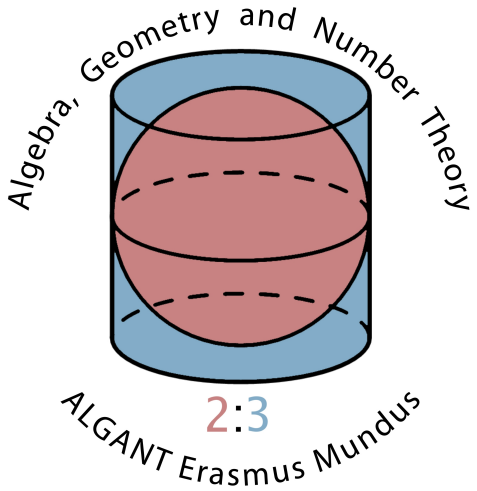

R. van Bommel

Almost all hyperelliptic Jacobians have a bad semi-abelian prime

Master's thesis, 23 June 2014

Supervisor: dr. D. Holmes

Mathematisch Instituut,
Universiteit Leiden

Département de Mathématiques,
Université Paris-Sud

Contents

Introduction

An elliptic curve over $\mathbb{Q}$ has good, bad additive or bad multiplicative reduction at each prime p. Each elliptic curve over $\mathbb{Q}$ has good reduction at almost all prime numbers p. Though there are elliptic curves without a prime of multiplicative reduction, for example the elliptic curves given by the equations $y^2 = x^3 + 1$ and $y^2 = x^3 + 2x$, we will prove that this rather exceptional.

Theorem 9 (p. 9)**.** *100% of elliptic curves over $\mathbb{Q}$ ordered by height have at least one prime of multiplicative reduction.*

We will also prove that most occurrences of bad reduction are multiplicative.

Theorem 8 (p. 7)**.** *Let $p \geqslant 4$ be a prime number. The proportion of elliptic curves over $\mathbb{Q}$ with multiplicative reduction at p inside the set of elliptic curves with bad reduction at p is at least $(1 - \frac{1}{p})^2$.*

Shafarevich proved that for any finite set of primes S, only finitely many elliptic curves over $\mathbb{Q}$ have good reduction outside S, cf. [14, th. 6.1, p. 293]. Moreover, it is even true that there is no elliptic curve over $\mathbb{Q}$ which has everywhere good reduction. In [16] Siman Wong proved that approximately 17.9% of elliptic curves over $\mathbb{Q}$ are semistable, i.e., they have no primes of additive reduction. Semistable elliptic curves are generally easier to handle than those with additive reduction at some prime. For example, Wiles proved the modularity theorem for semistable elliptic curves in 1995, several years before the general result was proven.

For hyperelliptic curves over $\mathbb{Q}$ the situation is similar. Bad semistable reduction (see def. 19 and def. 21) is the analogue of bad multiplicative reduction in the elliptic curve case. Grothendieck's famous semistable reduction theorem states that any curve over $\mathbb{Q}$ has potential semistable reduction at every prime number p, i.e., there is a finite field extension L of $\mathbb{Q}$ over which the curve has semistable reduction at the places above p. However, almost always it is the case that given a hyperelliptic curve there is a bad prime for which we can take L to be $\mathbb{Q}$. To be more precise, we will prove the following result.

Theorem 29 (p. 21)**.** *Let g be an integer greater than 1. Then 100% of hyperelliptic curves over $\mathbb{Q}$ of genus g have at least one prime of bad semistable reduction.*

The results will be proven by counting Weierstraß equations for which the discriminant is divisible exactly once by p. In the process of counting such equations we will use the Lang-Weil estimates and the properties of étale morphisms between schemes. Furthermore, we will use a sieve method to count points satisfying a number of congruence conditions. Sieving is a standard technique in number theory. For example, a similar sieve was used to prove Brun's theorem, that states that the sum of the reciprocals of the twin primes converges to a finite value.

Given a hyperelliptic curve one can consider its Jacobian. It is an abelian variety. Semi-abelian reduction for abelian varieties (see def. 43) is the analogue of semistable reduction for curves. The semistable reduction theorem also holds in this case, i.e., for any abelian variety over $\mathbb{Q}$ and any prime p there is a finite field extension L of $\mathbb{Q}$ over which the variety has semi-abelian reduction at all places of L above p. In the last chapter we will prove the following theorem.

Theorem 46 (p. 27)**.** *Let C be a hyperelliptic curve of genus $g \geqslant 2$ over $\mathbb{Q}$ and let p be an odd prime number. Suppose that we have a Weierstraß model of C over $\mathbb{Z}_{(p)}$ for which the discriminant is divisible exactly once by p. Then the Jacobian of C has semi-abelian reduction of toric rank 1 at p.*

By combining the results of corollary 28 and theorem 46, we get the following result.

Corollary 1. *100% of Jacobians of hyperelliptic curves over $\mathbb{Q}$ have at least one prime of semi-abelian reduction of toric rank 1.*

To conclude, I would like to thank my advisor David Holmes for his continuing support during the last semester. Furthermore, I would like to thank Bas Edixhoven for the insightful conversations that helped me to solve many of my problems.

1 Counting elliptic curves with a bad semistable prime

In this chapter we are going to look at elliptic curves over $\mathbb{Q}$ that have bad semistable, i.e. multiplicative, reduction at some prime p. We will prove that a proportion that is approximately $(1 - \frac{1}{p})^2$ of the elliptic curves that have bad reduction at p have bad semistable reduction at p. Furthermore, we will prove that 100% of elliptic curves have at least one prime of bad semistable reduction.

First of all let us define some notation that is frequently used.

Definition 2. Let $S = \operatorname{Spec} A$ be an affine scheme and let n be an integer. Then the affine space $\mathbb{A}^n_S = \operatorname{Spec}(A[x_1, \ldots, x_n])$ is sometimes denoted by $\mathbb{A}^n_S(x_1, \ldots, x_n)$ to indicate that the coordinates are called $x_1, \ldots, x_n$. The projective space $\mathbb{P}^n_S = \operatorname{Proj}(A[x_0, \ldots, x_n])$ is sometimes denoted by $\mathbb{P}^n_S(x_0 : \ldots : x_n)$ to indicate that the coordinates are called $x_0, \ldots, x_n$.

Definition 3. Let S be a scheme and let X be a scheme over S. Then X/S is called *projective* if it is projective in the sense of [7], i.e., if X is isomorphic over S to a closed subscheme of $\mathbb{P}^n_S$ for some non-negative integer n.

Lemma 4. *Let S be a scheme and X/S be an open subscheme of $\mathbb{A}^n_S$. Suppose that $\Delta \subset X$ is a hypersurface[1] that is smooth over S. Let $p \in \Delta$. Then there exists an open neighbourhood $U \subset X$ of p such that there exists a commutative diagram*

$$\begin{array}{ccc} \Delta \times_X U & \xrightarrow{\pi_1} & \mathbb{A}^{n-1}_S \\ \downarrow & & \downarrow \\ U & \xrightarrow{\pi_2} & \mathbb{A}^n_S \end{array},$$

where $\mathbb{A}^{n-1}_S \to \mathbb{A}^n_S$ is the map $(s_1, \ldots, s_{n-1}) \mapsto (s_1, \ldots, s_{n-1}, 0)$, such that π_1 and π_2 are étale.

Proof. The question is local, hence we may and do assume that S is affine, say $S = \operatorname{Spec} A$, and that $X = D(g) \subset \mathbb{A}^n_S(x_1, \ldots, x_n)$ for some $g \in A[x_1, \ldots, x_n]$. Furthermore, let $f \in A[x_1, \ldots, x_n]$ be such that $\Delta = Z(f) \subset X$. Let $B := A[x_1, \ldots, x_{n+1}]/(f, x_{n+1} \cdot g - 1)$, then $\Delta = \operatorname{Spec} B$.

Now the module of differentials $\Omega_{\Delta/S}$ is the quotient of the free B-module generated by $dx_1, \ldots, dx_n$ by the relation $0 = df = \sum_{i=1}^n f_i dx_i$, where

[1] this means: globally cut out by one regular element

$f_i = \frac{\partial f}{\partial x_i} \in B$. As Δ/S is smooth, the module $\Omega_{\Delta/S}$ is locally free of rank $n-1$, by [15, tag 02G1]. Hence, one of the f_i does not vanish at p, suppose w.l.o.g., by swapping coordinates if necessary, that f_n does not vanish.

Then take $U = D(f_n) \subset X$, it contains p. Next we define π_1 to be the projection on the first $n-1$ coordinates, i.e. the morphism that corresponds to the ring morphism

$$\begin{aligned} A[b_1, \dots, b_{n-1}] &\to \frac{A[b_1, \dots, b_{n-1}, x_1, \dots, x_{n+1}]}{(x_1 - b_1, \dots, x_{n-1} - b_{n-1}, f, x_{n+1} \cdot gf_n - 1)} \cong B_{f_n} \\ b_i &\mapsto x_i. \end{aligned}$$

The Jacobian determinant $\det(\partial h_i/\partial x_j)_{i,j=1}^{n+1}$, where $h_i = x_i - b_i$ for $i < n$, and $h_n = f$ and $h_{n+1} = x_{n+1}gf_n - 1$, is equal to $f_n^2 \cdot g$, which is a unit in B_{f_n}. Hence, by [15, tag 02GU], the map π_1 is étale.

Furthermore, we define π_2 as the morphism that is the projection on the first $n-1$ coordinates and f on the last coordinate, i.e. the morphism that corresponds to the ring morphism

$$\begin{aligned} A[a_1, \dots, a_n] &\to \frac{A[a_1, \dots, a_n, x_1, \dots, x_{n+1}]}{(x_1 - a_1, \dots, x_{n-1} - a_{n-1}, f - a_n, x_{n+1} \cdot gf_n - 1)} \cong A_{f_n} \\ a_i &\mapsto \begin{cases} x_i & \text{if } i \leqslant n-1 \\ f & \text{if } i = n. \end{cases} \end{aligned}$$

The Jacobian determinant $\det(\partial z_i/\partial x_j)_{i,j=1}^{n+1}$, where $z_i = x_i - a_i$ for $i < n$, and $z_n = f - a_n$ and $z_{n+1} = x_{n+1}gf_n - 1$, is equal to gf_n^2, which is a unit in A_{f_n}. Hence, by [15, tag 02GU] again, the map π_2 is étale. It is easy to see that π_1 and π_2 make the diagram commute. □

We can apply Lemma 4 to count $\mathbb{Z}/p^2\mathbb{Z}$-points in varieties, where p is a prime number.

Lemma 5. *Let $N, n \in \mathbb{Z}_{>0}$ be positive integers, let p be a prime number not dividing N and let $f \in \mathbb{Z}[1/N, x_1, \dots, x_n]$. Let X be an open subscheme of $\mathbb{A}^n_S(x_1, \dots, x_n)$, where $S = \operatorname{Spec}(\mathbb{Z}[1/N])$. For $i = 0, \dots, p-1$, let H_i be the hypersurfaces in X given by the equation $f - ip = 0$. Suppose that H_i is smooth over S for each $i \in \{0, \dots, p-1\}$. Then for every $i = 0, \dots, p-1$ and every point $(r_1, \dots, r_n) \in H_0(\mathbb{F}_p)$ there exist exactly p^{n-1} lifts in $H_i(\mathbb{Z}/p^2\mathbb{Z})$.*

Proof. Let $r = (r_1, \dots, r_n) \in H_0(\mathbb{F}_p)$ be an arbitrary point. Remark that there is a canonical one-to-one correspondence between $H_0(\mathbb{F}_p)$ and $H_i(\mathbb{F}_p)$,

hence we will consider r as point of $H_i(\mathbb{F}_p)$. Let P be the closed point of H_i corresponding to this point. Apply lemma 4 to this point P to find an open neighbourhood U of $P \in X$ and $\pi_1 : H_i \times_X U \to \mathbb{A}_S^{n-1}$ with π_1 étale.

$$\begin{array}{ccc} \operatorname{Spec} \mathbb{F}_p & \longrightarrow & H_i \times_X U \\ \downarrow & \nearrow & \downarrow \\ \operatorname{Spec} \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & \mathbb{A}_S^{n-1} \end{array}$$

As π_1 is étale, it is also formally étale. Hence, every pair of an element of $H_i(\mathbb{F}_p) \times_{X(\mathbb{F}_p)} U(\mathbb{F}_p)$ and an element of $\mathbb{A}_S^{n-1}(\mathbb{Z}/p^2\mathbb{Z}) = (\mathbb{Z}/p^2\mathbb{Z})^{n-1}$ that are compatible via π_1 and the reduction map $\mathbb{A}_S^{n-1}(\mathbb{Z}/p^2\mathbb{Z}) \to \mathbb{A}_S^{n-1}(\mathbb{F}_p)$ will give rise to a unique point of $H_i(\mathbb{Z}/p^2\mathbb{Z}) \times_{X(\mathbb{Z}/p^2\mathbb{Z})} U(\mathbb{Z}/p^2\mathbb{Z})$. Furthermore, every element of $H_i(\mathbb{Z}/p^2\mathbb{Z}) \times_{X(\mathbb{Z}/p^2\mathbb{Z})} U(\mathbb{Z}/p^2\mathbb{Z})$ gives rise to an element of $H_i(\mathbb{F}_p) \times_{X(\mathbb{F}_p)} U(\mathbb{F}_p)$ and an element of $\mathbb{A}_S^{n-1}(\mathbb{Z}/p^2\mathbb{Z})$, i.e. there is a one-to-one correspondence. Remark that the number of points of $(\mathbb{Z}/p^2\mathbb{Z})^{n-1}$ that reduce to $\pi_1(r)$ is p^{n-1}. In other words, every element of $H_i(\mathbb{F}_p) \times_{X(\mathbb{F}_p)} U(\mathbb{F}_p)$ has exactly p^{n-1} lifts in $H_i(\mathbb{Z}/p^2\mathbb{Z}) \times_{X(\mathbb{Z}/p^2\mathbb{Z})} U(\mathbb{Z}/p^2\mathbb{Z})$.

