Néron Models of Elliptic Curves.

Marco Streng

5th April 2007

These notes are meant as an introduction and a collection of references to Néron models of elliptic curves. We use Liu [Liu02] and Silverman [Sil94] as main references and many results and definitions are simply quoted from these books. For the prerequisites, we refer to Silverman [Sil86], Hartshorne [Har77] and the notes of Peter Bruin's talk [Bru07].

Contents

1 Néron Models

Let B be a Dedekind ring of dimension 1 with field of fractions K. Let X be a smooth and separated K-scheme of finite type. A *Néron model* of X is an B-scheme $\mathcal{N}$ which is smooth, separated and of finite type, which has generic fiber isomorphic to X and which satisfies the following universal property: For every smooth B-scheme Y, the natural map

$$\mathcal{N}(Y) \to X(Y_K)$$

is a bijection.

A Néron model does not always exist, but if it does, then the universal property implies that it is unique. These notes focus on the case where X is an elliptic curve. In that case, it has a Néron model (Theorem 3.2 and Theorem 3.3).

The most important special case of the universal property is obtained when we take $Y = \mathrm{Spec}(B)$. Then we get

$$\mathcal{N}(B) = X(K). \tag{1.1}$$

Another nice special case is when we take for Y a Néron model $\mathcal{N}'$ of X'. Then we get

$$\mathrm{Hom}_B(\mathcal{N}', \mathcal{N}) = \mathrm{Hom}_K(X', X). \tag{1.2}$$

It is easy to check using the universal property that if X is an abelian variety, then we may restrict to homomorphisms (i.e. morphisms respecting the group law) on both sides of (1.2).

2 Weierstrass models

In this section, we will consider Weierstrass equations and see what can and cannot be achieved with them over discrete valuation rings. We will relate them to Néron models later (Proposition 3.4).

Let R be a discrete valuation ring with uniformizer t, maximal ideal $\mathfrak{m} = tR$, field of fractions K and residue field $k = R/\mathfrak{m}$.

By the Riemann-Roch Theorem, we know that E is a plane projective curve, given by a *Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

A linear change of coordinates $x' = u^2x, y' = u^3y$ changes the coefficients a_i into a_iu^i, hence we can demand that the Weierstrass equation is *integral*, i.e. has coefficients $a_i \in R$.

The first kind of model for E over R that we will be looking at is the *Weierstrass model*:

Definition. Suppose that we are given an integral Weierstrass equation of E. We call the closed subscheme of $\mathbb{P}^2_R$ that it defines a *Weierstrass model* of E over R.

We will start with the following hopeful result:

Proposition 2.2. Let $\mathcal{W}$ be a Weierstrass model of E over R. If $\mathcal{W}$ is smooth as an R-scheme, then it is a Néron model for E.

Proof. This is [Sil94, IV 6.3]. See also [BLR90, 1.2.8] or [Art86, 1.4] in combination with [Sil94, IV.3.1.4]. □

This result should be motivation enough to look into Weierstrass models a bit more. First of all, the generic fiber of a Weierstrass model $\mathcal{W}$ is isomorphic to E, since it is the curve over K given by the Weierstrass equation.

Next, every K-valued point of E specializes to an R-valued point on $\mathcal{W}$, i.e.

$$\mathcal{W}(R) = E(K),$$

which is a desireable property, see (1.1). Actually, this is an elementary property of projective schemes over discrete valuation rings: Any point in $\mathbb{P}^n(K)$ can be written in homogeneous coordinates. We scale the coordinates in such a way that they are in R and at least one coordinate is in R^*. Then these are the coordinates of a point in $\mathbb{P}^n(R)$ which is in $\mathcal{W}(R)$ if and only if the original point is in $E(K)$.

Now let's look at the special fiber of a Weierstrass model. The special fiber $\mathcal{W}_k$ is a plane projective curve over k, given by a Weierstrass equation with coefficients ($a_i \bmod tR$). We know what such a curve looks like: it can be an elliptic curve, or a cubic curve with one singularity. We can distinguish between these possibilities using the *discriminant* of the Weierstrass equation.

The *discriminant* is an invariant of the Weierstrass equation, defined for example in [Sil86, III §1]. It is given by a polynomial in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. For example, if f is a monic polynomial of degree 3, then the discriminant of the Weierstrass equation

$$y^2 = f(x)$$

is $16\Delta(f)$.

Lemma 2.3. *Let F be a field and C/F a projective curve given by a Weierstrass equation. Then C is smooth if and only if the discriminant is non-zero. If the discriminant is zero, then C is smooth outside a single point where C is not smooth.*

Proof. By [Sil86, III.1.4], the discriminant characterizes regularity. The curve is regular (also after algebraic closure) if and only if the discriminant is non-zero. There is at most one non-regular point. □

In particular, the special fiber of a Weierstrass model is smooth if and only if the discriminant is in R^*.

