locate the

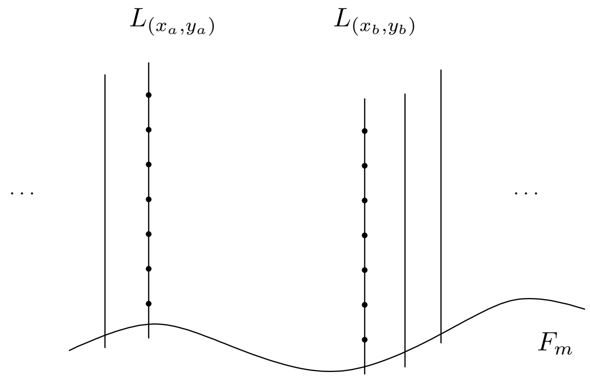

Figure 6.4: The line $L_{(x_a,y_a)}$ is of type A i.e. $x_a = 0$ or $x_a^m = 1$, and the line $L_{(x_b,y_b)}$ is of type B, so $(X - x_b)$ is a multiple factor of $\overline{\psi}(X^m, 1 - X^m)$ different from X.

possible singular points. The Jacobian matrix is of the form

$$J(X,Y,Z) = \begin{pmatrix} mX^{m-1} & mY^{m-1} & 0 \\ G(X)' & 0 & 0 \end{pmatrix},$$

where $G(X) := \overline{\psi}(X^m, 1 - X^m)$. If follows that a point $P = (x,y,z) \in U_1 \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{\mathbb{F}}_p$ is singular if and only if

$$-my^{m-1}G(x)' = 0\,.$$

Now, $y = 0$ implies $x^m - 1 = 0$ and so x is a m-th root of unity. In case $G(x)' = 0$ the element x is a m-th root of an element of $\mathbb{F}_p^*$ or 0 (Corollary 6.1.4). We continue our analyzation with the affine open subset U_2^{sh}. In fact, we just need to check if there are singular points lying on F_m (F_m is the only component of the special fiber of $\widetilde{\mathcal{X}}^{sh}$ which does not lie in U_1^{sh}): a point which lies on F_m corresponds to a maximal ideal

$$\mathfrak{m} = (\pi, W, X - X', Y - Y') \subset S_2^{sh}\,,$$

where $X'^m + Y'^m \equiv 1 \mod \pi$ (cf. (6.1.14)). Without loss of generality we may again assume $\pi \nmid Y'$. In S_2^{sh} we have

$$(Y - Y')\epsilon' \in (\pi, W, X - X') \subset S_2^{sh}\,,$$

where $\epsilon' = \prod_{i=1}^{m-1}(Y - Y'\zeta_m^i) \notin \mathfrak{m}$ (one uses similar arguments as in Proposition 6.1.9 together with (6.1.11)). This together with the fact that $\pi = WF_m$ in S_2^{sh}, gives us

$$\mathfrak{m}(S_2^{sh})_{\mathfrak{m}} = (W, X - X')\,,$$

hence S_2^{sh} is regular at $\mathfrak{m}$ (Corollary 1.1.4). Our analyzation shows that there are no singular points lying on components which are different from those of type A and of type B. □

Lemma 6.1.12 shows us that we have to focus on the components of type A and of type B. Let us analyze the former ones. A component $L_{(x_a,y_a)}$ of type A corresponds to a prime ideal

$$\mathfrak{P} = (\pi, X, Y - \zeta_m^i) \subset S_1^{sh}.$$

There is an affine open neighborhood U of $\mathfrak{P}$ with the property that $V(\mathfrak{P}) \subset U = \operatorname{Spec} A \subseteq U_1^{sh}$ and $\mathfrak{P}A = (\pi, X)$. To be more precise, we have $Y^m - 1 = (Y - \zeta_m^i)f$ where f is the product of the $(Y - \zeta_m^j)$ with $j \neq i$. Then we may take A to be

$$A = S/(\pi Z^p + \mu\psi(X^m, Y^m)), \tag{6.1.15}$$

where

$$S = \big(R^{sh}[X,Y,Z]/(F_m - Z\pi)\big)_f$$

is the localization of $R^{sh}[X,Y,Z]/(F_m - Z\pi)$ with respect to the set $\{1, f, f^2, f^3, \ldots\}$, hence U is isomorphic to the principal open subset $D(f)$ of U_1^{sh}. Notice, since $\mathfrak{P}$ is a regular prime ideal of height one, it is not a problem to find an affine open neighborhood U' so that $\mathfrak{P}$ will be generated by one element in this neighborhood. Unfortunately U' does not contain $V(\mathfrak{P})$. Next, we study schemes which naturally appear as blowing-ups of the scheme $\operatorname{Spec} A$.

Lemma 6.1.13. *Let $l \in \mathbb{N}$ with $1 \leq l \leq m-1$ and*

$$A_l := S[T_l]/(\pi - T_l X^l, g_l(T_l)), \tag{6.1.16}$$

where

$$g_l(T_l) = T_l Z^p + \mu\frac{\psi(X^m, 1 - X^m)}{X^l} + \mu\sum_{k=1}^{p-1}\binom{p}{k}p^{-1}(T_l Z)^{p-k}X^{l(p-k-1)}Y^{mk}(-1)^k. \tag{6.1.17}$$

Furthermore, let $U_l = \operatorname{Spec} A_l$. Then U_l is normal; the configuration of the special fiber of U_l is given in Figure 6.5. The only components of the special fiber which correspond to prime ideals that contain X are given by $L_{l,1}, \ldots, L_{l,p}$ and $L_{(x_a,y_a)}$. If $l = m-1$ there are no singular closed points lying on these components. If $l < m-1$, the only singular closed points are the points where the componets $L_{l,i}$ intersect the component $L_{(x_a,y_a)}$.

Proof: First of all notice that U_l is a closed subscheme of the regular integral scheme $V_l := \operatorname{Spec} S[T_l]/(\pi - T_l X^l)$. To see that V_l is integral and regular one may observe that even the ring

$$B := R^{sh}[X,Y,Z,T_l]/(F_m - Z\pi, \pi - T_l X^l)$$

has this properties: since π, X^l is a regular sequence in the integral ring $R^{sh}[X,Y,Z]/(F_m - Z\pi)$, the ring B is just one of the rings we get if we blow up $R^{sh}[X,Y,Z]/(F_m - Z\pi)$ along the ideal (π, X^l) (Lemma 1.2.5). It follows that B is integral (Lemma 1.2.2). To see the

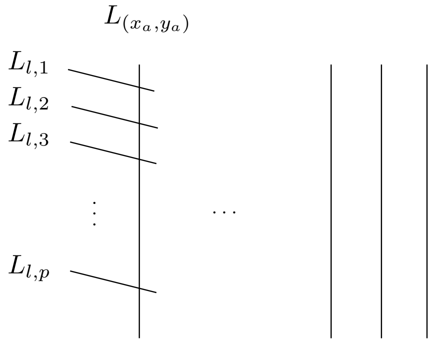

Figure 6.5: The configuration of the special fiber of U_l. If $l < m-1$, the components $L_{l,i}$ intersect the component $L_{(x_a,y_a)}$ in a singular point of U_l.

regularity we use the Jacobian criterion (Theorem 1.1.10) and find that the only maximal ideals which may be singular are of the form

$$\mathfrak{m} = (\pi, X, Y - \zeta_m^i, T - T', Z - Z')$$

with $T', Z' \in R^{sh}$ and $i \in \mathbb{Z}$. We have the chain of prime ideals $0 \subsetneq (\pi, X, Y - \zeta_m^i) \subsetneq (\pi, X, Y - \zeta_m^i, T - T') \subsetneq \mathfrak{m}$. On the other hand $\mathfrak{m}B_{\mathfrak{m}} = (X, T - T', Z - Z')$. This gives us $3 \leq \dim B_{\mathfrak{m}} \leq \dim_{k(\mathfrak{m})} \mathfrak{m}/\mathfrak{m}^2 \leq 3$, hence the regularity of $B_{\mathfrak{m}}$. It follows that B is regular (Proposition 1.1.6).

Let us return to the scheme U_l and show that it is normal. In order to do this we may first consider the affine open subscheme $U_l' = \operatorname{Spec}(A_l)_X$, where $(A_l)_X$ is the localization of A_l with respect to the set

$$\{1, X, X^2, X^3, \ldots\}\,.$$

The special fiber of U_l' has the same configuration as the one of U_l but with the difference that U_l' does not possess the components which correspond to prime ideals that contain X and π. An easy computation shows that $(A_l)_X \cong (S_1^{sh})_{Xf} = (S_1 \otimes_R R^{sh})_{Xf}$ (cf. (6.1.10)) where Xf is the multiplicative subset $\{1, f, X, Xf, X^2, f^2, \ldots\}$. It follows that U_l' is normal and that its special fiber has the same configuration as the special fiber of $U_1^{sh} = \operatorname{Spec} S_1^{sh}$ after removing the components $L_{(x,y)}$ with $x = 0$ (cf. Proposition 6.1.9). Next, let us analyze the components of the special fiber of U_l that do not lie in U_l' i. e. let us consider those components of $\operatorname{Spec}\left(A_l \otimes_{R^{sh}} \overline{\mathbb{F}}_p\right)$ whose corresponding prime ideal of A_l contains X (since the generic fiber of U_l is regular A_l is regular at every prime ideal which does not contain π). For a prime ideal $\mathfrak{P} \subset A_l$ with $\pi, X \in \mathfrak{P}$ we have

$$T_l Z^p + \mu T_l Z (\zeta_m^i)^{m(p-1)} = T_l Z (Z^{p-1} + \mu) \in \mathfrak{P}\,, \tag{6.1.18}$$

hence the only prime ideals of height one with this property are

$$(\pi, X, T_l), \tag{6.1.19}$$

$$(\pi, X, Z), \tag{6.1.20}$$

and

$$(\pi, X, Z - \theta\zeta_{p-1}^{i}), \tag{6.1.21}$$

where θ is an element of R^{sh} with $\theta^{p-1} = -\mu$ and $0 \leq i \leq p-2$. Notice that $\mathfrak{P}$ can just contain one of the elements T_l, Z or $Z - \theta\zeta_{p-1}^{i}$, because otherwise $\mathfrak{P} = A_l$ or $\mathfrak{P}$ is a maximal ideal, hence it is of height 2. Since $\pi = T_l X^l$ in A_l it follows with (6.1.17) and (6.1.18) that $\mathfrak{P}(A_l)_{\mathfrak{P}} = (X)$, and therefore the normality of U_l.
Let $\mathfrak{m} = (X, T_l - T', Z - Z')$ be a maximal ideal of A_l with $\pi \nmid T'$ (notice that $\pi \in \mathfrak{m}$ since $\pi = T_l X^l$ in A_l). It follows with (6.1.17) and (6.1.18) that $T'Z(Z^{p-1} + \mu) \in \mathfrak{m}$ and so we may assume without loss of generality that $Z' = 0$ or $Z' = \theta\zeta_{p-1}^{i}$. Since the factors

$$Z, (Z - \theta), (Z - \theta\zeta_{p-1}), (Z - \theta\zeta_{p-1}^{2}), \ldots, (Z - \theta\zeta_{p-1}^{p-2}) \tag{6.1.22}$$

are pairwise coprime, equation (6.1.17) and (6.1.18) show us that $(Z - Z')$ is contained in the ideal of $(A_l)_{\mathfrak{m}}$ which is generated by X and $(T - T')$, hence the ring A_l is regular at $\mathfrak{m}$. Next, let $\mathfrak{m} = (X, T_l, Z - Z')$, where $(Z - Z')$ is coprime to any of the factors in (6.1.22). Then $Z(Z^{p-1} + \mu)$ becomes a unit in the localization with respect to $\mathfrak{m}$. Again, equation (6.1.17) and (6.1.18) yield $\mathfrak{m}(A_l)_{\mathfrak{m}} = (X, Z - Z')$ and therefore the regularity of A_l at $\mathfrak{m}$. Now, the only situation left we have to consider is $\mathfrak{m} = (X, T_l, Z - Z')$, where $Z' = 0$ or $Z' = \theta\zeta_{p-1}^{i}$ with an integer i. We may distinguish here between two cases. In case $l = m - 1$, we have

$$-T_{(m-1)}Z(Z^{p-1} + \mu) = \mu X \left(\frac{\psi(X^m, 1 - X^m)}{X^m} + P(T_{(m-1)}) \right) \tag{6.1.23}$$

in $A_{(m-1)}$; here $P(T_{(m-1)}) \in S[T_{(m-1)}]$ is the polynomial given by

$$P(T_{(m-1)}) = \sum_{k=1}^{p-2} \frac{\binom{p}{k}}{p} (T_{(m-1)}Z)^{p-k} X^{(m-1)(p-k-1)-1} Y^{mk} (-1)^k .$$

Obviously we have $P(T_{(m-1)}) \in \mathfrak{m}$. If the term in brackets on the right-hand side of (6.1.23) was contained in $\mathfrak{m}$ then

$$\frac{\psi(X^m, 1 - X^m)}{X^m} \in \mathfrak{m} ,$$

a contradiction. Hence, this term becomes a unit in $(A_{(m-1)})_{\mathfrak{m}}$, and we have

$$\mathfrak{m}(A_{(m-1)})_{\mathfrak{m}} = (T_{(m-1)}, Z - Z') .$$

In other words, $A_{(m-1)}$ is regular at $\mathfrak{m}$. Now, consider the case $l < m - 1$. Let $\mathfrak{M}$ be the prime ideal of the regular ring $S[T_l]/(\pi - T_l X^l)$ which is given by the preimage of $\mathfrak{m}$. Since $(Y - \zeta_m^{i}) = -(X^m - Z T_l X^l) f^{-1}$ in $S[T_l]/(\pi - T_l X^l)$, we have $(Y - \zeta_m^{i}) \in \mathfrak{M}^2$, which yields

$$g_l(T_l) \equiv T_l Z^p + \mu T_l Z \equiv 0 \mod \mathfrak{M}^2 .$$

It follows that A_l is singular at $\mathfrak{m}$ (Proposition 1.1.7). Let us denote the components which correspond to the prime ideals (π, X, Z) and $(\pi, X, Z - \theta\zeta_{p-1}^{i})$ for $0 \leq i \leq p-2$ by $L_{l,1}, \ldots, L_{l,p}$. The configuration of $U_l \times_{\operatorname{Spec} R^{sh}} \operatorname{Spec} \overline{\mathbb{F}}_p$ is given in Figure 6.5. $\square$

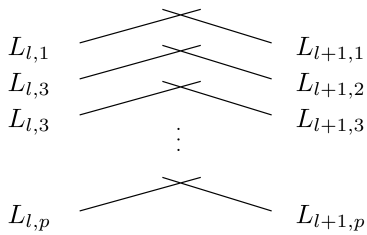

Figure 6.6: The configuration of $\operatorname{Spec} \widetilde{A}_{l+1} \times_{\operatorname{Spec} R^{sh}} \operatorname{Spec} \overline{\mathbb{F}}_p$. There are no singular points lying on the components.