We conclude by proving for $R = \operatorname{Spec} \mathbb{F}_p$ and $R = \operatorname{Spec} \mathbb{Z}/p^2\mathbb{Z}$ that elements of $H_i(R) \times_{X(R)} U(R)$ whose image is P canonically correspond to elements of $H_i(R)$ whose image is P. For this, remark that $H_i \times_X U \to H_i \times_X X = H_i$ is an open immersion as open immersions are stable under base change. For an open immersion the mentioned property is clear: for every map $\varphi : R \to H_i \times_X X$ there is a unique map $R \to H_i \times_X U$ which is given on sheaves by restricting φ. □

For the next part we consider the map

$$\mathbb{Z}^2 \setminus \{(a,b) : 4a^3 + 27b^2 = 0\} \to \{\text{elliptic curves over } \mathbb{Q}\}$$

mapping (a, b) to the curve given by $y^2 = x^3 + ax + b$. Every elliptic curve is isomorphic to one of these curves. From [14, table 3.1, p. 45] it follows that two pairs (a, b) and (c, d) give rise to isomorphic curves over $\mathbb{Q}$ if and only if there exists an $f \in \mathbb{Q}^*$ such that $c = f^4a$ and $d = f^6b$. Hence, we consider the subset L of $\mathbb{Z}^2$ consisting of these pairs (a, b) such that $4a^3 + 27b^2 \neq 0$ and such that there does not exist a prime p such that $p^4 \mid a$ and $p^6 \mid b$. Then each isomorphism class of elliptic curves over $\mathbb{Q}$ corresponds to exactly one element of L. Furthermore, for $B \in \mathbb{R}$ let $L_B := \{P \in L : h(P) \leqslant B\}$ for the height function h defined by $h((a, b)) = \max\{|a|, |b|\}$.

Proposition 6. *Let $p \geqslant 4$ be a prime number. Then there are p elements $(a, b) \in \mathbb{F}_p^2$ such that $4a^3 + 27b^2 = 0$.*

Proof. First of all remark that $(0,0)$ is a solution. If (a,b) is a non-zero solution, then both a and b are non-zero and we can consider $\lambda = \frac{a}{b} \in \mathbb{F}_p^*$. Then the equation becomes $0 = 4a^3 + 27b^2 = a^2(4a + 27\lambda^2) = 0$. Hence, for each $\lambda \in \mathbb{F}_p^*$ there is a unique $a \in \mathbb{F}_p^*$ such that $(a, \lambda \cdot a)$ is a solution, namely $a = -\frac{27}{4}\lambda^2$. Therefore, there are p solutions in $\mathbb{F}_p^2$ to the equation. □

Lemma 7. *Let $p \geqslant 4$ be a prime number. Then there are $p(p-1)^2$ pairs (a,b) in $(\mathbb{Z}/p^2\mathbb{Z})^2$ such that $4a^3 + 27b^2 \in p\mathbb{Z}/p^2\mathbb{Z} \setminus \{0\}$ and there are $2p^2 - p$ pairs with $4a^3 + 27b^2 = 0 \in \mathbb{Z}/p^2\mathbb{Z}$.*

Proof. For this proof we will count the points $(a,b) \in (\mathbb{Z}/p^2\mathbb{Z})^2$ satisfying $\Delta(a,b) := 4a^3 + 27b^2 = 0 \in \mathbb{Z}/p^2\mathbb{Z}$ and points with $\Delta(a,b) \in p\mathbb{Z}/p^2\mathbb{Z} \setminus \{0\}$. First we are going to define some schemes.

Consider the hypersurfaces $\Delta'_k := Z(\Delta(a,b) - kp) \subset \mathbb{A}^2_{\mathbb{Z}[1/6]}(a,b)$ where $k = 0, \ldots, p-1$. As they are not smooth, we intersect them with the open subscheme $T := D_+(a) \cup D_+(b) \subset \mathbb{A}^2_{\mathbb{Z}[1/6]}(a,b)$ to get hypersurfaces Δ_k of T. The hypersurfaces are smooth over $S := \mathrm{Spec}(\mathbb{Z}[1/6])$ (as either $3 \cdot 64 \cdot a^2$ or $-32 \cdot 27 \cdot b^2$ is a unit) and hence they satisfy the conditions of lemma 5.

For every non-zero pair $(a',b') \in \mathbb{F}_p^2$ with $\Delta(a',b') = 0$ we find a point in $\Delta'_0(\mathbb{F}_p)$. By proposition 6 there are $p-1$ such non-zero pairs (a',b'). By lemma 5 for every $k = 0, \ldots, p-1$ there are p lifts $(a,b) \in (\mathbb{Z}/p^2\mathbb{Z})^2$ of (a',b') such that $\Delta(a,b) = kp$. For the point $(0,0) \in \mathbb{F}_p^2$ all lifts $(a,b) \in (\mathbb{Z}/p^2\mathbb{Z})^2$ satisfy $\Delta(a,b) = 0$. In total we found $p(p-1)^2$ points (a,b) with $\Delta(a,b) \equiv 0 \mod p$ and $\Delta(a,b) \neq 0 \in \mathbb{Z}/p^2\mathbb{Z}$ and $p^2 + (p-1)p = 2p^2 - p$ points with $\Delta(a,b) = 0$. □

Theorem 8. *Let $p \geqslant 4$ be a prime number. For every $B \in \mathbb{R}$ let $Z_B \subset L_B$ be the subsets of pairs corresponding to elliptic curves with bad reduction at p and let $S_B \subset Z_B$ be the subsets of pairs corresponding to elliptic curves with multiplicative reduction (also called bad semistable reduction) at p. Then $\liminf_{B\to\infty} |S_B|/|Z_B| \geqslant (1 - \frac{1}{p})^2$.*

Proof. Let $B \in \mathbb{R}$ and let k be a positive integer. The main part of the proof of this theorem consists of giving a lower bound for $|S_B|$ and an upper bound for $|Z_B|$. Let $p_1, p_2, \ldots$ be the prime numbers not equal to p in increasing order. Let $m_k = \prod_{i=1}^k p_i^4$, $M_k = p^2 \cdot m_k$, $n_k = \prod_{i=1}^k p_i^6$ and $N_k = p^2 \cdot n_k$.

Note that the curves corresponding to $(a,b) \in L$ have bad reduction at p if and only if $\Delta(a,b) \equiv 0 \mod p$. First we consider the elements $(a,b) \in L$ with $\Delta(a,b) \equiv p, 2p, \ldots, p^2 - p \mod p^2$. Such elements have the property that

$\Delta(a,b)$ is divisible by p but not by p^2. Then the corresponding elliptic curves have multiplicative reduction at p, i.e., they have bad semistable reduction at p. We will give a lower bound on the number of such elements and hence a lower bound on $|S_B|$.

Let Q be the largest integer multiple of M_k strictly smaller than B and let R be the largest integer multiple of N_k strictly smaller than B. Then in $I_B := \{-\lfloor B \rfloor, \ldots, \lfloor B \rfloor\}$ every residue class of $\mathbb{Z}/M_k\mathbb{Z}$ (resp. $\mathbb{Z}/N_k\mathbb{Z}$) has at least $\frac{2Q}{M_k}$ (resp. $\frac{2R}{N_k}$) representatives. Hence every pair of residue classes in $\mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ has at least $\frac{4QR}{M_kN_k}$ representatives in $I_B \times I_B$.

In $I_B \times I_B$ we consider the subset Ω consisting of pairs (a,b) such that $\Delta(a,b) \equiv p, \ldots,$ or $p^2 - p \mod p^2$ and $(a,b) \neq (0,0) \in \mathbb{Z}/p_i^4\mathbb{Z} \times \mathbb{Z}/p_i^6\mathbb{Z}$ for all $i = 1, \ldots, k$. Denote by $W := \prod_{i=1}^{k}(p_i^{10} - 1)$ the number of elements in $\mathbb{Z}/n_k\mathbb{Z} \times \mathbb{Z}/m_k\mathbb{Z}$ satisfying the latter conditions modulo p_i for $i = 1, \ldots, k$. The number of elements in $\mathbb{Z}/p^2\mathbb{Z}$ satisfying the first condition is $p(p-1)^2$ according to theorem 7. Then the number of elements in $\mathbb{Z}/N_k\mathbb{Z} \times \mathbb{Z}/M_k\mathbb{Z}$ satisfying all the conditions is $W \cdot p(p-1)^2$ by the Chinese remainder theorem. Hence, there are at least $Wp(p-1)^2 \cdot \frac{4QR}{M_kN_k}$ elements in Ω.

However, not all elements (a,b) of Ω will necessarily be elements of L. The conditions imply that $\Delta(a,b) \neq 0$ for such pairs, however, there might still exist a prime q satisfying $p_k < q \leqslant B^{\frac{1}{4}}$ such that $q^4 \mid a$ and $q^6 \mid b$. We will give an upper bound on the number of elements in Ω for which such a prime q exists. We consider the reduction of the elements of Ω in $\mathbb{Z}/M_kq^4\mathbb{Z} \times \mathbb{Z}/N_kq^6\mathbb{Z}$. In I_B every residue class modulo M_kq^4 resp. N_kq^6 has at most $2\frac{Q}{M_kq^4} + 4$ resp. $2\frac{R}{N_kq^6} + 4$ representatives. Of the M_kN_k classes that reduce to 0 in $\mathbb{Z}/q^4\mathbb{Z} \times \mathbb{Z}/q^6\mathbb{Z}$ only $Wp(p-1)^2$ occur in Ω by the Chinese remainder theorem. Hence, there are at most $Wp(p-1)^2 \cdot (2\frac{Q}{M_kq^4} + 4)(2\frac{R}{N_kq^6} + 4)$ elements in Ω such that $q^4 \mid a$ and $q^6 \mid b$. Now we want to find an upper bound on the sum $\sum_q (\frac{2Q}{M_kq^4} + 4)(\frac{2R}{N_kq^6} + 4)$.

We can bound $\sum_q \frac{1}{q^j}$ for $j = 4, 6, 10$ by $\int_{p_k}^{\infty} \frac{1}{x^j} dx = \frac{1}{(j-1)p_k^{j-1}}$ and $\sum_q 1$ by $B^{\frac{1}{4}}$. We find that the sum we wanted to bound is at most

$$\frac{4QR}{9M_kN_kp_k^9} + \frac{8Q}{3M_kp_k^3} + \frac{8R}{5N_kp_k^5} + 16B^{\frac{1}{4}} = \frac{4QR}{M_kN_k} \cdot \left(\frac{1}{9p_k^9} + \varepsilon(B)\right)$$

where $\varepsilon(B) = \mathcal{O}(B^{-1})$ as we will let $B \to \infty$. The lower bound for the number of elements in S_B now becomes $Wp(p-1)^2 \cdot \frac{4QR}{M_kN_k}(1 - \frac{1}{9p_k^9} - \varepsilon(B))$.

