Università degli Studi di Padova
Universiteit Leiden

Smooth models of curves

Master Thesis by:
Michele Serra

Supervised by:
Dr. David Holmes

Academic year 2012-2013

Contents

Acknowledgements, Ringraziamenti

I would like to thank my advisor, Dr. David Holmes, for his guidance, help, and constant encouragement.

I also want to thank all my ALGANT-mates: Mima, Stefano, Valentina, Chiara, Héctor, Tomo, Abtien, Rosa, Corina, Catalina, Anna, Shuang, Brian, Lorenzo, Elena, Yan, Thieu, Hieu, Giulio for their invaluable friendship, teamwork and for the great time we spent together during the last two years.

Il primo grazie in italiano alla mia famiglia, per essere ciò che è. Ai miei amici di sempre: Sara, Robi, Nico, Fede, Gigi, Sara, Sara, per esserci sempre stati, dovunque fossimo. A chi in questi due anni mi ha fatto sentire a casa, anche quando casa era lontana: Eri, Giacomo, Pierpaolo, Samuele, Alberto. Grazie ai miei amici e compagni dell'Università di Cagliari, e un grazie speciale a Carlo, per tutta la matematica tragicomica fatta insieme e per la sua amicizia. Vorrei anche ringraziare i docenti, in particolar modo Stefano Montaldo e Andrea Loi, per i loro insegnamenti, gli utili consigli e il sostegno che continuano a darmi tuttora.

A Laura.

Introduction

In this thesis we study the reduction of algebraic curves. In particular we will focus on smooth curves of genus at least 2. Our main goal is to find algorithms to test whether a given curve has good reduction, potential good reduction and in this last case to find an extension of the base field, of the smallest possible degree, over which it acquires good reduction.

There are several important results in the theory of reduction of curves. In the case of elliptic curves (smooth projective curves of genus one with a rational point) there is an exhaustive theory: Tate proved that there exists no elliptic curve over $\mathbb{Q}$ with good reduction everywhere (Theorem 2.11) and Ogg gave the complete (finite) list of elliptic curves over $\mathbb{Q}$ with good reduction outside 2. Faltings generalized this result ineffectively to higher genus curves over number fields:

Theorem ([Fal83, Theorem 5])**.** *Let K be a number field, S a finite set of places of K and $g \geq 2$ an integer. There exist only finitely many curves of genus g over K having everywhere good reduction outside S up to K-isomorphism.*

Later, in [Sma97], Smart produced a complete list of ($\mathbb{Q}$-isomorphism classes of) curves of genus 2 over $\mathbb{Q}$ with good reduction outside 2: there are 428 such curves up to isomorphism.

The aforementioned results naturally lead to further questions and problems. For example, determining the finite set of curves of some fixed genus $g > 2$ with good reduction outside 2 (or some other prime p). A possibly easier, but to the author's knowledge still open, problem is the following: fix an integer $g > 2$ and find an explicit example of a number field K and a curve of genus g over K with good reduction at all places of K. For $g = 2$ the author is grateful to R. de Jong for pointing out the following example.

Example. Let $K = \mathbb{Q}(i, \sqrt[5]{2}, \sqrt{1-\zeta_5})$ and let C be the curve over K defined by $y^2 = x^5 - 1$. One can check that C has good reduction everywhere over K.

If we have an algorithm to test whether a given curve has good or potentially good reduction, one approach to find such a curve is simply to randomly generate curves over number fields and test to see whether they have good or potentially good reduction. Another approach would be to test all curves in certain finite families, for example to take Smart's list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2 and test whether any of these curves has potential good reduction.

With this aim in mind, we will focus on the reduction of smooth curves over the closed points of integral Dedekind schemes. The setting will be as follows: we fix an integral 1-dimensional Dedekind scheme S and denote by K its field of rational functions. A *curve* C over K is a 1-dimensional K-scheme of finite type. If C is a smooth projective curve over K, then a *model* of C over S is a flat projective scheme over S whose generic fibre is isomorphic to C. The curve C has good (resp. semi-stable, resp. stable) reduction if it admits a smooth (resp. semi-stable, resp. stable) model over S. We say that C has potential good (resp. semi-stable, resp. stable) reduction if there exists a finite extension L/K such that the base change of C to L has good (resp. semi-stable, resp. stable) reduction.

Introducing stable and semi-stable reduction will turn out to be very helpful in constructing algorithms to test whether a given curve has good or potentially good reduction. Indeed, we will give a characterization of potential good reduction in terms of properties of stable models.

Lemma. *Let S be an excellent Dedekind scheme, $K = K(S)$ its function field. Let C be a smooth, projective, geometrically connected curve over K of genus $g \geq 2$. Then C has potential good reduction* if and only if *every stable model over every extension of the base field that provides one is smooth.*

The above result, which is proven at the end of Section 2.3 (Lemma 2.29), tells us that testing potential good reduction is equivalent to testing smoothness of a stable model, whose existence is ensured by Theorem 2.28, due to Deligne and Mumford.

Unfortunately our goals are not completely achieved. Indeed, the first algorithm we present takes as input a smooth projective geometrically connected curve of genus $g \geq 2$ over the function field of an excellent Dedekind scheme and returns a regular model. However, to obtain a minimal regular model from these data it is necessary to contract certain curves on the regular model, known as (-1)-curves (see [Liu02, Section 9.3.1]). A proof that such a contraction exists is given in [Liu02, Proposition 8.3.30]. However, to explicitly construct the contraction requires the computation of the global sections of a certain line bundle on the regular model, and it is not at present clear to the author how to make this step effective.

We then show that if it were possible to construct a minimal regular model, then we could effectively test whether a given curve has good reduction by checking whether this minimal model is smooth. In Chapter 3, under this hypothesis, we also give an algorithm that tests potential good reduction over p-adic fields and finds an extension of smallest degree of the base field over which good reduction is achieved.

Preliminaries and notation

Here we recall some definitions and fix some notation that will be used throughout this thesis.

A scheme X is *reduced at a point* $x \in X$ if its stalk $\mathcal{O}_{X,x}$ is a reduced ring (a ring with no nilpotent elements). We say that X is *reduced* if it is reduced at all of its points. A scheme X is said to be *irreducible* if its underlying topological space is irreducible, and we say that X is *integral* if it is both reduced and irreducible. A scheme X is *normal at* $x \in X$ if the stalk $\mathcal{O}_{X,x}$ is a normal domain (integrally closed in its fraction field) and we say that X is *normal* if it is irreducible and normal at all of its points. Notice that, in particular, a normal scheme is connected. A normal, locally Noetherian scheme of dimension 1 is called a *Dedekind scheme.* We will often use the notion of a *normalization morphism.*

Definition 0.1. Let X be an integral scheme. A *normalization morphism* is a morphism $\pi\colon X' \to X$ where X' is normal and such that every dominant morphism $f\colon Y \to X$ with Y normal factors uniquely through π :

$$\begin{tikzcd} Y \arrow[r, "f"] \arrow[d, "\exists!"'] & X \\ X' \arrow[ur, "\pi"'] & \end{tikzcd}$$

We recall the notion of regularity: X is *regular* at x if the local ring $\mathcal{O}_{X,x}$ is regular. This means that if we denote by $\mathfrak{m}_x$ its maximal ideal and k its residue field then $\dim \mathcal{O}_{X,x} = \dim_k(\mathfrak{m}_x/\mathfrak{m}_x^2)$ where the first "dim" refers to the Krull dimension and the second one is the dimension as a k-vector space.

Definition 0.2. Let $f\colon X \to Y$ be a morphism of schemes. Let $V \subseteq Y$ be an affine open and let U be an affine open subset of $f^{-1}(V)$. Then, via the canonical morphism $\mathcal{O}_Y(V) \to \mathcal{O}_X(U)$, $\mathcal{O}_X(U)$ is an $\mathcal{O}_Y(V)$-algebra. If f is quasi-compact and for all V and U as above this algebra is finitely generated, we say that f is a *morphism of finite type*. If, moreover, for all $V \subset Y$ open affine, the pre-image $f^{-1}(V) \subset X$ is affine and $\mathcal{O}_X(f^{-1}(V))$ is a finitely generated $\mathcal{O}_Y(V)$-module, then we say that f is a *finite* morphism.

Definition 0.3. A morphism of schemes $f\colon X \to Y$ is *flat at* $x \in X$ if the induced morphism on stalks $f^{\#}\colon \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ is a flat morphism of rings, i.e., it makes $\mathcal{O}_{X,x}$ into a flat $\mathcal{O}_{Y,f(x)}$-module. We say that f is *flat* if it is flat at every $x \in X$.

One of the most important notions that we need is the one of *smoothness.*

Definition 0.4. Let k be a field and let X be a k-scheme of finite type. Let $\bar{k}$ be an algebraic closure of k. We say that X is *smooth at* $x \in X$ if the points lying above it in $X_{\bar{k}}$ are regular points. Let $f\colon X \to Y$ be a morphism of finite type of locally Noetherian schemes. We say that f is *smooth at* $x \in X$ if it is flat and $X_{f(x)} \to \operatorname{Spec} k(f(x))$ is smooth at x. We say that f is *smooth* if it is smooth at all $x \in X$.