Lemma 6.1.14. *We use the notation from Lemma 6.1.13. Let $l < m-1$. If we blow up along the ideal (X, T_l) the resulting scheme will be covered by the affine open subset U_{l+1} (cf. Lemma 6.1.13) and an affine open subset $\widetilde{U}_{l+1} = \operatorname{Spec} \widetilde{A}_{l+1}$. The configuration of the special fiber is given by Figure 6.5 (just interchange l by $l+1$) in U_{l+1} and by Figure 6.6 in $\widetilde{U}_{l+1}$. The scheme $\widetilde{U}_{l+1}$ is regular.*

Proof: We blow up along the ideal (X, T_l). Setting $\frac{X}{T_l} = \widetilde{X}$ one affine open subset of the blowing-up is given by the spectrum of

$$A_l\left[XT_l^{-1}\right] \cong S[T_l, \widetilde{X}]/(\pi - T_l^{l+1}\widetilde{X}^l, \widetilde{X}T_l - X, \widetilde{g}_l(\widetilde{X})) =: \widetilde{A}_{l+1}\,,$$

where

$$\widetilde{g}_l(\widetilde{X}) = Z^p + \mu\frac{\psi((\widetilde{X}T_l)^m, 1-(\widetilde{X}T_l)^m)}{\widetilde{X}^l T_l^{l+1}} + \mu\sum_{k=1}^{p-1}\binom{p}{k}p^{-1}T_l^{(l+1)(p-k-1)}\widetilde{X}^{l(p-k-1)}Z^{p-k}Y^{mk}(-1)^k\,.$$

Now, a prime ideal I which contains π, contains X and $Y - \zeta_m^i$, since $T_l \in I$ or $\widetilde{X} \in I$. Furthermore, in case $\widetilde{X} \in I$ it follows $Z^p + \mu Z \in I$. Hence, the prime ideals of height 1 which contain $\widetilde{X}$ are of the form $(\widetilde{X}, G(Z))$, where $G(Z)$ is one of the factors in (6.1.22). We will denote these prime ideals by $\mathfrak{P}_1, \ldots, \mathfrak{P}_p$. In case $T_l \in I$ we have $Z^p + \mu Z \in I$, too. Analog to the previous case we will denote the prime ideals $(T_l, G(Z))$ by $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_p$. A maximal ideal $\mathfrak{m}$ of $\widetilde{A}_{l+1}$ is of the form $\mathfrak{m} = (\widetilde{X}, G(Z), T_l - T')$ ($\mathfrak{m} = (T_l, G(Z), \widetilde{X} - X')$ resp.). If we localize with respect to this ideal, the corresponding ideal in the localization will be generated by $\widetilde{X}$ and $T_l - T'$ (T_l and $\widetilde{X} - X'$ resp.), hence the ring is regular at $\mathfrak{m}$. Since these are the only maximal ideals of this ring, the ring itself is regular (Proposition 1.1.6). The blowing-up-morphism $\widetilde{U}_{l+1} = \operatorname{Spec} \widetilde{A}_{l+1} \to \operatorname{Spec} A_l$ is an isomorphism away from $V(X, T_l)$. According to this isomorphism the components $L_{l,i}$ of U_l are the images of the components which correspond to the prime ideals $\mathfrak{P}_i \subset \widetilde{A}_{l+1}$ Therefore, we will denote these components as well by $L_{l,i}$. The components which lie above the singular points will be denoted by $L_{l+1,i}$. They correspond to the prime ideals $\mathfrak{Q}_i$. Then the special fiber has the configuration as in Figure 6.6. The component $L_{l,i}$ intersect the component $L_{l+1,i}$ in the point corresponding to some $\mathfrak{m} = (\widetilde{X}, T_l, G(Z))$. Let us take a look now at the other affine open subset of the blowing-up. Setting $T_{l+1} = \frac{T_l}{X}$ we get

$$A_l\left[T_l X^{-1}\right] \cong S[T_l, T_{l+1}]/(\pi - T_{l+1}X^{l+1}, T_{l+1}X - T_l, g_{l+1}(T_{l+1})) = A_{l+1}\,.$$

Notice, that the components $L_{l+1,i}$ of $U_{l+1} = \operatorname{Spec} A_{l+1}$ are the components $L_{l+1,i}$ of $\operatorname{Spec} \widetilde{A}_{l+1}$. □

Proof of Theorem 6.1.11: According to Lemma 6.1.12 there are just singular closed points on the components of type A and type B. Let $L_{(x_a,y_a)}$ be a component of type A that corresponds to a prime ideal $\mathfrak{P} = (\pi, X, Y - \zeta_m^i) \subset S_1^{sh}$. We consider everything in the affine open subset $U = \operatorname{Spec} A$, where A is the ring of (6.1.15). We blow up U along $V(\mathfrak{P}A)$. Since $\mathfrak{P}A = (\pi, X)$, the blowing-up will be covered by two affine open subsets. Setting $T_1 = \frac{\pi}{X}$ the first one is given by U_1. The only new components are $L_{1,1}, \dots, L_{1,p}$ (cf. Figure 6.5 with $l = 1$). Setting $X_1 = \frac{X}{\pi}$ the second subset is

$$\operatorname{Spec} S[X_1]/(X_1\pi - X, g(X_1))\,,$$

where

$$g(X_1) = Z^p + \mu\frac{\psi((X_1\pi)^m, 1 - (X_1\pi)^m)}{\pi} + \mu\sum_{k=1}^{p-1}\binom{p}{k}p^{-1}Z^{p-k}\pi^{p-k-1}Y^{mk}(-1)^k\,.$$

Here we only have to study the prime ideals $\mathfrak{m}$ with $X_1, \pi \in \mathfrak{m}$, since all the others that lie above π can be found in U_1. We have

$$Z^p + \mu Z = \pi P(X_1)$$

in $S[X_1]/(X_1\pi - X, g(X_1))$, with a polynomial $P(X_1) \in S[X_1]$. It follows $Z^p + \mu Z \in \mathfrak{m}$, which implies

$$Z \in \mathfrak{m} \text{ or } Z - \theta\zeta_{p-1}^i \in \mathfrak{m} \tag{6.1.24}$$

with $0 \leq i \leq p-2$; here $\theta \in R^{sh}$ is an element with $\theta^{p-1} = -\mu$. The prime ideal $\mathfrak{m}$ is of the form $\mathfrak{m} = (\pi, X_1, Z)$ ($\mathfrak{m} = (\pi, X_1, Z - \theta\zeta_{p-1}^i)$ resp.), hence maximal. In fact, they are the "end points" of the components $L_{1,i}$. Since the factors in (6.1.24) are pairwise coprime,

$$\mathfrak{m}\left(S[X_1]/(X_1\pi - X, g(X_1))\right)_{\mathfrak{m}}$$

will be generated by two elements, hence $S[X_1]/(X_1\pi - X, g(X_1))$ is regular at $\mathfrak{m}$. There are p singular closed points lying on $L_{(x_a,y_a)}$ (Lemma 6.1.13). If we blow up this line, we get another p new components $L_{2,1}, \dots, L_{2,p}$ (Lemma 6.1.14). There are no singular closed points lying on the $L_{1,i}$ (Lemma 6.1.14). The only singular closed points that lie on the $L_{2,i}$ or the line $L_{(x_a,y_a)}$, are the points where the $L_{2,i}$ intersect $L_{(x_a,y_a)}$ (Lemma 6.1.13). It is clear that repeating this process (i.e. blowing up the component $L_{(x_a,y_a)}$) (m-3)-times will give the resolution of the singularities that lie on this component, and will therefore yield the configuration we claimed. By symmetry we can argue the same way for components of type A which correspond to prime ideals of the form $\mathfrak{P} = (\pi, X - \zeta_m^i, Y)$. Finally, a similar (but simpler, since no inductive argument is needed) computation shows that we just have to blow up the components of type B once in order to get the remaining statements of the proof. $\square$

Theorem 6.1.15. *Let N be a squarefree odd natural number which has at least two prime factors, ζ_N a primitive N-th root of unity and $N = pm$ with a prime p. Furthermore, let R be the localization of $\mathbb{Z}[\zeta_N]$ with respect to a fixed prime ideal $\mathfrak{p} \in \operatorname{Spec} \mathbb{Z}[\zeta_N]$ that lies above p. We denote by $\mathfrak{F}_{N,\mathfrak{p}}^{min} \to \operatorname{Spec} R$ the minimal regular model of the Fermat curve F_N over R. Then the geometric special fiber*

$$\mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{\mathbb{F}}_p$$

has the configuration as in Figure 6.7; the Table 6.1 gives us the number, multiplicity, genus and self-intersection of the components. Finally, all intersection between components of the geometric special fiber are transverse.

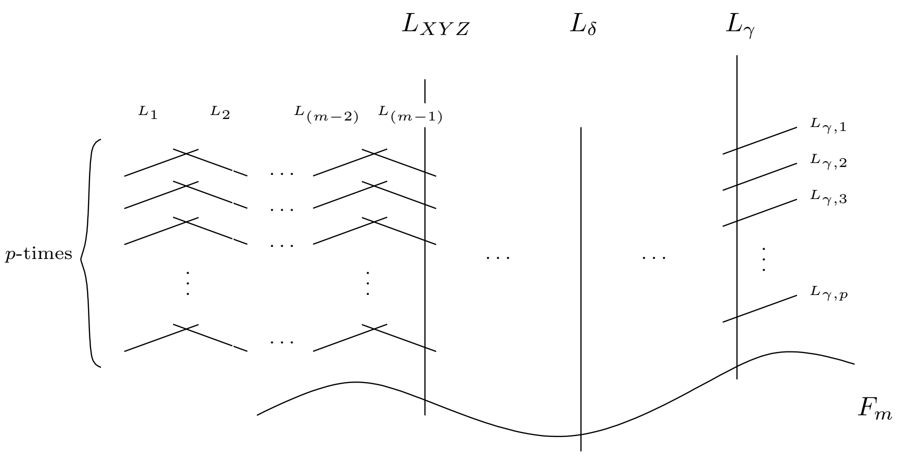

Figure 6.7: The configuration of the geometric special fiber $\mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\operatorname{Spec} R} \operatorname{Spec} \overline{\mathbb{F}}_p$.

Proof: The scheme

$$\mathfrak{F}_{N,\mathfrak{p}}^{0} = \operatorname{Proj} R[X_0, Y_0, Z_0]/(X_0^N + Y_0^N - Z_0^N)$$

is covered by the affine scheme $\mathcal{X}$ in (6.1.2) and

$$\mathcal{X}' = \operatorname{Spec} R[Y', Z']/(1 + Y'^N - Z'^N)$$

	Number of components	Multiplicity	Genus	Self-intersection
L_i	$3mp$	i	0	-2
L_{XYZ}	$3m$	m	0	$-p$
L_γ	$m\varrho$	2	0	$-p$
$L_{\gamma,j}$	$pm\varrho$	1	0	-2
L_δ	$m^2(p-3)-2m\varrho$	1	0	$-p$
F_m	1	p	$\frac{1}{2}(m-1)(m-2)$	$-m^2$

Table 6.1: ϱ denotes the number of factors with multiplicity two of $\Psi(X^m)$ over $\overline{\mathbb{F}}_p$ (cf. Definition 6.1.5).

where $Y' = \frac{Y_0}{X_0}$ and $Z' = \frac{Z_0}{X_0}$. To blow up $\mathfrak{F}^0_{N,\mathfrak{p}}$ along the ideal $V_+(X_0^m + Y_0^m - Z_0^m, \pi)$ is to blow up $\mathcal{X}$ along (π, F_m) and $\mathcal{X}'$ along $(\pi, 1+Y'^m - Z'^m)$ and then glue everything together; we denote these blowing-ups by $\widetilde{\mathcal{X}}$ and $\widetilde{\mathcal{X}}'$. Since $\mathcal{X}$ is isomorphic to $\mathcal{X}'$ and (π, F_m) to $(\pi, 1+Y'^m - Z'^m)$ via $X \mapsto Z'$ and $Y \mapsto -Y'$ the blowing-ups $\widetilde{\mathcal{X}}$ and $\widetilde{\mathcal{X}}'$ are isomorphic as well. The only components of $\widetilde{\mathcal{X}}'$ which are not in $\widetilde{\mathcal{X}}$ are the ones that correspond to prime ideals that contain Z'. According to the isomorphism above these components are isomorphic to the components of type A which contain X. It follows that we can easily use Theorem 6.1.11 to resolve the singularities of these schemes. The regular model of F_N we achieve in this way will be denoted by $\mathfrak{F}_{N,\mathfrak{p}}$. With the discussion above, it follows that it is enough to analyze the regular scheme from Theorem 6.1.11 and to remember that there are a few more components which we cannot see in this affine open subset. We give a sketch of the things one has to do to get the quantities in the table. In fact, we will verify these quantities for $\mathfrak{F}_{N,\mathfrak{p}}$ and at the end of the proof it will turn out that $\mathfrak{F}_{N,\mathfrak{p}} = \mathfrak{F}^{min}_{N,\mathfrak{p}}$. Let us start with the number of components of $\mathfrak{F}_{N,\mathfrak{p}}$. With Theorem 6.1.11 it is clear that the geometric special fiber of $\mathfrak{F}_{N,\mathfrak{p}}$ is of the form Figure 6.7. The vertical components are parametrized by pairs $(x, y) \in \overline{\mathbb{F}}_p$ with $x^m + y^m - 1 = x^m \prod_{i=0}^{m-1}(x - \overline{\zeta}^i_m)\overline{\Psi}(x^m)$ (Proposition 6.1.9). There are ϱ factors $(X - \overline{\gamma}_k)^2$ in $\overline{\Psi}(X^m)$, and for each $\overline{\gamma}_k$ the ploynomial $Y^m + \overline{\gamma}_k^m - 1 \in \overline{\mathbb{F}}_p[Y]$ has m solutions (remember that $\overline{\gamma}_k^m \neq 1$). Hence, we get $m\varrho$ lines. We denote these lines by L_γ (these are the ones of type B in Theorem 6.1.11). Furthermore, there are $m(p-3) - 2\varrho$ linear factors $(X - \overline{\delta})$ and with the same argument as before there are $m(m(p-3) - 2\varrho)$ lines which correspond to these. We denote these by L_δ. Now, the only solutions which are left are the following:

$$(0, \overline{\zeta}^i_m) \tag{6.1.25}$$

for $0 \leq i \leq m-1$, and

$$(\overline{\zeta}^i_m, 0) \tag{6.1.26}$$

for $0 \leq i \leq m-1$. This gives us $2m$ lines (these are the components of type A in Theorem 6.1.11). Like we mentioned before there are more lines which behave like the ones of type A but which cannot be seen in this affine picture. In fact, by the isomorphism we described at the beginning it is clear that there are m more lines, hence these together with the ones of (6.1.25) and (6.1.26) give us $3m$ lines. We denote them by L_{XYZ}. According to

Theorem 6.1.11, for each L_{XYZ} there are p chains of $m-1$ lines, where the ends of the chains intersect L_{XYZ}. These ends will be denoted by $L_{(m-1)}$ and the following lines by $L_{(m-2)}, L_{(m-3)}$, etc. As well according to Theorem 6.1.11 there are p lines intersecting each L_γ. We will denote these lines by $L_{\gamma,1}, \dots, L_{\gamma,p}$. Collecting this information we get the number of components of table 6.1.