On the other hand to find an upper bound for Z_B we first notice that each class of $\mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ has at most $(\frac{2Q}{M_k} + 4)(\frac{2R}{N_k} + 4)$ representatives in I_B.

There are $W \cdot p^3$ classes (a,b) in $\mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ such that $\Delta(a,b) \equiv 0 \mod p$ and $(a,b) \neq (0,0) \in \mathbb{Z}/p_i^4\mathbb{Z} \times \mathbb{Z}/p_i^6\mathbb{Z}$ for all $i = 1, \ldots, k$. We immediately find the upper bound $Wp^3 \cdot (\frac{2Q}{M_k} + 4)(\frac{2R}{N_k} + 4)$ for $|Z_B|$.

Finally we conclude that the quotient $\frac{|S_B|}{|Z_B|}$ is bounded from below by

$$\left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{2N_k}{R + 2N_k}\right) \left(1 - \frac{2M_k}{Q + 2M_k}\right) \left(1 - \frac{1}{9p_k^9} - \epsilon(B)\right)$$
$$= \left(1 - \frac{1}{p}\right)^2 \left(1 - \frac{1}{9p_k^9}\right) + \mathcal{O}(B^{-1}).$$

Hence, $\liminf_{B\to\infty} \frac{|S_B|}{|Z_B|} \geqslant (1 - \frac{1}{p})^2(1 - \frac{1}{9p_k^9})$ for all $k \in \mathbb{N}$. The result follows now as $\frac{1}{9p_k^9} \to 0$ as $k \to \infty$. □

Theorem 9. *For each $B \in \mathbb{R}$ let $Q_B \subset L_B$ be the subset of pairs corresponding to elliptic curves without a prime of semistable bad reduction. Then $\limsup_{B\to\infty} \frac{|Q_B|}{|L_B|} = 0$.*

Proof. Let $p_1, p_2, \ldots$ be the prime numbers ordered in the natural way and let $k \geqslant 3$ be an integer. Let $M_k = \prod_{i=1}^k p_i^4$ and $N_k = \prod_{i=1}^k p_i^6$. For a fixed $B \in \mathbb{R}_{>0}$ let $I_B := \{-\lfloor B \rfloor, \ldots, \lfloor B \rfloor\}$. Let Q and R be the largest integer multiples of M_k, resp. N_k, smaller than B. In $I_B \times I_B$ we consider the subset Ω of pairs (a,b) such that $\Delta(a,b) \equiv p, 2p, \ldots,$ or $p^2 - p \mod p^2$ for some $p \in \{p_3, \ldots, p_k\}$ and $(a,b) \not\equiv (0,0) \in \mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p^6\mathbb{Z}$ for all $p \in \{p_1, \ldots, p_k\}$.

There are $\prod_{i=1}^k (p_i^{10} - 1)$ classes $(a,b) \in \mathbb{Z}/M_k \times \mathbb{Z}/N_k$ that satisfy the latter condition that $(a,b) \not\equiv (0,0) \in \mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p^6\mathbb{Z}$ for all $p \in \{p_1, \ldots, p_k\}$. By lemma 7, for each $p \in \{p_3, \ldots, p_k\}$ there are $p^4 - (p-1)^2 p$ classes $(a,b) \in \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z}$ such that $\Delta(a,b) \not\equiv p, 2p, \ldots,$ or $p^2 - p \mod p^2$. Hence, there are $p^{10} - 1 - (p-1)^2 p^7$ non-zero classes $(a,b) \in \mathbb{Z}/p^4\mathbb{Z} \times \mathbb{Z}/p^6\mathbb{Z}$ satisfying this condition (remark that 0 did satisfy the condition). Therefore, there are

$$W_1 := \prod_{i=1}^k (p_i^{10} - 1) - (2^{10} - 1)(3^{10} - 1) \prod_{i=3}^k (p_i^{10} - 1 - (p_i - 1)^2 p_i^7)$$

classes (a,b) in $\mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ such that for each of these pairs there is at least one $p \in \{p_3, \ldots, p_k\}$ such that $\Delta(a,b) \equiv p, 2p, \ldots,$ or $p^2 - p \mod p^2$.

Each residue class of $\mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ has at least $\frac{4QR}{M_k N_k}$ representatives in $I_B \times I_B$ and hence Ω contains at least $\frac{4QR}{M_k N_k} W_1$ elements. However, not all

of them lie in L, for some pairs $(a,b) \in \Omega$ there might still exist a prime q satisfying $p_k < q \leqslant Q^{\frac{1}{4}}$ such that $q^4 \mid a$ and $q^6 \mid b$. In the same way as in the previous proof we will find that there are at most $\sum_q W_1 \cdot (\frac{2Q}{M_k q^4}+4)(\frac{2R}{N_k q^6}+4)$ such elements. Hence, the sum will be bounded by $W_1 \cdot \frac{4QR}{M_k N_k} \cdot (\frac{1}{9p_k^9} + \varepsilon(B))$ as before. Hence, $|L_B \cap \Omega| \geqslant W_1 \cdot \frac{4QR}{M_k N_k} \cdot (1 - \frac{1}{9p_k^9} - \varepsilon(B))$. As every curve in $L_B \cap \Omega$ has bad semistable reduction at $p_3, \ldots,$ or p_k, this also provides for a lower bound for $|L_B \setminus Q_B|$.

On the other hand, we consider the subset Λ of $I_B \times I_B$ of elements (a,b) such that there exists no prime number p such that both $p^4 \mid a$ and $p^6 \mid b$. By the Chinese remainder theorem there are $W_2 := \prod_{i=1}^k (p_i^{10} - 1)$ classes $(a,b) \in \mathbb{Z}/M_k\mathbb{Z} \times \mathbb{Z}/N_k\mathbb{Z}$ satisfying this condition. Furthermore, each representative class has at most $(\frac{2Q}{M_k}+4)(\frac{2R}{N_k}+4)$ representatives in $I_B \times I_B$. In this way, we find the upper bound $|L_B| \leqslant W_2 \cdot (\frac{2Q}{M_k}+4)(\frac{2R}{N_k}+4)$.

Now we conclude that

$$\begin{aligned}\frac{|L_B \setminus Q_B|}{|L_B|} &\geqslant \frac{W_1}{W_2}\left(1 - \frac{2N_k}{R+2N_k}\right)\left(1 - \frac{2M_K}{Q+2M_K}\right)\left(1 - \frac{1}{9p_k^9} - \varepsilon(B)\right) \\ &= \frac{W_1}{W_2}\left(1 - \frac{1}{9p_k^9}\right) + \mathcal{O}\left(\frac{1}{B}\right).\end{aligned}$$

In particular $1 - \limsup_{B\to\infty} \frac{|Q_B|}{|L_B|} = \liminf_{B\to\infty} \frac{|L_B \setminus Q_B|}{|L_B|} \geqslant \frac{W_1}{W_2}(1 - \frac{1}{9p_k^9})$. Now it suffices to show that $\lim_{k\to\infty} \frac{W_1}{W_2}(1 - \frac{1}{9p_k^9}) = 1$. Remark that

$$\frac{W_1}{W_2} = 1 - \prod_{i=3}^{k}\left(1 - \frac{(p_i-1)^2 p_i^7}{p_i^{10}-1}\right).$$

Surely the product $\lim_{k\to\infty}(1 - \frac{W_1}{W_2})$ converges to some number in $[0,1]$. Suppose that it is non-zero. Then the infinite product would converge to a non-zero number and the convergence criterium for infinite product (see for example [8, th. 4, p. 220]) would tell us that $\sum_{i=1}^M \frac{(p_i-1)^2 p_i^7}{p_i^{10}-1}$ converges as $M \to \infty$. Then also $\sum_{i=1}^M \frac{1}{p_i}$ must converge as $M \to \infty$, because $\frac{(p_i-1)^2 p_i^7}{p_i^{10}-1} \sim \frac{1}{p_i}$ as $i \to \infty$. However, by the prime number theorem we have $p_i \sim i \log i$, hence also $\sum_{i=2}^M 1/(i \log i)$ must converge as $M \to \infty$. This, however, is false as $\int_2^M di/(i \log i) = \log\log M - \log\log 2$ does not converge as $M \to \infty$. We get a contradiction and hence the product converges to 0. $\square$

2 Counting hyperelliptic curves with a bad semistable prime

In this chapter we will prove a result for hyperelliptic curves of a similar form to our result for elliptic curves in the previous chapter. The following proposition will help us to generalise the sufficient criterion for semistable reduction that we had for elliptic curves to the case of hyperelliptic curves. This proposition is a classical corollary of Hensel's lemma. However, we will give a proof for this proposition in the language of algebraic geometry.

Proposition 10. *Let k be a field of characteristic not equal to 2. Let $a \in k$ and let $f \in k[x]$ be such that $f(a)$ is a non-zero square. Then there exists a $g \in k[[x-a]]$ such that $f = g^2 \in k[[x-a]]$.*

Proof. Let $R = k[[x-a]]$, and let $\psi : R \to R[t]/(t^2 - f)$ be the natural morphism. Remark that $2 \in k^*$ and $f \in k[[x-a]]^*$ as $k[[x-a]]$ is a discrete valuation ring and $f \notin (x-a) \cdot k[[x-a]]$. Hence, $\frac{\partial(t^2-f)}{\partial t} = 2t$ is a unit in $R[t]/(t^2-f)$, because 2 and $t^2 = f$ are units. Hence, ψ is standard étale. In particular, it is formally étale.

$$\begin{array}{ccc} \operatorname{Spec}\left(\frac{R}{(x-a)}\right) & \longrightarrow & \operatorname{Spec}\left(\frac{R[t]}{(t^2-f)}\right) \\ \downarrow & \nearrow & \downarrow \\ \operatorname{Spec}\left(\frac{R}{(x-a)^2}\right) & \longrightarrow & \operatorname{Spec} R \end{array}$$

Let $b_1 \in k$ be such that $0 = b_1^2 - a = b_1^2 - f$ in $R/(x-a)$, which exists because a is assumed to be a square. Then, by the fact that ψ is formally étale, there is a unique $b_2 \in R/(x-a)^2$ such that $\overline{b_2} = b_1 \in R/(x-a)$ and $b_2^2 - f = 0 \in R/(x-a)^2$. Applying this again, we find an element $b_3 \in R/(x-a)^3$, restricting to b_2 such that $b_3^2 - f = 0 \in R/(x-a)^3$, et cetera. Now let $g = \lim_{n\to\infty} b_n$. then $g^2 - f = 0 \in R$ and we are done. □

Lemma 11. *Let k be a field of characteristic not equal to 2 and let $f \in k[x]$ be a non-zero polynomial. Let C be the scheme $Z(y^2 - f) \subset \mathbb{A}^2_k(x,y)$. Let $p = (p_x, p_y) \in \overline{k}^2$ be a closed point of $C_{\overline{k}}$. If $p_y \neq 0$ or p_x is a single zero of f, then $C_{\overline{k}}$ is smooth at p. If p_x is a zero of order two of f, then p is an ordinary double point, i.e. $\widehat{\mathcal{O}_{C_{\overline{k}},p}} \cong k[[T_1,T_2]]/(T_1T_2)$.*

Proof. To see that $C_{\overline{k}}$ is smooth at p use the Jacobian criterion: $\frac{\partial y^2}{\partial y}(p) = 0$ if and only if $p_y = 0$ if and only if $f(p_x) = 0$ and in this case $\frac{\partial f}{\partial x}(p_x) = 0$ if and only if p_x is a zero with multiplicity higher than 1 of f. Hence, $C_{\overline{k}}$ is smooth at p, if $p_y \neq 0$ or p_x is a single zero of f.

Now suppose that p_x is a double zero. Write $f = (x - p_x)^2 g$ for some $g \in \overline{k}[x]$. Then $g(p_x) \neq 0$, hence $g = h^2$ for some $h \in \overline{k}[[x - p_x]]$ by proposition 10. Hence, the completed local ring of $C_{\overline{k}}$ at p is isomorphic to $\overline{k}[[x - p_x, y]]/(y - (x - p_x)h)(y + (x - p_x)h) \cong \overline{k}[[a, b]]/(ab)$ by taking $a = y - (x - p_x)h$ and $b = y + (x - p_x)h$, cf. [12, p. 506]. Furthermore $C_{\overline{k}}$ is reduced as f is non-zero and hence $y^2 - f$ has no irreducible factors with multiplicity higher than 1 in its factorisation. This proves that p is an ordinary double point of $C_{\overline{k}}$. □

Next we will give the definition of a weighted projective space.