An A-scheme is *projective* if it is isomorphic, as a scheme over A, to a closed sub-scheme of $\mathbb{P}^n_A$ for some $n \geq 0$.
We will mainly focus on curves, so we give a definition here.

Definition 0.5. Let K be a field. A *curve over* K is a K-scheme of finite type whose irreducible components have dimension 1. If S is a scheme, by *a curve over* S we mean a flat S-scheme whose fibres are curves over the corresponding residue fields. By abuse of notation, if R is a ring, we will often call a curve over $\operatorname{Spec} R$ just “a curve over R”.

The notion of a *blow-up* will be also needed: here we briefly describe this construction. Let A be a Noetherian ring and let $I \subset A$ be an ideal. We set $I^0 := A$ and define the graded A-algebra

$$\tilde{A} := \bigoplus_{d \geq 0} I^d.$$

Let $f_1, \dots, f_n$ be a set of generators of I (as A is Noetherian I is finitely generated); as such, the f_i's can be regarded as homogeneous elements of degree 0 in $\tilde{A}$ (because they clearly belong to A) or as elements of degree 1 (because they belong to $\tilde{A}_1 = I$). To emphasize the distinction we will denote the latter by $t_1, \dots, t_n$. We have a surjective homomorphism of graded A-algebras

$$\varphi\colon A[T_1, \dots, T_n] \longrightarrow \tilde{A}, \qquad T_i \mapsto t_i.$$

Notice that if $P \in A[T_1, \dots, T_n]$ is a homogeneous polynomial, then $\varphi(P) = P(t_1, \dots, t_n) = 0 \iff P(f_1, \dots, f_n) = 0$ so

$$\ker \varphi = \{P \in A[T_1, \dots, T_n] \text{ s.t. } P(f_1, \dots, f_n) = 0\}.$$

Definition 0.6. Let $X = \operatorname{Spec} A$ be an affine Noetherian scheme and let I be an ideal of A. Let $\tilde{A}$ be defined as above and let $\tilde{X} = \operatorname{Proj} \tilde{A}$. Then the morphism $\tilde{X} \to X$ is called the *blow-up* of X along I.

Lemma 0.7. *Let A be a Noetherian ring, I an ideal of A.*

(a) Let $S_i = T_i/T_1 \in \mathcal{O}(D_+(T_1))$. Then

$$(\ker \varphi)_{(T_1)} = \left\{ \begin{matrix} P \in A[S_2, \dots, S_n] \ \textit{s.t.} \\ \exists d \geq 0,\ f_1^d P \in (f_1 S_2 - f_2, \dots, f_1 S_n - f_n) \end{matrix} \right\}$$

and $\tilde{A}_{(t_1)}$ is isomorphic to the sub-A-algebra of A_{f_1} generated by $f_2/f_1, \dots, f_n/f_1$.

(b) Consider the ideal $J = (f_i T_j - f_j T_i)_{i,j=1}^n$. Then we have $J \subset \ker \varphi$. Moreover, if the f_i's form a minimal set of generators for I and $Z := V_+(J)$ is a closed integral sub-scheme of $\mathbb{P}_A^{n-1}$ then the closed immersion $\operatorname{Proj} \tilde{A} \to Z$ is an isomorphism.

Proof. This is part of [Liu02, Lemma 8.1.2]. □

Corollary 0.8. *Let $X = \operatorname{Spec} A$ be a Noetherian affine scheme, let $I = (f_1, \dots, f_n)$ be an ideal of A and let $\tilde{X} \to X$ be the blow-up of X along I. For $i = 1, \dots, n$ let A_i be the sub-A-algebra of $\operatorname{Frac} A$ generated by $f_j f_i^{-1}$, $j = 1, \dots, n$. Then the* *blow-up of X along I is the glueing of the* $\operatorname{Spec} A_i$*'s:*

$$\tilde{X} = \bigcup_{i=1}^{n} \operatorname{Spec} A_i.$$

Proof. Since the morphism φ defined above is surjective, then we have $\tilde{A} = A[T_1, \dots, T_n]/\ker\varphi$. Now $\tilde{X} = \operatorname{Proj}\tilde{A}$ can be covered by affine charts $\operatorname{Spec}\tilde{A}_{(t_i)}$. Part (a) of Lemma 0.7 tells us that $\tilde{A}_{(t_i)} = A_i$. Now

$$A_i = A[f_1 f_i^{-1}, \dots, \widehat{f_i f_i^{-1}}, \dots f_n f_i^{-1}]$$

(the "hat" means that the corresponding element is omitted). Let us denote $X_i = \operatorname{Spec} A_i$. Then, for $j \neq i$ we have

$$X_{ij} = (X_i)_{f_i/f_j} = \operatorname{Spec} A\left[f_1 f_i^{-1}, \dots f_j f_i^{-1}, f_i f_j^{-1}, \dots, \widehat{f_i f_i^{-1}}, \dots f_n f_i^{-1}\right]$$

and

$$X_{ji} = (X_j)_{f_j/f_i} = \operatorname{Spec} A\left[f_1 f_j^{-1}, \dots f_i f_j^{-1}, f_j f_i^{-1}, \dots, \widehat{f_j f_j^{-1}}, \dots f_n f_j^{-1}\right]$$

We have, for all $k = 1, \dots, n$

$$\begin{cases} \dfrac{f_k}{f_i} = \dfrac{f_j}{f_i}\dfrac{f_k}{f_j} \\ \\ \dfrac{f_k}{f_j} = \dfrac{f_i}{f_j}\dfrac{f_k}{f_i}. \end{cases}$$

So we have isomorphisms $\varphi_{ij} \colon X_{ij} \to X_{ji}$ where the isomorphism is induced by the isomorphism on rings. Notice that $\{X_{ij}\}_{j\neq i}$ is an open cover of X_i for all i. So we can glue the X_i's together along the X_{ij}'s taking as glueing maps the isomorphisms φ_{ij}. $\square$

Chapter 1

Models

Unless specified otherwise, for the remainder of this thesis, S will denote a Dedekind scheme and $K = K(S)$ its field of rational functions.

Definition 1.1. A *fibred surface over* S is an integral projective flat S-scheme $X \to S$ of dimension 2.

Definition 1.2. Let C be a smooth projective connected curve over K. A *model of* C *over* S is a normal fibred surface $\mathcal{C} \to S$ together with an isomorphism $\mathcal{C}_\eta \simeq C$. When talking about a property of a model, we will refer to the property of the scheme $\mathcal{C}$ itself or to the property of the morphism $\mathcal{C} \to S$, according to which one applies (for example *regular model* means that $\mathcal{C}$ is regular while *smooth model* means that $\mathcal{C} \to S$ is smooth).

In the study of good reduction the notion of a *minimal regular model* (often shortened to *minimal model*) will be very relevant.

Definition 1.3. A regular fibred surface $X \to S$ is *minimal* if every birational map $Y \dashrightarrow X$ of regular fibred S-surfaces is a birational morphism. Given a curve C over $K(S)$, a *minimal regular model* is a regular model which is also minimal in the sense that we just specified.

In most of the cases we are interested in, minimal models exist.

Theorem 1.4. *Let* $X \to S$ *be a regular fibred surface with generic fibre* X_η *of arithmetic genus* $p_a \geq 1$. *Then* X *admits a unique minimal model over* S, *up to unique isomorphism.*

Proof. See [Liu02, Theorem 9.3.21]. □

In light of this proposition we will talk about *the* minimal regular model of a curve C and will denote it by $\mathcal{C}^{\min}$.

Let us consider the case of elliptic curves. We will show how one can define a model of an elliptic curve and we will see that some caution is needed when using the word "minimal". We start by recalling the scheme-theoretic definition of an elliptic curve.

Definition 1.5. An elliptic curve over a field K is a pair (E, O) where E is a smooth, projective, connected curve of genus 1 over K and $O \in E(K)$. We often omit O from the notation and just write E for the elliptic curve.

Remark 1.6. A connected K-scheme with a K-rational point is automatically geometrically connected (see [Sta, Tag 04KV]). Hence elliptic curves are geometrically connected.

As a first example of a model, we define the Weierstrass model of an elliptic curve.

Definition 1.7. Let $T = \operatorname{Spec} A$ be an integral affine scheme and let K be its field of rational functions. Let (E, O) be an elliptic curve over K. A *Weierstrass model for E over T* is a triple (f, W, φ) where:

- $f \in A[x, y, z]$ is a homogeneous polynomial of the form

$$f(x, y, z) = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3; \tag{1.1}$$

  for such a polynomial, the corresponding equation $f(x, y, z) = 0$ is called a *Weierstrass equation.*

- W is the projective scheme

$$W = \operatorname{Proj}\left(\frac{A[x, y, z]}{(f(x, y, z))}\right);$$

- φ is an isomorphism

$$\varphi \colon E \xrightarrow{\sim} W \times_{\operatorname{Spec} S} \operatorname{Spec} K$$

sending O to the point $(0:1:0)$.