Next, we want to study the multiplicity of the components. To do this one may use Remark 1.4.13. We will illustrate this in a few cases. For example let us return to the scheme $U_l = \operatorname{Spec} A_l$ in (6.1.16). The prime ideals of height 1 of A_l are (π, X, Z) and $(\pi, X, Z - \theta\zeta_{p-1}^i)$ for $0 \le i \le p-2$. These correspond to the components L_l. Furthermore, there is the prime ideal (π, X, T_l) which will correspond to a L_{XYZ} (after blowing up (m-1-l)-times). Let $\mathfrak{P}$ be a prime ideal that corresponds to L_l. In Theorem 6.1.11 we have seen that $\mathfrak{P}(A_l)_{\mathfrak{P}} = (X)$. Since $\pi = T_l X^l$ in A_l and T_l becomes a unit in $(A_l)_{\mathfrak{P}}$, we get $\nu_{L_l}(\pi) = l$, hence the multiplicity of L_l is l. Now, let $\mathfrak{P} = (\pi, X, T_l)$. Equation (6.1.17) shows us that $T_l = X^{m-l}\epsilon$ in $(A_l)_{\mathfrak{P}}$ with a unit $\epsilon \in (A_l)^*_{\mathfrak{P}}$. With the same argument as before we get $\nu_{L_{XYZ}}(\pi) = m$, hence the component L_{XYZ} has multiplicity m. To get the multiplicities of the other components one can continue in the same way with the other components. The genera of the components are clear; the formula $\frac{1}{2}(m-1)(m-2)$ is just the well known genus formula for curves which are given by a homogenous polynomial of degree m.

Next, we prove that all intersections are transverse. Let us denote by $\mathfrak{F}_\pi$ the geometric special fiber of $\mathfrak{F}_{N,\mathfrak{p}}$. According to Remark 1.4.14 we have

$$\mathfrak{F}_\pi = \sum d_\Gamma \Gamma \,,$$

where the sum runs over all components together with their multiplicity (the symbol Γ stands for any of the components in Figure 6.7). To each component Γ of the right-hand side, we have

$$0 < \Gamma(\mathfrak{F}_\pi - d_\Gamma \Gamma) \,.$$

Let us denote by I_Γ the sum of the multiplicities of the components that have a positive intersection number with Γ. Obviously we have

$$I_\Gamma \le \Gamma(\mathfrak{F}_\pi - d_\Gamma \Gamma)$$

and equality holds for all Γ if and only if all intersections are transverse. We get the following table:

Γ	I_Γ
L_i	$2i$
L_{XYZ}	$p + p(m-1)$
L_γ	$2p$
$L_{\gamma,j}$	2
L_δ	p
F_m	$m^2 p$

Let us denote by $\mathcal{K}$ a canonical divisor of $\mathfrak{F}_{N,\mathfrak{p}}$. By the adjunction formula (Theorem 1.4.9) and Proposition 1.4.15 we have

$$\begin{aligned}2g_a(F_N) - 2 &= \mathcal{K} \cdot \mathfrak{F}_\pi \\ &= \sum d_\Gamma \mathcal{K} \cdot \Gamma \\ &= \sum d_\Gamma(-\Gamma^2 + 2g_a(\Gamma) - 2) \\ &= \sum \Gamma(\mathfrak{F}_\pi - d_\Gamma \Gamma) + 2pg_a(F_m) - 2\sum d_\Gamma \\ &\geq \sum I_\Gamma + 2pg_a(F_m) - 2\sum d_\Gamma\,,\end{aligned}$$

hence the intersections are transverse if and only if

$$2g_a(F_N) - 2 = \sum I_\Gamma + 2pg_a(F_m) - 2\sum d_\Gamma\,. \tag{6.1.27}$$

Using the known quantities of Table 6.1 and the table for the I_Γ we get

$$\sum I_\Gamma = 3m^3p - 2m^2p + 2pm\varrho + m^2p^2$$

and

$$-2\sum d_\Gamma = -3m^3p + m^2p - 2pm\varrho - 2p\,.$$

We have

$$2g_a(F_N) - 2 = m^2p^2 - 3mp$$

and

$$\begin{aligned}\sum I_\Gamma - 2\sum d_\Gamma + 2pg_a(F_m) &= -m^2p + m^2p^2 - 2p + p(m-1)(m-2) \\ &= m^2p^2 - 3mp\,,\end{aligned}$$

which yields the equality (6.1.27) and therefore the transversality of the intersections. Since we know the intersection numbers and the configuration of the geometric special fiber, one can use Proposition 1.4.15 (1.) to get the self-intersection number of the components. Finally, since there are no exceptional divisors, Corollary 2.2.9 tells us, that $\mathfrak{F}_{N,\mathfrak{p}}$ is already the minimal regular model. $\square$

Corollary 6.1.16. *Let $\mathfrak{F}_{N,\mathfrak{p}}^{normal}$ be the normalization of the scheme*

$$\mathfrak{F}_{N,\mathfrak{p}}^0 = \operatorname{Proj} R[X,Y,Z]/(X^N + Y^N - Z^N)\,.$$

Then all singular (closed) points are rational singularities.

Proof: Let $f^{nor} : \mathfrak{F}^{min}_{N,\mathfrak{p}} \to \mathfrak{F}^{nor}_{N,\mathfrak{p}}$ be the desingularization of $\mathfrak{F}^{normal}_{N,\mathfrak{p}}$, where $\mathfrak{F}^{min}_{N,\mathfrak{p}}$ is the minimal regular model from Theorem 6.1.15. Let $P \in \mathfrak{F}^{normal}_{N,\mathfrak{p}}$ be a singular point and $\mathcal{C}_1, \ldots, \mathcal{C}_n$ the components of $\mathfrak{F}^{min}_{N,\mathfrak{p}}$ with $f^{nor}(\mathcal{C}_i) = P$. Then P is rational if and only if the fundamental cycle $\mathcal{Z}_P$ with respect to P fulfills $p_a(\mathcal{Z}_P) = 0$ (see. [Ar2], p.132: Theorem 3.). Using Theorem 6.1.15 it can be easily seen that

$$\mathcal{Z}_P = \sum_{i=1}^{n} \mathcal{C}_i \,.$$

Now, the adjunction formula together with an inductive argument yields

$$p_a(\mathcal{Z}_P) = \sum_{i=1}^{n} p_a(\mathcal{C}_i) + \sum_{1 \le i < j \le n} \mathcal{C}_i \cdot \mathcal{C}_j - (n-1) = \sum_{1 \le i < j \le n} \mathcal{C}_i \cdot \mathcal{C}_j - (n-1)\,.$$

Finally, it can be easily seen - using the configuration described in Theorem 6.1.15 - that $p_a(\mathcal{Z}_P) = 0$. $\square$

Remark 6.1.17. Let $U \subset \operatorname{Spec} \mathbb{Z}[\zeta_N]$ be the open subset consisting of the prime ideals $\mathfrak{p}$ with $N \notin \mathfrak{p}$, hence $U = \operatorname{Spec} \mathbb{Z}[\zeta_N, 1/N]$. We set $\mathfrak{F}^{min}_{N,U} := \mathfrak{F}^0_N \times_{\operatorname{Spec} \mathbb{Z}[\zeta_N]} U$, where

$$\mathfrak{F}^0_N = \operatorname{Proj} \mathbb{Z}[\zeta_N][X,Y,Z]/(X^N + Y^N - Z^N)\,;$$

the scheme $\mathfrak{F}^{min}_{N,U}$ is regular by Proposition 1.1.13. For a prime ideal $\mathfrak{p}$ with $N \in \mathfrak{p}$ we take the minimal regular model $\mathfrak{F}^{min}_{N,\mathfrak{p}}$ from Theorem 6.1.15, where $\mathfrak{p} \cap \mathbb{Z} = (p)$. Now, we glue the scheme $\mathfrak{F}^{min}_{N,U}$ and all the $\mathfrak{F}^{min}_{N,\mathfrak{p}}$ together and obtain the minimal regular model $\mathfrak{F}^{min}_N$of the Fermat curve F_N over $\operatorname{Spec} \mathbb{Z}[\zeta_N]$ (see Section 2.3). This model is indeed the minimal regular model, since it is regular and there are no exceptional divisors. Notice, that the bad primes in this situation are exactly the primes $\mathfrak{p}$ with $N \in \mathfrak{p}$. Hence, a prime $\mathfrak{p}$ is bad if and only if $p|N$, where $\mathfrak{p} \cap \mathbb{Z} = (p)$. The special fiber above a good prime $\mathfrak{q} \in U$ just consists of one component. This component is of multiplicity one. Similar to Remark 4.1.3 the morphism $\beta : F_N \to \mathbb{P}^1$ in (3.2.12) extends to a morphism

$$\beta : \mathfrak{F}^{min}_N \to \mathbb{P}^1_{\mathbb{Z}[\zeta_N]}$$

($\beta : \mathfrak{F}^{min}_{N,\mathfrak{p}} \to \mathbb{P}^1_R$ resp.) since we were just performing a sequence of blowing-ups.

With the regular model we are ready now to compute a first upper bound for the arithmetic self-intersection number of the dualizing sheaf. In order to do this we will use the results of Subsection 3.2.2 to approximate the geometric contribution.

Theorem 6.1.18. *Let N be a squarefree odd integer with at least two prime factors, and let $\mathfrak{F}^{min}_N$ be the minimal regular model of the fermat curve F_N over* $\operatorname{Spec} \mathbb{Z}[\zeta_N]$. *Then the* *arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}} \leq (2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_N):\mathbb{Q}](\kappa_1 \log N + \kappa_2)\right)$$

$$+ (2g-2) \sum_{\mathfrak{p}\supset(N)} \frac{4gN^{8\frac{N}{p}+4}}{3^{8\frac{N}{p}-2}(N^2-9)} \log \mathrm{Nm}(\mathfrak{p}),$$

where $\kappa_1, \kappa_2 \in \mathbb{R}_+^*$ are positive constants independent of N.

Proof: In Remark 3.2.18 we saw that the morphism $\beta : F_N \to \mathbb{P}^1$ fulfills the requirements of Theorem 3.2.2, hence we only have bound the geometric contribution. In order to do this we will use Proposition 3.2.9 and Theorem 3.2.10. Using the notation of Proposition 3.2.9 we have $3^2 \leq u_\mathfrak{p} = \max\{p, m^2\} \leq \left(\frac{N}{3}\right)^2$, $l_\mathfrak{p} = 1$ and $c_\mathfrak{p} = 2m = 2\frac{N}{p}$ (cf. Theorem 6.1.15). Since $0 \leq \varrho \leq \frac{m}{2}(p-3)$ we get

$$\begin{aligned} r_\mathfrak{p} - c_\mathfrak{p} - 1 &= 3mp(m-1) + m + \varrho m(p-1) + m^2(p-3) \\ &\leq 3mp(m-1) + m + \frac{m^2}{2}(p-3)(p+1) \\ &< N + \frac{3N^2}{2}. \end{aligned}$$

We will approximate

$$\sum_{l=0}^{k-1} u^l < \frac{u^k}{u-1}$$

and

$$\begin{aligned} \sum_{k=1}^{c_\mathfrak{p}} u^{2k} &= \frac{(u^{c_\mathfrak{p}+1}-u)(u^{c_\mathfrak{p}+1}+u)}{(u-1)(u+1)} \\ &= \frac{u}{u-1}\frac{u}{u+1}(u^{2c_\mathfrak{p}}-1) < \frac{u^2}{u^2-1}u^{2c_\mathfrak{p}} \end{aligned}$$

in order to obtain

$$\begin{aligned} b_\mathfrak{p} &= \left(\sum_{k=1}^{c_\mathfrak{p}}\left(\sum_{l=1}^{k} u_\mathfrak{p}^{l-1}\right)^2 + (r_\mathfrak{p} - c_\mathfrak{p} - 1)\left(\sum_{l=1}^{c_\mathfrak{p}} u_\mathfrak{p}^{l-1}\right)^2\right) u_\mathfrak{p} \\ &< \left(\sum_{k=1}^{c_\mathfrak{p}} u_\mathfrak{p}^{2k} + (N + \frac{3N^2}{2})u_\mathfrak{p}^{2c_\mathfrak{p}}\right)\frac{u_\mathfrak{p}}{(u_\mathfrak{p}-1)^2} \\ &< \left(\frac{81}{80} + N + \frac{3N^2}{2}\right)\frac{u_\mathfrak{p}^{2c_\mathfrak{p}+1}}{(u_\mathfrak{p}-1)^2} \end{aligned} \tag{6.1.28}$$

Now since $\frac{81}{80} + N + \frac{3N^2}{2} < 2N^2$ and $u_{\mathfrak{p}} \leq \left(\frac{N}{3}\right)^2$ the term (6.1.28) is smaller than

$$2N^2 \frac{\left(\frac{N}{3}\right)^{8\frac{N}{p}+2}}{(\left(\frac{N}{3}\right)^2 - 1)^2} = \frac{2N^{8\frac{N}{p}+4}}{3^{8\frac{N}{p}-2}(N^2-9)} \, .$$

Therefore, it follows with Theorem 3.2.10

$$\sum_{\mathfrak{p} \text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) < \sum_{\mathfrak{p} \text{ bad}} \frac{4gN^{8\frac{N}{p}+4}}{3^{8\frac{N}{p}-2}(N^2-9)} \log \mathrm{Nm}(\mathfrak{p}) \, ,$$

hence the claim. □

Remark 6.1.19. One may use the results of Subsection 3.2.2 less wastefully in order to get an improvement of Theorem 6.1.18. However, this is not our intention since we will compute the geometric contribution exactly in the next subsection. Taking a look at Theorem 6.1.18 one could get the impression in case of the Fermat curves in question that the geometric contribution is the dominating term in the inequality (3.2.1). In the next subsection it will turn out as well that this is not the case.