Of all integral Weierstrass equations of an elliptic curve E over K, it therefore makes sense to pick one such that the valuation of the discriminant $v(\Delta)$ is minimal. We call such an equation a *minimal Weierstrass equation*, its discriminant modulo R^* the *minimal discriminant* and the resulting Weierstrass model a *minimal Weierstrass model.*

Lemma 2.4. *The minimal Weierstrass model of K over R is unique (up to isomorphism).*

Proof. We know what an isomorphism of Weierstrass curves over K looks like and what it does with the discriminant ([Sil86, III.3.1 and Table III.1.2]) It is then not hard to prove that an isomorphism over K between integral Weierstrass equations with discriminants of equal valuation induces an isomorphism over R. For the details, see [Sil86, Proposition VII.1.3(a)]. Alternatively, there is a proof of this statement in [Liu02, Theorem 9.4.35(d)]. □

From now on, let $\mathcal{W}$ denote the minimal Weierstrass model and let $\mathcal{W}^0$ be its smooth locus. Following [Sil86, VII], we call the special fiber $\widetilde{E} = \mathcal{W}_k$ of the minimal Weierstrass model the *reduction of E modulo* $\mathfrak{m}$ and we say that E has *good reduction* if $\widetilde{E}$ is smooth, i.e. if $\Delta \in R^*$. By [Sil86, III.1], there are two classes for the curve $\widetilde{E}$ if it is not smooth: it can have a cusp, in which case the smooth part $\widetilde{E}_{\mathrm{ns}}$ birational to the additive group $\mathbb{G}_{\mathrm{a}}$ and we say that E has *additive reduction*; or it can have a node, in which case $\widetilde{E}_{\mathrm{ns}}$ is (possibly after a quadratic extension) birational to the multiplicative group $\mathbb{G}_{\mathrm{m}}$ and we say that E has *multiplicative reduction* (see [Sil86, III.2.5]).

Lemma 2.5. *A Weierstrass model is integral and flat over R.*

Proof. Each affine part of the polynomial that gives the Weierstrass equation is irreducible, hence $\mathcal{W}$ is an integral scheme. By [Liu02, Corollary 3.10], every non-constant morphism from an integral scheme to a Dedekind scheme is flat. □

Lemma 2.6. *If E has good reduction, then $\mathcal{W}^0 = \mathcal{W}$ is the Néron model of E. Otherwise $\mathcal{W} \setminus \mathcal{W}^0$ consists of the unique non-smooth point of $\widetilde{E}$.*

Proof. The Weierstrass model is of finite presentation and by Lemma 2.5 it is also flat. The third and last part of the definition of smoothness is that the fiber $X_{f(x)}$ should be geometrically regular at x for every point $x \in \mathcal{W}$. This is a condition on the fiber only, hence satisfied at all smooth points of the fibers, so Lemma 2.3 says exactly where $\mathcal{W}$ is smooth.

We have already said that a smooth Weierstrass model is a Néron model (Proposition 2.2). □

If E has bad reduction, then we know that $\mathcal{W}$ cannot be the Néron model, because it is not smooth. On the other hand, $\mathcal{W}^0$ may be too small to be a Néron model, as we will see.

2.1 Example

A change of coordinates changes the discriminant of a Weierstrass equation by a 12-th power ([Sil86, III.1.2]), hence if we are given a Weierstrass equation with $v(\Delta) < 12$, then we know that it is minimal.

Let us consider the elliptic curve E over K, given by the Weierstrass equation

$$E : y^2 = x^3 + t^n \tag{2.7}$$

for some non-negative integer n and where $\mathrm{char}(k) \neq 2, 3$. By a change of coordinates $x' = t^2x$, $y' = t^3y$, we can assume $n < 6$. The discriminant is $-2^4 3^3 t^{2n}$. As $\mathrm{char}(k) \neq 2, 3$, we know that the Weierstrass equation is minimal. Let $\mathcal{W}$ be the Weierstrass model given by (2.7). If $n = 0$, then the Weierstrass model is smooth, hence a Néron model, so let us assume $n > 0$. Then $\mathcal{W}$ is smooth everywhere except at the point given by the maximal ideal generated by x, y and t. The local ring there has maximal ideal $\mathfrak{m}$ generated by x, y and t and the square $\mathfrak{m}^2$ of the maximal ideal is generated by $x^2, xy, xt, y^2 = x^3 + t^n, yt$ and t^2. Therefore, $t \in \mathfrak{m}^2$ if and only if $n = 1$, so $\mathcal{W}$ is regular if and only if $n = 1$.

If $n \geq 2$, then the Weierstrass model is not regular any more. Moreover, if for example $n = 2$, then we have an R-valued point $(0 : t : 1)$ on $\mathcal{W}$ which is not on $\mathcal{W}^0$, because it reduces to the singular point $(0:0:1)$ on $\mathcal{W}_k$. This means in particular that $\mathcal{W}^0(R) \neq \mathcal{W}(R) = E(K)$, so $\mathcal{W}^0$ cannot be the Néron model. To see what we have to do to get the Néron model, we will look at the theory of models of curves in a more general setting.

3 Models of curves

Let B be a Dedekind ring of dimension 1 with field of fractions K.

Definition. A *fibered surface over B* is an integral, projective, flat B-scheme $\pi : Y \to \mathrm{Spec}(B)$ of dimension 2.

We say that the fibered surface is *regular* if Y is a regular scheme.

Let C be a normal, connected, projective curve over K.

Definition. A *(projective) model of C over B* is a normal fibered surface $M \to \mathrm{Spec}(B)$ together with an isomorphism $M_K \cong C$. We say that the model is *regular* if M is regular.

This is a very strict definition of model. In fact, Néron models are not always models according to this definition, because they are not always projective (we will remove points from projective models in order to construct the Néron model). Weierstrass models however are models, although not always regular.

Lemma 3.1. *Let E/K be an elliptic curve over the field of fractions of a discrete valuation ring R such that $2 \in R^*$ and let $\mathcal{W}$ be a Weierstrass model of E. Then $\mathcal{W}$ is a model of E over R.*

Probably we do not need $2 \in R^*$ here, but it makes the proof a lot easier.