For the remainder of this section S will denote an affine Dedekind scheme $S = \operatorname{Spec} A$ and K the function field $K = K(S)$.

Theorem 1.8. *Every elliptic curve E over K admits a Weierstrass model over* $\operatorname{Spec} K$.

Proof. See [Sil09, Proposition III.3.3] □

Corollary 1.9. *Every elliptic curve E over K admits a Weierstrass model over S.*

Proof. Let $f_0(x, y) = y^2 + a_1xy + a_3y - x_3 - a_2x^2 - a_4x - a_6 = 0$ be an affine Weierstrass equation of E over K. Recall that $K = \operatorname{Frac} A$ so there exists $0 \neq l \in A$ such that $f_1 = l^6 f_0 \in A[x, y]$. Now take the change of coordinates $l^2x = X,\ l^3y = Y$. Then

$$\begin{aligned}
f_1(x, y) &= l^6(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) \\
&= l^6(\frac{1}{l^6}Y^2 + \frac{a_1}{l^5}XY + \frac{a_3}{l^3}Y - \frac{1}{l^6}X^3 - \frac{a_2}{l^4}X^2 - \frac{a_4}{l^2}X - a_6) \\
&= Y^2 + la_1XY + l^3a_3Y - X^3 - l^2a_2X^2 - l^4a_4X - l^6a_6 =: f(X, Y).
\end{aligned}$$

Now $f(X, Y) = 0$ is an integral Weierstrass equation for E and the model associated is a Weierstrass model. □

Definition 1.10. Given an elliptic curve E over K we call a Weierstrass model over S like the one described in Corollary 1.9 an *integral Weierstrass model.*

Note that an integral Weierstrass equation is not in general unique:

Example 1.11. Consider the following integral Weierstrass equation over $\mathbb{Q}$

$$y^2 = x^3 + x$$

and take the change of variables

$$\begin{cases} u = 2^{-2}x; \\ v = 2^{-3}y. \end{cases} \tag{1.2}$$

We obtain the equation $2^{-6}v^2 = 2^{-6}u^2 + 2^{-2}u$ which is equivalent to

$$v^2 = u^3 + 16u.$$

If we take a new change of variables

$$\begin{cases} x = 2^2 u \\ y = 2^3 v \end{cases} \tag{1.3}$$

it is easy to see that (1.2) and (1.3) are mutual inverses. Hence the two integral equations that we found define the same elliptic curve over $\mathbb{Q}$.

Now we are going to define the notion of minimal Weierstrass model of an elliptic curve. First we need to define the discriminant.

Definition 1.12. Let us consider the Weierstrass equation $f(x, y, z) = 0$ where $f \in K[x, y, z]$ is as in (1.1). We define the following quantities:

$$\begin{cases} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{cases}$$

The *discriminant associated to the equation* $f = 0$ is defined to be

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6. \tag{1.4}$$

It is clear that $\Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ and it follows that if the equation is integral then $\Delta \in A$. Moreover, it can be shown that if we apply a change of coordinates yielding an equivalent integral Weierstrass equation then the discriminants will differ by a constant factor that belongs to A^*, see Remark 1.15 below.

Definition 1.13. Let $f(x, y, z) = 0$ be an integral Weierstrass equation of discriminant Δ and let W be the corresponding Weierstrass model. Let Δ_W be the class of Δ in the quotient A/A^*. We call Δ_W the *discriminant of the model* W. By what is remarked above this is independent of the choice of the integral Weierstrass equation.

Now we can define the minimal Weierstrass model.

Definition 1.14. Let E be an elliptic curve over K and let W be a Weierstrass model over $S = \operatorname{Spec} A$ with discriminant $\Delta_W \in A/A^*$. Suppose there exists a discrete valuation v on A, normalized in such a way that $v(K^*) = \mathbb{Z}$. We say that W is *minimal at* v if $v(\Delta_W)$ is minimal among the valuations of the discriminants of all the integral Weierstrass equations of E. We say that W is a *minimal Weierstrass model* if it is minimal at all discrete valuations on A.

Remark 1.15. Given two integral Weierstrass equations for an elliptic curve E with discriminants Δ and Δ', it can be shown that they are related by $\Delta = u^{12}\Delta'$ for some invertible element $u \in K^*$. Therefore, if the discriminant of an integral Weierstrass equation satisfies $0 \leq v(\Delta) < 12$ then we can immediately conclude that the associated Weierstrass model is minimal.

Theorem 1.16. *If $S = \operatorname{Spec} A$ with A a DVR and $K = K(S)$ then every elliptic curve E over K admits a minimal Weierstrass model over S.*

Proof. This follows immediately from the fact that the valuation is discrete. □

Remark 1.17. The minimal Weierstrass model of an elliptic curve need not coincide with the minimal regular model, as we show in the following example.

Example 1.18. Consider the following Weierstrass equation over $\mathbb{Q}_p$, for some non-zero prime $p \in \mathbb{Z}$:

$$y^2z = x^3 + 2x^2z + 4z^3. \tag{1.5}$$

It is integral, because all coefficients are in $\mathbb{Z}$, and in particular in $\mathbb{Z}_p$. Recall that the p-adic valuation of an integer n is

$$v_p(n) = \operatorname{ord}_p(n) = \max\{m \in \mathbb{N} \text{ s.t. } p^m | n\}$$

The discriminant of the equation (1.5) is $\Delta = -7424 = -2^8 \cdot 29$ therefore

$$v_p(\Delta) = \begin{cases} 8 & \text{if } p = 2 \\ 1 & \text{if } p = 29 \\ 0 & \text{otherwise} \end{cases}$$

So for all $0 \neq p \in \operatorname{Spec} \mathbb{Z}$ we have $0 \leq v_p(\Delta) < 12$ hence (1.5) is a minimal Weierstrass equation. Therefore

$$X = \operatorname{Proj}\left(\frac{\mathbb{Z}[x, y, z]}{(y^2 z - x^3 - 2x^2 z - 4z^3)}\right)$$

is a minimal Weierstrass model. On the other hand, it is not regular. Indeed, let us consider the closed point on the affine chart $z = 1$ corresponding to the maximal ideal $\mathfrak{m} = (x, y, 2)$. We see that all the monomials appearing in the equation belong to $\mathfrak{m}^2$. This means that the equation gives no condition modulo $\mathfrak{m}^2$ hence none of $x, y, 2$ can be generated by the others in $\mathfrak{m}/\mathfrak{m}^2$. Therefore we have $\dim_{\mathbb{F}_2} \mathfrak{m}/\mathfrak{m}^2 = 3 > 2$ hence X is not regular at $\mathfrak{m}$ and it cannot be the minimal regular model of E.

Chapter 2

Reduction

Here we give the definitions and the important properties of various types of reduction. Recall that S denotes a Dedekind scheme and K its field of rational functions.

2.1 Good reduction

Definition 2.1. Let C be a smooth projective curve over K and let $s \in S$ be a closed point. Consider a model $\mathcal{C} \to S$. The fibre $\mathcal{C}_s$ is called the *reduction of C at s in $\mathcal{C}$*. If $S = \operatorname{Spec} A$ call $\mathfrak{m} \subset A$ the ideal corresponding to s. Then $\mathcal{C}_s$ is called the *reduction of C modulo $\mathfrak{m}$ in $\mathcal{C}$*.

Remark 2.2. In this setting the reduction modulo $\mathfrak{m}$ (or s) does not depend only on $\mathfrak{m}$ (or s) but also on the choice of the model.

Definition 2.3. We say that a curve C over K *has good reduction at $s \in S$* if there exists a smooth model of C over $\operatorname{Spec} \mathcal{O}_{S,s}$. We say that C *has bad reduction* at s if it does not have good reduction at s.

We are going to prove some results that will be the main theoretical tools for an algorithm to test good reduction and search for a smooth model of a curve of genus at least 2.

Lemma 2.4. *Let S be a Dedekind scheme and let $\pi \colon Y \to S$ be a fibred surface with smooth generic fibre Y_η. Then there exists a non-empty open subset $U \subset S$*

such that $\pi^{-1}(U) \to S$ is smooth. In particular, since $\dim S = 1$ there exist at most finitely many closed points $s \in S$ such that $\pi^{-1}(s) \to S$ is not smooth.