6.2 Explicit geometric contributions to Kühn's formula for $\overline{\omega}_{\mathbf{Ar}^2}$ in the squarefree case

Let N be a squarefree odd integer, which is not a prime number, and $\mathfrak{F}_N^{min}$ the minimal model described in Section 6.1, which was obtained by glueing the models $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ of Theorem 6.1.15 and the model $\mathfrak{F}_{N,U}^{min}$ (cf. Remark 6.1.17).

Proposition 6.2.1. *Let S be a cusp of F_N and $\mathcal{S}$ the horizontal divisor obtained by taking the Zariski-closure of S in $\mathfrak{F}_{N,\mathfrak{p}}^{min}$. Then $\mathcal{S}$ only intersects one component of the geometric special fiber, namely one of the L_1 (see. Figure 6.7). Again, this intersection is transverse.*

Proof: We use Notation 3.2.19. Without loss of generality we assume $S = S_{x_i}$, with an integer i. If we take the Zariski-closure of S in

$$\mathfrak{F}_{N,\mathfrak{p}}^0 = \mathrm{Proj}\, R[X,Y,Z]/(X^N + Y^N - Z^N) \tag{6.2.1}$$

we get a horizontal divisor $\mathcal{S}^0$, which corresponds to the prime ideal $(X, Y - \zeta_N^i, Z - 1)$. It intersects the special fiber in the point $P_{x_i} = V_+((X, Y - \zeta_N^i, Z - 1, \pi))$. Now, our minimal regular Model $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ comes together with a birational morphism

$$f : \mathfrak{F}_{N,\mathfrak{p}}^{min} \to \mathfrak{F}_{N,\mathfrak{p}}^0 \, ; \tag{6.2.2}$$

in fact, f is just the composition of the blowing-ups in Proposition 6.1.7, Theorem 6.1.11 and Theorem 6.1.15. We have

$$\mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \overline{\mathbb{F}}_p \cdot \mathcal{S} = \deg_{K^{sh}} S = 1 \, , \tag{6.2.3}$$

where $K^{sh} = \mathrm{Frac}(R^{sh})$ (see e.g. [Liu], p.388: Remark 1.31.). It follows that $\mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, \overline{\mathbb{F}}_p \cap \mathcal{S}$ is reduced to a point P and that P belongs to a single irreducible component which is of multiplicity one (compare e.g. with [Liu], p.388: Corollary 1.32.). Furthermore, (6.2.3) shows us that $\mathcal{S}$ intersects this component transversally (see e.g. [Liu], p.378: Proposition 1.8.). On the other hand, we have $P \in f^{-1}(P_{x_i})$. But $f^{-1}(P_{x_i})$ consists of one component L_{XYZ} and p chains of components $L_1, L_2, \ldots, L_{(m-1)}$, where the $L_{(m-1)}$ intersect the component L_{XYZ} (compare with Figure 6.7). Since the only components of $f^{-1}(P_{x_i})$ of multiplicity one are the L_1, P must lie on one of them. □

Remark 6.2.2. We use Notation 3.2.19. In the proof of Proposition 6.2.1 we saw that the horizontal divisor $\mathcal{S}_{x_i}$, which was obtained as the Zariski-closure of the cusp S_{x_i}, just intersects one of the components L_1, which lies in $f^{-1}(P_{x_i})$; here $P_{x_i} = V_+((X, Y - \zeta_N^i, Z - 1, \pi))$ and $f : \mathfrak{F}_{N,\mathfrak{p}}^{min} \to \mathfrak{F}_{N,\mathfrak{p}}^0$ is the minimal desingularization of $\mathfrak{F}_{N,\mathfrak{p}}^0$. Analog to this we obtain that the horizontal divisor that corresponds to a cusp S_{y_i} (S_{z_i} resp.) intersects a component L_1 that lies in $f^{-1}(P_{y_i})$ ($f^{-1}(P_{z_i})$ resp.), where $P_{y_i} = V_+((X - \zeta_N^i, Y, Z - 1, \pi))$ and $P_{z_i} = V_+((X - \zeta_N^i, Y + 1, Z, \pi))$.

Since there are $3N$ components L_1 and $3N$ cusps we could guess that each L_1 was intersected by exactly one horizontal divisor which comes from a cusp. In fact, we show in the next proposition that this is the case.

Proposition 6.2.3. *For the cusps S and S' of F_N we denote by $\mathcal{S}$ and $\mathcal{S}'$ the associated horizontal divisors of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$. According to Proposition 6.2.1 these horizontal divisors intersect components L and L' of the special fiber (both are one of the L_1). We have $S = S'$ if and only if $L = L'$.*

Proof: We use Notation 3.2.19. We only have to show that $L = L'$ implies $S = S'$ (the other direction is tautological). Let us assume that this is not true. Then there exist S and S' with $S \neq S'$ and $L = L'$. According to Remark 6.2.2 we may assume without loss of generality that $S = S_{x_i}$ and $S' = S_{x_j}$ with $0 \le j < i < N$. Remember that the morphism f in (6.2.2) factors $f : \mathfrak{F}_{N,\mathfrak{p}}^{min} \xrightarrow{f_1} \mathfrak{F}_{N,\mathfrak{p}}^1 \xrightarrow{f_0} \mathfrak{F}_{N,\mathfrak{p}}^0$, where $\mathfrak{F}_{N,\mathfrak{p}}^1$ is the blowing-up of $\mathfrak{F}_{N,\mathfrak{p}}^0$ along $V(X^m + Y^m - Z^m, \pi)$. The scheme $\mathfrak{F}_{N,\mathfrak{p}}^1$ is covered by $\widetilde{\mathcal{X}}$ and $\widetilde{\mathcal{X}}'$ (cf. beginning of the proof of Theorem 6.1.15). and its special fiber just consists of the components $F_m, L_{XYZ}, L_{\gamma_i}$ and L_δ. According to our assumption we must have $\mathrm{Supp}\, f_1(\mathcal{S}_{x_i}) \cap \mathrm{Supp}\, f_1(\mathcal{S}_{x_j}) = P$ with a closed point P which lies in the special fiber of $\mathfrak{F}_{N,\mathfrak{p}}^1$ (this follows since all the components L_i were blown down to points by f_1). In fact P is a singular point which lies in $\widetilde{\mathcal{X}}$. It makes therefore sence to analyze $\widetilde{\mathcal{X}}$ (cf. Proposition 6.1.7) again. Since all the singular points of $\widetilde{\mathcal{X}}$ lie in $U_1 = \mathrm{Spec}\, S_1$ (cf. (6.1.10) and proof of Lemma 6.1.12) we can restrict our attention to this affine open subset. Because $F_m = Z\pi$ in S_1 an easy computation shows that

$$f_1(\mathcal{S}_{x_i})|_{U_1} = V\left(X, Y - \zeta_N^i, Z - \frac{(\zeta_N^{im} - 1)}{\pi}\right)$$

and

$$f_1(\mathcal{S}_{x_j})|_{U_1} = V\left(X, Y - \zeta_N^j, Z - \frac{(\zeta_N^{jm} - 1)}{\pi}\right)$$

(notice that $\frac{(\zeta_N^{km}-1)}{\pi} \in R^*$ or $\frac{(\zeta_N^{km}-1)}{\pi} = 0$ since ζ_N^m is a primitive p-th root of unity). Let $\mathfrak{m}$ be the maximal ideal of S_1 with $V(\mathfrak{m}) = P$. Then

$$\zeta_N^i - \zeta_N^j = \zeta_N^j(\zeta_N^{i-j} - 1) \in \mathfrak{m}$$

and since $\pi \in \mathfrak{m}$ we must have $p \nmid i - j$. Indeed, let us assume that p divides $i - j$. Then the order of ζ_N^{i-j} is coprime to p and therefore $\mathfrak{m}$ contains a natural number coprime to p, hence a contradiction. On the other hand, since

$$\frac{(\zeta_N^{im} - 1)}{\pi} - \frac{(\zeta_N^{jm} - 1)}{\pi} = \frac{\zeta_N^{jm}(\zeta_N^{(i-j)m} - 1)}{\pi} \in \mathfrak{m}\,,$$

we have $\zeta_N^{(i-j)m} = 1$, hence $p | i - j$. This gives us another contradiction and shows that $S = S'$. $\square$

Similar to the situation in Section 4.2 we will compute now the canonical divisor for our schemes $\mathfrak{F}_N^{min}$ and $\mathfrak{F}_{N,\mathfrak{p}}^{min}$. Let us consider first the scheme $\mathfrak{F}_{N,\mathfrak{p}}^{min}$. Again, we can use Lemma 3.2.16, which tells us that if we have a horizontal divisor $\mathcal{S}_j$ coming from a cusp S_j, then there exists a canonical divisor of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ of the form

$$\mathcal{K}_{j,\mathfrak{p}} = (2g-2)\mathcal{S}_j + \mathcal{V}_{j,\mathfrak{p}}\,, \tag{6.2.4}$$

where $\mathcal{V}_{j,\mathfrak{p}}$ is a vertical divisor with support in the special fiber.

We can interpret any vertical divisor of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ as a divisor of $\mathfrak{F}_N^{min}$. Using this we can show the following:

Proposition 6.2.4. *We interpret the vertical divisors $\mathcal{V}_{j,\mathfrak{p}}$ of (6.2.4) as divisors of $\mathfrak{F}_N^{min}$. If we set*

$$\mathcal{V}_j = \sum_{\mathfrak{p}\text{ bad}} \mathcal{V}_{j,\mathfrak{p}}\,,$$

where the sum runs over all bad prime ideals $\mathfrak{p}$, then

$$\mathcal{K}_j = (2g-2)\mathcal{S}_j + \mathcal{V}_j \tag{6.2.5}$$

is a canonical divisor of $\mathfrak{F}_N^{min}$. In particular, if we set $\mathcal{F}_{j,\mathfrak{p}} = \frac{1}{(2g-2)}\mathcal{V}_{j,\mathfrak{p}}$, then $\mathcal{F}_j = \sum_{\mathfrak{p}\text{ bad}} \mathcal{F}_{j,\mathfrak{p}}$ fulfills (3.2.2).

Proof: Any divisor, who satisfies the adjunction formula and whose restriction to the generic fiber F_N is a canonical divisor of F_N, is a canonical divisor of $\mathfrak{F}_N^{min}$ (Proposition 1.4.16). Obviously $\mathcal{K}_j|_{F_N}$ is a canonical divisor of F_N, hence the only thing to verify is that $\mathcal{K}_j$ fulfills the adjunction formula. Now, let $\mathcal{E}$ be a vertical prime divisor of $\mathfrak{F}_N^{min}$. If $\mathcal{E}$ is contained in a special fiber above a bad prime $\mathfrak{p}$, then

$$\mathcal{K}_j \cdot \mathcal{E} = \mathcal{K}_{j,\mathfrak{p}} \cdot \mathcal{E} = 2p_a(\mathcal{E}) - 2 - \mathcal{E}^2 .$$

Otherwise $\mathcal{E}$ is a special fiber itself, which lies above a "good" prime $\mathfrak{q}$ (Remark 6.1.17 and Proposition 1.4.11). We have

$$\mathcal{K}_j \cdot \mathcal{E} = 2p_a(F_N) - 2 ,$$

(Proposition 1.4.15 (1.) and [Liu], p.388: Remark 1.31.). On the other hand we have $p_a(\mathcal{E}) = p_a(F_N)$ and $\mathcal{E}^2 = 0$ (Proposition 1.4.15 and [Liu], p. 350: Corollary 3.6.), hence the adjunction formula is fulfilled. This yields the first claim. The second claim is obvious. □

With Proposition 6.2.4 in mind it seems to be useful to determine the $\mathcal{K}_{x,\mathfrak{p}}$ in (6.2.4), because this yields a canonical divisor for $\mathfrak{F}_N^{min}$. In order to construct this divisor explicitly we need to distinguish between the components in the special fiber. For this reason we will number these components.

Notation 6.2.5. We use the notation from Theorem 6.1.15. Let us fix a cusp S and a corresponding horizontal divisor $\mathcal{S}$. We know that $\mathcal{S}$ just intersects one of the component of the special fiber, in fact it must be one of the L_1 (Proposition 6.2.1). In the geometric special fiber of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ there are $3m$ components L_{XYZ}. To distinguish between these components we will number them and denote by $L^{(i)}$ the i-th one of the L_{XYZ}. Now, for each component $L^{(i)}$ there are p chains of components $L_1, L_2, \dots L_{(m-1)}$, where the $L_{(m-1)}$ intersect $L^{(i)}$. Again, we will number these chains. We denote the components of the chains by $L_{j,k}^{(i)}$, where the superscript shows the belonging to $L^{(i)}$, the first subscript j indicates that it is one of the components L_j and the second subscript k shows that it is a component of the k-th chain. In the same way we proceed with the components L_γ and L_δ. We will number them and denote them by $L_\gamma^{(i)}$ and $L_\delta^{(i)}$. The components $L_{\gamma,j}$ will be denoted by $L_{\gamma,j}^{(i)}$, where the superscript i indicates that $L_{\gamma,j}^{(i)}$ intersects $L_\gamma^{(i)}$. Without loss of generality we assume that we did this numbering in a way that $\mathcal{S}$ intersects the component $L_{1,1}^{(1)}$.

