Diss. ETH No. 19482

An effective proof of the hyperelliptic Shafarevich conjecture and applications

A dissertation submitted to
ETH Zurich

for the degree of
Doctor of Sciences

presented by
Rafael von Känel
MSc ETH Math., ETH Zurich
born August 7, 1985
citizen of Aeschi bei Spiez BE

Examiner:
Prof. Dr. Gisbert Wüstholz

Co-Examiners:
Prof. Dr. David Masser
PD Dr. Clemens Fuchs

2010

Curriculum Vitae

Personal

07.08.1985 Born in Lenzburg

Education

2009-2010 PhD studies at ETH Zurich under the supervision of Prof. G. Wüstholz, Assistent in the group of Prof. G. Felder

2008-2009 MSc in Mathematics at ETH Zurich with distinction, Grade: 6.0 (100/100), Teaching assistent in the group of Prof. G. Wüstholz

2008-2009 Six month exchange student in "Master 2 Analyse, arithmétique et géométrie" (joint program of École Polytechnique, École Normale Superieure and Université Paris-Sud 11), Orsay (Paris), France

2005-2008 BSc in Mathematics at ETH Zurich, Grade: 5.41 (88/100)

2001-2004 High school in Liestal, Grade: 4.5 (70/100)

1997-2001 Secondary school in Liestal

1992-1997 Primary school in Liestal

Prizes

May 2010 Willi Studer Prize 2010 of ETH Zurich for best Master student in 2009

May 2010 Medal 2010 of ETH Zurich for outstanding Master thesis in 2009

Oct. 2009 Polya Prize 2009 of the Departement of Mathematics ETH Zurich for best Master degree in 2009

Acknowledgments

This version (December 17, 2010) differs from the version which I submitted in July 2010 only insofar, as the comments and suggestions of the referees have been taken into account.

Thanks

First of all, I would like to thank Prof. Gisbert Wüstholz and Clemens Fuchs for their excellent support during my Bachelor-, Master-, and Ph.D. studies. It is a great honor to have been a student of them.

Many thanks go to Dr. Philipp Habegger and Dr. Sergej Gorchinskiy for interesting and stimulating mathematical discussions (see also the remark above Lemma 2.4).

Finally I would like to thank deeply my family and my friends for everything.

Summary

The purpose of this thesis is to combine the theory of logarithmic forms with geometric tools to deduce new results in Diophantine geometry. Let K be a number field and let S be a finite set of places of K.

We first prove an effective Shafarevich theorem for elliptic curves. It gives an effectively determinable Dedekind domain $R \subset K$ and an effective constant Ω, depending only on K and S, such that for each elliptic curve E defined over K with good reduction outside S there is a globally minimal Weierstrass model of E over $\mathrm{Spec}(R)$ with height bounded by Ω. This chapter 1 is joint work with Professor Gisbert Wüstholz and Clemens Fuchs.

In chapter 2 we introduce a new method to generalize and improve the results of the first chapter. Let C be an arbitrary hyperelliptic curve of genus $g \geq 1$ defined over K with good reduction outside S. We show that C has a Weierstrass scheme over the ring of integers of K, arising from a hyperelliptic equation for C with height effectively bounded in terms of g, S and K. Then we give a new interpretation of this effective Shafarevich theorem for hyperelliptic curves in terms of bad reduction which will be the main tool to deduce the Diophantine applications of the last chapter.

In chapter 3 we generalize Szpiro's famous Discriminant Conjecture for elliptic curves over K to arbitrary hyperelliptic curves C over K and we give an effective proof of an exponential version of the generalized conjecture. Then we interpret these results in terms of Arakelov theory and we get also some applications in the theory of geometric Mumford discriminants and minimal regular models respectively. Furthermore, we generalize the Height Conjecture of Frey for elliptic curves to general hyperelliptic curves over K with a K-rational Weierstrass point and we prove an effective exponential version of this generalized conjecture. As an application we get that the elliptic $\mathbb{Q}$-factors of modular Jacobian's can be determined effectively.

Zusammenfassung

Der Zweck dieser Arbeit ist, durch kombinieren von geometrischen Hilfsmitteln mit der Theorie der logarithmischen Formen, neue Resultate in der Diophantischen Geometrie herzuleiten. Im folgenden sei K ein Zahlkörper und S eine endliche Stellenmenge von K.

Im ersten Kapitel beweisen wir einen effektiven Satz von Shafarevich für elliptische Kurven. Dieser gibt ein effektiv berechenbarer Dedekindring $R \subset K$ und eine effektive Konstante Ω, welche nur von K und S abhängt, so dass für jede über K definierte elliptische Kurve E mit guter Reduktion ausserhalb von S ein global minimales Weierstrass model von E über $\mathrm{Spec}(R)$ existiert, dessen Höhe durch Ω beschränkt ist. Dieses Kapitel 1 entstand in Zusammenarbeit mit Professor Gisbert Wüstholz und Clemens Fuchs.