Proof. The set Y_{sm} of points of Y where π is smooth is open ([Liu02, Cor. 6.2.12]), so its complement is closed, therefore, since π is projective and hence proper, the image $\pi(Y \setminus Y_{\mathrm{sm}})$ is also closed. Let $U = S \setminus \pi(Y \setminus Y_{\mathrm{sm}})$. This is an open subset of S containing the generic point, so it is also non-empty and, by construction, the restriction $\pi\colon \pi^{-1}(U) \to U$ is smooth. □

Proposition 2.5. *Let C be a smooth projective curve of genus $g \geq 1$ over $K = K(S)$, where S is an affine Dedekind scheme. Then C has good reduction* if and only if *the minimal regular model $\mathcal{C}^{\min}$ is smooth over S.*

Proof. See [Liu02, Prop 10.1.21.b]. □

In the case of curves of genus 1, it is necessary to distinguish the case of elliptic curves (smooth projective curves of genus 1 with a marked rational point) from the general case. Let R be a discrete valuation ring, $K = \operatorname{Frac} R$ and v a normalized valuation.

Definition 2.6. Let $\mathfrak{m} \subset R$ be the maximal ideal of R. Let E/K be an elliptic curve and fix a Weierstrass model (f, W, φ) of E over $\operatorname{Spec} R$. The special fibre $W_{\mathfrak{m}} \to k(\mathfrak{m}) = R/\mathfrak{m}$ is called the *reduction of E modulo $\mathfrak{m}$ in W.*

By definition, we have $W = \operatorname{Proj}(R[x, y, z]/(f))$, hence $W_{\mathfrak{m}} = \operatorname{Proj}\big(R[x, y, z]/(\bar{f})\big)$ where $\bar{f} \equiv f \pmod{\mathfrak{m}}$. We will always study the reduction of an elliptic curve with respect to a minimal Weierstrass model $\mathcal{W}_{\min}$. Let $\mathcal{W}_{\mathfrak{m}}$ be the reduction of E modulo $\mathfrak{m}$ in $\mathcal{W}_{\min}$. The equation $\bar{f} = 0$ defining it has discriminant $\bar{\Delta}_{\min} \equiv \Delta_{\min} \pmod{\mathfrak{m}}$ and is singular if and only if $\bar{\Delta}_{\min} = 0$ that is if and only if $\Delta_{\min} \equiv 0 \pmod{\mathfrak{m}}$ (i.e., $\Delta_{\min} \notin R^*$). This is in fact a necessary and sufficient condition for good reduction. Indeed we have the following

Proposition 2.7. *Let E be an elliptic curve over K. Let $s \in S$ be a closed point, let $\mathcal{W}$ be a minimal Weierstrass model of E over $\operatorname{Spec} \mathcal{O}_{S,s}$, and $\Delta_{\min}$ the discriminant of $\mathcal{W}$. Then the following properties are equivalent*

1. *E has good reduction at s;*

2. $\mathcal{W}_s$ *is a smooth curve over* $k(s)$.

Proof. See [Liu02, Corollary 10.1.23]. □

Remark 2.8. It follows immediately from the above discussion that another condition equivalent to those of the previous proposition is $\Delta_{\min} \in \mathcal{O}^*_{S,s}$.

Definition 2.9. Let R be a DVR with field of fractions K and maximal ideal $\mathfrak{m}$. Let E be an elliptic curve over K and let (f, W, φ) be a Weierstrass model of E over $\operatorname{Spec} R$. The *reduction type* of E at $\mathfrak{m}$ with respect to W is

- *good* if $W_{\mathfrak{m}}$ is a smooth cubic curve;
- *multiplicative* if $W_{\mathfrak{m}}$ is a nodal cubic curve;
- *additive* if $W_{\mathfrak{m}}$ is a cuspidal cubic curve.

Remark 2.10. If $\mathcal{W}, \mathcal{W}'$ are two minimal Weierstrass models then the reduction of E with respect to them will be the same.

Notice that having only two possibilities for the bad reduction is a special property of the Weierstrass models of elliptic curves. Many more possible singular curves can occur as reduction of a more general smooth cubic curve.

Let E be an elliptic curve over a number field K and consider an integral Weierstrass equation for it. Let v be a non-Archimedean valuation on K. Then we can take a Weierstrass equation for E minimizing the discriminant with respect to this valuation. Let Δ_v be the corresponding discriminant. Then E has good reduction at v *if and only if* $v(\Delta_v) = 0$. Let us state

Theorem 2.11 (Tate)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then E has bad reduction at some prime. Equivalently,* $\Delta_{\min} \neq \pm 1$. □

It is possible to define elliptic curves over extensions of $\mathbb{Q}$ that have good reduction at every prime, as the following example, also due to Tate, shows.

Example 2.12. The elliptic curve defined over $\mathbb{Q}(\sqrt{29})$ by

$$E : y^2 + xy + \varepsilon^2 y = x^3, \qquad \varepsilon = \frac{5+\sqrt{29}}{2}$$

has good reduction everywhere. Indeed, we have $\Delta(E) = \varepsilon^6(1-27\varepsilon^2)$. It is easy to see, by computing norms, that both ε and $1-27\varepsilon^2$ are units, therefore the valuation of the discriminant at every prime is zero hence we have a minimal Weierstrass equation. Moreover no prime divides the discriminant and hence the curve has good reduction everywhere.

If a curve over a field K does not have good reduction it is natural to ask whether it is possible to extend the field K in such a way that, over the extension, it does have good reduction. This leads to the definition of *potential good reduction.*

Definition 2.13. Recall that we fixed a Dedekind scheme S and denote by K its function field. Let C be a smooth projective curve over K. We say that C has potential good reduction if there exists a finite field extension L/K such that $C' = C \times_K L \to \operatorname{Spec} L$ has good reduction.

In the case of elliptic curves this is very easy to check.

Proposition 2.14. *Let E be an elliptic curve over a number field K, let $p \in \mathcal{O}_K$ be a prime and let L/K be a field extension. Then the following assertions hold.*

1. *If L/K is unramified, then the reduction type (see Definition 2.9) of E at a prime $\mathfrak{p} \in L$ lying above p is the same as the one at p over K;*
2. *If L/K is finite and E has good (resp. multiplicative) reduction at p over K then it will be again good (resp. multiplicative) over the primes of L lying above p;*
3. *There exists an extension K'/K such that E has good or multiplicative reduction over K' at the primes lying above p.*

Proof. See [Sil09, Proposition VII.5.4]. □

Potential good reduction of elliptic curves is easy to check over local fields. Let K be a local field with valuation v, R its ring of integers (i.e., $\{x \in K \text{ s.t. } v(x) \geq 0\}$) and $\mathfrak{m}$ the maximal ideal of R (i.e., $\mathfrak{m} = \{x \in K \text{ s.t. } v(x) > 0\} = R \setminus R^*$).

Proposition 2.15. *An elliptic curve E over a local field K has potential good reduction* if and only if *its j-invariant belongs to the ring of integers of K.*

Proof. See [Sil09, Proposition VII.5.5]. □

Using this proposition it is also easy to check potential good reduction over number fields. Indeed, since there are only finitely many primes of bad reduction (the minimal discriminant has only finitely many prime factors) we can reduce to the local case and check potential good reduction at each of them.

2.2 Stable and Semi-stable reduction

Definition 2.16. Let k be an algebraically closed field and C a curve over k. We say that C is *semi-stable* if it is reduced and its singular points are ordinary double points (i.e., their pre-image under the normalization morphism consists of 2 points). We say that C is *stable* if, moreover, the following properties hold:

1. C is connected, projective of arithmetic genus $p_a \geq 2$;
2. for any irreducible component Γ that is isomorphic to $\mathbb{P}^1_k$, let $\tilde{\Gamma}$ be the union of the other irreducible components. Then $\#(\Gamma \cap \tilde{\Gamma}) \geq 3$.

We also define the notion of (semi-)stability for morphisms.

Definition 2.17. Let $f : X \to S$ be a morphism of schemes of finite type. Then f is called *semi-stable* or we say that X is a *semi-stable curve over* S if f is flat and for all geometric points $s \in S$ the fibre X_s is a semi-stable curve over $k(s)$. Assume f is proper, flat and all fibres over geometric points are stable curves of the same genus $g \geq 2$; then we say that f is *stable of genus* g or that X is a *stable curve of genus* g *over* S.

The following two propositions relate the notions of (semi-)stability with the ones of smoothness, normality, regularity and show that (semi-)stability is well behaved under base-change.

Proposition 2.18. *A regular semi-stable curve over a field* k *is smooth over* k.

Proof. [Liu02, Prop. 10.3.7]. □

Proposition 2.19. *Let* $f \colon X \to S$ *be a semi-stable (resp. stable) curve. Then*

1. *If $S' \to S$ is a morphism, then $X \times_S S' \to S'$ is semi-stable (resp. stable);*

2. *If S is a Dedekind scheme with generic point η and X_η is normal then X is normal.*

Proof. 1. This follows almost immediately from the definition of stability (resp. semi-stability) when we recall that flatness and properness of morphisms are preserved under base-change;

2. This is a consequence of the fact that $X \to S$ has reduced geometric fibres (see [Liu02, Lemma 4.1.18]).

□

We include some relevant results that can be found, for example, in Section 10.3 of [Liu02].