Proof. By Lemma 2.5 and the fact that $\mathcal{W}$ is defined as a closed subscheme of the projective plane, all properties of models are satisfied except possibly that $\mathcal{W}$ is normal. We know that $\mathcal{W}$ is regular at all points except possibly one point, hence it is normal outside that point ([Liu02, 4.2.16]) .

We will prove that $\mathcal{W}$ is normal in that point under the assumption $2 \in R^*$. First, we do a change of variables such that $y^2 = f(x)$, where f is a monic polynomial of degree 3 in x with coefficients in R. Then we will follow [Liu02, Example 4.1.9] to show that the ring $A = R[x, y]$ is integrally closed in its field of fractions. That suffices, because then every localization is normal as well ([Liu02, 4.1.4]).

Let $A = R[x, y]$. Then $\mathrm{Frac}(A) = K(x)[y]$. Suppose that $g = g_1 + g_2 y$ is integral over A for $g_1, g_2 \in K(x)$. By the automorphism $x \mapsto x, y \mapsto -y$ of $\mathrm{Frac}(A)$ over $K(x)$, we find that $g_1 - g_2 y$ is also integral, hence so are $2g_1$ and $(2g_2 y)^2 = 4g_2^2 f(x)$. Since A is integral over $R[x]$, this implies that $2g_1$ and $4g_2^2 f(x)$ are integral over $R[x]$, hence are in fact inside $R[x]$. As f has no double roots and $R[x]$ is factorial, this implies that $2g_1$ and $2g_2$ are in $R[x]$. Since 2 is invertible, we have $g_1, g_2 \in R[x]$, hence $g = g_1 + g_2 y \in A$. $\square$

Definition. Let X and Y be integral schemes over a scheme S with $Y \to S$ separated. A *rational map f from X to Y*, denoted $f : X \dashrightarrow Y$ is an equivalence class of morphisms of S-schemes from a non-empty open subscheme X to Y. We call two such morphisms $U \to Y$ and $V \to Y$ equivalent if they coincide on $U \cap V$.

In every equivalence class, there exists an element $f : U \to Y$ such that for every element $g : V \to Y$ of the equivalence class, we have $V \subset U$ and $g = f_{|V}$.[Liu02, exercise 3.3.13] We call U the *domain of definition* of the rational map and identify the rational map with f. We say that a rational map $f : X \dashrightarrow Y$ *is a morphism* or is *defined everywhere* if its domain of definition is equal to X.

If X, Y, Z are integral schemes over S, Y and Z are separated over S and $f : X \dashrightarrow Y$, $g : Y \dashrightarrow Z$ are rational maps, then we can compose f and g as follows: Let $f_0 : U \to Y$ and $g_0 : V \to Z$ be representatives. Then $g \circ f$ is the equivalence class of $g_0 \circ f_{0|f_0^{-1}(V)} : f_0^{-1}(V) \to Z$. This is a well-defined composition map. A *birational* map is a rational map $f : Y \dashrightarrow Z$ with a rational inverse g (i.e. s.t. $f \circ g$ and $g \circ f$ are equivalent to the identity morphisms of Z and Y). In other words, a birational map $f : Y \dashrightarrow Z$ is the equivalence class of an isomorphism from a non-empty open subset of Y to an open subset of Z. A *birational morphism* is a morphism which is a birational map.

If X and Y are models of the same curve C over a discrete valuation ring, then the identification of the generic fibers gives a birational map between X and Y.

More generally, suppose that X and Y are models of the same curve C over a Dedekind domain B. Let $f : X_K \to Y_K$ be the identification of the generic fibers. We embed X resp. Y in a projective space $\mathbb{P}^m_B$ resp. $\mathbb{P}^n_B$. There is a tuple $\phi = (f_1 : \cdots : f_n)$, where the f_j are homogeneous polynomials of the same degree in m variables as follows: Let V be the locus of $\mathbb{P}^m_K$ where the f_j vanish simultaneously. Then V does not contain X and f is given on $X \setminus V$ by ϕ. By multiplication by an element of B, we eliminate the denominators from the coefficients of f_j. Let Z be the locus in $\mathbb{P}^m_B$ where the f_j vanish simultaneously. Then Z is closed and ϕ defines a morphism $\mathbb{P}^m_B \setminus Z \to \mathbb{P}^n_B$. Now we want two things: 1) The morphism factors through Y and 2) Its class as a birational map $X \to Y$ does not depend on the choices that were made. Is this true? If so, then we call this the natural morphism from X to Y that is induced by the identification of the special fibers. See also [Liu02, Exercises 3.2.6, 3.3.13 and 3.3.14]

Definition. A *minimal regular model of C over B* is a regular model $\mathcal{E}$ over B such that for every regular model Y over B, the natural birational map $f : Y \dashrightarrow \mathcal{E}$ is a morphism.

We now get to the main theorems:

Theorem 3.2. *Let B be a Dedekind ring of dimension* 1*, with field of fractions K. Let C be a smooth geometically connected projective curve of genus $g \geq 1$ over K. Then there is a unique minimal regular model $\mathcal{C}_{\min}$ of C over B.*

Proof. Uniqueness follows from the definition, so we only have to prove existence of a minimal regular model. We start with the existence of a model. If C is an elliptic curve, then we can take a Weierstrass model. In general, following [Liu02, 10.1.8], we take $\mathcal{C}_0$ as in [Liu02, 10.1.4] and then we take the normalization of the Zariski closure of C in $\mathcal{C}_0$ is a model.