Now we are ready to compute a canonical divisor of the scheme $\mathfrak{F}_{N,\mathfrak{p}}^{min}$. We set

$$\mathcal{V} = \sum_{i=1}^{3m} \left(\sum_{j=1}^{m-1} \sum_{k=1}^{p} \lambda_{j,k}^{(i)} L_{j,k}^{(i)} + \lambda^{(i)} L^{(i)} \right) \tag{6.2.6}$$

and

$$\mathcal{V}_\Sigma = \sum_{i=1}^{m\varrho} \left(\sum_{j=1}^{p} \lambda_{\gamma,j}^{(i)} L_{\gamma,j}^{(i)} + \lambda_\gamma^{(i)} L_\gamma^{(i)} \right) + \sum_{i=1}^{m^2(p-3)-2m\varrho} \lambda_\delta^{(i)} L_\delta^{(i)} , \tag{6.2.7}$$

where ϱ is the number introduced in Definition 6.1.5 and the coefficients are defined by

$$\lambda^{(1)} = \frac{2g-2}{p} - \frac{m(p-2)}{p}\,, \tag{6.2.8}$$

$$\lambda^{(1)}_{j,1} = \frac{1}{m}\left(\lambda^{(1)}j + (m-j)(2g-2)\right) \qquad 1 \le j \le m-1, \tag{6.2.9}$$

$$\lambda^{(1)}_{j,k} = \frac{1}{m}\lambda^{(1)}j \qquad 1 \le j \le m-1;\ 2 \le k \le p, \tag{6.2.10}$$

$$\lambda^{(i)} = -\frac{m(p-2)}{p} \qquad 2 \le i \le 3m, \tag{6.2.11}$$

$$\lambda^{(i)}_{j,k} = -\frac{p-2}{p}j \qquad 2 \le i \le 3m;\ 1 \le j \le m-1;\ 1 \le k \le p \tag{6.2.12}$$

$$\lambda^{(i)}_{\gamma,j} = -\frac{p-2}{p} \qquad 1 \le j \le p;\ 1 \le i \le m\varrho \tag{6.2.13}$$

$$\lambda^{(i)}_{\gamma} = -2\left(\frac{p-2}{p}\right) \qquad 1 \le i \le m\varrho \tag{6.2.14}$$

$$\lambda^{(i)}_{\delta} = -\frac{p-2}{p} \qquad 1 \le i \le m^2(p-3) - 2m\varrho\,. \tag{6.2.15}$$

Similar to the previous subsection we can show the following lemma:

Lemma 6.2.6. *The divisor*

$$\mathcal{K}_{\mathfrak{p}} = (2g-2)\mathcal{S} + \mathcal{V} + \mathcal{V}_{\Sigma}\,, \tag{6.2.16}$$

where $\mathcal{V}$ *and* $\mathcal{V}_{\Sigma}$ *are given by* (6.2.6) *and* (6.2.7)*, is a canonical divisor of* $\mathfrak{F}^{min}_{N,\mathfrak{p}}$.

Proof: According to Proposition 1.4.16 it is enough to check that $\mathcal{K}_{\mathfrak{p}}$ fulfills the adjunction formula. This can be verified using the quantities computed in Theorem 6.1.15. □

Lemma 6.2.7. *Let* $\mathcal{V}$ *and* $\mathcal{V}_{\Sigma}$ *be the divisors of* (6.2.6) *and* (6.2.7)*. Then we have*

$$\mathcal{V}\cdot\mathcal{V} = -(3m-1)pm\left(\frac{p-2}{p}\right)^2 + \lambda^{(1)}\left((p-2) - \frac{(2g-2)}{m}\right) - \frac{m-1}{m}(2g-2)^2\,, \tag{6.2.17}$$

$$\mathcal{V}_{\Sigma}\cdot\mathcal{V}_{\Sigma} = -pm^2(p-3)\left(\frac{p-2}{p}\right)^2 \tag{6.2.18}$$

and

$$\mathcal{V}\cdot\mathcal{V}_{\Sigma} = 0\,. \tag{6.2.19}$$

Proof: Let us prove (6.2.17). By the adjunction formula we have $\mathcal{V}\cdot L^{(i)} = \mathcal{K}_{\mathfrak{p}}\cdot L^{(i)} = p-2$ for all components $L^{(i)}$; the divisor $\mathcal{K}_{\mathfrak{p}}$ is the canonical divisor of Lemma 6.2.6. For a component $L^{(i)}_{j,k}$ with $ijk \neq 1$ we have $\mathcal{V}\cdot L^{(i)}_{j,k} = \mathcal{K}_{\mathfrak{p}}\cdot L^{(i)}_{j,k} = 0$. Furthermore, the intersection of $L^{(1)}_{1,1}$ with $\mathcal{V}$ is $-(2g-2)$, since $0 = \mathcal{K}_{\mathfrak{p}}\cdot L^{(1)}_{1,1} = ((2g-2)\mathcal{S}+\mathcal{V})\cdot L^{(1)}_{1,1} = (2g-2)+\mathcal{V}\cdot L^{(1)}_{1,1}$. Now, using equation (6.2.6), we get

$$\mathcal{V}\cdot\mathcal{V} = \mathcal{V}\cdot\sum_{i=1}^{3m}\left(\sum_{j=1}^{m-1}\sum_{k=1}^{p}\lambda^{(i)}_{j,k}L^{(i)}_{j,k} + \lambda^{(i)}L^{(i)}\right) \tag{6.2.20}$$

$$= \sum_{i=1}^{3m}\left(\sum_{j=1}^{m-1}\sum_{k=1}^{p}\lambda^{(i)}_{j,k}(\mathcal{V}\cdot L^{(i)}_{j,k}) + \lambda^{(i)}(\mathcal{V}\cdot L^{(i)})\right) \tag{6.2.21}$$

$$= -\lambda^{(1)}_{1,1}(2g-2) + (p-2)\lambda^{(1)} - (3m-1)(p-2)m\left(\frac{p-2}{p}\right), \tag{6.2.22}$$

where we used equation (6.2.11) in the last line. Substituting the number of (6.2.9), we get

$$\mathcal{V}\cdot\mathcal{V} = -\frac{1}{m}\left(\lambda^{(1)} + (m-1)(2g-2)\right)(2g-2) + (p-2)\lambda^{(1)} - (3m-1)pm\left(\frac{p-2}{p}\right)^2.$$

After rearranging the terms we will get the formular for the self-intersection of $\mathcal{V}$.

Next, we show (6.2.18). If we take a look at the configuration of the geometric special fiber given in Figure 6.7, we see that the components $L^{(i)}_{\delta}$ and $L^{(i)}_{\gamma}$ intersect F_m and itself. While these are the only components in case of the $L^{(i)}_{\delta}$, a component $L^{(i)}_{\gamma}$ intersects more components, namely the $L^{(i)}_{\gamma,j}$ for $1\leq j\leq p$. Finally, a component $L^{(i)}_{\gamma,j}$ just intersects the component $L^{(i)}_{\gamma}$ and itself. Since F_m does not appear in the sum $\mathcal{V}_\Sigma$, it follows

$$\mathcal{V}_\Sigma\cdot\mathcal{V}_\Sigma = \sum_{i=1}^{m\varrho}\left(\sum_{j=1}^{p}\lambda^{(i)}_{\gamma,j}L^{(i)}_{\gamma,j} + \lambda^{(i)}_{\gamma}L^{(i)}_{\gamma}\right)^2 + \sum_{i=1}^{m^2(p-3)-2m\varrho} -p\left(\lambda^{(i)}_{\delta}\right)^2.$$

We have

$$\left(\sum_{j=1}^{p}\lambda^{(i)}_{\gamma,j}L^{(i)}_{\gamma,j} + \lambda^{(i)}_{\gamma}L^{(i)}_{\gamma}\right)\cdot L^{(i)}_{\gamma,j} = \mathcal{V}_\Sigma\cdot L^{(i)}_{\gamma,j} = \mathcal{K}_{\mathfrak{p}}\cdot L^{(i)}_{\gamma,j} = 0$$

for every i and j, hence

$$\begin{aligned}\left(\sum_{j=1}^{p}\lambda^{(i)}_{\gamma,j}L^{(i)}_{\gamma,j} + \lambda^{(i)}_{\gamma}L^{(i)}_{\gamma}\right)^2 &= \left(\sum_{j=1}^{p}\lambda^{(i)}_{\gamma,j}L^{(i)}_{\gamma,j} + \lambda^{(i)}_{\gamma}L^{(i)}_{\gamma}\right)\cdot\lambda^{(i)}_{\gamma}L^{(i)}_{\gamma}\\ &= 2p\left(\frac{p-2}{p}\right)^2 - 4p\left(\frac{p-2}{p}\right)^2\\ &= -2p\left(\frac{p-2}{p}\right)^2\end{aligned}$$

It follows that

$$\mathcal{V}_\Sigma \cdot \mathcal{V}_\Sigma = -2pm\varrho \left(\frac{p-2}{p}\right)^2 - pm^2(p-3)\left(\frac{p-2}{p}\right)^2 + 2pm\varrho\left(\frac{p-2}{p}\right)^2 ,$$

which yields our claim.

Finally, equation (6.2.19) follows since $\operatorname{Supp}\mathcal{V} \cap \operatorname{Supp}\mathcal{V}_\Sigma = \emptyset$.

□

Next we want to find a divisor $\mathcal{D}_\mathfrak{p}$ of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$, where the invertible sheaf which is associated to $N^2\mathcal{D}_\mathfrak{p}$ is isomorphic to the pullback of the twisting sheaf of Serre $\beta^*\mathcal{O}_{\mathbb{P}^1_R}(1)$. Without loss of generality we continue assuming that $\mathcal{S}$ just intersects the component $L_{1,1}^{(1)}$ in the special fiber. We set

$$\mathcal{G}_\mathfrak{p} = \sum_{j=1}^{m-1}\sum_{k=1}^{p} \mu_{j,k} L_{j,k}^{(1)} + \mu L^{(1)} , \tag{6.2.23}$$

where

$$\mu = \frac{1}{p}, \tag{6.2.24}$$

$$\mu_{j,1} = \frac{j(1-p)}{mp} + 1, \tag{6.2.25}$$

$$\mu_{j,k} = \frac{j}{mp}, \text{ for } k \neq 1 . \tag{6.2.26}$$

Similar to the results in the prime-exponent-case (Lemma 4.2.4) we get now the following result:

Lemma 6.2.8. *Let*

$$\mathcal{D}_\mathfrak{p} = \mathcal{S} + \mathcal{G}_\mathfrak{p} , \tag{6.2.27}$$

where $\mathcal{G}_\mathfrak{p}$ is the vertical divisor in (6.2.23)*. Then $\mathcal{D}_\mathfrak{p}$ is a divisor of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ which is associated with $\left(\beta^*\mathcal{O}_{\mathbb{P}^1_R}(1)\right)^{\otimes\frac{1}{N^2}}$; here β denotes the extension of $\beta : F_N \to \mathbb{P}^1$ (cf. Remark 6.1.17).*

Proof: Analog to the proof of Lemma 4.2.4 we can show that N^2S is associated with $\beta^*\mathcal{O}_{\mathbb{P}^1_K}(1)$, where K is the fraction field of R. Since

$$\beta^*\mathcal{O}_{\mathbb{P}^1_R}(1)|_{F_N} \cong \beta^*\mathcal{O}_{\mathbb{P}^1_K}(1) ,$$

it is clear that $\mathcal{D}_\mathfrak{p}$ can be chosen as $\mathcal{D}_\mathfrak{p} = \mathcal{S} + \mathcal{G}_\mathfrak{p}$ with a vertical divisor $\mathcal{G}_\mathfrak{p}$. Again, the divisor $\mathcal{D}_\mathfrak{p}$ has to fulfill the equations

$$(N^2\mathcal{D}_\mathfrak{p}) \cdot \mathcal{C} = 0 \tag{6.2.28}$$

for all components $\mathcal{C}$ which are different from F_m (see e.g. [Liu], p.398: Theorem 2.12. (a)), and

$$N^2 = N^2\mathcal{D}_{\mathfrak{p}} \cdot \mathfrak{F}_{N,\mathfrak{p}}^{min} \times_{\operatorname{Spec} R} \operatorname{Spec} \mathbb{F}_p = N^2\mathcal{D}_{\mathfrak{p}} \cdot pF_m \tag{6.2.29}$$

(see e.g. [Liu], p.388: Remark 1.31.). Now, one can use the quantities computed in Theorem 6.1.15 to verify that our choice of $\mathcal{G}_{\mathfrak{p}}$ in (6.2.23) indeed satisfies the equations (6.2.28) and (6.2.29). □

Corollary 6.2.9. *We interpret the divisors $\mathcal{G}_{\mathfrak{p}}$ as divisors of $\mathfrak{F}_N^{min}$ and denote by $\mathcal{S}$ the Zariski-closure of S in $\mathfrak{F}_N^{min}$. Then the divisor*

$$\mathcal{D} = \mathcal{S} + \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{\mathfrak{p}} \tag{6.2.30}$$

is associated with $(\beta^* \mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}}(1))^{\otimes \frac{1}{N^2}}$; here β denotes the extension of $\beta : F_N \to \mathbb{P}^1$ (cf. Remark 6.1.17).