Lemma 2.20. *Let R be a discrete valuation ring with valuation v, field of fractions K and residue field k. Let X be an integral flat curve over R. Let x be a closed point of the special fibre outside which X is regular. Moreover, assume there exists $c \in R$ with $e = v(c) \geq 1$ and the property that $\hat{R}_{X,x} \simeq \hat{R}[[x, y]]/(xy - c)$ (we denote by $\hat{R}$ the completion of R with respect to v). Then*

(a) there exists a sequence

$$X_n \to \ldots \to X_1 \to X \tag{2.1}$$

of proper birational morphisms where each X_i normal with a unique singular point x_i and the map $X_{i+1} \to X_i$ is the blow-up of X_i with centre x_i;

(b) the sequence is finite, with $n = e/2$;

(c) the fibre of $X_n \to X$ above x consists of $e-1$ copies of $\mathbb{P}^1_k$, with multiplicity 1 in the special fibre, meeting transversally at rational points.

Proof. See [Liu02, Lemma 10.3.21]. □

Proposition 2.21. *Let $X \to S$ be semi-stable and let x be a singular point of the fibre X_s for some $s \in S$. Then there exists a scheme S' finite étale over S and a* *base change*

$$\begin{array}{ccc} C\times_S S' = X' & \longrightarrow & X \\ \big\downarrow & & \big\downarrow \\ S' & \longrightarrow & S \end{array}$$

such that every point of X' lying above x and belonging to a fibre $X'_{s'}$ is a split ordinary double point over $k(s')$ (i.e., its pre-image under the normalization morphism consists of two $k(s')$-rational points). Under these hypotheses there is an isomorphism

$$\hat{\mathcal{O}}_{X',x'} \simeq \hat{\mathcal{O}}_{S',s'}[[u,v]]/(uv-c)$$

for some $c \in \mathfrak{m}_{s'}$. The valuation of the element c is called the thickness *of x in X.*

Proof. See [Liu02, Corollary 10.3.22]. □

The following corollary will be very important in the study of stable and semi-stable reduction.

Corollary 2.22. *Let $X \to S$ be a semi-stable projective curve and assume its generic fibre X_η is smooth. Let $\pi\colon X' \to X$ be the minimal desingularization* [1] *and for $s \in S$ let $x \in X_s$ be a split ordinary double point of thickness e. Then $\pi^{-1}(x)$ consists of a chain of $e-1$ copies of $\mathbb{P}^1_{k(s)}$ meeting transversally at rational points. They have multiplicity 1 inside X' and self intersection -2.*

Proof. See [Liu02, Corollary 10.3.25]. □

Now we are going to define semi-stable and stable reduction.

Definition 2.23. Let C be a curve over K and let $s \in S$. We say that C has *(semi-)stable* reduction at s if there exists a model $\mathcal{C}$ that is a (semi-)stable curve over $\operatorname{Spec} \mathcal{O}_{S,s}$. If we just say that C has (semi-)stable reduction we mean that this holds for all points of S.

Theorem 2.24. *Let S be an affine Dedekind scheme, C a projective smooth curve over $K(S)$ of genus $g > 0$. If C has semi-stable reduction over S then:*

1. *The minimal regular model of C is semi-stable over S;*

[1] It exists. Indeed by [Liu02, Corollary 8.3.51] there exists a desingularization and by [Liu02, Prop. 9.3.2] every normal fibred surface admitting a desingularization admits a minimal one.

2. *If $g \geq 2$ and C is geometrically connected then it admits a unique stable model over S.*

Proof. See [Liu02, Theorem 10.3.34] □

2.3 Potential (semi-)stable reduction

In what follows we need the notion of an *excellent scheme*.

Definition 2.25. A Noetherian ring A is said to be *excellent* if

1. $\operatorname{Spec} A$ is universally catenary;

2. for every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$ the formal fibres of $A_{\mathfrak{p}}$ are geometrically regular;

3. for every finitely generated A-algebra B the set of regular points of $\operatorname{Spec} B$ is open in B.

A scheme X is *excellent* if it is locally Noetherian and admits an affine open covering $\{U_i\}_i$ such that for all i the ring $\mathcal{O}_X(U_i)$ is excellent. Excellent schemes and their main properties are treated in [Liu02, Section 8.2.3].

Definition 2.26. Let X be an integral scheme, $K = K(X)$ its function field and L a finite extension of K. The *normalization of X in L* is an integral morphism $\pi\colon X' \to X$ such that $K(X') = L$, X' is normal and π extends the canonical morphism $\operatorname{Spec} L \to X$.

Definition 2.27. Let S be a Dedekind scheme, $K = K(S)$ its function field and let C be a smooth, projective, geometrically connected curve over $K(S)$. Let L be a finite extension of K and let S' be the normalization of S in L. It is again a Dedekind scheme. Indeed, it is normal, because it is a normalization of S; moreover, since S is excellent the normalization morphism is finite therefore[2] $\dim \tilde{S} = \dim S = 1$. We say that C has (semi-)stable reduction over S' if its extension $C_L = C \times_K L \to \operatorname{Spec} L$ has (semi-)stable reduction over S'.

[2] To see this, we can assume S and $\tilde{S}$ to be affine, so a finite morphism of integral schemes $\operatorname{Spec} A \to \operatorname{Spec} B$ corresponds to an integral extension of rings $B \subset A$ and A is a normal ring. Then the Going-Up and Going-Down theorems tell us that that the maximal length of a chain of prime ideals in A and B is the same, hence they have the same dimension.

The fundamental result in the theory of the reduction of curves is the following

Theorem 2.28 (Deligne-Mumford)**.** *Let S be a Dedekind scheme and let C be a smooth, projective, geometrically connected curve of genus $g \geq 2$ over $K(S)$. Then there exists a Dedekind scheme S', finite flat over S such that $C_{K(S')}$ has a stable model over S'. Moreover, if S'/S is a finite flat extension such that a stable model exists over S' then the stable model is unique up to isomorphism.*

Proof. This follows from [Liu02, Theorem 10.4.3 and Lemma 10.4.28]. □

This theorem was proven by Deligne and Mumford in [DM69]. A proof due to Artin and Winters (see [AW71]) can also be found in [Liu02, Section 10.4.2].

The following lemma is important in determining whether a curve satisfying certain conditions has potential good reduction. It gives a characterization of potential good reduction for high genus curves in terms of stable models. As we could not find this result in the literature, we include a complete proof.

Lemma 2.29. *Let S be an excellent Dedekind scheme, $K = K(S)$ its function field. Let C be a smooth, projective, geometrically connected curve over K of genus $g \geq 2$. Then C has potential good reduction* if and only if *every stable model over every extension of the base field that provides one is smooth.*

Proof. If every stable model is smooth, then C admits a smooth model upon base change because, by Theorem 2.28, it admits a stable one. Hence C has potential good reduction.

Assume C has potential good reduction. Then there exists a finite extension L/K such that C_L admits a smooth model over $\tilde{S}$, where $\tilde{S}$ is the normalization of S inside L. Notice that, as S is excellent, $\tilde{S}$ is again a Dedekind scheme (see Definition 2.27 and the discussion thereby). By Proposition 2.5 as a smooth model of C_L over $\tilde{S}$ we can take the minimal regular model, which we denote by $\mathcal{C}_L^{\min}$.

Let S' be a finite flat S-scheme with function field $K' = K(S')$ such that the curve $C_{K'}$ admits a stable model $\mathcal{C}_{K'}^{\mathrm{st}}$ over S' and assume, for the purpose of contradiction, that $\mathcal{C}_{K'}^{\mathrm{st}}$ is not smooth over S'. We have the following diagram, where the four inner squares are cartesian and the top arrows are given by the isomorphism between C_L (resp. $C_{K'}$) and the generic fibre of $\mathcal{C}_L^{\min}$ (resp. $\mathcal{C}_{K'}^{\mathrm{st}}$):

$$
\begin{tikzcd}
\mathcal{C}_{K'}^{\mathrm{st}} \arrow[dddr, bend right] & & & & \mathcal{C}_L^{\min} \arrow[dddl, bend left] \\
& C_{K'} \arrow[ul] \arrow[r] \arrow[d] & C \arrow[d] & C_L \arrow[l] \arrow[ur] \arrow[d] & \\
& \operatorname{Spec} K' \arrow[r] \arrow[d] & \operatorname{Spec} K \arrow[d] & \operatorname{Spec} L \arrow[l] \arrow[d] & \\
& S' \arrow[r] & S & \tilde{S} \arrow[l] &
\end{tikzcd}
$$

Let $M = L.K'$ be the composite of the fields L and K' and let $T \to S$ be the normalization of S inside M. We can also normalize S' and $\tilde{S}$ inside M to obtain $N_M(S') \to S'$ and $N_M(\tilde{S}) \to \tilde{S}$. We also have morphisms $T \to N_M(S')$ and $T \to N_M(\tilde{S})$ hence, by composition we have maps $T \to S'$ and $T \to \tilde{S}$. The following diagram summarizes this:

$$
\begin{tikzcd}
S' \arrow[r] & S & \tilde{S} \arrow[l] \\
N_M(S') \arrow[u] & T \arrow[l] \arrow[r] \arrow[u] \arrow[ul, dotted] \arrow[ur, dotted] & N_M(\tilde{S}) \arrow[u]
\end{tikzcd}
$$

Using these two maps, we can base-change the two models to T:

$$
\begin{aligned}
\mathcal{D}_L &:= \mathcal{C}_L^{\min} \times_{\tilde{S}} T \longrightarrow T; \\
\mathcal{D}_{K'} &:= \mathcal{C}_{K'}^{\mathrm{st}} \times_{S'} T \longrightarrow T.
\end{aligned}
$$

Notice that $\mathcal{D}_L$ is smooth over T, that $\mathcal{D}_{K'}$ is stable and non-smooth and both have generic fibre isomorphic to C_M.