Definition 12. Let R be a ring, let n be a non-negative integer and let $w_0, \ldots, w_n$ be positive integers. Then *the weighted projective space over R with weights $w_0, \ldots, w_n$* is the scheme $\mathbb{P}_R(w_0, \ldots, w_n) := \operatorname{Proj}(R[x_0, \ldots, x_n])$, where the grading of $R[x_0, \ldots, x_n]$ is such that x_i is homogeneous of degree w_i for $i = 0, \ldots, n$. Sometimes we denote it by $\mathbb{P}_R(w_0, \ldots, w_n)(x_0 : \ldots : x_n)$ to indicate that the coordinates are called $x_0, \ldots, x_n$.

Example 13. Let $n \geqslant 0$ and $w > 0$ be integers. Let R be a ring. Then $\mathbb{P}_R(w, \ldots, w)(x_0 : \ldots : x_n)$ is isomorphic to $\mathbb{P}^n_R$. The standard opens $D_+(x_i)$ are the spectra of the rings $R[x_0, \ldots, x_n]_{(x_i)} = R[x_0 x_i^{-1}, \ldots, x_n x_i^{-1}]$, and they glue to $\mathbb{P}_R(w, \ldots, w)$ independently of w.

Example 14. Let $g > 1$ be an integer and let R be a ring. Then the weighted projective space $\mathbb{P}_R(1, 1, g + 1)(x : s : y)$ is covered by the three standard opens $D_+(x)$, $D_+(s)$ and $D_+(y)$. As $R[x, s, y]_{(x)} = R[sx^{-1}, yx^{-g-1}]$, we have that $D_+(x)$ is isomorphic to $\mathbb{A}^2_R$. Analogously $D_+(s)$ is isomorphic to $\mathbb{A}^2_R$. However, one can check that the R-algebra

$$R[x, s, y]_{(y)} = R[x^{g+1}y^{-1}, x^g s^1 y^{-1}, \ldots, s^{g+1}y^{-1}]$$

cannot be generated by two elements, hence $D_+(y)$ is not isomorphic to $\mathbb{A}^2_R$.

Lemma 15. *Let R be a noetherian ring, let n be a non-negative integer and let $w_0, \ldots, w_n$ be positive integers. Then the weighted projective space $W := \mathbb{P}_R(w_0, \ldots, w_n)(x_0 : \ldots : x_n)$ is projective over* $\operatorname{Spec} R$.

Proof. Let $w = \prod_{i=0}^{n} w_i$. Give $R[y_0, \ldots, y_n]$ the structure of a graded R-algebra by letting $y_0, \ldots, y_n$ be of degree w. Consider the graded R-algebra homomorphism $R[y_0, \ldots, y_n] \to R[x_0, \ldots, x_n]$ defined by $y_i \mapsto x_i^{w/w_i}$. As the $D_+(x_i^{w/w_i}) = D_+(x_i)$ cover W, this morphism of graded R-algebras induces a morphism of schemes $\varphi : W \to P := \mathbb{P}_R^n(w, \ldots, w)(y_0 : \ldots y_n)$ by [15, tag 01MY].

Remark that $R[x_0, \ldots, x_n]$ is a finite $R[y_0, \ldots, y_n]$-module, as it is generated by the monomials of the form $x_0^{e_0} \cdot \ldots \cdot x_n^{e_n}$ with $e_0 \in \{0, \ldots, \frac{w}{w_0} - 1\}$, $\ldots$, $e_n \in \{0, \ldots, \frac{w}{w_n} - 1\}$. In particular $R[x_0, \ldots, x_n]_{(x_i)}$ is a finite $R[y_0, \ldots, y_n]_{(y_i)}$-module for all $i = 0, \ldots, n$ and the morphism φ is finite. Hence, by example 13 there is a finite morphism $\psi : W \to \mathbb{P}_R^n$.

On $\mathbb{P}_R^n$ we have the ample sheaf $\mathcal{L} := \mathcal{O}_{\mathbb{P}_R^n}(1)$. Now let $\mathcal{G}$ be a coherent sheaf on W. By [15, tag 01Y6], $\psi_*\mathcal{G}$ is a coherent sheaf on $\mathbb{P}_R^n$. Hence, by [7, prop. III.5.3, p. 229], there exists an integer n_0, such that for each $i > 0$ and each $n \geqslant n_0$ we have $H^i(\mathbb{P}_R^n, \psi_*\mathcal{G} \otimes \mathcal{L}^n) = 0$. Now $\mathcal{L}^n$ is a locally free sheaf and the projection formule (see for example [15, tag 01E8]) yields $\psi_*\mathcal{G} \otimes \mathcal{L}^n \cong \psi_*(\mathcal{G} \otimes \psi^*(\mathcal{L}^n))$. Remark that W and $\mathbb{P}_R^n$ are noetherian and separated over $\operatorname{Spec} R$. Hence, we can use Čech cohomology to conclude that $0 = H^i(\mathbb{P}_R^n, \psi_*(\mathcal{G} \otimes \psi^*(\mathcal{L}^n))) \cong H^i(W, \mathcal{G} \otimes \psi^*(\mathcal{L}^n))$. As $\psi^*(\mathcal{L}^n) \cong (\psi^*\mathcal{L})^n$, this yields that $\mathcal{L}$ is ample, by using [7, prop. III.5.3, p. 229] again. In particular W is projective over $\operatorname{Spec} R$. □

Let $g > 1$ be an integer. We are considering curves of the following form over $\mathbb{Q}$: $Z(y^2 - f(x, s)) \subset \mathbb{P}_{\mathbb{Q}}(1, 1, g+1)(x : s : y)$ where $f(x, s)$ is a homogeneous polynomial of degree $n := 2g + 2$ with coefficients in $\mathbb{Z}$ and without double zeros (in $\mathbb{P}_{\mathbb{C}}^1$). We will let f vary over the set of such polynomials.

First, we let $S = \operatorname{Spec}(\mathbb{Z}[\frac{1}{2}])$. Consider the scheme $H = \mathbb{A}_S^{n+1}(c_0, \ldots, c_n)$. It represents the functor that maps a $\mathbb{Z}[\frac{1}{2}]$-algebra R to the set of homogeneous polynomials in two variables x and s of degree n with coefficients in R, that is, for each $\mathbb{Z}[\frac{1}{2}]$-algebra R the set $H(R)$ is identified with set $\{\sum_{i=0}^{n} c_i x^i s^{n-i} \in R[x, s]\}$.

Definition 16. Let R be a ring. The *discriminant* $\Delta(f)$ of a polynomial $f = \sum_{i=0}^{n} c_i x^i s^{n-i}$ is defined as the determinant of the modified Sylvester

matrix

$$M_f := \begin{pmatrix} z & c_{n-1} & c_{n-2} & \dots & 0 & 0 & 0 \\ 0 & c_n & c_{n-1} & \dots & 0 & 0 & 0 \\ 0 & 0 & c_n & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & c_1 & c_0 & 0 \\ 0 & 0 & 0 & \dots & c_2 & c_1 & c_0 \\ zn & (n-1)c_{n-1} & (n-2)c_{n-2} & \dots & 0 & 0 & 0 \\ 0 & nc_n & (n-1)c_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2c_2 & 1c_1 & 0 \\ 0 & 0 & 0 & \dots & 3c_3 & 2c_2 & 1c_1 \end{pmatrix},$$

where $z = (-1)^{\frac{n(n-1)}{2}}$, the first $n-1$ rows contain the coefficients of $f(x,1)$ and the last n rows contain the coefficients of $\frac{\partial f}{\partial x}(x,1)$.

One easily sees that the discriminant $\Delta(f)$ can be expressed as a polynomial in $\mathbb{Z}[c_0,\dots,c_n]$, which we will denote by Δ.

Proposition 17. *Let k be a field and suppose that the homogeneous polynomial $f = \sum_{i=0}^{n} c_i x^i s^{n-i} \in k[x,s]$ factors as $\prod_{j=1}^{n}(\alpha_j x - \beta_j s) \in \overline{k}[x,s]$. Then $\Delta(f) = \prod_{j<\ell}(\alpha_\ell\beta_j - \alpha_j\beta_\ell)^2$.*

Proof. As the equality that we need to prove is an algebraic one it suffices to prove it on the Zariski dense subset $\bigcap_{j=1}^{n} D(\alpha_j)$ of $\mathbb{A}_{\overline{k}}^{2n}(\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n)$. Now $f(x,1)$ factors as $a\prod_{j=1}^{n}(x-\gamma_j)$ where $a = \prod_{j=1}^{n}\alpha_j$ and $\gamma_j = \frac{\beta_j}{\alpha_j}$. By the theory of discriminants on univariate polynomials (see for example [10, prop. 8.5, p. 204]) we know that $\Delta(f) = a^{2n-2}\prod_{j<\ell}(\gamma_j-\gamma_\ell)^2 = \prod_{j<\ell}(\alpha_\ell\beta_j-\alpha_j\beta_\ell)^2$. □

First we will define what it means for a hyperelliptic curve to have good, bad and semistable reduction.

Definition 18. For a scheme $X/\operatorname{Spec}\mathbb{Q}$ and a ring $\mathbb{Z}\subset R\subset\mathbb{Q}$ we define an *R-model of X* to be a scheme $\mathfrak{X}/\operatorname{Spec}R$ together with an isomorphism $\mathfrak{X}_\eta \cong X$, where η is the generic point of $\operatorname{Spec}R$. We say that the model is *proper/projective/flat/smooth/normal* if $\mathfrak{X}/\operatorname{Spec}R$ is.

Definition 19. Let $X/\operatorname{Spec}\mathbb{Q}$ be a proper smooth scheme and let $p\in\mathbb{Z}$ be a prime number. Then we say that X has *good reduction at p* if there exists a proper smooth $\mathbb{Z}_{(p)}$-model $\mathfrak{X}$ of X. We say that X has *bad reduction at p* if it does not have good reduction.

Definition 20. Let k be a field and let $C/\operatorname{Spec} k$ be a scheme, locally of finite type, whose irrreducible components are of dimension 1. We call C *semistable* if $C_{\overline{k}}$ is reduced and if its singular points are ordinary double points, i.e., for every singular point $x \in C_{\overline{k}}$ there is an isomorphism $\widehat{\mathcal{O}}_{C_{\overline{k}},x} \cong \overline{k}[[T_1, T_2]]/(T_1T_2)$.

Definition 21. Let $X/\operatorname{Spec}\mathbb{Q}$ be a smooth projective scheme of dimension 1 and let $p \in \mathbb{Z}$ be a prime number. Then we say that X has *semistable reduction at p* if there exists a proper flat $\mathbb{Z}_{(p)}$-model $\mathfrak{X}$ of X such that $(\mathfrak{X} \times_{\operatorname{Spec}\mathbb{Z}_{(p)}} \operatorname{Spec}\mathbb{F}_p)/\operatorname{Spec}\mathbb{F}_p$ is semistable.

Theorem 22. *Let g be a positive integer and let $f(x,s) \in \mathbb{Z}[x,s]$ be a homogeneous polynomial of degree $n = 2g+2$. Let C be the scheme given by $y^2 = f(x,s)$ inside $\mathbb{P}_{\mathbb{Q}}(1,1,g+1)(x:s:y)$. Let p be an odd prime. If $p \nmid \Delta(f)$, then C has good reduction at p. If $p \mid \Delta(f)$ and $p^2 \nmid \Delta(f)$, then C has semistable bad reduction at p.*

Proof. First consider the model $\mathcal{C} = Z(y^2 - f(x,s))$ of C inside the weighted projective space $\mathbb{P}_{\mathbb{Z}_{(p)}}(1,1,g+1)(x:s:y)$ over $\mathbb{Z}_{(p)}$. It is weighted projective, hence it is projective by lemma 15. We will check that $\mathcal{C}$ is flat over $\mathbb{Z}_{(p)}$. As there are no points on $\mathcal{C}$ with $x = s = 0$, it suffices to consider the affine open $D_+(s) \cap \mathcal{C} \subset \mathcal{C}$ (the other affine open $D_+(x) \cap \mathcal{C}$ can be treated analogously). This affine open is isomorphic to $Z(y^2 - f(x,1)) \subset \mathbb{A}^2_{\mathbb{Z}_{(p)}}(x,y)$ just like in example 14. The $\mathbb{Z}_{(p)}$-module $\mathbb{Z}_{(p)}[x,y]/(y^2 - f(x,1))$ is free with basis $\{x^i y^j : (i,j) \in \mathbb{Z}_{\geqslant 0} \times \{0,1\}\}$, in particular it is flat.