In Kapitel 2 führen wir eine neue Methode ein, um die Resultate von Kapitel 1 zu verbessern und zu verallgemeinern. Sei C eine beliebige über K definierte hyperelliptische Kurve mit Geschlecht $g \geq 1$ und mit guter Reduktion ausserhalb von S. Wir zeigen, dass C ein Weierstrass Schema über dem Ganzheitsring von K besitzt, welches durch eine hyperelliptische Gleichung definiert ist, so dass die absolute Weil Höhe der Koeffizienten der Gleichung durch eine nur von g, S und K abhängigen effektiven Konstanten beschränkt ist. Anschliessend geben wir eine neue Interpretation von einem effektiven Satz von Shafarevich mittels schlechter Reduktion, welche dann für die Diophantischen Anwendungen eine entscheidende Rolle spielen wird.

In Kapitel 3 verallgemeinern wir Szpiro's berühmte Diskriminanten Vermutung für elliptische Kurven auf beliebige hyperelliptische Kurven und wir geben einen effektiven Beweis einer exponentiellen Variante dieser verallgemeinerten Vermutung. Danach interpretieren wir diese Resultate mittels Arakelov Theorie, dann mit geometrischen Mumford Diskriminanten und schliesslich mit minimalen regulären Modellen. Weiter verallgemeinern wir die "Bounded Height"-Vermutung von Frey für elliptische Kurven auf allgemeinere hyperelliptische Kurven C mit einem K-rationalen Weierstrasspunkt und wir beweisen eine exponentielle effektive Variante dieser verallgemeinerten Vermutung. Als Anwendung erhalten wir, dass die über $\mathbb{Q}$ definierten elliptischen Faktoren von modularen Jakobi Varietäten effektiv bestimmt werden können.

Contents

0 Introduction

In 1966 Baker stated his groundbreaking effective lower bounds for linear forms in logarithms of algebraic numbers (see [4]) which had striking Diophantine applications. The main goal of this thesis is now to combine the theory of logarithmic forms with geometric tools to deduce new results in Diophantine geometry.

We first consider a result obtained by Baker himself. In [5] he gave an upper bound for the absolute value of the integer solutions $(x, y) \in \mathbb{Z}^2$ of hyperelliptic equations $Y^2 = f(X)$ with integer coefficients. For given f his bound allowed to find in principal all the solutions. Based on the theory of logarithmic forms, Bugeaud (see [13]) deduced in 1997 upper bounds for the absolute height of the S-integral solutions of superelliptic equations defined over the ring of integers $\mathcal{O}_K$, where K is a number field and S is a finite set of places of K. In the proof he reduced the problem to solve effectively S-unit equations.

This is the starting point of the thesis. We apply these results of Bugeaud to solve effectively a "Moduli problem", i.e. to parametrize certain geometrical objects by integral points on curves. It has already been known for some time that effective results on the Mordell equation would lead to an effective version of a theorem due to Shafarevich for elliptic curves over arbitrary number fields. The classical qualitative theorem says that there are only finitely many K-isomorphism classes of elliptic curves with good reduction outside S. An effective version amounts to the statement that for every elliptic curve E over K with good reduction outside S, one can find a K-isomorphic elliptic curve defined by an equation having coefficients with height bounded by an effective constant.

The proof of this statement first uses the fact that one can associate to each elliptic curve E an equation $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ with discriminant Δ which has a minimality property. Here an important conceptual point is that the elliptic curve is understood as a purely geometric object defined to be a smooth, projective, connected curve of genus one over $\mathrm{Spec}(K)$ together with a section in $E(K)$. We obtain an equation $\Delta = -16(27a_6^2 + 4a_4^3)$ to which results of the theory of logarithmic forms can be applied to get effective bounds for $(a_4, a_6) \in \mathcal{O}_S^2$, where $\mathcal{O}_S$ denotes the ring of S-integers in K. In chapter 1 this leads to a first effective version of Shafarevich's theorem for elliptic curves over K. More precisely, it says that for given K and S there is an affine Dedekind scheme $\mathrm{Spec}(R)$ of dimension one with $2, 3$ invertible in R and an effective constant Ω with the following properties. If E is an elliptic curve over K with good reduction outside S, then there is a globally minimal

Weierstrass model $\mathcal{W}$ of E over $\operatorname{Spec}(R)$ that is given by an equation in short Weierstrass form with coefficients having absolute height at most Ω.

This improves and generalizes for example results of Coates [15], Poulakis [53, 54], Brumer and Silverman [12]. We mention that this first chapter is joint work with Professor Gisbert Wüstholz and Clemens Fuchs.