Proof: By the same arguments as in Lemma 4.2.4 and Lemma 6.2.8 we can assume that the divisor we are looking for is of the form $\mathcal{D} = \mathcal{S} + \mathcal{G}$ with a vertical divisor $\mathcal{G}$ with support in the fibers which are above the bad primes. Analog to the previous lemma we make the following observation: For a component $\mathcal{C}$ which lies in the special fiber above $\mathfrak{p}$ (here $\mathfrak{p} \cap \mathbb{Z} = p$ and $p|N$) and which is different from the component $F_{N/p}$, $\mathcal{D}$ has to fulfill the equation

$$(N^2\mathcal{D}) \cdot \mathcal{C} = 0\,.$$

As well, $\mathcal{D}$ has to fulfill

$$N^2 = N^2\mathcal{D} \cdot \mathfrak{F}_N^{min} \times_{\operatorname{Spec} R} \operatorname{Spec} \mathbb{F}_p = N^2\mathcal{D} \cdot pF_{N/p}\,.$$

On the other hand, if we take $\mathcal{G} = \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{\mathfrak{p}}$, then these equations are satisfied, because a component $\mathcal{C}$ which belongs to the fiber above $\mathfrak{p}$ just intersects $\mathcal{G}_{\mathfrak{p}}$. Hence, we have shown that our choice of the divisor $\mathcal{G}$ is the correct one. □

Theorem 6.2.10. *Let $\mathcal{K}_{\mathfrak{p}} = (2g-2)\mathcal{S} + \mathcal{V} + \mathcal{V}_\Sigma$ be the canonical divisor of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ from Lemma 6.2.6 and $\mathcal{D}_{\mathfrak{p}} = \mathcal{S} + \mathcal{G}_{\mathfrak{p}}$ the divisor defined in Lemma 6.2.8. We set $\mathcal{F}_{\mathfrak{p}} = \frac{1}{2g-2}(\mathcal{V} + \mathcal{V}_\Sigma)$. Then*

$$\mathcal{F}_{\mathfrak{p}} \cdot \mathcal{F}_{\mathfrak{p}} = -\frac{N^4 - N^3(p+5) + N^2(6p+2) - N(9p-15) + 4(N/p)^2 - 12(N/p)}{(N^2-3N)^2}$$

and

$$\mathcal{G}_{\mathfrak{p}} \cdot \mathcal{G}_{\mathfrak{p}} = -\frac{N-p+1}{N}\,.$$

Proof: Since $g(F_N) = \frac{1}{2}(m^2p^2 - 3mp + 2)$ Lemma 6.2.7 gives us

$$
\begin{aligned}
(2g-2)^2\mathcal{F}_{\mathfrak{p}}^2 =& \mathcal{V}^2 + \mathcal{V}_\Sigma^2 \\
=& -m^2(p-2)^2 + \frac{m(p-2)^2}{p} \\
&+ \left(\frac{m^2p^2 - 3mp}{p} - \frac{m(p-2)}{p}\right)\left(p - 2 - \frac{m^2p^2 - 3mp}{m}\right) \\
&- \frac{(m-1)(m^2p^2 - 3mp)^2}{m} \\
=& -2m^2p^2 - 4m^2 - 15mp + 12m + 5m^3p^3 - p^4m^4 + p^4m^3 - 6m^2p^3 + 9mp^2 \, .
\end{aligned}
$$

Now, substituting $N = pm$ gives us the first equation. In order to verify the second equation one observes that

$$0 = \mathcal{D} \cdot L_{j,k}^{(1)} = \mathcal{G}_{\mathfrak{p}} \cdot L_{j,k}^{(1)}$$

for all $L_{j,k}^{(1)}$ with $jk \neq 1$. As well, we have

$$0 = \mathcal{D} \cdot L^{(1)} = \mathcal{G}_{\mathfrak{p}} \cdot L^{(1)}$$

and therefore

$$\mathcal{G}_{\mathfrak{p}} \cdot \mathcal{G}_{\mathfrak{p}} = \mu_{1,1}^2 \left(L_{1,1}^{(1)}\right)^2 + \mu_{1,1}\mu_{2,1} = -\mathcal{S} \cdot \mu_{1,1} L_{1,1}^{(1)} = \frac{p-1}{mp} - 1 \, ,$$

which completes our proof. □

Lemma 6.2.11. *Let N be a squarefree odd integer with at least two prime factors, and let $\mathfrak{F}_N^{min}$ be the minimal regular model of the fermat curve F_N over* $\operatorname{Spec} \mathbb{Z}[\zeta_N]$ *which was constructed in Section 6.1. Furthermore, let S_j be a cusp (with respect to the morphism $\beta : F_N \to \mathbb{P}^1$ in* (3.2.12)*) which lies above the branch point ∞. For each bad prime $\mathfrak{p}$ we number the components of $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ so that S_j is the fixed cusp from Notation 6.2.5, and we compute $\mathcal{F}_{\mathfrak{p}}$ and $\mathcal{G}_{\mathfrak{p}}$ from Theorem 6.2.10 and Lemma 6.2.8 with respect to this numbering. Let us set*

$$\mathcal{F}_j = \sum_{\mathfrak{p} \text{ bad}} \mathcal{F}_{\mathfrak{p}}$$

and

$$\mathcal{G}_j = \sum_{\mathfrak{p} \text{ bad}} \mathcal{G}_{\mathfrak{p}} \, ,$$

where we interpret the $\mathcal{F}_{\mathfrak{p}}$ and $\mathcal{G}_{\mathfrak{p}}$ as divisors of $\mathfrak{F}_N^{min}$. Then $\mathcal{F}_j$ ($\mathcal{G}_j$ resp.) fulfills (3.2.2) *(*(3.2.3) *resp.).*

Proof: For $\mathcal{F}_j$ the statement follows directly by Proposition 6.2.4. In case of the $\mathcal{G}_i$ we can argue as follows: the cusp S_j lies above the branch point ∞. The Zariski-closure $\overline{\infty}$ of ∞ in $\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}$ is associated with $\mathcal{O}_{\mathbb{P}^1_{\mathbb{Z}[\zeta_N]}}(1)$. Hence, the claim follows with Corollary 6.2.9. □

Lemma 6.2.12. *In the situation of Lemma 6.2.11 we set $\mathcal{F}_p^2 = \mathcal{F}_\mathfrak{p}^2$ and $\mathcal{G}_p^2 = \mathcal{G}_\mathfrak{p}^2$ for each prime p with $p|N$; here $\mathfrak{p}$ is any prime ideal above p and $\mathcal{F}_\mathfrak{p}^2$ and $\mathcal{G}_\mathfrak{p}^2$ are the numbers computed in Theorem 6.2.10. Then*

$$\overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{p|N} \varphi(N)/\varphi(p)\mathcal{F}_p^2 \log p$$

and

$$\overline{\mathcal{O}}(\mathcal{G}_j)^2 = \sum_{p|N} \varphi(N)/\varphi(p)\mathcal{G}_p^2 \log p\,.$$

Proof: We have

$$\overline{\mathcal{O}}(\mathcal{F}_j)^2 = \sum_{\mathfrak{p}\text{ bad}} \overline{\mathcal{O}}(\mathcal{F}_\mathfrak{p})^2 = \sum_{p|N} \sum_{\substack{\mathfrak{p}\text{ bad}\\ \mathfrak{p}\cap\mathbb{Z}=(p)}} \overline{\mathcal{O}}(\mathcal{F}_\mathfrak{p})^2\,,$$

with $\overline{\mathcal{O}}(\mathcal{F}_\mathfrak{p})^2 = \mathcal{F}_\mathfrak{p}^2 \log \mathrm{Nm}(\mathfrak{p})$, where $\mathcal{F}_\mathfrak{p}^2$ is the number computed in Theorem 6.2.10. For each prime p let us denote by r_p the number of prime ideals of $\mathbb{Z}[\zeta_N]$ that lie above p. For a prime ideal $\mathfrak{p}$ with $\mathfrak{p}\cap\mathbb{Z} = (p)$, we have

$$r_p \log \mathrm{Nm}(\mathfrak{p}) = \varphi(N)/\varphi(p)\log(p)$$

(cf. proof of Lemma 5.3.2). For prime ideals of $\mathbb{Z}[\zeta_N]$, that lie above the same prime number p, the special fibers of $\mathfrak{F}_N^{min}$ are isomorphism, hence it follows that

$$\sum_{\substack{\mathfrak{p}\text{ bad}\\ \mathfrak{p}\cap\mathbb{Z}=(p)}} \overline{\mathcal{O}}(\mathcal{F}_\mathfrak{p})^2 = r_p\mathcal{F}_\mathfrak{p}^2 \log \mathrm{Nm}(\mathfrak{p}) = \varphi(N)/\varphi(p)\mathcal{F}_\mathfrak{p}^2 \log p\,.$$

Now, if we sum up over all prime numbers p with $p|N$, we obtain the formula for $\overline{\mathcal{O}}(\mathcal{F}_j)^2$. The formula for $\overline{\mathcal{O}}(\mathcal{G}_j)^2$ can be computed in a similar way. □

Theorem 6.2.13. *Let N be a squarefree odd integer with at least two prime factors, and let $\mathfrak{F}_N^{min}$ be the minimal regular model of the fermat curve F_N over $\operatorname{Spec}\mathbb{Z}[\zeta_N]$ which was constructed in Section 6.1. Then the arithmetic self-intersection number of its dualizing sheaf equipped with the Arakelov metric satisfies*

$$\begin{aligned}\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}} \leq &(2g-2)\left(\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 + [\mathbb{Q}(\zeta_N):\mathbb{Q}](\kappa_1 \log N + \kappa_2)\right)\\ &+ (2g-2)\sum_{p|N}\frac{\varphi(N)}{\varphi(p)}\left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N-3)}\right)\log p\,,\end{aligned}$$

where $\kappa_1, \kappa_2 \in \mathbb{R}_+^*$ are positive constants independent of N.

Proof: In Remark 6.1.17 and Remark 3.2.18 we saw that the morphism $\beta : \mathfrak{F}_N^{min} \to \mathbb{P}^1_{\mathbb{Z}[\zeta_N]}$ is a morphism of arithmetic surfaces as in Assumption 3.2.1 and that the induced morphism $\beta : F_N \to \mathbb{P}^1$ fulfills the requirements of Theorem 3.2.2. Analog to the prime exponent case we have $\deg \beta = N^2$ and $\beta^*\infty = \sum_{i=1}^N NS_i$, hence $b_j = b_{\max} = N$. It follows that in our case the formula (3.2.4) of Theorem 3.2.2 becomes

$$\begin{aligned}\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) &= -2g\overline{\mathcal{O}}(\mathcal{G}_j)^2 + (2g-2)\overline{\mathcal{O}}(\mathcal{F}_j)^2 \\ &= \sum_{p\mid N} \frac{\varphi(N)}{\varphi(p)} \left(-2g\mathcal{G}_p^2 + (2g-2)\mathcal{F}_p^2\right) \log p \\ &= \sum_{p\mid N} \frac{\varphi(N)}{\varphi(p)} \left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N-3)}\right) \log p\,,\end{aligned}$$

where we used Lemma 6.2.12 for the second equality and Theorem 6.2.10 for the last equality. □

Remark 6.2.14. Notice that the analytic contribution dominates the geometric contribution again. Since N is a squarefree odd integer and

$$|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}| = \frac{N^{\varphi(N)}}{\prod_{p\mid N} p^{\varphi(N)/(p-1)}} \tag{6.2.31}$$

we have

$$\begin{aligned}\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) &= \sum_{p\mid N} \frac{\varphi(N)}{\varphi(p)} \left(\frac{3N^2 - 2Np - 10N + 6p - 6 - 4\left(\frac{N}{p}\right)^2 + 12\left(\frac{N}{p}\right)}{N(N-3)}\right) \log p \\ &\le \sum_{p\mid N} \frac{\varphi(N)}{\varphi(p)} \frac{3N}{N-3} \log p \le \sum_{p\mid N} \frac{15}{4} \log p^{\frac{\varphi(N)}{(p-1)}} \qquad (6.2.32) \\ &= \frac{15}{4} \log(\Delta^{-1} N^{\varphi(N)}) \in \mathcal{O}(\log(\Delta^{-1} N^{\varphi(N)}))\,, \qquad (6.2.33)\end{aligned}$$

for the geometric contribution; here $\Delta = |\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|$. In order to show the claimed relation of dominance we just need to show that

$$\varphi(N)\kappa_1 \log N + \varphi(N)\kappa_2 - \sum_{p\mid N} \frac{15}{4} \log p^{\frac{\varphi(N)}{(p-1)}}$$

is positive for big N (N being odd and squarefree). If fact, we will show that

$$\sum_{p\mid N} \left(\kappa_1 - \frac{15}{4(p-1)}\right) \log p$$

is positive since this will imply the previous statement. Let us denote by p_i the i-th odd prime number. Furthermore let $l \in \mathbb{N}$ be the maximum with $\kappa_1 - 15/(4p_l - 4) \leq 0$ and $k \in \mathbb{N}$ the minimum with $\sum_{i=1}^{l}(\kappa_1 - 15/(4p_i - 4)) \log p_i + (\kappa_1 - 15/(4p_k - 4)) \log p_k > 0$. Then, for N with $\prod_{i=1}^{k} p_i \leq N$ it follows that N must have a prime factor p' with $p' \geq p_k$ since N is squarefree. Hence,

$$\sum_{p|N}\left(\kappa_1 - \frac{15}{(4p-4)}\right)\log p \geq \sum_{i=1}^{l}\left(\kappa_1 - \frac{15}{(4p_i-4)}\right)\log p_i + \left(\kappa_1 - \frac{15}{(4p'-4)}\right)\log p' > 0\,,$$

and the positivity is shown.

Corollary 6.2.15. *With the notation from the Theorem 6.2.13 we have the asymptotic bound*

$$\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}} \leq (2g-2)\varphi(N)(2+\kappa_1)\log N + \mathcal{O}(g\varphi(N) + g\log(\Delta^{-1}N^{\varphi(N)}))\,, \tag{6.2.34}$$

where $\Delta = |\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|$.