Now, by proposition 17, $\overline{f(x,1)} \in \mathbb{F}_p[x]$ has no double zeros in $\overline{\mathbb{F}_p}$ if $p \nmid \Delta$. If $p \mid \Delta$ and $p^2 \nmid \Delta$, then $\overline{f}$ has exactly one double zero and no zeros of higher order by the same proposition. Applying lemma 11 we find that $\mathcal{C}$ is smooth if $p \nmid \Delta(f)$ and it is semistable if $p \mid \Delta(f)$ and $p^2 \nmid \Delta(f)$. In particular this proves the first part of the theorem. To prove that C has bad reduction at p in the latter case, we need to check that every other proper flat model is not smooth.

Suppose on the contrary that there does exist a proper smooth model $\mathcal{C}$ of C. Because $\operatorname{Spec}\mathbb{Z}_{(p)}$ is a regular noetherian scheme and $\mathcal{C} \to \operatorname{Spec}\mathbb{Z}_{(p)}$ is a smooth morphism, $\mathcal{C}$ is regular by [12, th. 3.36, p. 142]. In particular the connected components of $\mathcal{C}$ are normal by [12, th. 2.17, p. 130]. Furthermore, $\mathcal{C} \to \operatorname{Spec}\mathbb{Z}_{(p)}$ is flat, its generic fibre is integral, as it is isomorphic to $Z(y^2 - f(x,s)) \subset \mathbb{P}_{\mathbb{Q}}(1,1,g+1)(x:s:y)$, and $\operatorname{Spec}\mathbb{Z}_{(p)}$ is integral. Hence, [12, prop. 3.8, p. 137] yields that $\mathcal{C}$ is integral. Hence, it is connected and it is normal. □

Now let p be an odd prime number. Inside $H = \mathbb{A}_S^{n+1}(c_0, \ldots, c_n)$ we consider the closed subschemes $H_i := Z(\Delta - ip) \subset H$ for $i = 0, \ldots, p-1$. Let $S_i \subset H_i$ be the smooth locus of the map $H_i \to S$, it is an open subscheme of H_i. Let $N_i := H_i \setminus S_i$ be its complement with the induced reduced scheme structure.

Proposition 23. *Let k be a field of characteristic not two. Then, the scheme $H_0 \times_S \operatorname{Spec} \overline{k}$ is irreducible.*

Proof. Consider the map from $\mathbb{A}_{\overline{k}}^{2n}$ to $H \times_S \operatorname{Spec} \overline{k}$ mapping the $2n$-tuple $(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n)$ to the polynomial $(\alpha_1 x - \beta_1 s) \cdot \ldots \cdot (\alpha_n x - \beta_n s)$. Over $\overline{k}$ every univariate polynomial factors in linear factors and therefore every bivariate homogeneous polynomial factors in linear factors. Hence, this map is surjective.

Inside $\mathbb{A}_{\overline{k}}^{2n}$ consider the closed subscheme given by $\{\alpha_1 = \alpha_2 \wedge \beta_1 = \beta_2\}$. It is irreducible and by applying proposition 17 we see that it surjects onto $H_0 \times_S \operatorname{Spec} \overline{k}$. As the image of an irreducible set is irreducible this proves that $H_0 \times_S \operatorname{Spec} \overline{k}$ is irreducible. □

Lemma 24. *The scheme H_0 has a smooth point which lies in the fibre of $\operatorname{Spec} \mathbb{F}_p \subset S$.*

Proof. Let $\sum_{i=0}^{n-2} h_{i+2} x^i \in \mathbb{F}_p[x]$ be a separable polynomial of degree $n-2$ not divisible by x, e.g. the minimal polynomial of a non-zero generator of $\mathbb{F}_{p^{n-2}}/\mathbb{F}_p$. Then consider the point $P \in H_0$ representing the homogeneous polynomial $h = \sum_{i=2}^{n} h_i x^i s^{n-i} \in \mathbb{F}_p[x, s]$ in H_0. Then the claim is that P is a smooth point of H_0.

To prove the latter we will calculate the tangent space at P of H_0 and H. The tangent space can be identified to the set of morphisms ρ from $\operatorname{Spec}(\mathbb{F}_p[\varepsilon]/\varepsilon^2)$ to H_0 resp. H such that the image of ρ is P. That is, the tangent space of H at P consists of polynomials $f = \sum_{i=0}^{n} f_i x^i s^{n-i} \in \mathbb{F}_p[\varepsilon, x, s]/\varepsilon^2$ such that the reduction $\overline{f} \in \mathbb{F}_p[x, s]$ is equal to h. The tangent space of H_0 at P is the subspace consisting of these polynomials f that satisfy $\Delta(f) = 0$. We will prove that this subspace has codimension 1. As P is a smooth point of H, this will immediately prove that P is a smooth point in the fibre above p of H_0.

Consider the modified Sylvester matrix of f, where $z = (-1)^{\frac{n(n-1)}{2}}$:

$$\begin{pmatrix} z & f_{n-1} & f_{n-2} & \dots & 0 & 0 & 0 \\ 0 & f_n & f_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & f_1 & f_0 & 0 \\ 0 & 0 & 0 & \dots & f_2 & f_1 & f_0 \\ zn & (n-1)f_{n-1} & (n-2)f_{n-2} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2f_2 & f_1 & 0 \\ 0 & 0 & 0 & \dots & 3f_3 & 2f_2 & f_1 \end{pmatrix}$$

Now, we are going to calculate its determinant by expanding at the rightmost column. Remark that f_0 and f_1 will be multiples of ε as h is a multiple of x^2. For this reason, the contribution from the bottom entry in the rightmost column, f_1, will be zero, as all entries except the bottom entry of the second rightmost column are also multiples of ε. Hence, we only get a non-zero contribution from the n-th entry of the rightmost column, f_0. If we then expand the residual matrix in the rightmost column, we see that we only get a non-zero contribution from the bottom entry, $2f_2$. To summarize, the determinant of the matrix is equal to

$$\tau := (-1)^{(2n-1)+(n-1)+(2n-2)+(2n-2)} \cdot 2f_1f_2 \cdot \det M = (-1)^n \cdot 2f_1f_2 \cdot \det M,$$

where

$$M = \begin{pmatrix} z & f_{n-1} & f_{n-2} & \dots & 0 & 0 \\ 0 & f_n & f_{n-1} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & f_1 & 0 \\ 0 & 0 & 0 & \dots & f_2 & f_1 \\ zn & (n-1)f_{n-1} & (n-2)f_{n-2} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2f_2 & 0 \\ 0 & 0 & 0 & \dots & 3f_3 & 2f_2 \end{pmatrix}$$

As f_1 is a multiple of ε, we get that $\tau = (-1)^n \cdot 2f_1h_2 \cdot \det \overline{M}$, where $\overline{M}$ is the reduction of M to $\mathbb{F}_p$. Remark, that by subtracting the first row from the n-th row in $\overline{M}$, the second row from the $n+1$-st row, the third row from the $n+2$-nd row, and so on, we get the following matrix, where we define h_1

to be zero.

$$\begin{pmatrix} z & h_{n-1} & h_{n-2} & \dots & 0 & 0 \\ 0 & h_n & h_{n-1} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_1 & 0 \\ 0 & 0 & 0 & \dots & h_2 & h_1 \\ z(n-1) & (n-2)h_{n-1} & (n-3)h_{n-2} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_2 & 0 \\ 0 & 0 & 0 & \dots & 2h_3 & h_2 \end{pmatrix}$$

The determinant of $\overline{M}$ is equal to the determinant of the above matrix which is, by definition, equal to the determinant of $\frac{h}{x}$. As $\sum_{i=0}^{n-2} h_{i+2}x^i$ was chosen to be separable and not divisible by x, also the polynomial $h_n x^{n-1} + \ldots + h_1$ is separable. Remark that this in particular implies that $h_2 \neq 0$. Hence, by proposition 17, its discriminant is non-zero. Now, $(-1)^n$, 2, h_2 and $\det \overline{M}$ are all non-zero. Hence, $\tau = 0$ is equivalent to the non-zero linear condition $f_1 = 0$ and the tangent space has indeed codimension 1, as we wanted to prove.

Now we will use the third criterion of [15, tag 01V9] to prove that P is a smooth point of H_0. Remark that the stalk of the sheaf of differentials is dual to the tangent space, by [15, tag 00TR]. Hence, the only thing that we need to check is that the map of local rings $\mathbb{Z}_{(p)} = \mathcal{O}_{S,p} \to \mathcal{O}_{H_0,P}$ is flat. In fact, we will prove that H_0/S is flat.

We already showed that the irreducible scheme $H_0 \times_S \operatorname{Spec} \overline{\mathbb{F}_p}$ has a smooth point. In particular, Δ must be irreducible in $\overline{\mathbb{F}_p}[c_0, \ldots, c_n]$, hence it is also irreducible in $\mathbb{Q}[c_0, \ldots, c_n]$. Hence, H_0 is an integral scheme. For every odd prime number ℓ there exist separable polynomials over $\mathbb{F}_\ell$, i.e., not all coefficients of Δ are divisible by ℓ. Hence, the morphism $H_0 \to S$ is not constant and hence [12, cor. 4.3.10, p. 137] implies that it is flat. □

Corollary 25. *For every $i = 0, \ldots, p-1$ the scheme H_i is irreducible of dimension $n+1$.*

Proof. We know that $X := H_0 \times_S \operatorname{Spec} \mathbb{F}_p$ is irreducible by proposition 23 and that $X \neq H \times_S \operatorname{Spec} \mathbb{F}_p = \mathbb{A}^{n+1}_{\mathbb{F}_p}$ as there exist separable polynomials of degree n over $\mathbb{F}_p$. Hence, X is a hypersurface and $\overline{\Delta} \in \mathbb{F}_p[c_0, \ldots, c_n]$ must be a power of an irreducible polynomial. By proposition 24 we know that

X has at least one smooth point. Hence, $\overline{\Delta}$ actually must be an irreducible polynomial.

Remark that Δ is homogeneous of degree $2n-2$ and one of the coefficients of Δ is not divisible by p by the observations just made. Hence, $\Delta - ip \in \mathbb{Z}[c_0, \ldots, c_n]$ is irreducible for all $i = 0, \ldots, p-1$. This implies that H_i is irreducible. As H_i is a hypersurface of $\mathbb{A}_S^{n+1}$ which has dimension $n+2$, it has dimension $n+1$. □

Theorem 26. *For every $i = 0, \ldots, p-1$ the space N_i has dimension at most n.*

Proof. As $H_i \times_S \operatorname{Spec} \mathbb{F}_p$ is naturally isomorphic to $H_0 \times_S \operatorname{Spec} \mathbb{F}_p$, we know by lemma 24 that H_i has a smooth point. Therefore, N_i is a closed subscheme of H_i and it does not contain all points of H_i. By corollary 25 we have that H_i is an irreducible scheme of dimension $n+1$. Hence, N_i has dimension at most n. □

Again we will use lemma 5 to do some counting. Let X be an open subset of $H = \mathbb{A}_S^{n+1}$ such that $X \cap H_i = S_i$ and equip it with the structure of an open subscheme of H. Write $X = \bigcup_{j=1}^m D(g_j)$ for some polynomials $g_j \in \mathbb{Z}[\frac{1}{2}, c_0, \ldots, c_n]$.[2] Let s_p be the number of elements of $S_0(\mathbb{F}_p)$ and let n_p be the number of elements of $H_0(\mathbb{F}_p) \setminus S_0(\mathbb{F}_p) \cong N_0(\mathbb{F}_p)$.

Lemma 27. *There exists a constant C, such that for every odd prime p there are at least $p^{2n+1} - Cp^{2n+\frac{1}{2}}$ elements $(a_0, \ldots, a_n) \in (\mathbb{Z}/p^2\mathbb{Z})^{n+1}$ satisfying $\Delta(a_0, \ldots, a_n) \in \{p, 2p, \ldots, p^2 - p\} \subset \mathbb{Z}/p^2\mathbb{Z}$.*

Proof. By proposition 23 we know that $H_0 \times_S \operatorname{Spec} \mathbb{F}_p$ is absolutely irreducible of dimension n. In particular, $S_0 \times_S \operatorname{Spec} \mathbb{F}_p$ is reduced, absolutely irreducible of dimension n, because it is a non-empty open subscheme and it is smooth over the base. As S_0 is of the form of the scheme in theorem 52, we can apply the Lang-Weil estimate of theorem 52 to conclude that there exists a constant D not depending on p, such that $|s_p - p^n| \leqslant Dp^{n-\frac{1}{2}}$.