In chapter 2 we introduce a new method in order to generalize and improve the results of chapter 1. For given K, S and $g \geq 1$ we show that there exist an effective constant Ω_0 and an effectively constructable set of places $T \supseteq S$ of K with the following properties. If C is a hyperelliptic curve over K of genus g with good reduction outside S, then there exists a globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_K$. It arises from a hyperelliptic equation

$$Y^2 = f(X), \quad \text{with discriminant } \Delta \in \mathcal{O}_T^\times \cap \mathcal{O}_K,$$

such that the absolute logarithmic Weil heights of the coefficients of $f \in \mathcal{O}_K[X]$ are at most Ω_0. From this we deduce for example a completely effective Shafarevich theorem for hyperelliptic curves which generalizes and improves the results of chapter 1 and of Coates [15]. We also discuss an other application which leads into the direction of an effective Mordell Conjecture.

For the proof we need a new approach, since the one of chapter 1 does not extend to deal with the more general case of arbitrary hyperelliptic curves over K. In the case where the curve has a K-rational Weierstrass point we use geometry to reduce the problem to solve effectively some unit equations which then leads to explicit bounds. In view of the actual state of the art in the theory of logarithmic forms (see Baker and Wüstholz [8] or [7]) the shape of these bounds is best possible. In the remaining case we use that the moduli spaces of binary forms and hyperelliptic curves are isomorphic and then we apply effective results for binary forms with given discriminant. We point out that the above mentioned effective resolution of unit equations (see Győry and Yu [29]) and the effective results for binary forms (see Evertse and Győry [22]) are both based on the theory of logarithmic forms.

We also note that our method of proof can be exhausted to deal with the corresponding problem for some more general curves. Moreover, in course of our proofs we established some completely explicit estimates for monic polynomials which improve the actual best effective results (compare with [26] and the references in [9] and [27]).

In the remaining part of this thesis we deduce from the results obtained in chapter 2 some Diophantine applications. Here the basic ingredient is a new interpretation of the effective Shafarevich theorem for hyperelliptic curves in terms of bad reduction. Inter alia we shall prove effective exponential versions of the following two famous conjectures. We mention that both conjectures are equivalent to the celebrated *abc*-Conjecture of Masser and Oesterlé [41] and to state them we let Δ_E and N_E be the minimal discriminant and the conductor of an elliptic curve E over $\mathbb{Q}$ respectively.

Conjecture 0.1 (Szpiro's Discriminant Conjecture [70])**.** *There exist absolute constants c, κ such that if E is an elliptic curve defined over $\mathbb{Q}$ then*

$$\Delta_E \leq c N_E^{\kappa}.$$

Let $h_{\mathrm{rel}}(E)$ be the relative Faltings height of E. We now state a conjecture of Frey.

Conjecture 0.2 (Frey's Height Conjecture [25])**.** *There exist absolute constants c, κ such that if E is an elliptic curve defined over $\mathbb{Q}$ then*

$$h_{\mathrm{rel}}(E) \leq \kappa \log N_E + c.$$

We start in chapter 3 with a generalization of Szpiro's Discriminant Conjecture to arbitrary hyperelliptic curves C over K and then we prove an effective exponential version of the generalized conjecture. This has several consequences in Diophantine geometry. On using results of Szpiro [72] and Ullmo [73] we deduce an effective upper bound for the Arakelov degree of an elliptic curve over K in terms of its conductor. Next we combine results of Bloch [10], Deligne [19], Liu [36], Mumford [47] and Saito [57] with our theorem. If C is an elliptic curve or a smooth, projective and geometrically connected curve of genus 2 over K, then we derive an effective estimate for the geometric discriminant of C in terms of the conductor of the Jacobian of C. The same upper bound holds then also for the global number of singular points on the geometric special fibers of a minimal regular model of C over the ring of integers in K.

In the next subsection we first introduce quasi-minimal Weierstrass schemes of a hyperelliptic curve C over K which has a K-rational Weierstrass point. Then we generalize the Height Conjecture in terms of quasi-minimal Weierstrass schemes to the more general curves C and we give an effective proof of an exponential version of this generalized conjecture. As an application we get that the elliptic $\mathbb{Q}$-factors of modular Jacobian's can be determined effectively.

All results described in course of this introduction are new in the stated generality and starting with the crucial new interpretation in chapter 2 they are new even for elliptic curves defined over $\mathbb{Q}$.

We conclude this introduction by an outlook on some further applications of our method which are not included in this thesis. In [75] we get from our exponential version of the Height Conjecture new interpretations of numerous results (for example Masser-Wüstholz [42],[43], Raynaud [55], Silverman [65]) for elliptic curves E over K in terms of reductions. This has the following applications. We answer precisely an old question, posed by Serre in 1981 (see [59, Question 3, p. 399]), on the surjectivity of Galois representations on division fields of E, we give an effective result which is related to the criterion of Néron-Tate-Shafarevich, and we determine effectively the elliptic K-quotients of modular Jacobians $J_0(N)$, $J_1(N)$ in terms of N.

In [74] we deduce an exponential version of the Modular Degree Conjecture (see [25]). Suppose that E is defined over $\mathbb{Q}$ and let $X_0(N)$ be the usual modular curve over $\mathbb{Q}$ of level $N = N_E$. We prove that there is a non-constant $\mathbb{Q}$-morphism $\phi_E : X_0(N) \to E$ with degree bounded exponentially in terms of N. This then leads to general estimates for congruence primes in terms of their level.