We will show in Proposition 4.17 that we can make a model regular using a technique called *blowing-up*. Finally, we show in Proposition 4.22 that we can make a regular model minimal using a technique called *contraction*.

See also [Liu02, 10.1.8]. □

Theorem 3.3. *Let B be a Dedekind ring of dimension 1 with field of fractions K. Let E be an elliptic curve over K with minimal regular model $\mathcal{E}$ over B. Then the open subscheme $\mathcal{N}$ of smooth points of $\mathcal{E}$ is the Néron model of E over B.*

Proof. See [Liu02, 10.2.14]. □

Let $\mathcal{N}$ be a Néron model of an elliptic curve E over a discrete valuation ring R with residue field k. Kodaira and Néron give a classification of the special fibers $\mathcal{N}$ in the case where k is algebraically closed. See Table 15.1 in Appendix C of [Sil86] or Table 4.1 in Chapter IV of [Sil94]. For genus 2 curves, the analogous classification of special fibers of Néron models has approximately 120 types ([Liu02, 10.2.6] or [Sil94, IV.8.2.4], compared to 10 in the elliptic case). Tate's algorithm [Sil94, IV.9.4] gives the same classification (without demanding $k = \overline{k}$) by asking questions about divisibility of coefficients and decompositions of certain polynomials in the residue field k. Behind the scenes, it performs a series of blowing-ups.

The special fiber of $\mathcal{N}$ may consist of multiple components. One of them contains the closed point of the identity section. The scheme obtained from $\mathcal{N}$ by removing all non-identity components of the special fiber is called the *identity component of the Néron model* and denoted $\mathcal{N}^0$. This name is a bit strange, because $\mathcal{N}$ is connected: the special fiber is connected and dense in $\mathcal{N}$. Let $\mathcal{W}^0$ be the smooth part of the minimal Weierstrass model. By the universal property of the Néron model, the inclusion of $\mathcal{W}^0_K$ into E induces a map from $\mathcal{W}^0$ to $\mathcal{N}$.

Proposition 3.4. The natural map $\mathcal{W}^0 \to \mathcal{N}$ induces an isomorphism $\mathcal{W}^0 \cong \mathcal{N}^0$.

Proof. [Sil94, Corollary IV.9.1]. □

Let $\mathcal{N}^1(R) = \mathcal{W}^1(R) \subset \mathcal{N}^0(R) = \mathcal{W}^0(R)$ be the set of points that restrict to the unit point of the special fiber. The subgroup $E_0(K)$ (resp. $E_1(K)$) of $E(K)$ is defined in [Sil86] as the subgroup of $E(K)$ that correspond to $\mathcal{W}^0(R)$ (resp. $\mathcal{W}^1(R)$) through the natural isomorphism $\mathcal{W}(R) \cong E(K)$. Let $\widetilde{E}_{\mathrm{ns}}(k)$ be the set of non-singular points of $\widetilde{E}(k)$. We get an exact sequence

$$0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{\mathrm{ns}}(k),$$

where the rightmost map is surjective if K is complete ([Sil86, VII.2.1]). We know that $\widetilde{E}_{\mathrm{ns}}(k)$ is an elliptic curve or k^+ or a torus, so we can study this with the smaller field k and we can study $E_1(K)$ using formal groups ([Sil86, IV and VII]). The Néron model gives information about $E(K)/E_0(K) = \mathcal{N}(R)/\mathcal{N}^0(R)$ ([Sil94, Table 4.1 on page 365]): It is a finite abelian group. More precisely, if E has multiplicative reduction, then $E(K)/E_0(K)$ is a cyclic group of order $-v(j(E))$ (for j, see [Sil86, III]); otherwise, $E(K)/E_0(K)$ has order $1, 2, 3$ or 4.

A nice corollary of the theory of Néron models is the following.

Lemma 3.5. *Homomorphisms of elliptic curves induce homomorphisms of the smooth parts of the reduced curves.*

Proof. By the universal property (1.2), a morphism of elliptic curves induces a morphism of Néron models. The identity component gets mapped to the idenity component by continuity and the assumption that the zero section goes to the zero section. Consequently, we get a homomorphism of smooth parts of minimal Weierstrass models. If we base-change to k, then we get a homomorphism of the smooth parts of the reduced curves. □

4 Construction of a Néron model

We need to perform two procedures in order to actually find the minimal regular model starting from any model. The first is blowing up, which makes a model regular. The second is contraction, which makes a regular model minimal.

4.1 Blowing up

Blowing up at a point of a scheme is a way of removing singularities from a scheme.

We will start with the definition of the *blowing-up of a Noetherian affine scheme* $\mathrm{Spec}(A)$ *along a closed subscheme* $V(I)$ as in [Liu02, 8.1.1]. So let A be a Noetherian ring and I an ideal of A. Let us consider the graded A-algebra

$$\widetilde{A} = \bigoplus_{d \geq 0} I^d,$$

where of course $I^0 = A$.

Definition. Let $X = \mathrm{Spec}(A)$ be an affine Noetherian scheme and I an ideal of A. We let $\widetilde{X} = \mathrm{Proj}(\widetilde{A})$ and call the canonical morphism $\pi : \widetilde{X} \to X$ the *blowing-up of* X *along* $V(I)$.