We can ease the proof by making some simplifications of the base-schemes. Indeed, we can assume $S, \tilde{S}, S'$ to be local. Moreover, by Proposition 2.21, there exists a local scheme W, finite étale over T such that every irreducible component of the special fibre of $\mathcal{D}_{K'} \times_T W \to W$ is geometrically irreducible and all its singular points are split ordinary double points. Recall that finite étale base-changes preserve stability, minimality, and regularity so $\mathcal{D}_L \times_T W$ is again minimal and regular and $\mathcal{D}^{\mathrm{st}}_{K'} \times_T W$ is again stable. By these observations we can replace T by W. Let $\tilde{\mathcal{D}}_{K'}$ be the minimal desingularization of $\mathcal{D}_{K'}$. Then Corollary 2.22 applies and we can deduce that $\tilde{\mathcal{D}}_{K'} \to W$ is not smooth. The situation is the following

$$\begin{tikzcd}
\mathcal{C}^{\mathrm{st}}_{K'} \arrow[ddr, bend right] & & & & \mathcal{C}^{\mathrm{min}}_{L} \arrow[ddl, bend left] \\
& C_{K'} \arrow[ul] \arrow[r] \arrow[d] & C \arrow[d] & C_L \arrow[l] \arrow[ur] \arrow[d] & \\
\tilde{\mathcal{D}}_{K'} \arrow[uu, bend left] \arrow[ddrr, bend right] & \operatorname{Spec} K' \arrow[r] \arrow[d] & \operatorname{Spec} K \arrow[d] & \operatorname{Spec} L \arrow[l] \arrow[d] & \mathcal{D}_L \arrow[uu, bend right] \arrow[ddll, bend left] \\
& S' \arrow[r] & S & \tilde{S} \arrow[l] & \\
& & W \arrow[ul] \arrow[u] \arrow[ur] & &
\end{tikzcd}$$

Let $E \subset \mathcal{D}_{K'}$ be a vertical prime divisor. As $\mathcal{D}_{K'}$ is stable, either E is not isomorphic to $\mathbb{P}^1$ or E intersects the union of the irreducible components of the special fibre of $\mathcal{D}_{K'}$ at at least three points. Now let $F \subset \tilde{\mathcal{D}}_{K'}$ be a vertical prime divisor and let k_F be the residue field of W. Assume $F \simeq \mathbb{P}^1_{k_F}$. We want to show that F has self intersection different from -1. We have two cases:

- If F is contracted by the desingularization map $\pi\colon \tilde{\mathcal{D}}_{K'} \to \mathcal{D}_{K'}$ then by Corollary 2.22 we have $F^2 = -2$.

- Assume F is not contracted by π. Then $\pi(F)$ intersects the union of the other irreducible components of the special fibre of $\mathcal{D}_{K'}$ at at least three points. Let $Y \subset \tilde{\mathcal{D}}_{K'}$ be the special fibre of $\mathcal{D}_{K'}$ and denote by Y_0 the union of the irreducible components of Y different than F. Then F meets Y_0 at least three points: $F \cdot Y_0 \geq 3$. But we know $Y \cdot F = 0$. Also $Y_0 + F = Y$ so

$$F^2 = F \cdot (Y - Y_0) = -F \cdot Y_0 \leq -3.$$

This shows, by Castelnuovo's criterion ([Liu02, Theorem 9.3.8]), that $\tilde{\mathcal{D}}_{K'}$ does not contain exceptional divisors. So it is a minimal regular model of C over W. Therefore, by the uniqueness of the minimal regular model, we have $\tilde{\mathcal{D}}_{K'} \simeq \mathcal{D}_L$, which is a contradiction, because $\mathcal{D}_L$ is smooth over W while $\tilde{\mathcal{D}}_{K'}$ is not and this completes the proof. $\square$

Chapter 3

Algorithms

3.1 Testing for good reduction

The following algorithm takes as input a smooth projective geometrically connected curve C of genus $g \geq 2$ over the field of functions K of a Dedekind scheme S, and returns a regular model of C over S. We assume the curve to be given as the zero set, in some projective space, of a finite collection of homogeneous polynomials. For clarity, we begin by giving an outline of the algorithm, before going into more detail concerning how the steps are accomplished.

For $g = 1$, if C has a rational point, we have an elliptic curve, and the problem is very easy to solve. The general genus 1 case is not treated here.

Algorithm 1 (Outline)**.** Let $C \subset \mathbb{P}^n$ be a smooth projective curve of genus $g \geq 2$, together with a chosen projective embedding, over $K = K(S)$ with S an affine Dedekind scheme. We construct a regular model $\tilde{\mathcal{C}}$ of C over S: (The existence is ensured by Theorem 1.4, which actually ensures the existence of a minimal one.)

Take the Zariski closure of C inside $\mathbb{P}^n_S$: denote it by $\mathcal{C}$; this is an integral scheme and it is flat and projective over S.
if $\mathcal{C}$ is regular **then**
  Set $\mathcal{C} = \tilde{\mathcal{C}}$
else
  Resolve singularities to obtain a regular model $\tilde{\mathcal{C}}$

6: **end if**

7: Output $\tilde{\mathcal{C}}$

We now give more details on how steps 1 and 5 in the algorithm are carried out.

1. By assumption C is a smooth projective curve given as the zero-set of some polynomials $f_1, \dots, f_m \in K[x_0, \dots, x_n]$. Multiply them by a suitable non-zero element of $\mathcal{O}_K$ to get $g_1, \dots, g_m \in \mathcal{O}_K[x_0, \dots, x_n]$ defining an isomorphic curve over K. Now let

$$C' = \operatorname{Proj}\left(\mathcal{O}_K[x_0, \dots, x_n]/(g_1, \dots, g_m)\right).$$

We know that the Zariski closure $\mathcal{C}$ of C in C' is just the irreducible component of C' that contains C. So the problem of finding the Zariski closure is reduced to the problem of finding the irreducible components of C'. Now, we can cover C' by (at most) $n+1$ affine charts, that are of the form $C'_i = \operatorname{Spec}\left(\mathcal{O}_K[x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n]/(g_{i1}, \dots, g_{in})\right)$ where the polynomial g_{ij} is obtained form g_j by setting $x_i = 1$. The irreducible components correspond to the prime ideals of the primary decomposition of $(g_{i,1}, \dots, g_{i,n})$, and finding such a decomposition can be done, using Gröbner bases. There exist algorithms to solve this problem that have been implemented in computers (for example, see [GTZ88]).

5. The model $\mathcal{C}$ found in Step 1 is a fibred surface over a Dedekind scheme with a smooth fibre (the generic fibre is smooth because it is isomorphic to C, which is smooth over $K(S)$). From this we deduce the following consequences:

   – Let us denote by $\pi\colon \mathcal{C} \to S$ the S-scheme structure morphism. Then there exists a non-empty open subset $U \subset S$ such that $\pi^{-1}(U) \to S$ is smooth (see Lemma 2.4). Moreover, since $\dim S = 1$, then $S \setminus U$ is finite, so the set of singular fibres is finite. To find such a set U the Jacobian criterion can be used. Indeed, U can be taken as the set of points for which the Jacobian matrix has full rank. This can be found just by computing the determinants of the (finitely many) maximal-order minors of the Jacobian matrix and finding the set of points $V \subset S$ at which all the determinants vanish. Then we can take $U = S \setminus V$.

– Let

$$\ldots \to \mathcal{C}_{n+1} \to \mathcal{C}_n \to \ldots \to \mathcal{C}_1 \to \mathcal{C} \tag{3.1}$$

be the sequence where $\mathcal{C}_{i+1} \to \mathcal{C}_i$ is the composition of the normalization $\bar{\mathcal{C}}_i \to \mathcal{C}$ and the blow-up $\mathcal{C}_{i+1} \to \bar{\mathcal{C}}_i$ along the singular locus of $\bar{\mathcal{C}}_i$. Under our conditions, since there are only finitely many singular fibres, the sequence (3.1) is well defined and finite (see [Liu02, Theorem 8.3.50]).