Moreover, we derive a geometric, and therefore intrinsic version of Baker's effective theorem [3, 5] on integral solutions to (hyper)elliptic equations defined over K. It bounds effectively integral points (outside a canonical horizontal divisor) on the minimal regular model over $\text{Spec}(\mathcal{O}_K)$ of a (hyper)elliptic curve. For instance this gives a completely effective version of Lang's conjecture on the number of integral solutions to quasi-minimal elliptic equations (see Hindry-Silverman's quantitative result [30]). This geometric version has a very explicit application in the theory of Diophantine equations. It leads to an effective upper bound for the absolute value of the integer solutions to elliptic equations that depends only on the discriminant and on the degree, but not on the height of the equation. This is surprising, since the discriminant of a separable polynomial can be arbitrarily small compared to its height.

For arbitrary number fields K our method establishes the equivalence between the *abc*-Conjecture [41] and Frey's Height Conjecture [25] and it shows that any of these conjectures implies Szpiro's Discriminant Conjecture [70]. This is interesting, since it seems that the classical links between these Conjectures over $\mathbb{Q}$ (through Frey curves) do not extend all to arbitrary number fields. As an application we get that the *abc*-Conjecture implies for all number fields of degree at most d and with discriminant of absolute value at most d^d that the cardinality of the K-torsion points of any elliptic curve E over K is bounded polynomially in terms of d. The actual best bounds are exponential in d.

Finally, we remark that it seems possible, up to minor problems only of technical nature, to use our method to generalize straight forward many of the above results obtained for abelian varieties of dimension 1 and hyperelliptic curves to abelian surfaces or hyperelliptic Jacobian's and superelliptic curves respectively.

1 An effective Shafarevich theorem for elliptic curves

This chapter is joint work with Professor Gisbert Wüstholz and Clemens Fuchs, where the results were obtained in the Bachelor- and Master thesis of the author supervised by them. We mention that a theorem of chapter 2 generalize and improve the results given here. Moreover, the method introduced in chapter 2 is more powerful and it is, in particular in the case of elliptic curves, crucial for the theoretical applications obtained at the end of this thesis. On the other hand the method used in this chapter is from a computational point of view still of great interest, since it depends directly on the effective resolution of the Mordell equation.

1.1 Introduction

Let K be a number field and let S be a finite subset of the set of places of K containing the infinite places. In 1963 Shafarevich [62] proved that there are only finitely many K-isomorphism classes of elliptic curves defined over K with good reduction outside S (this statement is known as Shafarevich's theorem). In 1970 Coates [15] got for the special case $K = \mathbb{Q}$ and $2, 3 \in S$ an effective constant Ω such that in each $\mathbb{Q}$-isomorphism class of elliptic curves defined over $\mathbb{Q}$ with good reduction at the rational primes not in S there is an elliptic curve

$$E: \quad Y^2 = 4X^3 - g_2X - g_3, \quad g_2, g_3 \in \mathbb{Z},$$

with $\max(|g_2|, |g_3|) \leq \Omega$. For the proof he considered the Mordell equation

$$V^2 = U^3 + r, \quad r \in \mathbb{Z} \setminus \{0\},$$

and used the reduction theory of binary forms to get an explicit upper bound for the absolute value of the solutions (u, v) of the Mordell equation in $\mathbb{Z}^2$. This led to an upper bound for the absolute value of the coefficients g_2, g_3 which provided the first effective proof of Shafarevich's theorem. In the same setting Brumer and Silverman [12] deduced in 1996 an upper bound for the number N of $\mathbb{Q}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}$ with good reduction outside S. They applied an estimate obtained by Evertse and Silverman [23]. Later in 1999 this upper bound for N was improved by Poulakis [53, 54]. He used an estimate for the number of solutions of the unit equation $x + y = 1$ obtained in [21] to establish his explicit upper bound for

N. After Baker stated in [4] his groundbreaking effective lower bounds for linear forms in logarithms of algebraic numbers the existence of an effective proof of the general Shafarevich theorem for arbitrary number fields became well-known. Ideas for such an effective proof can be found for example in Masser and Wüstholz [42], Holzapfel [32] and Serre [60, 61]. For the sake of completeness we also refer to a paper of Cremona and Lingham from 2007 (see [16]) in which an algorithm to determine the classes in question is described.

An elliptic curve E over K can be defined as the solution set in $\mathbb{P}^2(C)$ of a homogeneous equation with coefficients in K. However in view of Shafarevich's theorem this point of view is somewhat unnatural since there are different defining equations for the same curve and to deal with this is a crucial point in the theorem. Therefore we shall consider an elliptic curve as a geometric object in this chapter. The precise definition and also the notions Weierstrass model and good reduction will be introduced in section 1.2 below.