So what does this look like? Let $f_1, \ldots, f_n$ be a system of generators of I. Let $t_i \in I = \widetilde{A}_1$ denote the element f_i considered as a homogeneous element of degree 1, which is not to be confused with the element f_i itself, which is in $I \subset A = A_0$, i.e. of degree 0. Then we have a surjective homomorphism of graded A-algebras

$$\begin{aligned} \phi : A[T_1, \ldots, T_n] &\to \widetilde{A} \\ T_i &\mapsto t_i. \end{aligned}$$

This implies that $\widetilde{X}$ is isomorphic to a closed subscheme of $\mathbb{P}_A^{n-1}$ ([Liu02, 8.1.1 and 2.3.41]).

Lemma 4.1. *If $P(T) \in A[T_1, \ldots, T_n]$ is a homogeneous polynomial, then $P(T)$ is in the kernel of ϕ if and only if $P(f_1, \ldots, f_n) = 0$.*

Proof. Let m be the degree of P. Then $P(f_1, \ldots, f_n)$ is an element of I^m. If we identify I^n with $\widetilde{A}_n$, then $P(f_1, \ldots, f_n)$ corresponds to $P(t_1, \ldots, t_n)$, which is the image of $P(T)$ under ϕ. □

In particular, the kernel of ϕ contains at least the ideal $J \subset A[T_1, \ldots, T_n]$ generated by the elements $f_i T_j - f_j T_i$.

Example 4.2. Let F be a field and $A = F[x_1, \ldots, x_n]$. We will blow up $\mathrm{Spec}(A) = \mathbb{A}_F^n$ in the point $x_1 = \cdots = x_n = 0$. In this case, $\ker\phi = J$ ([Liu02, 8.1.2]), so $\widetilde{X}$ is the subscheme of $\mathbb{P}_A^{n-1} = \mathbb{A}_F^n \times_F \mathbb{P}_F^{n-1}$ given by J. In any local ring in the subscheme "$x_i \neq 0$" of $\widetilde{X}$, we have $T_j = x_j T_i x_i^{-1}$, hence the natural morphism $\widetilde{X}_{(x_i)} \to X_{(x_i)}$ is an isomorphism (on local rings, hence on the subscheme). The fiber of the point 0 is a projective $(n-1)$-dimensional space, since there are no relations there except $x_i = 0$.

So blowing up in a point of $\mathbb{A}_F^n$ leaves the scheme invariant except for the point in which we blow up, which gets replaced by a $\mathbb{P}_F^{n-1}$.

Usually, J is not equal to $\ker(\phi)$. The following lemma allows us to compute the blowing-up. Another way of computing the blowing-up is presented below Proposition 4.13.

Lemma 4.3. *The blowing-up $\widetilde{X}$ is the union of the affine open subschemes* $\mathrm{Spec}A_i, 1 \leq i \leq n$*, where A_i is the sub-A-algebra of A_{f_i} generated by the $f_j f_i^{-1} \in A_{f_i}, 1 \leq j \leq n$.*

In particular, if A is integral, then A_i is the sub-A-algebra of $\mathrm{Frac}(A)$ *generated by the $f_j f_i^{-1}$.*

Proof. The scheme $\widetilde{X}$ is covered by the affine schemes $D_+(t_i) = \mathrm{Spec}(\widetilde{A}_{(t_i)})$, where $\widetilde{A}_{(t_i)}$ is the subring of $\widetilde{A}_{t_i}$ made up o the elements of degree 0, i.e. the elements of the form at_i^{-N}, where $a \in \widetilde{A}$ has degree N.

The ring $A_{(t_i)}$ is computed in [Liu02, 8.1.2(e)]. Another proof of the special case where A is integral is [Liu02, 8.1.4]. □

Example 4.4. Now let's take another example: The curve $X : y^2 = x^3$ in the affine plane over F. It has a cusp in the origin, so that is where we blow up. We have $X = \mathrm{Spec}(A)$, where $A = F[X, Y]/(Y^2 - X^3) = F[x, y]$ and we blow up in the point $I = xA + yA$.

The blowing-up is covered by two affine charts with coordinate rings $A_1 = F[x/y, y]$ and $A_2 = F[y/x, x]$ (as subrings of $\mathrm{Frac}(A) = F(x)[y]$, where $y^2 = x^3$). In the first ring, we have the relation $(x/y)^3 y = 1$, so $(x/y) \neq 0$, hence we have $\widetilde{X} = \mathrm{Spec}(A_2)$. Let $t = y/x$. Then we have the relation $t^2 = x$, hence $A_2 = F[t]$ and $\widetilde{X} = \mathbb{A}_F^1$ is simply the normalization of X.

If X is not affine, but only locally Noetherian and Z is a closed subscheme of X, then we give the following definition of the *blowing-up of X along Z*:

Proposition 4.5. There is a unique morphism $\pi : \widetilde{X} \to X$ such that for every affine open subscheme $U \subset X$, we have an isomorphism $\pi^{-1}(U) \cong \widetilde{U}$, where $\widetilde{U}$ is the blowing-up of U along $Z \cap U$ and the isomorphisms are compatible with restriction.

Proof. This morphism is given in [Liu02, 8.1.11 and 8.1.8] or alternatively [Har77, II.7]. □

The following proposition makes precise and general what we have seen in Example 4.2.

Proposition 4.6. Let $\pi : \widetilde{X} \to X$ be the blowing-up of a locally Noetherian scheme X along a closed subscheme Z.