– The sequence (3.1) can be computed in a finite number of steps. Indeed, computing each element $\mathcal{C}_{i+1} \to \mathcal{C}_i$ of the sequence involves a normalization and a blow-up.

  For the normalization, we first cover our scheme $\mathcal{C}_i$ by affine charts. Each of them will be the spectrum of a ring A_{ij} which is the quotient of a polynomial ring by a finitely generated ideal. Notice that the A_{ij}'s are reduced and noetherian (indeed, computing the Zariski closure we ended up with an integral scheme which is, in particular, reduced). There exist algorithms for computing the normalization of such rings (for example, see [GLS10]), we take the spectra of the normalized rings to obtain the normalization of the corresponding affine scheme and glue them together to obtain the normalization $\bar{\mathcal{C}}_i$ of $\mathcal{C}_i$.

  Now we need to blow-up $\bar{\mathcal{C}}_i$ along its singular locus. It was remarked above that this is contained in a finite union of closed fibres. This ensures the existence of a desingularization, by [Liu02, Theorem 8.3.50]. In the proof of the quoted theorem it is also shown that, after the first normalization, we obtain $\mathcal{C}_1$ whose singular locus consists of a finite set of closed points. Hence, we need to blow-up at finitely many closed points, and this is true, a fortiori, for the other steps. Therefore, all we need is an algorithm allowing us to construct the blow-up of a normal scheme at a single closed point.

  Let P be a singular closed point of $\bar{\mathcal{C}}_i$. As we noticed above, we can cover $\bar{\mathcal{C}}_i$ by a finite number of affine charts that are spectra of reduced Noetherian rings:

$$\bar{\mathcal{C}}_i = \bigcup_{j=1}^{m_i} \operatorname{Spec} A_{ij}.$$

Let j_0 be the smallest index such that $P \in \operatorname{Spec} A_{ij_0}$ and denote by $\mathfrak{m}_P$ the corresponding maximal ideal of which we know the (finitely many) generators: $\mathfrak{m}_P = (f_1, \ldots, f_s)$. In order to ease the notation, let us denote by A the ring A_{ij_0} and let $X = \operatorname{Spec} A$. For $l = 1, \ldots s$ let A_l be the sub-A-algebra of $\operatorname{Frac} A$ generated by $f_t f_l^{-1}$, $t = 1, \ldots, s$. Then, by Corollary 0.8 we know that the blow-up of $\operatorname{Spec} A$ is

$$\tilde{X} = \bigcup_{l=1}^{s} \operatorname{Spec} A_l.$$

As the blow-up is a local procedure, having blown-up $\operatorname{Spec} A_{ij_0}$ does not affect the other affine charts. Therefore, it is enough to replace $\operatorname{Spec} A_{ij_0}$ by $\tilde{X}$. Now we repeat this procedure for the other singular points of $\bar{\mathcal{C}}_i$ and end up with a regular fibred surface $\tilde{\mathcal{C}} \to S$.

Suppose now that we have an algorithm allowing us to contract an exceptional component of $\tilde{\mathcal{C}}$. By Propositions 2.4 and 2.5, in order to test good reduction, it suffices to compute the minimal regular model of C: this model will be smooth if and only if C has good reduction. To compute the minimal regular model, we first apply Algorithm 1 to obtain a regular model. Notice that its generic fibre has genus $g \geq 1$ because it is isomorphic to C. This implies that $\tilde{\mathcal{C}}$ admits a unique minimal model ([Liu02, Theorem 9.3.21]). Moreover, note that there are only finitely many fibres containing exceptional components. Indeed, there are only finitely many non-smooth fibres and the smooth fibres have genus at least 1 so, by Castelnuovo's criterion ([Liu02, Theorem 9.3.8]), they cannot be contracted; each non-smooth fibre has only finitely many irreducible components and, in particular, finitely many exceptional ones. Using our hypothetical contraction algorithm we construct a sequence of contraction morphisms

$$\tilde{\mathcal{C}} \to \mathcal{C}_1 \to \ldots \to \mathcal{C}_n = \mathcal{C}^{\min}$$

such that $\mathcal{C}^{\min}$ has no exceptional divisors. Let us recall that a contraction of an exceptional divisor maps the divisor to a regular point and is an isomorphism outside it. Therefore, the above chain will give rise to a scheme $\mathcal{C}^{\min}$ that preserves the regularity of $\tilde{\mathcal{C}}$ but that contains no exceptional divisors: a minimal regular model. Then, we can check if this model is smooth.

3.2 Testing for potential good reduction

Let K be a p-adic field (a finite extension of $\mathbb{Q}_p$) and assume we have a curve C over K, smooth and of genus at least 2. We want to determine whether there exists an extension of K over which C attains good reduction, and if it does, find such an extension of minimal degree. We observe that that any p-adic field admits finitely many extensions of fixed degree and that smoothness is preserved under base-change. An algorithm to compute all the extension of a fixed degree of a given p-adic field K is described in [PR01]. The following algorithm uses the previous one to check whether the curve C has potential good reduction. In particular we work under the hypothesis that we have an algorithm allowing us to contract exceptional divisors on regular models. The test is done by applying Algorithm 1 to all extensions of K of a fixed degree, starting from degree 1, and increasing the degree until we find one over which C has good reduction. Therefore, if C has potential good reduction the algorithm will return the extension of smallest degree over which C acquires good reduction.

Algorithm 2. Let C be a smooth projective curve over K. Again, we assume it to be given as the zero-set of a finite collection of homogeneous polynomials.

1: Set $d = 1$.
2: Let $L_1, \dots L_{N(d)}$ be the set of all extensions of K of degree d.
3: $i \leftarrow 1$;
4: **if** $i \leq N(d)$ **then**
5:     Apply Algorithm 1 to get a regular model $\mathcal{C}_{L_i}$ and contract exceptional components to obtain the minimal regular model $\mathcal{C}_{L_i}^{\min}$;
6: **else**
7:     go to step 14;
8: **end if**
9: **if** $\mathcal{C}_{L_i}^{\min}$ is smooth **then**
10:     **return** L_i

11: **else**
12: set $i \leftarrow i+1$ and go back to step 4
13: **end if**
14: Set $d \leftarrow d+1$ and go back to step 2

We also include an easy and efficient algorithm to test good and potential good reduction for elliptic curves.

Algorithm 3. Let E be an elliptic curve over a field K.

Compute the minimal discriminant $\Delta_{\min}$.
if $\Delta_{\min} \in \mathcal{O}_K^*$ **then**
  E has good reduction and, a fortiori, potential good reduction. Terminate.
else
  E does not have good reduction.
end if
Compute the j-invariant $j(E)$.
if $j(E) \in \mathcal{O}_K$ **then**
  E has potential good reduction
else
  E does not have potential good reduction.
end if

The software Sage[1] contains several tools to treat elliptic curves: the last algorithm can be completely run in Sage. Assume E to be given as the zero set of a Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then we can apply the following:

```
E=EllipticCurve(K, [a_1,a_2,a_3,a_4_a_6])
M=E.minimal_model()
D=M.discriminant()
J=E.j_invariant()
R=K.ring_of_integers()
D.is_unit()
J in R
```

[1] http://www.sagemath.org/

Let us describe what each of the commands above does.

1. Defines as `E` the elliptic curve E taking as input the field K and the coefficients of the Weierstrass equation.

2. Finds a minimal Weierstrass equation for E and defines it as `M`. It does *not* find the minimal regular model in the sense that we used in this thesis.

3. Defines as `D` the minimal discriminant.

4. Defines as `J` the j-invariant.

5. Defines as `R` the ring of integers of K.

6. Returns `True` if the minimal discriminant is a unit in R, so *if and only if* E has good reduction and returns `False` otherwise. Clearly, if this command returns `True` it is not necessary to run the last one, because if E has good reduction then a fortiori it has potential good reduction.

7. Returns `True` if the j-invariant is in R, so *if and only if* E has potential good reduction and returns `False` otherwise.

Chapter 4

Examples

Example 4.1. We give a detailed example of application of Algorithm 1. We consider the following curve over $\mathbb{Q}$:

$$C = \operatorname{Spec}\left(\frac{\mathbb{Q}[x,y]}{(y^2 - x^3 + 49)}\right).$$

We construct a regular model of C over $\operatorname{Spec}\mathbb{Z}$. Let

$$X = \operatorname{Spec}\left(\frac{\mathbb{Z}[x,y]}{(y^2 - x^3 + 49)}\right)$$

Reducing modulo 7 we obtain the equation $y^2 = x^3$ over $\mathbb{F}_7$ which is not smooth at (0,0). Indeed, this corresponds to the ideal $\mathfrak{m} = (x, y, 7)$. All terms occurring in the equation $y^2 = x^3$ belong to $\mathfrak{m}^2$, so this equation gives no condition. Hence, none of $7, x, y$ can be generated by the others $\mod \mathfrak{m}^2$. Therefore $\dim_{\mathbb{F}_7}(\mathfrak{m}/\mathfrak{m}^2) = 3 > 2$ so the scheme is not regular at $\mathfrak{m}$.