The main goal of this chapter is then to establish, for given K and S, the existence of an effectively computable affine Dedekind scheme $\mathrm{Spec}(R)$ with quotient field K and $2, 3 \in R^\times$ and an effective constant Ω depending only on quantities (specified in section 1.3) given by K and S such that the following holds: For each elliptic curve E defined over K with good reduction outside S there exists a globally minimal Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(R)$ which is smooth. Furthermore, the Weierstrass scheme structure of $\mathcal{W}$ over $\mathrm{Spec}(R)$ admits an equation which can be associated to E and which takes the form

$$\mathcal{W}: \ Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

with $a_4, a_6 \in R$ such that

$$\max(h(a_4), h(a_6)) \leq \Omega;$$

here h is the absolute logarithmic Weil height of K which will be defined in section 1.3. We immediately get extensions of the previously mentioned results of Coates, Evertse, Brumer, Silverman and Poulakis to arbitrary number fields K. Our result improves in the case $K = \mathbb{Q}$ parts of the known results and it provides a new effective proof of Shafarevich's theorem.

The plan of the remaining of chapter 1 is as follows: We start in section 1.2 with the precise definition of an elliptic curve in geometric terms, then we define Weierstrass models and their properties and finally we explain what good reduction means. In section 1.3 we introduce the absolute height, state the main theorem, give corollaries and discuss how they improve and generalize the known results. Then in section 1.4 we slightly extend the result of Bugeaud [13, Theorem 1], we prove two lemmas from algebraic number theory and a lemma from geometry which provides the existence of a Weierstrass model of an elliptic curve with some special properties. The proof of the main theorem is given in section 1.5. We start by constructing R, then apply the geometric lemma from which we obtain a Weierstrass model $\mathcal{W}$ over $\mathrm{Spec}(R)$ for each elliptic curve E defined over K with good reduction outside S. The defining equation for $\mathcal{W}$ can be chosen in short Weierstrass form with coefficients $a_4, a_6 \in R$ such that the discriminant $\Delta = -16(4a_4^3 + 27a_6^2) \in R^\times$ of the Weierstrass equation has a minimality property. We transform the equation for the discriminant into a Mordell equation with coefficients in $\mathcal{O}_K$ and apply an effective result which provides bounds for the height of the S-integral solutions. Some further estimates assure that the bounds depend only on quantities given by K and S. In section 1.6 we prove the corollaries to the main theorem. We show that one can get a Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_K)$ with globally controlled reduction. Furthermore, the results are discussed in the special cases when $\mathcal{O}_S$ is a principal ideal domain and when $K = \mathbb{Q}$.

1.2 Geometric preliminaries

In this section we define an elliptic curve in a geometric way, we define and discuss Weierstrass models and explain the term good reduction.

An elliptic curve (E, O) over a number field K is a smooth, projective and connected curve E of genus one over $\mathrm{Spec}(K)$ together with a section $O \in E(K)$. Unless stated otherwise we identify the pair (E, O) with the $\mathrm{Spec}(K)$-scheme E and we say that two elliptic curves are K-isomorphic if they are isomorphic in the category of schemes over $\mathrm{Spec}(K)$. We can associate to E (see [18]) a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \; a_i \in K, \qquad (1)$$

such that E is K-isomorphic to the closed subscheme of the projective plane $\mathbb{P}^2_K = \mathrm{Proj}(K[X, Y, Z])$ given by (1).

Let $R \subset K$ be a Dedekind domain with fraction field K and

$$\mathcal{W} = \mathrm{Proj}(R[X, Y, Z]/(F))$$

where $F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ and has coefficients in R. The pair $(\mathcal{W}, f)$ with f a K-isomorphism from the generic fiber $\mathcal{W} \times_{\operatorname{Spec}(R)} \operatorname{Spec}(K)$ to E is called a Weierstrass model of E over $\operatorname{Spec}(R)$ and we take the discriminant of the Weierstrass equation $F = 0$ as its discriminant $\Delta_{\mathcal{W}}$. For simplicity we suppress f and use $\mathcal{W}$ instead of $(\mathcal{W}, f)$.

Let $\mathfrak{p}$ be a non-zero prime ideal of R and $R_{\mathfrak{p}}$ the local ring of R at $\mathfrak{p}$. We say that the model $\mathcal{W}$ is minimal at $\mathfrak{p}$ if the order of $\mathfrak{p}$ in $\Delta_{\mathcal{W}}$ is minimal when taken over all Weierstrass models of E over $\operatorname{Spec}(R_{\mathfrak{p}})$. A minimal Weierstrass model at $\mathfrak{p}$ always exists. The Weierstrass model $\mathcal{W}$ is globally minimal if it is minimal at each non-zero prime of R. The existence of a globally minimal Weierstrass model depends on R.

The elliptic curve E over K has good reduction at $\mathfrak{p}$ if and only if there exists a smooth Weierstrass model of E over $\operatorname{Spec}(R_{\mathfrak{p}})$ and it has good reduction outside a subset S of $\operatorname{Spec}(R)$ if it has good reduction at all $\mathfrak{p}$ not in S.