Proof: In Remark 6.2.14 we have seen that

$$\sum_{\mathfrak{p}\text{ bad}} a_{\mathfrak{p}} \log \mathrm{Nm}(\mathfrak{p}) \in \mathcal{O}(\log(\Delta^{-1}N^{\varphi(N)}))\,.$$

The analytic contribution is

$$\varphi(N)(\kappa_1 \log N + \kappa_2) = \varphi(N)\kappa_1 \log N + \mathcal{O}(\varphi(N))\,.$$

Finally, the term $\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 = \log \Delta^2$ becomes

$$\log|\Delta_{\mathbb{Q}(\zeta_N)|\mathbb{Q}}|^2 = 2\log N^{\varphi(N)} + \mathcal{O}(\log(\Delta^{-1}N^{\varphi(N)})))\,.$$

Now, the statement follows with Theorem 6.2.13. □

Remark 6.2.16. Notice that (6.2.34) is valid for arbitrary squarefree odd integer N, hence odd prime numbers as well. This follows with (4.2.14) and $p = |\Delta_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}|^{-1}p^{\varphi(p)}$. However, since in the prime exponent case the term $\varphi(p)\kappa_2$ will dominate the term $\log p$, as the size of the prime numbers increases, it makes sense not to include $\varphi(p)\kappa_2$ in the "big O"-part. If N is not a prime number the situation looks different. In this case we neither have $\varphi(N) \in \mathcal{O}(\log(\Delta^{-1}N^{\varphi(N)}))$ nor $\log(\Delta^{-1}N^{\varphi(N)}) \in \mathcal{O}(\varphi(N))$. In other words, non of the fractions

$$\frac{\varphi(N)}{\log(\Delta^{-1}N^{\varphi(N)})} \tag{6.2.35}$$

and

$$\frac{\log(\Delta^{-1}N^{\varphi(N)})}{\varphi(N)} \tag{6.2.36}$$

is bounded by a constant as N varies over the squarefree odd integers. To see this we will construct for each fraction a sequence of integers for which there exists no bound. Let us denote by p_i the i-th odd prime number. We define the first sequence of integers by $N_i := p_i p_{i+1}$. Now, for (6.2.35) we obtain

$$\frac{\varphi(N_i)}{\log(\Delta^{-1} N_i^{\varphi(N_i)})} = \frac{1}{\log \prod_{p|N_i} p^{\frac{1}{p-1}}} > \frac{1}{2 \log p_i^{\frac{1}{p_i-1}}} ,$$

hence $\lim_{i\to\infty} \log(\Delta^{-1} N_i^{\varphi(N_i)})^{-1} \varphi(N_i) = \infty$. For the second fraction we define a different sequence. Set $N_i := \prod_{j=1}^{i} p_j$. Then

$$\frac{\log(\Delta^{-1} N_i^{\varphi(N_i)})}{\varphi(N_i)} = \log \prod_{p|N_i} p^{\frac{1}{p-1}} = \sum_{j=1}^{i} \frac{1}{p_j - 1} \log p_j \geq \sum_{j=1}^{i} \frac{1}{p_j} =: s_i .$$

It is a well known fact of number theory that the sequence $(s_i)_i$ diverges. It follows

$$\lim_{i\to\infty} \varphi(N_i)^{-1} \log(\Delta^{-1} N_i^{\varphi(N_i)}) = \infty .$$

We see that the relation of domination depends strongly on the factorization of N into prime numbers.

Chapter 7

Remarks on the Fermat curve for the remaining cases

With Chapter 4 and Chapter 6 we obtained a description of the minimal regular model of the Fermat curves F_N of squarefree odd exponent N over the ring of integers of the N-th cyclotomic field. In this chapter we give a few remarks on the situation of the "squarefree even"-case and the case of non-squarefree exponents. Furthermore, we sketch a different construction of the results of Section 6.1 and a different general approach.

7.1 The minimal regular model of the Fermat curve for squarefree even exponent

Let N be a squarefree natural number which is divisible by 2 and F_N the Fermat curve of exponent N. The purpose of this section is to discuss the construction of the minimal regular model of F_N and the differences to the construction of the model in the odd-case. Since we do not restrict ourselves to the situation that N has at least two different prime divisors we may start our analyzation with the case $N = 2$. Again, we would like to work over a number field which contains the roots of unity in question. However, since the second roots of unity are just 1 and -1 our number field will be $\mathbb{Q}$ and the ring of integers will be $\mathbb{Z}$. The origin of our construction is the scheme

$$\mathfrak{F}_2^0 = \operatorname{Proj} \mathbb{Z}[X, Y, Z]/(X^2 + Y^2 - Z^2)\,.$$

We analyze the affine open subscheme

$$\mathcal{X} = \operatorname{Spec} \mathbb{Z}[X, Y]/(X^2 + Y^2 - 1)\,.$$

Contrary to the odd-case this scheme is normal. This can be easily seen by writing the equation $X^2 + Y^2 - 1$ as

$$X^2 + Y^2 - 1 = (X + Y - 1)^2 + 2(X + Y - 1 - XY)$$

and then by showing that the Ideal $I = (X + Y - 1, 2)$ can be generated by $(X + Y - 1)$ in the localization with respect to I. A few computations - which are similar to the one in Section 6.1 - yield that the blowing-up of $\mathcal{X}$ along I is covered by

$$\operatorname{Spec}\mathbb{Z}[X,Y,Z]/(F_1 - 2Z, 2Z^2 + X + Y - 1 - XY)$$

and

$$\operatorname{Spec}\mathbb{Z}[X,Y,W]/(WF_1 - 2, F_1 + W(X + Y - 1 - XY)),$$

where $F_1 = X+Y-1$, and that this scheme is regular. The configuration of the special fiber is given by a component L, which has multiplicity 2 and self-intersection -1, and components L_X and L_Y, which have multiplicity 1 and self-intersection -2. The components L_X and L_Y do not intersect each other but intersect L transversally. Remembering the situation for odd N one could ask if there is a third component L_Z which cannot be seen in this picture. A symmetry argument will not work since the scheme $\mathcal{X}$ is not isomorphic to $\mathcal{X}' = \operatorname{Spec}\mathbb{Z}[X,Z]/(X^2+1-Z^2)$. To see this one could just verify that $\mathcal{X}$ has two singular closed points and $\mathcal{X}'$ just one. In fact, there is no third component.

Since the genus of the Fermat curve F_2 is 0 we cannot expect that there exists a minimal regular model (cf. Remark 2.2.8). In fact, if we blow down the (-1)-component L we end up with the situation that the components L_X and L_Y intersect each other transversally and that both have multiplicity 1 and self-intersection -1. If we now blow down the component L_X we will get a relatively minimal model which is not isomorphic to the relatively minimal model we get when we blow down L_Y. Hence, there does not exist a minimal model of F_2.

Let us next consider the case that N is a squarefree even number that has at least two different prime divisors. Since the genus of this curve is greater than 0 we know that there exists a minimal regular model (Theorem 2.2.7). If we make the construction of this model fiber by fiber we have to distinguish between two cases: The construction for a fiber over 2 and the construction for a fiber over p, where $p \neq 2$. We start with the latter case, hence $N = pm$, where $2|m$. Most of the results in Section 6.1 do not use the fact that m is assumed to be odd, hence it should be possible as well to adapt these results to the current situation. If we consider the fiber above 2 the situation looks slightly different. Here we have $N = 2m$, where m is a squarefree odd number. Since exponentiating with 2 does not respect minus signs the results of Subsection 6.1.1 cannot be applied to this situation. However, in this case we can rewrite the Fermat equation as

$$X^N + Y^N - 1 = (X^m + Y^m - 1)^2 + 2(X^m + Y^m - 1 - X^mY^m).$$

Analog to the situation of the Fermat curve of exponent 2 we can use this equation to show that the components of the special fiber over 2 are regular, hence we do not need to normalize in this part. Another thing which is similar to this situation and different to the odd-case is that the affine open subschemes $\operatorname{Spec}\mathbb{Z}[\zeta_m][X,Y]/(X^{2m} + Y^{2m} - 1)$ and $\operatorname{Spec}\mathbb{Z}[X,Z][\zeta_m]/(X^{2m} + 1 - Z^{2m})$ are not isomorphic. However, the author conjectures that most of the results in Section 6.1 can be used after a small modification and that Theorem 6.1.15 remains true for squarefree even natural numbers with the difference that the model $\mathfrak{F}_{N,\mathfrak{p}}^{min}$ for a prime ideal with $2 \in \mathfrak{p}$ has just $2m$ components L_{XYZ}, $4m$ components L_i and no components L_γ and L_δ.

7.2 An alternative way to the results in Section 6.1

In this section the author reviews a different approach to the result of Section 6.1. This approach was suggested by Franz Király.

The idea is the following: Let $\mathfrak{F}_p^{min}$ be the minimal regular model of the Fermat curve F_p of odd prime exponent p which was constructed by William G. McCallum (see Section 4.1 or the original article [Mc]). We consider the normalization of this scheme in the function field $K(F_N)$ of the Fermat curve F_N of exponent N, where N is a squarefree odd natural number with $N = pm$ (just as in Section 6.1); this normalization will be denoted by

$$\mathcal{Y} = N(\mathfrak{F}_p^{min}, K(F_N)) .$$

It is birational to the minimal regular model $\mathfrak{F}_N^{min}$ of the curve F_N and since it is normal there can be just isolated singularities i.e. all singular points left are closed points. Now, if one can locate these singular points and determine their desingularization behavior, the model $\mathfrak{F}_N^{min}$ can be obtained by this information. We sketch how this could possibly be done.

The morphism of curves $F_N \to F_p$, which is given by $(a : b : c) \mapsto (a^m : b^m : c^m)$, induces a Galois extension $K(F_N)/K(F_p)$ of the function fields and in fact F_p can be interpreted as the quotient curve F_N^G, where G is this Galois group $G(K(F_N)/K(F_p))$. Furthermore one observes that this Galois group operates on the scheme $\mathcal{Y}$ as well[1], and it follows that the quotient scheme $\mathcal{Y}^G$ exists since G is finite (cf. [Liu], p.59: Exercise 3.3.23.). Because of the universal property of the quotient scheme we have a morphism $\mathcal{Y}^G \to \mathfrak{F}_p^{min}$, and since $K(\mathcal{Y}^G) = K(\mathcal{Y})^G = K(F_N)^G = K(F_p)$ the uniqueness of the normalization yields that this morphism is in fact an isomorphism. Now we want to relate the schemes $\mathcal{Y}$ and $\mathcal{Y}^G$. In order to do this let us denote by f the quotient morphism $f : \mathcal{Y} \to \mathcal{Y}^G = \mathfrak{F}_p^{min}$. Then for an element $y \in \mathcal{Y}$ we have $\mathcal{O}_{\mathcal{Y}^G, f(y)} = (\mathcal{O}_{\mathcal{Y},y})^G$. Király suggests that in this situation a theorem of Serre ([CES], p.352: Theorem 2.3.9.) can be used in order to verify whether or not $y \in \mathcal{Y}$ is a singular point[2]. For that only the knowledge of the minimal regular model $\mathfrak{F}_p^{min}$ and the knowledge of the function field $K(F_N)$ is needed. Serre's theorem works in this situation since the characteristic of the residue field $k(y)$ ($k(f(y))$ resp.) does not divide the order of the group. Furthermore, Király conjectures that the singular points of $\mathcal{Y}$ are tame cyclic quotient singularities in the sense of ([CES], p.351: Definition 2.3.7.). The desingularization of these singularities is well known.

It is planned by Király and the author to verify this approach and publish the results in a forthcoming paper.

[1] In case of affine schemes this is easy to see. Take for example a ring A with field of fractions $\mathrm{Frac}(A) = K$ and a finite Galois extension L of K. Furthermore let B be the integral closure of A in L and $G = (L/K)$ the Galois group of the field extension. By definition, for each element $b \in B$ there exists a monic polynomial $f(T) \in A[T]$ with $f(b) = 0$. Now, for every $\sigma \in G$ we have $0 = \sigma(f(b)) = f(\sigma(b))$, hence $\sigma(b) \in B$. It follows $\sigma(B) = B$. For arbitrary schemes this statement remains true because of the construction of the normalization and the statement in the affine case.

[2] Notice, that we cannot apply the theorem of Serre directly since the Galois extension $K(F_N)/K(F_p)$ is not cyclic. However, we can find an intermediate extension so that $K(F_N)/K(F_p)$ splits into two cyclic extensions for which we can use this theorem.

7.3 Difficulties in the non-squarefree case

Let p be a prime number and F_{p^k} the Fermat curve of exponent p^k, where $k > 1$. If we assume that one has constructed minimal regular models of these curves for all primes p, then the construction of minimal regular models of Fermat curves of arbitrary exponent (or at least of exponent of the form mp^k with $\gcd(p, m) = 1$ and m squarefree) should not be a big problem. However, it seems to be very difficult to say something about the minimal regular model of the curve F_{p^k}. A direct approach, as it was made by McCallum and the author in the squarefree-case, will probably get stuck in this case since the complexity of the equations involved increases too rapidly. In order to make an approach as it is described in Section 7.2 one would need a result similar to the one of Serre but with the difference that here the characteristic of the residue field divides the order of the group. As an improvement of Serre's theorem Király and Lütkebohmert give in [KL] exactly such result (see [KL], p.2: Theorem 1 and Corollary 3). After constructing a normal model (which can be done the same way it was done in Section 7.2) their work could be used in order to find the singularities of this model just by the minimal regular model $\mathfrak{F}_p^{min}$ and the function field $K(F_{p^k})$. However, it seems to be likely that the desingularization of these singularities is complicated, and it is therefore not clear if this approach can be used in order to find a (easy) construction of the minimal regular model of F_{p^k}.

7.4 Stable and semi-stable models of the Fermat curve

In this section we sketch an approach how one could possibly obtain a regular model of the Fermat curve F_N once a (semi-) stable model of this curve has been constructed. For example, for F_p, where p is an odd prime number, a stable model of F_p was given by Hironobu Maeda [Mae1],[Mae2] and by Jeroen J. van Beele [vB]. In order to use the approach for the Fermat curve of another exponent one would need to construct the (semi-) stable model of this curve. However, in general the construction of these models is not easy.

The approach: it is well known that there exists a number field E so that the Fermat curve F_N has a stable model over the ring of integers $\mathcal{O}_E$ of this number field ([DM])[3]. Let us assume that we have found such a stable model over $\mathcal{O}_E$. Then one can make a finite étale base change to a ring R in order to obtain a stable model that only has split ordinary double points (see [Liu], p.510: Proposition 3.15. and p.514: Corollary 3.22.). Furthermore, if one can determine the thickness of these singularities then a regular model can be obtained as well (cf. [Liu], p.515: Corollary 3.25.). Finally, blowing down (-1)-curves will yield a minimal regular model over R.

[3] In fact, this statement - and therefore the approach - is not restricted to Fermat curves.

Bibliography

[AU] *A. Abbes, E. Ullmo:* Auto-intersection du dualisant relatif des courbes modulaires $X_0(N)$. J. Reine Angew. Math. **484** (1997), 1–70.

[Ara] *S. J. Arakelov:* An intersection theory for divisors on an arithmetic surface. Izv. Akad. Nauk SSSR Ser. Mat. **38** (1974), 1179–1192.