Let us blow up X at this point. Take coordinates $(x, y, 7 \mid u : v : w)$. So we have the system of equations

$$\begin{cases} y^2 = x^3 - 7^2; \\ 7u = xw; \\ 7v = yw; \\ uy = xv. \end{cases}$$

Now let us check regularity of the blow-up for each affine chart.

- $u = 1$. Let X_1 be the affine patch given by this equation. We have

$$\begin{cases} y^2 = x^3 - 7^2; \\ y = xv; \\ 7 = xw; \\ 7v = yw. \end{cases}$$

  Notice first that the second and the third equation make the last equation mute. Therefore, our system becomes:

$$\begin{cases} x^2v^2 - x^3 + x^2w^2 = x^2(v^2 - x + w^2) = 0; \\ 7 - xw = 0. \end{cases}$$

  The first equation gives either $x^2 = 0$ that gives the exceptional component, either $v^2 - x + w^2 = 0$. We can use Jacobian criterion:

$$J(x, v, w) = \begin{pmatrix} -1 & 2v & 2w \\ -w & 0 & -x \end{pmatrix}.$$

  Now X_1 is smooth *if and only if* J has rank 2 at all points of X_1. Assume the rank drops at some point $(x, v, w) \in X_1$. Then the determinant of all the 2×2 minors must vanish, as well as the equations defining X_1:

$$\begin{cases} v^2 - x + w^2 = 0; \\ 7 - xw = 0; \\ 2vw = 0; \\ -x - 2w^2 = 0; \\ -2vx = 0. \end{cases}$$

  The last equation gives either $v = 0$ or $x = 0$.

  - Let $v = 0$. Then the first equation becomes $x = w^2$. This one, together with the fourth equation, gives $x = w = 0$ which, together with the second equation, gives $7 = 0$.

  - Let $x = 0$. This already contradicts the second equation. Then the fourth equation gives $w = 0$ and plugging these in the other equations we obtain $v = 7 = 0$.

We see that the closed point corresponding to the ideal $\mathfrak{p} = (x, v, w, 7)$ is not smooth. We need to check whether it is regular. The residue field at this ideal is $\mathbb{F}_7$ so the point is regular *if and only if* $\dim_{\mathbb{F}_7}(\mathfrak{p}/\mathfrak{p}^2) = 2$. So we need to check whether $\mathfrak{p}$ can be generated by two elements modulo $\mathfrak{p}^2$. Recall that X_1 is defined by the system

$$\begin{cases} x^2(v^2 - x + w^2) = 0; \\ 7 - xw = 0. \end{cases}$$

and $x^2 = 0$ gives the exceptional component. Then the first equation tells us that $x = v^2 + w^2 \in \mathfrak{p}^2$. Then from the second equation we see that also $7 \in \mathfrak{p}^2$. This means that $\mathfrak{p} \equiv (v, w) \pmod{\mathfrak{p}^2}$ so $\dim_{\mathbb{F}_7}(\mathfrak{p}/\mathfrak{p}^2) = 2$. Therefore X_1 is regular at $\mathfrak{p}$ and hence regular.

- $v = 1$. We have

$$\begin{cases} y^2 = x^3 - 7^2; \\ 7 = yw; \\ uy = x; \\ 7u = xw. \end{cases}$$

Again, using the second and third equations we see that the last one becomes mute and we have:

$$\begin{cases} y^2(1 - yu^3 + w^2) = 0; \\ 7 = yw. \end{cases}$$

The first equation is satisfied by $y = 0$ that is the exceptional component, and by $1 - yu^3 + w^2 = 0$. Let us apply again the Jacobian criterion:

$$J(y,u,w) = \begin{pmatrix} -u^3 & -3u^2y & 2w \\ w & 0 & y \end{pmatrix}.$$

The 2×2 minors of this matrix are

$$-3u^2wy; \quad u^3y + 2w^2; \quad 13u^2y^2.$$

The third equation gives either $u = 0$ or $y = 0$, both of which, substituted in the second equation, give $w = 0$. If we substitute this in the equation $1 - yu^3 + w^2 = 0$ we get $1 = 0$: a contradiction. We conclude that X_2 is smooth over the regular base $\operatorname{Spec}\mathbb{Z}$ and hence regular.

- $w = 1$. We have

$$\begin{cases} y^2 = x^3 - 7^2; \\ 7u = x; \\ 7v = y; \\ uy = xv. \end{cases}$$

  If we use the second and third equations to replace x and y in the forth, we obtain a mute equation $7uv = 7uv$. The first one becomes $7^2(v^2 - 7u^2 - 1) = 0$. The Jacobian is then $(-2u, 2v)$, which only has rank zero for $u = v = 0$. But this is not a solution of $v^2 - 7u^2 - 1 = 0$, therefore $X_3 \to \operatorname{Spec}\mathbb{Z}$ is smooth and as the base is regular, then X_3 is regular.

So the scheme $\tilde{X}$ obtained by blowing-up X at $\mathfrak{m}$ is a regular model of C over $\mathbb{Z}$.

Example 4.2. In this example we consider the projective version of the example given above. Let

$$C = \operatorname{Proj}\left(\frac{\mathbb{Q}[x,y,z]}{(y^2z - x^3 + 49z^3)}\right)$$

To construct a regular model of C over $\mathbb{Z}$ let

$$Y = \operatorname{Proj}\left(\frac{\mathbb{Z}[x,y,z]}{(y^2z - x^3 + 49z^3)}\right)$$

This is a projective scheme over $\mathbb{Z}$ that can be covered by three affine schemes Y_1, Y_2, Y_3. The first is just the previous example. The other two are smooth and hence regular:

- $Y_2 = \operatorname{Spec}\left(\frac{\mathbb{Z}[x,z]}{(z-x^3-49z^3)}\right)$. Differentiating we obtain the Jacobian $J(x,z) = (-3x^2, 1-3\cdot 49z^2)$ Then we try to solve the system

$$\begin{cases} -3x^2 = 0; \\ \\ 1-3\cdot 49z^2 = 0; \\ \\ z - x^3 - 49z^3 = z(1-49z^2) - x^3 = 0 \end{cases}$$

  but the three equations are incompatible. Indeed, the first one gives $x = 0$ or $3 = 0$. For $3 = 0$ the second equation becomes $1 = 0$, a contradiction. For $x = 0$ the third equation gives $z = 0$ or $49z^2 = 1$ and both are incompatible with the second equation. Then $Y_2 \to \operatorname{Spec}\mathbb{Z}$ is smooth and so Y_2 is regular.

- $Y_3 = \operatorname{Spec}\left(\frac{\mathbb{Z}[y,z]}{(y^2z-1-49z^3)}\right)$. The Jacobian is $J(y,z) = (2yz, y^2 - 3\cdot 49z^2)$. Then we have the system

$$\begin{cases} 2yz = 0; \\ \\ y^2 - 3\cdot 49z^2 = 0; \\ \\ y^2z - 1 - 49z^3 = 0. \end{cases}$$

  The first equation gives the following three cases.

  - $2 = 0$. The second equation becomes $y^2 - z^2 = 0$ that gives $y = \pm z$. If we plug this in the third equation we obtain $z^3 - 1 - z^3 = 0$ so $1 = 0$ which is a contradiction.
  - $y = 0$. The second equation gives $z = 0$ and then the third becomes $1 = 0$. Again a contradiction.

- $z = 0$. The second equation gives $y = 0$ and again, the third equation gives the contradiction $1 = 0$.

So we have an incompatible system, therefore $Y_3 \to \operatorname{Spec} \mathbb{Z}$ is smooth and hence Y_3 is regular.

So, to find a regular model of C over $\mathbb{Z}$ we just need to blow-up the first affine chart as we did in the previous example.

Bibliography

[AW71] M. Artin and G. Winters. Degenerate fibres and stable reduction of curves. *Topology*, 10:373–383, 1971.

[DM69] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Inst. Hautes Études Sci. Publ. Math.*, (36):75–109, 1969.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[GLS10] G.-M. Greuel, S. Laplagne, and F. Seelisch. Normalization of rings. *J. Symbolic Comput.*, 45(9):887–901, 2010.

[GTZ88] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2-3):149–167, 1988. Computational aspects of commutative algebra.

[Liu02] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[PR01] S. Pauli and X.-F. Roblot. On the computation of all extensions of a p-adic field of a given degree. *Math. Comp*, 70:1641–1659, 2001.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sma97] N. P. Smart. S-unit equations, binary forms and curves of genus 2. *Proc. London Math. Soc. (3)*, 75(2):271–307, 1997.

[Sta] The Stacks Project Authors. Stacks project. `http://stacks.math.columbia.edu`.