1.3 Statement of the results

Let K be a number field of degree d and with ring of integers $\mathcal{O}_K$, let M_K be the set of places of K, $M_{K,\text{fin}}$ the set of finite places and $M_{K,\infty}$ the set of the infinite places of K. Instead of $v \in M_{K,\infty}$ we also write $v \mid \infty$ and there is a natural bijection between the set of finite places and prime ideals in $\mathcal{O}_K$ given by $v \mapsto \mathfrak{p}_v$ and $\mathfrak{p} \mapsto v_{\mathfrak{p}}$. The infinite places $v \mid \infty$ correspond to embeddings $\sigma : K \hookrightarrow \mathbb{C}$ and give absolute values $|\alpha|_v = |\sigma(\alpha)|^{d_v}$ with $d_v = 1$ if v corresponds to a real embedding and $d_v = 2$ if the embedding is not real. The norm of an ideal $\mathfrak{a} \neq 0$ in $\mathcal{O}_K$ is defined as $\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ and for $\alpha \in K$ and $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$ we let $\operatorname{ord}_{\mathfrak{p}}(\alpha)$ be the order of $\mathfrak{p}$ in the principal ideal (α) defined by α and we put $\operatorname{ord}_v(\alpha) = \operatorname{ord}_{\mathfrak{p}_v}(\alpha)$. The places $v \in M_{K,\text{fin}}$ define absolute values $|\alpha|_v$ on K if we put $|\alpha|_v = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}_v)^{-\operatorname{ord}_v(\alpha)}$ for $\alpha \neq 0$ and $|0|_v = 0$.

We use absolute values to define the height of a vector $(\alpha_1, \ldots, \alpha_n) \in K^n$ as

$$H_K(\alpha_1, \ldots, \alpha_n) = \prod_{v \in M_K} \max(1, |\alpha_1|_v, \ldots, |\alpha_n|_v).$$

It is customary to use also the absolute height H which is independent of K and satisfies $H_K = H^d$. The case $n = 1$ includes also the definition of the absolute height $H(\alpha)$ of $\alpha \in K$. Very often we use the absolute logarithmic height $h = \log H$. The height function satisfies $H(\alpha + \beta) \leq 2H(\alpha)H(\beta)$ and $H(\alpha\beta) \leq H(\alpha)H(\beta)$ for $\alpha, \beta \in K$. The height of a monic polynomial

$f(X) = X^n + \beta_1 X^{n-1} + \cdots + \beta_n \in K[X]$ is $H(f) = H(\beta_1, \ldots, \beta_n)$. Let E be an elliptic curve over K and $\mathcal{W}$ a Weierstrass model of E over $\mathrm{Spec}(R)$ given by $F = 0$. We define the height $H(\mathcal{W})$ of the model as the height of the coefficient vector of F.

Let S be a finite set of places of K, let s be the number of finite places in S, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of $\mathcal{O}_K$ corresponding to the finite places in S and for $1 \leq i \leq s$ let $p_i \in \mathbb{N}$ be defined as $p_i\mathbb{Z} = \mathfrak{p}_i \cap \mathbb{Z}$. Then we put $p = \max(3, p_1, \ldots, p_s)$ where we have included 3 to make sure that $\log\log p > 0$. We denote by $\mathcal{O}_S$ the ring of S-integers and by $\mathcal{O}_S^\times$ the group of units of $\mathcal{O}_S$. Observe that by Dirichlet's unit theorem (see [11, Theorem 1.5.13]) $\mathcal{O}_S^\times$ is finitely generated and has rank $|S| - 1$.

We denote by D_K the discriminant and by h_K the class number of K. In the sequel $\Omega_1, \Omega_2, \ldots, \Omega_5$ are effectively computable real positive constants depending just on d.

Main Theorem. *There exists an effectively computable set of places T of K containing S such that if E is an elliptic curve over K with good reduction outside S, then there exists a globally minimal Weierstrass model $\mathcal{W}$ of E over* $\mathrm{Spec}(\mathcal{O}_T)$ *which is smooth and satisfies*

$$h(\mathcal{W}) \leq \exp(\exp(\Omega_1(s + h_K \log|D_K| + \log\log p)^2)).$$

There are various ways to attach a height to an elliptic curve. One possibility is to follow Silverman [64] and to define

$$h(E) = \frac{1}{12} \inf h(a^3, b^2)$$

with the infimum taken over all $a, b \in K$ such that there is Weierstrass model of E over $\mathrm{Spec}(K)$ given by $Y^2Z = X^3 + aXZ^2 + bZ^3$. Another height has been introduced by Faltings and this height does not use models in its definition. Each of the heights has special features and each of them has some disadvantage inherent. They can be compared asymptotically and both can be expressed in terms of the height $h(j(E))$ of the value of the j-function at E up to a weight factor $1/12$ and the unstable discriminant (compare [63]). Our theorem shows then that for every elliptic curve E defined over K with good reduction outside S any of the heights is bounded.