1. The morphism π induces an isomorphism $\pi^{-1}(X \setminus Z) \to X \setminus Z$.
2. If X is integral and $Z \neq X$, then $\widetilde{X}$ is integral.
3. If X is regular and Z is a regular closed subscheme, then $\widetilde{X}$ is regular and for every $x \in Z$, the fiber $\widetilde{X}_x$ is isomorphic to $\mathbb{P}^{r-1}_{k(x)}$, where $r = \dim_x X - \dim_x Y$.

Proof. Parts (1) and (2) are in [Liu02, 8.1.12(d)]. Alternatively, (1) is [Har77, II.7.13(b)] and (2) follows immediately from Lemma 4.3. Part (3) is [Liu02, 8.1.19(a) and (b)]. □

Some statements are better phrased in terms of quasi-coherent sheafs of ideals. By [Har77, II.5.9], quasi-coherent sheafs of ideals correspond bijectively to closed subschemes. We will need the definition of the *inverse image sheaf*. We quote it here from [Har77].

Definition. Let $f : Y \to X$ be a morphism of schemes, and let $\mathcal{I} \subset \mathcal{O}_X$ be a sheaf of ideals on X. We define the *inverse image sheaf* $f^{-1}\mathcal{I} \cdot \mathcal{O}_Y \subset \mathcal{O}_Y$ (also denoted $\mathcal{I}\mathcal{O}_Y$) as follows. First consider f as a continuous map of topological spaces $Y \to X$ and let $f^{-1}\mathcal{I}$ be the inverse image of the sheaf $\mathcal{I}$. Then $f^{-1}\mathcal{I}$ is a sheaf of ideals in the sheaf of rings $f^{-1}\mathcal{O}_X$ on the topological space Y. Now there is a natural homomorphism of sheaves of rings on Y, $f^{-1}\mathcal{O}_X \to \mathcal{O}_Y$, so we define $f^{-1}\mathcal{I} \cdot \mathcal{O}_Y$ to be the ideal sheaf in $\mathcal{O}_Y$, generated by the image of $f^{-1}\mathcal{I}$.

Proposition 4.7. Let $\pi : \widetilde{X} \to X$ be the blowing-up of a locally Noetherian scheme X along a closed subscheme $V(\mathcal{I})$.

1. The morphism π is an isomorphism if and only if $\mathcal{I}$ is an invertible sheaf on X.
2. The sheaf $\pi^{-1}\mathcal{I} \cdot \mathcal{O}_{\widetilde{X}}$ is invertible on $\widetilde{X}$.

Proof. Recall that a sheaf of $\mathcal{O}_X$-modules is called *invertible* if it is locally free of rank 1. Both assertions are in [Liu02, 8.1.12]. However, since this is an important property that characterizes the blowing-up, we will give a complete proof in the case X integral.

Part (2) is also [Har77, II.7.13(a)]. Cover X by affine open subschemes. If $U = \mathrm{Spec}(A)$ is such an affine open and $I = (f_1, \ldots, f_n) = \mathcal{I}(U)$ with $f_i \neq 0$, then Lemma 4.3 gives a covering of its pre-image. We only have to show that the ideal $J \subset A_i$ generated by the image of I is free of rank one. The ideal J is generated by $f_1, \ldots, f_n$ and we have that $f_j f_i^{-1} \in A_i$, hence J is generated by f_i. If f_i is not a zero divisor, then J is free of rank 1. This proves that $\mathcal{I}\mathcal{O}_{\widetilde{X}}$ is locally free of rank 1 if X is integral.

Part (1): Suppose that $\mathcal{I}$ is invertible. Then X is covered by affine open subsets of the form $\mathrm{Spec}(A)$ on which $\mathcal{I}$ is free on one generator f. Then the morphism $\phi : A[T] \to \widetilde{A}$ is an isomorphism, hence π is an isomorphism between $\mathrm{Proj}(\widetilde{A})$ and $\mathrm{Spec}(A)$. This proves that π is an isomorphism $\widetilde{X} \to X$. The converse follows from (2). □

Example 4.8. Every non-zero sheaf of ideals on the projective line $\mathbb{P}^1_F$ over a field F is invertible, hence the blowing-up $\widetilde{X}$ of $X = \mathbb{P}^1_F$ along a closed subscheme $Z \neq X$ is equal to X.

Proposition 4.9. *Let $f : Y \to X$ be a morphism of noetherian schemes, and let $\mathcal{I}$ be quasi-coherent sheaf of ideals of X. Let $\widetilde{X}$ be the blowing-up of X along $V(\mathcal{I})$, and let $\widetilde{Y}$ be the blowing-up of Y along $V(f^{-1}\mathcal{I} \cdot \mathcal{O}_Y)$. Then there is a unique morphism $\widetilde{f} : \widetilde{Y} \to \widetilde{X}$ making the following diagram commute:*

$$\begin{array}{ccc} \widetilde{Y} & \xrightarrow{\widetilde{f}} & \widetilde{X} \\ \downarrow & & \downarrow \\ Y & \xrightarrow[f]{} & X. \end{array} \tag{4.10}$$

Moreover, if f is a closed immersion and the image of f is not contained in $V(\mathcal{I})$, then $\widetilde{f}$ is a closed immersion.

Proof. [Har77, II.7.15] or [Liu02, 8.1.15 and 8.1.17]. □

The following two statements show that blowing up is a natural thing to do.