Now we are going to apply lemma 5. Remarking that $S_i(\mathbb{F}_p) = S_0(\mathbb{F}_p)$ for all $i = 0, \ldots, p-1$, this lemma will tell us that for each $i = 0, \ldots, p-1$ the set $S_i(\mathbb{Z}/p^2\mathbb{Z})$ contains $p^n \cdot s_p$ elements. That is, each of these sets contains at least $p^{2n} - Dp^{2n-\frac{1}{2}}$ elements.

[2] Here we could take the g_j to be the derivatives of Δ.

Remark that $S_i(\mathbb{Z}/p^2\mathbb{Z})$ only contains elements $(a_0, \ldots, a_n) \in (\mathbb{Z}/p^2\mathbb{Z})^{n+1}$ that satisfy $\Delta(a_0, \ldots, a_n) = i \cdot p \in \mathbb{Z}/p^2\mathbb{Z}$. Hence, there are at least

$$(p-1)(p^{2n} - Dp^{2n-\frac{1}{2}}) = p^{2n+1} - Dp^{2n+\frac{1}{2}} - p^{2n} + Dp^{2n-\frac{1}{2}} \geqslant p^{2n+1} - Cp^{2n+\frac{1}{2}}$$

elements in $(\mathbb{Z}/p^2\mathbb{Z})^{n+1}$ satisfying the conditions of the lemma statement, where we take C to be $2D + 1$. □

Now we are ready to state and prove an analogue of theorem 9 for hyperelliptic curves. Let $L \subset \mathbb{Z}^{n+1}$ be the subset of $n+1$-tuples $(c_0, \ldots, c_n)$ such that $\Delta(c_0, \ldots, c_n) \neq 0$, i.e. such that $f = c_n x^n + c_{n-1} x^{n-1} s + \ldots + c_0 s^n$ does not have a double zero. Such an $n+1$-tuple defines a hyperelliptic curve over $\mathbb{Q}$ by means of the equation $y^2 = f$. Such a tuple is called *nowhere bad semistable* if the corresponding hyperelliptic curve does not have bad semistable reduction at p for every prime p. For any $B \in \mathbb{R}$ let L_B the subset of $n+1$-tuples $(c_0, \ldots, c_n)$ such that $|c_i| \leqslant B$ for $i = 0, \ldots, n$.

Corollary 28. *For every $B \in \mathbb{R}$ let $Q_B \subset L_B$ be the subset of tuples $(c_0, \ldots, c_n)$ such that there does not exist a prime p satisfying $p \mid \Delta(c_0, \ldots, c_n)$ and $p^2 \nmid \Delta(c_0, \ldots, c_n)$. Then $\limsup_{B\to\infty} \frac{|Q_B|}{|L_B|} = 0$.*

Proof. Let $p_1, p_2, \ldots$ be the odd prime numbers ordered in the usual way and let $k \in \mathbb{Z}_{>0}$ be a positive integer. Let $M_k = \prod_{i=1}^{k} p_i^2$. For $B \in \mathbb{R}_{>0}$ let $I_B = \{-\lfloor B \rfloor, \ldots, \lfloor B \rfloor\} \subset \mathbb{Z}$. Let Q be the largest integer multiple of M smaller than B. In I_B^{n+1} we consider the subset Ω of $n+1$-tuples $(a_0, \ldots, a_n)$ such that $\Delta(a_0, \ldots, a_n) \equiv p, 2p, \ldots,$ or $p^2 - p \mod p^2$ for some $p \in \{p_1, \ldots, p_k\}$.

For every $p \in \{p_1, \ldots, p_k\}$ at least $p^{2n+1} - Cp^{2n+\frac{1}{2}}$ of the p^{2n+2} residue classes (A, B) of $(\mathbb{Z}/p_i^2\mathbb{Z})^{n+1}$ satisfy the condition $\Delta(A, B) = p, 2p, \ldots,$ or $p^2 - p$. That is, there are at most $p^{2n+2} - p^{2n+1} + Cp^{2n+\frac{1}{2}}$ elements that do not satisfy the conditions.

By applying the Chinese remainder theorem we get that there are at most $\prod_{i=1}^{k}(p_i^{2n+2} - p_i^{2n+1} + Cp_i^{2n+\frac{1}{2}})$ classes $(A_0, \ldots, A_n)$ in $(\mathbb{Z}/M_k\mathbb{Z})^{n+1}$ for which there is no i such that $\Delta(A_0, \ldots, A_n) \equiv p_i, 2p_i, \ldots,$ or $p_i^2 - p_i \mod p_i^2$. Each class $(A_0, \ldots, A_n) \in (\mathbb{Z}/M_k\mathbb{Z})^{n+1}$ has at least $(\frac{2Q}{M_k})^{n+1}$ and at most $(\frac{2Q}{M_k} + 4)^{n+1}$ representatives in I_B^{n+1}.

Remark that every tuple $(c_0, \ldots, c_n)$ satisfying both $p \mid \Delta(c_0, \ldots, c_n)$ and $p^2 \nmid \Delta(c_0, \ldots, c_n)$, also satisfies $\Delta(a_0, \ldots, a_n) \neq 0$. Hence, $L_B \setminus Q_B$ contains

at least

$$\left(\frac{2Q}{M_k}\right)^{n+1}\left(M_k^{n+1}-\prod_{i=1}^{k}\left(p_i^{2n+2}-p_i^{2n+1}+Cp_i^{2n+\frac{1}{2}}\right)\right)$$
$$=(2Q)^{n+1}\left(1-\prod_{i=1}^{k}\left(1-p_i^{-1}+Cp_i^{-\frac{3}{2}}\right)\right)$$

elements. Furthermore I_B contains at most $1+2Q+2M_K \leqslant 2Q+4M_k$ elements, hence L_B contains at most $(2Q+4M_K)^{n+1}$ elements. We combine the two inequalities to get

$$\frac{|L_B \setminus Q_B|}{|L_B|} \geqslant U_{k,B} := \left(\frac{2Q}{2Q+4M_k}\right)^{n+1} \cdot \left(1-\prod_{i=1}^{k}\left(1-p_i^{-1}+Cp_i^{-\frac{3}{2}}\right)\right).$$

Remark that $p_i^{-1}-Cp_i^{-\frac{3}{2}} \sim p_i^{-1}$ as $i \to \infty$. Hence, $\sum_{i=1}^{M} p_i^{-1}-Cp_i^{-\frac{3}{2}} \to \infty$ if $M \to \infty$ and by the product convergence criterion (see for example [8, th. 4, p. 220]), the product $\prod_{i=1}^{\infty}(1-p_i^{-1}+Cp_i^{-\frac{3}{2}})$ must converge to 0. In particular, we have

$$1-\limsup_{B\to\infty}\frac{|Q_B|}{|L_B|}=\liminf_{B\to\infty}\frac{|L_B\setminus Q_B|}{|L_B|} \geqslant \lim_{k\to\infty}\lim_{B\to\infty} U_{k,B}$$
$$=1-\prod_{i=1}^{\infty}\left(1-p_i^{-1}+Cp_i^{-\frac{3}{2}}\right)=1.$$

Hence, $\limsup_{B\to\infty}\frac{|Q_B|}{|L_B|} \leqslant 0$ and the other inequality trivially holds. □

Corollary 29. *For every $B \in \mathbb{R}$ let $W_B \subset L_B$ be the subset of nowhere bad semistable tuples. Then* $\limsup_{B\to\infty}\frac{|W_B|}{|L_B|}=0$.

Proof. For any tuple $(c_0,\ldots,c_n)$ such that we have $p \mid \Delta(c_0,\ldots,c_n)$ and $p^2 \nmid \Delta(c_0,\ldots,c_n)$ for some odd prime number p, its associated hyperelliptic curve has bad semistable reduction at p by theorem 22. The statement now follows immediately from corollary 28. □

3 Semi-abelian reduction of hyperelliptic Jacobians

Suppose that we have a hyperelliptic curve C over $\mathbb{Q}$ given by $y^2 = f(x, s)$ and suppose that the discriminant of f is divisible exactly once by the prime number p. Then we will prove that the Jacobian of C has bad semi-abelian reduction of toric rank 1 at p. In particular, by corollary 28 for almost all hyperelliptic Jacobians there is a prime p such that its reduction at p has this property.

First let us give some definitions.

Definition 30. A *group scheme* over S is a scheme G/S together with a factorisation of the functor of points $\mathbf{Sch}/S \to \mathbf{Set}$ through the forgetful functor $\mathbf{Grp} \to \mathbf{Set}$. For two group schemes G/S and H/S a *morphism* from G to H is a morphism of schemes $G \to H$, such that for each object $X \in \mathbf{Sch}/S$, the map $G(X) \to H(X)$ is a morphism of groups. A group scheme G/S is called *commutative* if all groups $G(X)$ for $X \in \mathbf{Sch}/S$ are abelian.

Example 31. Let k be a field and let $\mathbb{G}_m$ be the scheme $\mathrm{Spec}\,(k[x, x^{-1}])$. For every scheme X/k the set $\mathbb{G}_m(X) = \{k[x, x^{-1}] \to \mathcal{O}_X(X)\} = \mathcal{O}_X(X)^*$ is a group by taking the product of $\mathcal{O}_X(X)^*$ as the group operation. This is functorial and hence it gives a factorisation $\mathbf{Sch}/S \to \mathbf{Grp} \to \mathbf{Set}$ of $\mathbb{G}_m(-)$. The induced group scheme is also denoted by $\mathbb{G}_m$. It is a commutative group scheme.

Definition 32. Let G be a group scheme over S. Then we define the *unit section* of G to be the morphism $e_G : S \to G$ that is the identity element of the group $G(S)$.

Remark 33. By [15, tag 047L] a group scheme over a field is always separated.

Definition 34. Let $f : G \to H$ be a morphism of group schemes over S. Then we define the *kernel* of f to be $\ker f : G \times_H S \to G$, where we consider S to be an H-scheme via the unit section e_H and $\ker f$ is the first projection.

Remark 35. We will show that the scheme $K := G \times_H S$ is a group scheme over S. For every $X \in \mathbf{Sch}/S$ the group $K(X)$ consists of these elements of $(g, s) \in G(X) \times S(X)$ such that $f_X(g) = (e_H)_X(s)$. Note that the group $S(X)$ has one element, namely the structure morphism $s : X \to S$ of X/S. By functoriality we have that $(e_H)_X(s) = e_H \circ s \in H(X)$ is the identity

element. Hence, $K(X)$ can be identified with the subset of elements in $G(X)$ that map to the identity element in $H(X)$, i.e., the kernel of $G(X) \to H(X)$. This gives K the structure of a group scheme.

Now we are ready to define the main objects of this chapter.

Definition 36. Let S be a scheme and $g \in \mathbb{Z}_{\geqslant 0}$ a non-negative integer. An *abelian scheme of relative dimension g over S* is a group scheme A/S that is proper, smooth, and whose geometric fibres are connected and of dimension g.

Definition 37. Let k be a field, let $A = \mathbb{G}_m^n$ over k for some $n \in \mathbb{Z}_{\geqslant 0}$, let C be an abelian scheme over $\operatorname{Spec} k$ and let B be a group scheme over $\operatorname{Spec} k$. Let $0 \to A \to B \to C \to 0$ be a sequence of morphisms of group schemes over $\operatorname{Spec} k$. Then we say that this sequence is an *exact sequence* if $B \to C$ is smooth and surjective, and $A \cong \ker(B \to C)$ both as scheme over B and as group scheme over $\operatorname{Spec} k$.