The set T in the main theorem will be effectively constructed with the properties that it contains $M_{K,\infty}$, that $2, 3$ are invertible in $\mathcal{O}_T$ and that $\mathcal{O}_T$ is a principal ideal domain.

We briefly discuss the basic ingredients for the proof of the main theorem. The existence of a globally minimal Weierstrass model will follow from Lemma 1.7 even with the extra information that the model is given by a short Weierstrass equation and that it is smooth over $\mathrm{Spec}(\mathcal{O}_T)$. Here we need that T contains S, that $\mathcal{O}_T$ is a principal ideal domain and that $2, 3$ are invertible in $\mathcal{O}_T$. The discriminant $\Delta_{\mathcal{W}}$ takes the form

$$-27a_6^2 = 4a_4^3 + \frac{1}{16}\Delta_{\mathcal{W}} \tag{2}$$

with $\Delta_{\mathcal{W}} \in \mathcal{O}_T^\times$ and using an improved version of a result of Bugeaud [13] given in Proposition 1.4 we shall effectively bound the integral solutions a_4 and a_6 of the discriminant equation in terms of K and T. For the height bound in the theorem we use that T is effective in terms of S. The proposition requires that the coefficients of the equation in (2) are in $\mathcal{O}_K$ which is not the case in general. It can be achieved however in a controlled way by suitable transformations of the equation.

A natural question is whether there exists a globally minimal Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_K)$ with height bounded as in the main theorem. The obstruction comes from the class group of $\mathcal{O}_K$. It is known that for every elliptic curve $E \to \mathrm{Spec}(K)$ there exists a globally minimal Weierstrass model over $\mathrm{Spec}(\mathcal{O}_K)$ if and only if $h_K = 1$ (see [66, Corollary 8.3]). By a suitable transformation of the Weierstrass model over $\mathrm{Spec}(\mathcal{O}_T)$ given in the main theorem we construct a Weierstrass model over $\mathrm{Spec}(\mathcal{O}_K)$, in general not globally minimal anymore, and this establishes an extension to arbitrary number fields K of the result of Coates.

Corollary 1.1 (Model over $\mathrm{Spec}(\mathcal{O}_K)$)**.** *There exists an effectively computable set of places T of K containing S such that if E is an elliptic curve over K with good reduction outside S, then there exists a Weierstrass model $\mathcal{W}$ of E over* $\mathrm{Spec}(\mathcal{O}_K)$ *which is smooth over* $\mathrm{Spec}(\mathcal{O}_T)$ *and satisfies*

$$h(\mathcal{W}) \leq \exp(\exp(\Omega_2(s + h_K \log|D_K| + \log\log p)^2)).$$

For the smoothness it is needed that the set T has the additional property that all rational primes ℓ that divide the norm of $\mathfrak{p}_v$ for some $v \in T$ are invertible in $\mathcal{O}_T$.

In the special case when $\mathcal{O}_S$ is a principal ideal domain our bounds can be improved.

Corollary 1.2. *There exists an effectively computable set of places T of K containing S such that if E is an elliptic curve over K with good reduction* *outside S, then there exists a globally minimal Weierstrass model $\mathcal{W}$ of E over* $\operatorname{Spec}(\mathcal{O}_T)$ *and a Weierstrass model $\mathcal{W}'$ of E over* $\operatorname{Spec}(\mathcal{O}_K)$ *which both are smooth over* $\operatorname{Spec}(\mathcal{O}_T)$ *such that their logarithmic heights are bounded by*

$$\exp(\Omega_3^{(s+1)^2} |D_K|^{d+2} (\log p)^{d(s+2)}).$$

When $K = \mathbb{Q}$ we can do slightly better. The double exponentiation gets reduced to a single one. Let S be a finite set of rational primes. We put $s = |S|$ and $p = \max S \cup \{3\}$.

Corollary 1.3 (Effective Shafarevich theorem over the rationals)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with good reduction outside S. There exists a globally minimal Weierstrass model $\mathcal{W}$ over* $\operatorname{Spec}(\mathcal{O}_S[1/6])$ *and a Weierstrass model $\mathcal{W}'$ of E over* $\operatorname{Spec}(\mathbb{Z})$ *which both are smooth over* $\operatorname{Spec}(\mathcal{O}_S[1/6])$ *such that their heights satisfy*

$$\max(H(\mathcal{W}), H(\mathcal{W}')) \leq \exp(\Omega_4^{(s+1)^2} p^{10^3(s+3)}).$$

Coates showed in [15] that in each $\mathbb{Q}$-isomorphism class of elliptic curves with good reduction outside S there exists an elliptic curve defined by an equation in short Weierstrass form with coefficients $g_2, g_3 \in \mathbb{Z}$ such that

$$\max(|g_2|, |g_3|) \leq \exp(2^{10^7(s+1)^4} p^{10^9(s+1)^3}).$$

The bound in Corollary 1.3 is asymptotically better with respect to the parameters s and p than the bound obtained by Coates.