[Ar1] *M. Artin:* Lipman's proof of resolution of singularities for surfaces. In *Arithmetic Geometry* (Storrs, Conn., 1984). Springer, New York, (1986), 267–287.

[Ar2] *M. Artin:* On isolated rational singularities of surfaces. Amer. J. Math. **88** (1966), 129–136.

[BG] *E. Bombieri, W. Gubler:* Heights in Diophantine Geometry. New Mathematical Monographs **4**. Cambridge University Press, Cambridge, 2006.

[BLR] *S. Bosch, W. Lütkebohmert, M. Raynaud:* Néron Models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)] **21**. Springer-Verlag, Berlin, 1990.

[BMMB] *J.-B. Bost, J.-F. Mestre, L. Moret-Bailly:* Sur le calcul explicite des "classes de Chern" des surfaces arithmétiques de genre 2. Astérisque **183** (1990), 69–105.

[Bo] *J.-B. Bost:* Potential theory and Lefschetz theorems for arithmetic surfaces. Ann. Sci. École Norm. Sup. (4) **32** (1999), 241–312.

[Cha] *H. Chang:* On the singularities of the Fermat scheme over $\mathbf{Z}$. Chinese J. Math. **17** (1989), 243–257.

[Chi] *T. Chinburg:* Minimal models for curves over Dedekind rings. In *Arithmetic Geometry* (Storrs, Conn., 1984). Springer, New York, (1986), 309–326.

[CES] *B. Conrad, B. Edixhoven, W. Stein:* $J_1(p)$ has connected fibers. Doc. Math. **8** (2003), 331–408 (electronic).

[CK] *C. Curilla, U. Kühn:* On the arithmetic self-intersection number of the dualizing sheaf for Fermat curves of prime exponent, 2009, `http://arxiv.org/pdf/0906.3891`.

[De] *P. Deligne:* Intersections sur les surfaces régulières. In *SGA 7 II*. Lect. Notes Math. **340**, (1973), 1–38.

[DM] *P. Deligne*, *D. Mumford:* The irreducibility of the space of curves of given genus. Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[DR] *P. Deligne*, *M. Rapoport:* Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II*. Lecture Notes in Math. **349**. Springer, Berlin, (1973), 143–316.

[DS] *F. Diamond*, *J. Shurman:* A First Course in Modular Forms. Graduate Texts in Mathematics **228**. Springer-Verlag, New York, 2005.

[EH] *D. Eisenbud*, *J. Harris:* The Geometry of Schemes. Graduate Texts in Mathematics **197**. Springer-Verlag, New York, 2000.

[Ei] *D. Eisenbud:* Commutative Algebra (with a View Toward Algebraic Geometry). Graduate Texts in Mathematics **150**. Springer-Verlag, New York, 1995.

[El] *R. Elkik:* Le théorème de Manin-Drinfel′d. Astérisque **183** (1990), 59–67.

[FGI$^+$] *B. Fantechi*, *L. Göttsche*, *L. Illusie*, *S. L. Kleiman*, *N. Nitsure*, *A. Vistoli:* Fundamental Algebraic Geometry (Grothendieck's FGA Explained). Mathematical Surveys and Monographs **123**. American Mathematical Society, Providence, RI, 2005.

[GS] *H. Gillet*, *C. Soulé:* Arithmetic intersection theory. Inst. Hautes Études Sci. Publ. Math. **72** (1990), 93–174.

[Gr1] *A. Grothendieck:* Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. Inst. Hautes Études Sci. Publ. Math. (1965), 231.

[Gr2] *A. Grothendieck:* Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. Inst. Hautes Études Sci. Publ. Math. (1966), 255.

[Gr3] *A. Grothendieck:* Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. Inst. Hautes Études Sci. Publ. Math. (1967), 361.

[Ha] *R. Hartshorne:* Algebraic Geometry. Graduate Texts in Mathematics **52**. Springer-Verlag, New York, 1977.

[Hu] *C. Huneke:* Symbolic powers of prime ideals and special graded algebras. Comm. Algebra **9** (1981), 339–366.

[JK1] *J. Jorgenson, J. Kramer:* Bounds for special values of Selberg zeta functions of Riemann surfaces. J. Reine Angew. Math. **541** (2001), 1–28.

[JK2] *J. Jorgenson, J. Kramer:* Bounding the sup-norm of automorphic forms. Geom. Funct. Anal. **14** (2004), 1267–1277.

[KM] *N. M. Katz, B. Mazur:* Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies **108**. Princeton University Press, Princeton, NJ, 1985.

[KL] *F. Király, W. Lütkebohmert:* Invariants of normal local rings by p-cyclic group actions, 2010, `http://arxiv.org/abs/1001.1945`.

[Kü1] *U. Kühn:* Generalized arithmetic intersection numbers. J. Reine Angew. Math. **534** (2001), 209–236.

[Kü2] *U. Kühn:* On the arithmetic self-intersection number of the dualizing sheaf on arithmetic surfaces, 2009, `http://arxiv.org/pdf/0906.2056`.

[KW] *E. Kunz, R. Waldi:* Integral differentials and Fermat congruences. Univ. Iagel. Acta Math. (2007), 97–116.

[La] *S. Lang:* Introduction to Arakelov Theory. Springer-Verlag, New York, 1988.

[Li] *S. Lichtenbaum:* Curves over discrete valuation rings. Amer. J. Math. **90** (1968), 380–405.

[Lip1] *J. Lipman:* Rational singularities, with applications to algebraic surfaces and unique factorization. Inst. Hautes Études Sci. Publ. Math. **36** (1969), 195–279.

[Lip2] *J. Lipman:* Desingularization of two-dimensional schemes. Ann. Math. (2) **107** (1978), 151–207.

[Liu] *Q. Liu:* Algebraic Geometry and Arithmetic Curves. Oxford Graduate Texts in Mathematics **6**. Oxford University Press, Oxford, 2002.

[LL] *Q. Liu, D. Lorenzini:* Models of curves and finite covers. Compositio Math. **118** (1999), 61–102.

[Mae1] *H. Maeda:* Die stabile Reduktion der Fermatkurve über einem Zahlkörper. Manuscripta Math. **56** (1986), 333–342.

[Mae2] *H. Maeda:* Auflösung der Flächensingularitäten und stabile Reduktion der Fermatkurve. J. Number Theory **65** (1997), 305–315.

[Mat1] *H. Matsumura:* Commutative Algebra. Second ed.. Mathematics Lecture Note Series **56**. Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[Mat2] *H. Matsumura:* Commutative ring theory. Second ed.. Cambridge Studies in Advanced Mathematics **8**. Cambridge University Press, Cambridge, 1989.

[Mc] *W. G. McCallum:* The degenerate fibre of the Fermat curve. In *Number theory related to Fermat's last theorem* (Cambridge, Mass., 1981). Progr. Math. **26**. Birkhäuser Boston, Mass., (1982), 57–70.

[MU] *P. Michel*, *E. Ullmo:* Points de petite hauteur sur les courbes modulaires $X_0(N)$. Invent. Math. **131** (1998), 645–674.

[Mi] *J. S. Milne:* Étale cohomology. Princeton Mathematical Series **33**. Princeton University Press, Princeton, N.J., 1980.

[MB] *L. Moret-Bailly:* Métriques permises. Astérisque **127** (1985), 29–87.

[Mur] *J. P. Murre:* Lectures on an Introduction to Grothendieck's Theory of the Fundamental Group. Lectures on Mathmatics **40**. Tata Institute of Fundamental Research, Bombay, 1967.

[MR] *V. K. Murty*, *D. Ramakrishnan:* The Manin-Drinfel′d theorem and Ramanujan sums. Proc. Indian Acad. Sci. Math. Sci. **97** (1987), 251–262.

[Ne] *J. Neukirch:* Algebraic Number Theory. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **322**. Springer-Verlag, Berlin, 1999.

[Og] *A. P. Ogg:* Rational points on certain elliptic modular curves. In *Analytic Number Theory* (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972). Amer. Math. Soc., Providence, R.I., (1973), 221–231.

[Pa] *A. N. Parshin:* Application of ramified coverings in the theory of Diophantine equations. Mat. Sb. **180** (1989), 244–259.

[Ro] *D. E. Rohrlich:* Points at infinity on the Fermat curves. Invent. Math. **39** (1977), 95–127.

[Sh] *G. Shimura:* Introduction to the Arithmetic Theory of Automorphic Functions. Publications of the Mathematical Society of Japan **11**. Princeton University Press, Princeton, NJ, 1994.

[Si] *J. H. Silverman:* Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics **151**. Springer-Verlag, New York, 1994.

[SABK] *C. Soulé*, *D. Abramovich*, *J.-F. Burnol*, *J. Kramer:* Lectures on Arakelov Geometry. Cambridge Studies in Advanced Mathematics **33**. Cambridge University Press, Cambridge, 1992.

[So] *C. Soulé:* Géométrie d'Arakelov des surfaces arithmétiques, Séminaire Bourbaki, Vol. 1988/89. Astérisque **177-178** (1989), 327–343.

[Sz] *L. Szpiro:* Sur les propriétés numériques du dualisant relatif d'une surface arithmétique. In *The Grothendieck Festschrift, Vol. III.* Progr. Math. **88**. Birkhäuser Boston, Boston, MA, (1990), 229–246.

[Ue] *K. Ueno:* Algebraic Geometry. 3. Translations of Mathematical Monographs **218**. American Mathematical Society, Providence, RI, 2003.

[Ul] *E. Ullmo:* Positivité et discrétion des points algébriques des courbes. Ann. of Math. **147** (1998), 167–179.

[V′] *N. K. V′et:* Minimal models of algebraic curves. Mat. Sb. **180** (1989), 625–634.

[vB] *J. J. van Beele:* Models and Modularity Questions Concerning Fermat and Klein Curves (dissertation Rijksuniversiteit te Leiden), 1994.

[Vo] *P. Vojta:* Diophantine Inequalities and Arakelov Theory. In *Introduction to Arakelov Theory* (Lang [La]). Springer, (1988), 155–178.

[ZS] *O. Zariski*, *P. Samuel:* Commutative Algebra. Vol. II. Graduate Texts in Mathematics **29**. Springer-Verlag, New York, 1975.

[Zh] *S. Zhang:* Admissible pairing on a curve. Invent. Math. **112** (1993), 171–193.

Index

Zusammenfassung

In dieser Arbeit untersuchen wir die Arithmetik und Geometrie der Fermat-Kurven

$$F_N : X^N + Y^N = Z^N$$

mit quadratfreien Exponenten N. Darüber hinaus befassen wir uns mit Anwendungen in der Arakelov-Theorie. Die Hauptresultate, die wir erhalten, sind eine explizite Konstruktion des minimalen regulären Modells $\mathfrak{F}_N^{min}$ über $\operatorname{Spec}\mathbb{Z}[\zeta_N]$, wobei $\mathbb{Z}[\zeta_N]$ der Ganzheitsring zu dem N-ten Kreisteilungskörper ist, und obere Schranken für die arithmetische Selbstschnittzahl des hermiteschen Geradenbündels $\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}}$, wobei $\overline{\omega}_{\mathfrak{F}_N^{min},\mathrm{Ar}}$ das Geradenbündel

$$\omega_{\mathfrak{F}_N^{min}/\operatorname{Spec}\mathbb{Z}} = \omega_{\mathfrak{F}_N^{min}/\operatorname{Spec}\mathcal{O}_E} \otimes_{\mathcal{O}_{\mathfrak{F}_N^{min}}} f^*\omega_{\operatorname{Spec}\mathcal{O}_E/\operatorname{Spec}\mathbb{Z}}$$

versehen mit der Arakelov-Metrik ist.

Ausgangspunkt der Berechnung des minimalen regulären Modells ist das Modell über dem Ring R, welches durch die Fermat-Gleichung gegeben ist; der Ring R ist hierbei die Lokalisierung von $\mathbb{Z}[\zeta_N]$ nach einem Primideal, das die Zahl N enthält. Wir arbeiten mit der Technik des Aufblasens, wobei wir uns besonders mit der sinnvollen Wahl der Zentren beschäftigen. Die bei der Konstruktion durch das Aufblasen entstehenden Komponenten der speziellen Faser des Modells unterteilen wir in unterschiedliche Typen, die wir dann gesondert analysieren. In jedem Schritt benutzen wir diverse Techniken zum Auffinden der singulären Loci und zur Bestimmung von Regularität und Normalität. Das Hauptresultat beschreibt dann die Zusammensetzung der speziellen Fasern von $\mathfrak{F}_N^{min}$ gemeinsam mit der genauen Anzahl, dem Geschlecht, der Selbstschnittzahl und der Multiplizität der Komponenten. Durch ein kombinatorisches Argument folgt die Transversalität der Schnitte.

Ein Vorteil unserer expliziten Konstruktion ist, dass wir sie für weitere Berechnungen, die das Modell betreffen, nutzen können. Für bestimmte Punkte auf der generischen Faser berechnen wir beispielsweise, welche vertikalen Komponenten der speziellen Faser von den horizontalen Divisoren, die wir als Zariski-Abschluss dieser Punkte erhalten, geschnitten werden. Dies können wir nutzen, um kanonische Divisoren zu konstruieren, die besondere für andere Anwendungen nützliche Eigenschaften haben.

Um obere Schranken für die arithmetische Selbstschnittzahl von $\overline{\omega}^2_{\mathfrak{F}_N^{min},\mathrm{Ar}}$ zu berechnen, benutzen wir ein Theorem von Kühn, welches dieses Problem auf die Berechnung gewisser endlicher Selbstschnittzahlen reduziert. Diese Selbstschnittzahlen können wir mit unserem Modell bestimmen und erhalten damit asymptotische obere Schranken.

Lebenslauf

01.06.1979	geboren in Elmshorn
1998	Abitur, Kooperative Gesamtschule Elmshorn
1999-2006	Studium der Mathematik, Universität Hamburg
2001-2002	Studium der Mathematik, Loughborough University, England im Rahmen des SOKRATES/ERASMUS- Austauschprogramms
2006	Diplom in Mathematik, Universität Hamburg
2007-2009	Promotionsstipendium der Universität Hamburg (HmbNFG)
2009-2010	wissenschaftlicher Mitarbeiter an der Universität Hamburg