Corollary 4.11 (Universal property of the blowing-up). *Let $\pi : \widetilde{X} \to X$ be the blowing-up along $V(\mathcal{I})$ of a locally Noetherian scheme. Then the sheaf $(\pi^{-1}\mathcal{I})\mathcal{O}_{\widetilde{X}}$ is invertible. Moreover, for any morphism $f : W \to X$ such that $(f^{-1}\mathcal{I})\mathcal{O}_W$ is an invertible sheaf of ideals on W, there exists a unique morphism $g : W \to \widetilde{X}$ such that $f = \pi \circ g$.*

Proof. This is [Har77, II.7.14] or [Liu02, 8.1.16]. We present it here as a corollary of the above (as does [Liu02]). The first statement is (2) of Proposition 4.7. Now suppose that the sheaf $(f^{-1}\mathcal{I})\mathcal{O}_W$ is invertible. By (1) of Proposition 4.7, we find that $\widetilde{W} = W$ in Proposition 4.9. Therefore, we can take $g = \widetilde{f}$. □

Proposition 4.12. Let $f : Y \to X$ be a projective birational morphism of integral schemes. Suppose that X is quasi-projective over an affine Noetherian scheme. Then f is the blowing-up morphism of X along a closed subscheme.

Proof. [Liu02, 8.1.24]. □

Definition. If f in Proposition 4.9 is a closed immersion and the image is not contained in $V(\mathcal{I})$, then we call the image of $\widetilde{Y}$ in $\widetilde{X}$ the *strict transform* of Y.

Proposition 4.13. As a set, the strict transform of Y is the Zariski closure of $\pi^{-1}(Y \setminus V(\mathcal{I}))$ in $\widetilde{X}$, where π is the map from $\widetilde{X}$ to X.

Proof. This is [Liu02, Exercise 8.1.1]. If F is a field and Y is a closed subvariety of $X = \mathbb{A}^n_F$ passing through the point P and we blow up in P, then this is also [Har77, II.7.14.1]. □

If Y is an integral affine scheme over a scheme S, then we can embed Y into an affine plane $X = \mathbb{A}^n_S$. Let Z be a closed subscheme of Y and suppose we want to compute the blowing-up $\widetilde{Y}$ of Y along Z. Then we can compute the blowing-up of X along Z, which is very easy to compute and then compute the strict transform $\widetilde{Y}$ of Y as follows: Proposition 4.13 computes $\widetilde{Y}$ as a closed subset of $\widetilde{X}$ and it must have the reduced subscheme structure by (2) of Proposition 4.6. Another way to compute $\widetilde{Y}$ is given by Lemma 4.3.

Example 4.14. As an example, let X be the affine plane over F and Y the line in X given by $ay = bx$ with $a, b \in F$ not both zero. We will blow up along the point $(0, 0)$, which is given by the ideal (x, y). We identify Y with an affine line via the parametrization $f : t \mapsto (at, bt)$. Then $Y = \mathrm{Spec}(F[t])$ and $X = \mathrm{Spec}(F[x, y])$ and f is given as a homomorphism of F-algebras by $x \mapsto at, y \mapsto bt$. The inverse image ideal of (x, y) is generated by at and bt, hence by t.

We get that $\widetilde{Y} = \mathbb{A}^1_F$ (it is the subvariety of $\mathbb{A}^1_F \times \mathbb{P}^0_F$ with no relations). Next, $\widetilde{X}$ is a plane with the origin replaced by a projective line. It is given as a subvariety of $\mathbb{A}^2_F \times \mathbb{P}^1_F$ by $xt - ys = 0$ where t, s are the homogeneous coordinates of the projective line. Let J be the ideal that defines the strict transform of Y. The function $ay - bx$ is zero on $\pi^{-1}(Y \setminus 0)$, hence it is inside J. Moreover, the ideal J contains $b(xt - ys) = y(at - bs)$ and $a(xt - ys) = x(at - bs)$. As it is prime and does not contain both x and y (it could contain one, if a or b is zero), we have that $(at - bs)$ is in J. The only point in the projective line $x = y = 0$ that satisfies that equation is $(a : b)$. The line with direction $(a : b)$ therefore goes through the point $(a : b)$ of the projective line. The conclusion: lines on X that go through $(0, 0)$ in different directions do not intersect on $\widetilde{X}$.

We now give the statement of how a regular model is obtained by blowing up. Let B be a Dedekind ring of dimension 1 and $X \to \mathrm{Spec}(B)$ a fibered surface with smooth generic fiber. We define a sequence

$$X = X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow \cdots \tag{4.15}$$

of proper birational morphisms as follows: Let $S_i = X_i \setminus \mathrm{Reg}(X_i)$ be the singular locus of X_i. Claim: S_i is closed. We will prove this below. Give S_i the reduced (closed) subscheme structure and then blow X_i up along S_i. Then we let X_{i+1} be the normalization of the blowing-up.

Proposition 4.16. Consider the sequence (4.15). Each S_i is closed and there is an n such that S_i is empty, i.e. the the sequence ends with a regular scheme $Z = X_n$ with a projective birational morphism $\pi : Z \to X$. Moreover, Z is projective over B and π is an isomorphism above every regular point of X.

Proof. Everything follows from [Liu02, 8.3.50] and the proof of [Liu02, 8.3.51], except projectivity of Z over B. However, Z is projective over X and it is true by assumption that X is projective over B. Using the Segre embedding, one can prove ([Har77, II Exercise 4.9]) that a composition of projective morphisms is projective. □

Proposition 4.17. If X is a model of a regular connected projective curve C, then Z as in the above proposition is a regular model of C.