Remark 38. In general a sequence of group schemes $0 \to A \to B \to C \to 0$ is said to be exact if A is the kernel of $B \to C$ and $B \to C$ is surjective in the fppf topology. In our case these two definitions are equivalent. Namely, if $B \to C$ is smooth surjective, then it is fppf and hence surjective in the fppf topology. On the other hand, suppose that $B \to C$ is surjective in the fppf topology. Then this yields that there exists a diagram

$$\begin{array}{ccc} & & C' \\ & \swarrow & \downarrow{\scriptstyle g} \\ B & \longrightarrow & C \end{array}$$

such that g is fppf. In particular, the map $p : B \to C$ from the exact sequence is surjective. By base changing to B using the map p, we get a diagram

$$\begin{array}{ccccc} C' \times_C B & \longrightarrow & B \times_C B & \xrightarrow{p_2} & B \\ \downarrow{\scriptstyle p'} & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle p} \\ C' & \longrightarrow & B & \longrightarrow & C \\ & \searrow & & \nearrow & \\ & & {\scriptstyle g} & & \end{array}$$

in which p_1 and p_2 are the projections onto the first and second coordinate and the two squares are cartesian. The morphism $\psi : B \times_{\operatorname{Spec} k} A \to B \times_C B$ that maps (b, a) to (b, ab) is an isomorphism. Furthermore $p_1 \circ \psi$ is the first projection $B \times_{\operatorname{Spec} k} A \to B$ and as a base change of the smooth morphism

$A \to \operatorname{Spec} k$ it is smooth. Hence, p_1 is smooth and hence also p' is smooth. By [15, tag 02VL] smoothness is fppf-local on the base, hence p is smooth as g is fppf.

Definition 39. Let k be an algebraically closed field, let $G/\operatorname{Spec} k$ be a commutative group scheme and let r be a non-negative integer. Then G is called a *semi-abelian of toric rank* r if it is smooth and connected and there exists an abelian scheme $A/\operatorname{Spec} k$ and an exact sequence $0 \to \mathbb{G}_m^r \to G \to A \to 0$.

Lemma 40. *Let k be an algebraically closed field and let $G/\operatorname{Spec} k$ be a group scheme. Let r, r' be two non-negative integers such that G is semi-abelian of toric rank both r and r'. Then $r = r'$.*

Proof. Suppose that two exact sequences $0 \to \mathbb{G}_m^r \to G \to A \to 0$ and $0 \to \mathbb{G}_m^{r'} \to G \to A' \to 0$ as in definition 39 are given. Let g and g' be the relative dimensions of A respectively A' over $\operatorname{Spec} k$. We will prove that the relative dimension of G over A (resp. A') is the same as the relative dimension of its kernel $\mathbb{G}_m^r$ (resp. $\mathbb{G}_m^{r'}$) over $\operatorname{Spec} k$, which is r (resp. r'). Then we find that $r + g = r' + g'$.

To prove our claim we will use [15, tag 02NM]. Remark that $G \to A$ is smooth surjective by definition. In particular it is flat and locally of finite presentation. Moreover, as $A \to \operatorname{Spec} k$ is smooth, also $G \to \operatorname{Spec} k$ is smooth. Hence, G is locally noetherian and hence the fibres of $G \to A$ are locally noetherian. Furthermore, all local rings of these fibres are Cohen-Macaulay, because they are regular local rings. Hence, the fibres are Cohen-Macaulay and we can apply the lemma. As G is connected, it will follow that $G \to A$ is equidimensional of some relative dimension d and then the base change $\mathbb{G}_m^r \to \operatorname{Spec} k$ must be equidimensional of that same dimension d. Then we get that $d = r$ (resp. $d = r'$ for the morphism $G \to A'$) and we are done.

Next we will prove that the sequence $0 \to \mathbb{G}_m^r(k) \to G(k) \to A(k) \to 0$ is still exact. The left exactness follows from remark 35. Remark that both G and A are locally of finite type over k. Hence, to prove surjectivity of the morphism $G(k) \to A(k)$ we may and will assume that

$$G = \operatorname{Spec}\left(\frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_m)}\right) \text{ and } A = \operatorname{Spec}\left(\frac{k[y_1, \ldots, y_k]}{(g_1, \ldots, g_\ell)}\right).$$

Suppose that $a \in A(k)$ is a point and let $\mathfrak{p}$ be the corresponding point (i.e. its image) of A. It is a closed point, hence its preimage is non-empty and closed. As G is of finite type over k, this implies that the preimage of $\mathfrak{p}$ contains a

closed point $\mathfrak{q}$. By the weak Nullstellensatz this point corresponds to a point of $G(k)$, because k is algebraically closed.

Let p be a prime number, not a multiple of $\operatorname{char} k$. Then consider the p-torsion subgroups of $\mathbb{G}_m^r(k)$, $G(k)$ and $A(k)$. By basic group theory, the sequence $0 \to \mathbb{G}_m^r(k)[p] \to G(k)[p] \to A(k)[p]$ is exact. Now we will prove that the last map is surjective. Let $a \in A(k)[p]$ be an element. Then there is a $g_1 \in G(k)$ that maps to it. Then $p \cdot g_1$ maps to 0 and hence it is the image of an element $f \in \mathbb{G}_m^r(k)$. Remark that $\mathbb{G}_m(k) = k^*$ is a p-divisible group, because k is algebraically closed and hence the equation $X^p - f$ has a solution. In particular $\mathbb{G}_m^r(k)$ is also p-divisible and $f = p \cdot h$ for some $h \in \mathbb{G}_m^r(k)$. Let g_2 be the image of h in $G(k)$ and consider $g := g_1 - g_2$. As g_2 maps to 0 in $A(k)$, this element maps to a. Furthermore, we have $p \cdot g = 0$ as the difference between f, which maps to $p \cdot g_1$, and $p \cdot h$, which maps to $p \cdot g_2$, is zero by construction. Hence, $g \in G(k)[p]$ lies in the preimage of a and the map is surjective.

In particular, we have an exact sequence

$$0 \to \mathbb{G}_m^r(k)[p] \to G(k)[p] \to A(k)[p] \to 0.$$

We know that $\mathbb{G}_m^r(k)[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^r$ as $\mathbb{Z}/p\mathbb{Z}$-module, because p is coprime to $\operatorname{char} k$ and hence k^* has exactly p roots of unity of order p. On the other hand, by [13, §6, p. 64], the group $A(k)[p]$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{2g}$. In particular, we find that $G(k)[p]$ has p^{2g+r} elements. Analogously, we find that it has $p^{2g'+r'}$ elements. We see that $r + 2g = r' + 2g'$. Altogether, this yields $r = r'$ and $g = g'$, which proves what we wanted to prove. □

Remark 41. In fact, there is even more we can say. As there are no non-trivial morphisms from a torus to an abelian variety, the tori $\mathbb{G}_m^r$ and $\mathbb{G}_m^{r'}$ are maximal inside G, hence, cf. [4, th. 6.6, p. 220], they are conjugated. As G is assumed to be commutative, this means that they are the same subgroup scheme of G. Then also the quotients A and A', taken in the fppf topology, are uniquely unique. In particular there is an isomorphism between the exact sequences $0 \to \mathbb{G}_m^r \to G \to A \to 0$ and $0 \to \mathbb{G}_m^{r'} \to G \to A \to 0$ that is the identity on the middle term, G.

Definition 42. A group scheme G/S is called *semi-abelian* if it is separated, smooth and all its geometric fibres are semi-abelian.

Definition 43. Let $A/\mathbb{Q}$ be an abelian scheme, let $r \geqslant 0$ be an integer and let p be a prime number. Then we say that A has *semi-abelian reduction of toric rank r at p* if there exists a semi-abelian model $\mathcal{A}/\mathbb{Z}_{(p)}$ such that the

fibre over $\overline{\mathbb{F}_p}$ has toric rank r. In the case $r = 0$, we also say that A has *good reduction at* p. We say that A has *bad reduction at* p if it does not have good reduction at p.

Lemma 44. *Let $A/\mathbb{Q}$ be an abelian scheme, let $r, r' \geqslant 0$ be integers and let p be a prime number. Suppose that A has semi-abelian reduction of both toric rank r and toric rank r' at p. Then $r = r'$.*

Proof. Let $\mathcal{A}/\mathbb{Z}_{(p)}$ and $\mathcal{A}'/\mathbb{Z}_{(p)}$ be semi-abelian models as in definition 43. Remark that $\mathbb{Z}_{(p)}$ is an integrally closed, noetherian, integral domain. By definition $\mathcal{A}$ and $\mathcal{A}'$ are smooth over $\mathbb{Z}_{(p)}$. Hence, because $\operatorname{Spec} \mathbb{Z}_{(p)}$ contains two points of which one is non-open, they are of finite type over $\mathbb{Z}_{(p)}$. Furthermore $\mathcal{A}$ and $\mathcal{A}'$ are separated over $\mathbb{Z}_{(p)}$. Now we are in the position to apply [6, prop. IX.3.2, p. 347]. As $\mathcal{A}$ and $\mathcal{A}'$ are connected, they are both isomorphic to the fibrewise connected component of the identity of the Neron model of A. In particular, $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic. The statement now follows from lemma 40. □

Next we will restate a statement about semistable curves we will need to use, but first we need define some notions.

A multigraph Γ is a tuple (V, E), where V is a finite set and E is a finite multiset whose elements are multisets of cardinality 2 containing only elements of V. In other words, Γ consists of a finite number of *vertices*, the elements of V, and a finite number of *edges*, the elements of E, connecting two vertices which do not necessarily need to be distinct. Also, there might be multiple edges between two points.

Suppose that X is a semi-stable curve over some algebraically closed field k. Then we will construct a multigraph, which will be called $\Gamma(X)$. Its vertices are the irreducible components of X. Every singular point is an ordinary double point. Hence, it lies on exactly two components if counted with multiplicity. The edges of $\Gamma(X)$ correspond to the singular points of X and they connect the two irreducible components the singular point lies on.

Furthermore, for a multigraph $\Gamma = (V, E)$, the first cohomology group is $H^1(\Gamma, \mathbb{Z})$. It can be viewed in the following way. Suppose that each edge is assigned an arbitrary orientation. Then $H^1(\Gamma, \mathbb{Z})$ is the subset of assignments of integers to all edges of Γ, i.e. the subset of $\mathbb{Z}^E$, such that at each vertex the sum of the integers assigned to the incoming edges equals the sum of the integers assigned to the outgoing edges. It is easy to check that this is unique

up to canonical isomorphism for the different choices of orientations on the edges of Γ.

Theorem 45 ([2, ex. 8, p. 246])**.** *Let X be a semi-stable curve over a field k. Then $\mathrm{Pic}^0_{X/k}$ is canonically an extension of an abelian variety by a torus T. The rank of the torus part T is equal to the rank of the cohomology group $H^1(\Gamma(X_{\overline{k}}), \mathbb{Z})$.*

Now we are ready to prove the main statement of this chapter.

Theorem 46. *Let $g \geqslant 1$ be an integer. Let $f \in \mathbb{Z}[x, s]$ be a homogeneous polynomial of degree $n = 2g + 2$. Let $C = Z(y^2 - f(x, s))$ inside the weighted projective space $\mathbb{P}_{\mathbb{Q}}(1, 1, g + 1)(x : s : y)$. Let p be an odd prime number such that $p \mid \Delta(f)$ and $p^2 \nmid \Delta(f)$, where Δ is defined as on page 13. Then the Jacobian $\mathrm{Pic}^0_{C/\mathbb{Q}}$ of C has bad semi-abelian reduction of toric rank 1 at p.*

Proof. Consider the model $\mathcal{C} = Z(y^2 - f(x, s)) \subset \mathbb{P}_{\mathbb{Z}_{(p)}}(1, 1, g + 1)(x : s : y)$ over $\operatorname{Spec} \mathbb{Z}_{(p)}$. Let k be an algebraic closure of $\mathbb{F}_p$. Then the geometric special fibre $\mathcal{C}_k$ has exactly one singular point, which is an ordinary double point. Furthermore, $f(x, s)$ is not a square in $k[x, s]$, as this would yield $p^2 \mid \Delta(f)$ because $n \geqslant 4$. Hence, $y^2 - f(x, s)$ is irreducible in $k[x, s, y]$ and $\mathcal{C}_k$ is integral. Then $\Gamma(\mathcal{C}_k)$ consists of 1 vertex and 1 edge that connects this vertex with itself. In particular, we see that $H^1(\Gamma(\mathcal{C}_k, \mathbb{Z})) \cong \mathbb{Z}$. By theorem 45 we get that $\mathrm{Pic}^0_{\mathcal{C}_k/k}$ is an extension of an abelian variety by a torus of rank 1. As $\mathrm{Pic}^0_{\mathcal{C}_k/k}$ is the connected component of the identity in $\mathrm{Pic}_{\mathcal{C}_k/k}$, it is connected. Furthermore, it is smooth by [5, prop. 9.5.19, p. 285]. Hence, it is semi-abelian of toric rank 1.

By lemma 15 the scheme $\mathcal{C}/\mathbb{Z}_{(p)}$ is projective. By [5, th. 9.4.8, p. 263] the scheme $\mathrm{Pic}_{\mathcal{C}/\mathbb{Z}_{(p)}}$ exists and is separated over $\operatorname{Spec} \mathbb{Z}_{(p)}$. By [5, prop. 9.5.19, p. 285] the scheme $\mathrm{Pic}_{\mathcal{C}/\mathbb{Z}_{(p)}}$ is smooth over $\operatorname{Spec} \mathbb{Z}_{(p)}$. By [1, th. XIII.4.7, p. 647] the fibrewise connected component of the identity is represented by an open subscheme $\mathrm{Pic}^0_{\mathcal{C}/\mathbb{Z}_{(p)}}$ of $\mathrm{Pic}_{\mathcal{C}/\mathbb{Z}_{(p)}}$. Now $\mathrm{Pic}^0_{\mathcal{C}/\mathbb{Z}_{(p)}}$ as an open subscheme of $\mathrm{Pic}_{\mathcal{C}/\mathbb{Z}_{(p)}}$ is separated and smooth over $\mathbb{Z}_{(p)}$. Its geometric fibres, $\mathrm{Pic}^0_{C_q/q}$ and $\mathrm{Pic}^0_{C_k/k}$, where q is an algebraic closure of $\mathbb{Q}$, are both semi-abelian, by the previous paragraph and theorem 45. The latter fibre has toric rank 1. Hence, $\mathrm{Pic}^0_{C/\mathbb{Q}}$ has semi-abelian reduction of toric rank 1 at p. By lemma 44 it must have bad reduction at p. □

Appendices

A Lang-Weil estimate

In 1954 Lang and Weil published their famous theorem estimating the number of rational points over a finite field on projective varieties. In the literature there are many varations of their theorem, but very often they are stated without proof. Here we try to derive the statement we want to use from the statements in their original paper.

First let us define some notions.

Definition 47. Let k be a field, $n, s \in \mathbb{Z}_{\geqslant 0}$ integers. Let $X \subset \mathbb{P}^n_k$ be a reduced projective scheme such that all its irreducible components have dimension s. Let $V \subset \mathbb{P}^n_{\overline{k}}$ be a linear subspace of $\mathbb{P}^n_{\overline{k}}$ of the form $Z(g_1, \ldots, g_s)$, where $g_1, \ldots, g_s$ are linear functions in the coordinates of $\mathbb{P}^n_{\overline{k}}$. Suppose that $\dim(V \cap X_{\overline{k}}) = 0$. Then *the degree of* X is defined as

$$\sum_{P \in V \cap X_{\overline{k}}} \dim_{\overline{k}} \left(\mathcal{O}_{X,P} / (g_1, \ldots, g_s) \right).$$

Remark 48. One can show that for any reduced projective scheme $X \subset \mathbb{P}^n_k$ there exists such a linear subspace V and furthermore that the quantity $\sum_{P \in V \cap X_{\overline{k}}} \dim_{\overline{k}} \mathcal{O}_{X,P}/(g_1, \ldots, g_s)$ does not depend on the choice of V. Furthermore, this definition coincides with the definition where one defines the degree as the number of intersection points with a linear subspace of dimension $n - s$ in general position, and with the definition where one defines the degree as a multiple of the leading coefficient of the Hilbert polynomial.

Example 49. Let k be a field. We will check that a hypersurface defined by a non-zero square-free homogeneous polynomial $f \in k[x_0, \ldots, x_n]$ of degree $d > 0$ has degree d. Consider the hypersurface $X := Z(f) \subset \mathbb{P}^n_k(x_0 : \ldots : x_n)$, which has dimenson $n - 1$. Then after a linear change of coordinates we may and will assume that f is not contained in $k[x_2, \ldots, x_n]$. Let V be $Z(x_2, \ldots, x_n) \subset \mathbb{P}^n_{\overline{k}}$. Then $V \cap X_{\overline{k}} = Z(f, x_2, \ldots, x_n) \subset \mathbb{P}^n_{\overline{k}}$ is isomorphic to $Z(g) \subset \mathbb{P}^1_{\overline{k}}(x_0 : x_1)$, where $g = f(x_0, x_1, 0, \ldots, 0)$ is non-zero, homogeneous of degree d. Hence, $V \cap X_{\overline{k}}$ contains finitely many points and for any point $P = (\alpha : \beta : 0 : \ldots : 0) \in C \cap X_{\overline{k}}$, the dimension $\dim_{\overline{k}} \mathcal{O}_{X,P}/(x_2, \ldots, x_n)$, is the number of times the factor $(\beta x_0 - \alpha x_1)$ occurs in g. Hence, the sum of these dimensions is d and the hypersurface $Z(f) \subset \mathbb{P}^n_k$ has degree d.

The following two results are from Lang and Weil's paper.

Theorem 50 ([9, p. 819])**.** *For each triple of non-negative integers (n, d, r) there exists a constant $A(n, d, r)$ such that for any finite field k and any reduced absolutely irreducible projective scheme $V \subset \mathbb{P}^n_k$ of dimension r and degree d we have*

$$|V(k) - q^r| \leqslant (d-1)(d-2)q^{r-\frac{1}{2}} + A(n, d, r)q^{r-1},$$

where $q = |k|$.

For any field k a positive cycle Z in $\mathbb{P}^n_k$ of degree $d > 0$ and dimension r is a finite formal sum $\sum_i a_i V_i$ with $a_i \in \mathbb{Z}_{>0}$ of reduced irreducible projective schemes $V_i \subset \mathbb{P}^n_k$ such that $d = \sum_i a_i \cdot \deg V_i$ and $\dim V_i = r$ for each i. A point on Z is an element of $(\bigcup_i V_i)(k)$.

Lemma 51 ([9, p. 820])**.** *There exists a constant $A_1(n, d, r)$ depending only on n, d and r such that for any finite field k and any positive cycle Z in $\mathbb{P}^n_k$, of degree d and of dimension r, Z has at most $A_1(n, d, r) \cdot q^r$ points, where $q = |k|$.*

The two results can be combined into a theorem that we will use in our estimates.

Theorem 52. *Let non-constant homogeneous polynomials $f, g_1, \ldots, g_m$ in $\mathbb{Z}[x_0, \ldots, x_n]$ be given. Consider the scheme V that is the closed subscheme of $\bigcup D_+(g_m) \subset \mathbb{P}^n_{\mathbb{Z}}$ given by $f = 0$. Let $\mathcal{P}$ be the set of primes for which $Z(f) \subset \mathbb{P}^n_{\mathbb{F}_p}$ is absolutely irreducible, reduced and of dimension $n-1$ and $V \times_{\mathbb{Z}} \mathbb{F}_p \neq \emptyset$. Then there exists a constant C such that for any prime $p \in \mathcal{P}$ we have*

$$|V(\mathbb{F}_p) - p^{n-1}| \leqslant Cp^{n-\frac{3}{2}}.$$

Proof. Let $p \in \mathcal{P}$ and let $V_p := V \times_{\mathbb{Z}} \mathbb{F}_p \subset \mathbb{P}^n_{\mathbb{F}_p}$ and let W_p be the closed subscheme $Z(f)$ of $\mathbb{P}^n_{\mathbb{F}_p}$. Then W_p is absolutely irreducible, reduced and of dimension $n-1$. Remark that the degree of W_p is the degree of f. Hence, by theorem 50 we know that $W_p(\mathbb{F}_p)$ has at most

$$p^{n-1} + (\deg(f) - 1)(\deg(f) - 2)p^{n-\frac{3}{2}} + B(n, \deg(f))p^{n-2}$$

elements, where for $w \in \mathbb{Z}$ we define $B(n, w) := \max_{0 \leqslant d \leqslant w} A(n, d, n-1)$, which does not depend on p. In particular this is also an upper bound for $|V(\mathbb{F}_p)|$.

On the other hand, $W_p(\mathbb{F}_p)$ has at least

$$l_p := p^{n-1} - (\deg(f)-1)(\deg(f)-2)p^{n-\frac{3}{2}} - B(n,\deg(f))p^{n-2}$$

elements. Unfortunately not every point of W_p is contained in V_p. For $j = 1,\dots,m$ let $T_{p,j} := Z(f,g_j) \subset \mathbb{P}^n_{\mathbb{F}_p}$. The points of W_p that are not contained in V_p are in one of the $T_{p,j}$. Hence, $|V_p(\mathbb{F}_p)| \geqslant l_p - |(\bigcup_j T_{p,j})(\mathbb{F}_p)|$.

As $V_p \neq \emptyset$ we have $T_{p,j} \subsetneq W_p$. In particular, the dimension of each irreducible component of $T_{p,j}$ is at most $n-2$ as W_p is irreducible. On the other hand, it is at least $n-2$ as it is a hypersurface in W_p. Hence, each irreducible component of $T_{p,j}$ has dimension $n-2$. Furthermore, by Bézout's theorem the degree of $T_{p,j}$ is at most $u_j := \deg(f)\deg(g_j)$ which does not depend on p. Consider the cycle Z which is defined as the sum of the irreducible components of the $T_{p,j}$. It has dimension $n-2$ and degree at most $u := \sum_j u_j$ and at least 0. Hence, by lemma 52 we get that $\bigcup_j T_{p,j}$ has at most $B_1(n,u)\cdot p^{n-2}$ points, where we define $B_1(n,u) := \max_{0\leqslant d\leqslant u} A_1(n,d,n-2)$, which does not depend on p.

If we combine the inequalities we get

$$|V_p(\mathbb{F}_p)| \geqslant p^{n-1} - (\deg(f)-1)(\deg(f)-2)p^{n-\frac{3}{2}} - (B(n,\deg(f)) + B_1(n,u))p^{n-2}.$$

In particular, we get the inequality of the theorem statement if we choose C to be $(\deg(f)-1)(\deg(f)-2) + B(n,\deg(f)) + B_1(n,u)$. □

Remark 53. By applying [15, tag 055A] to the generic point of $\operatorname{Spec}\mathbb{Z}$, we see that $\mathcal{P}$ is either finite if $Z(f) \subset \mathbb{P}^n_{\mathbb{Q}}$ does not have exactly one absolutely irreducible component, or cofinite in the set of primes if $Z(f) \subset \mathbb{P}^n_{\mathbb{Q}}$ has exactly one absolutely irreducible component.

References

[1] P. Berthelot, A. Grothendieck, L. Illusie. *Séminaire de Géométrie Algébrique du Bois Marie - 1966-67 - Théorie des intersections et théorème de Riemann-Roch (SGA 6)*. Spinger-Verlag, Berlin New York, 1971.

[2] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron Models*. Springer-Verlag, Berlin Heidelberg, 1990.

[3] M. Demazure, A. Grothendieck. *Séminarie de Géométrie Algébrique du Bois Marie - 1962/64 - Schémas en groupes (SGA 3) - vol. 1*. Springer-Verlag, Berlin New York, 1970.

[4] M. Demazure, A. Grothendieck. *Séminarie de Géométrie Algébrique du Bois Marie - 1962/64 - Schémas en groupes (SGA 3) - vol. 2*. Springer-Verlag, Berlin New York, 1970.

[5] B. Fantechi, L. Göttsche, L. Illusie, S.L. Kleiman, N. Nitsure, A. Vistoli. *Fundamental Algebraic Geometry. Grothendieck's FGA Explained*. American Mathematical Society, Providence, 2000.

[6] A. Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie - 1967-69 - Groupes de monodromie en géométrie algébrique (SGA 7 I)*. Springer-Verlag, Berlin Heidelberg New York, 1972.

[7] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[8] K. Knopp. *Theory and applications of infinite series*. Second Edition. Translated by R.C.H. Young. Blackie & Son limited, London and Glasgow, 1951.

[9] S. Lang, A. Weil. Number of Points of Varieties in Finite Fields, *American Journal of Mathematics* **74**.4 (1954): 819–827.

[10] S. Lang. *Algebra*. Revised 3rd edition. Springer-Verlag, New York Berlin Heidelberg, 2002.

[11] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète, *Transaction of the American Mathematical Society* **348**.11 (1996): 4577–4610.

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

[13] D. Mumford. *Abelian varieties*. Second edition. Oxford University Press, Oxford, 1985.

[14] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Second Edition. Springer, Dordrecht Heidelberg London New York, 2000.

[15] The Stacks Project Authors. *Stacks Project*. <`http://stacks.math.columbia.edu`>.

[16] S. Wong. On the Density of Elliptic Curves, *Compositio Mathematica* **127** (2001): 23–54.