Proof. The morphism π is an isomorphism above the generic fiber C of X. This gives the isomorphism between the generic fiber of Z and C. Moreover, Z is regular and projective. By construction, Z is also integral ((2) of Proposition 4.6), hence flat [Liu02, 4.3.10]. It is normal because it is regular and irreducible ([Liu02, 4.2.17]). Finally, [Liu02, 8.2.7] says that dimension is invariant under proper birational morphisms of locally Noetherian integral schemes, hence the dimension of Z is 2. □

Example 4.18. The proof of Tate's algorithm [Sil86, IV.9.4] starts with a Weierstrass model and performs various changes of coordinates and blowings-up. With suitable blowings-up, this leads to a series of case distinctions about divisibilities and numbers of zeroes of certain polynomials over k and $\overline{k}$. The result is a diagram of questions and changes of variables ending in the reduction type of the elliptic curve. This diagram is called Tate's algorithm. The proof is a nice way to practice blowing up fibered surfaces.

4.2 Contraction

Let B be a Dedekind ring of dimension 1 with field of fractions K.

Definition. Let $X \to B$ be a regular fibered surface. A prime divisor E on X is called an *exceptional divisor* or *(-1)-curve* if there exist a regular fibered surface $Y \to S$ and a morphism $f : X \to Y$ of B-schemes such that $f(E)$ is reduced to a point, and that

$$f : X \setminus E \to Y \setminus f(E)$$

is an isomorphism.

We call the morphism f the *contraction* of E.

Lemma 4.19. *The contraction f of E is also the blowing-up of Y along the closed point $f(E)$.*

Proof. See [Liu02, 9.3.2 or 9.2.3]. □

We can recognize exceptional divisors with Castelnuovo's criterion.

Proposition 4.20 (Castelnuovo's criterion). Let $X \to S$ be a regular fibered surface. Let $D \subset X_s$ be a prime divisor. Let us set $k' = \mathrm{H}^0(D, \mathcal{O}_D)$. Then D is an exceptional divisor if and only if $D \cong \mathbb{P}^1_{k'}$ and $D^2 = -[k' : k(s)]$.

Proof. This is [Liu02, 9.3.8]. See also [Sil94, IV.7.5] if k is algebraically closed. □

We will not discuss intersection theory here in detail, but refer to [Liu02, 9.1.2]. However, we will say the following: let $X \to \mathrm{Spec}(B)$ be a regular fibered surface and let $s \in \mathrm{Spec}(B)$ be a closed point. Then the intersection pairing on X over s is a bilinear map $i_s : \mathrm{Div}(X) \times \mathrm{Div}_s(X) \to \mathbb{Z}$, which is symmetric on $\mathrm{Div}_s(X) \times \mathrm{Div}_s(X)$ and satisfies $i_s(D', D) = 0$ if D' is a principal divisor. In particular, if D is a divisor in the fiber X_s over a closed point s and we take for D' the fiber X_s, then it follows that $D^2 = -(D' \setminus D)D$. In other words, D^2 is minus the intersection number of D with the other components of the special fiber.

If there are no exceptional divisors to contract, then we have found the minimal regular model:

Lemma 4.21. *Let X be a regular fibered surface over a Dedekind domain B of dimension 1 and with with generic fiber X_K of arithmetic genus $p_a(X_K) \geq 1$. If X does not contain any exceptional fibers, then X is a minimal model of X_K.*

Proof. This is [Liu02, 9.3.24]. See also [Sil94, IV.7.5]. □

We call a regular fibered surface *relatively minimal* if it does not contain any exceptional fibers.

Proposition 4.22. Let X be a regular fibered surface over a Dedekind domain B of dimension 1 and let

$$X \to X_1 \to X_2 \to \cdots \to X_n \to \cdots$$

be a sequence of contractions of exceptional divisors. Then the sequence is finite and ends in a relatively minimal regular fibered surface Y over B, together with a birational morphism $X \to Y$ over B.

If X is a regular model of a smooth projective geometrically connected curve C of genus $g \geq 1$, then Y is the minimal regular model of X.

Proof. Finiteness of the sequence is [Liu02, 9.3.19]. By definition of the contraction, the curves are regular and the morphism $X \to Y$ is birational.

If the generic fiber C of X is a smooth projective geometrically connected curve, then the birational map $X \to Y$ is an isomorphism of generic fibers, hence Y is a regular model of C. It is minimal by Lemma 4.21. □

5 Potential good reduction

We say that E has *potential good (resp. potential multiplicative) reduction* if there is a discrete valuation ring R' that dominates R such that E has good (resp. multiplicative) reduction over R'.

Lemma 5.1. *An elliptic curve E over K has potential good reduction if and only if $j(E) \in R$ and potential multiplicative reduction if and only if $j(E) \notin R$.*

Proof. This is [Liu02, 10.2.33] or [Sil86, VII.5.5]. □

If K is a (localization or non-archimedean completion of) a number field and E/K has complex multiplication, then the j-invariant is an algebraic integer ([Sil94, II §6]) which eliminates the cases with $v(j) < 0$ from the table of Kodaira and Néron ([Sil94, Table 4.1 on page 365]). In particular, elliptic curves over K with complex multiplication have potential good reduction.

Index

References

[Art86] M. Artin. Néron models. In Gary Cornell and Joseph H. Silverman, editors, *Arithmetic Geometry*, 1986.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1990.

[Bru07] Peter Bruin. Differentials, smooth morphisms, étale morphisms. http://www.math.leidenuniv.nl/ pbruin/smooth.ps, 2007.

[Har77] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, 1977.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford Science Publications, 2002.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.