From our bounds for the heights it is easy to deduce that all K-isomorphism classes of elliptic curves over K with good reduction outside S can be determined effectively and estimates for their number $N(K,S)$ can be given. This leads to bounds which are not as good as the results published by Evertse, Brumer, Silverman and Poulakis in the case $K = \mathbb{Q}$. For example the bound for the number of isomorphism classes becomes

$$N(\mathbb{Q}, S) \leq \exp(\Omega_5^{(s+1)^2} p^{10^3(s+3)})$$

when $K = \mathbb{Q}$. In this special case the bound obtained by Poulakis in [53, 54] by a different method is sharper and fully explicit.

1.4 Auxiliary results

In this section we give some results which we need for the proof of the main theorem. Let T be a finite set of places of K. One of the main tools used in the proof is an effective upper bound for the height of the solutions in $\mathcal{O}_T$ of a hyperelliptic equation over $\mathcal{O}_K$. This upper bound will be established at the beginning of this section. After that we prove two technical lemmas, where the second gives an effective construction of a finite subset of $M_{K,\mathrm{fin}}$ such that $\mathcal{O}_T$ is a principal ideal domain if T contains this set. At the end of the section we prove a geometric lemma which provides a specific model for an elliptic curve with good reduction outside S.

The following proposition is an extension of a result of Bugeaud [13, Theorem 1]. He assumes, and for simplicity we also do, that T contains the archimedean places of K. We denote by t and q the quantities associated to T that correspond to s and p which we have associated to S.

Proposition 1.4. *Let $a \neq 0$ be an element in $\mathcal{O}_K$ and let g be a monic separable polynomial over $\mathcal{O}_K$ with discriminant Δ_g and degree $n \geq 3$. We set $A = \max(\left|N_{K/\mathbb{Q}}(a)\right|, 3)$ and $H = \max(H(g), 27)$. Then the solutions $(x, y) \in \mathcal{O}_T \times K$ of the equation $aY^2 = g(X)$ satisfy*

$$H(x) \leq H^2\, e^{\lambda}$$

with $\lambda = \lambda_1 \lambda_2 \lambda_3$ and

$$\begin{aligned} \lambda_1 &= C_1^{(t+1)^2} q^{4n^3 d} (\log q)^{4n^2 dt}, \\ \lambda_2 &= |D_K|^{15n^2/2} A^{3n^2} \left|N_{K/\mathbb{Q}}(\Delta_g)\right|^{12n}, \\ \lambda_3 &= (\log \left|A D_K N_{K/\mathbb{Q}}(\Delta_g)\right|)^{6n^2 d} \log\log H. \end{aligned}$$

The constant C_1 is effective and depends only on d and n.

Proof. Since all conditions of [13, Theorem 1] are satisfied, we get the upper bound with an effective constant depending only on d, n and t as stated. We now follow the proof given in [13] to get in addition an explicit dependence of the constants on the parameter t. By $k_1, \ldots, k_{46}$ we shall denote effective constants depending on d and n but not on t. In our proof we keep the notation introduced in [13].

In a first step we work out the dependence on t of the constant c_{12} in [13, Lemma 4]. Following the proof and using the same arguments as in the proof of the main theorem of [14] one sees that the constants c_{13} up to c_{20} can be replaced by $\exp(k_{13}(t+1)^2)$ up to $\exp(k_{20}(t+1)^2)$ and c_{21} up to c_{24} by $k_{21}(t+1)$ up to $k_{24}(t+1)$ respectively. This implies that c_{25} can be replaced by $\exp(k_{25}(t+1)^2)$ and finally c_{12} by $\exp(k_{12}(t+1)^2)$. Since the constants in the remaining lemmas and propositions are given explicitly or are independent of t, we are now ready to work out also the dependence of c_1 in terms of t.

We begin with replacing c_{33} up to c_{35} by k_{33} up to k_{35} and we change c_{36} and c_{37} into $k_{36}(t+1)$ and $k_{37}(t+1)$ respectively. Further we take k_{38}, k_{39} as c_{38}, c_{39} and $\exp(k_{40}(t+1))$ for c_{40}. Using the term which replaces c_{12} we see that c_{41} can be substituted by $\exp(k_{41}(t+1)^2)$ and then we can take c_{42} for $k_{42}(t+1)$ and $\exp(k_{43}(t+1)^2)$ up to $\exp(k_{46}(t+1)^2)$ for c_{43} up to c_{46} respectively. We conclude that c_1 can be substituted by $\exp(k_1(t+1)^2)$ and the statement follows with $C_1 = k_1$. □

We remark that by the above arguments we have, more generally, that the effective constant of the first bound of Bugeaud [13, Theorem 1], depending on d, n and t, is at most $\exp((t+1)^2 \log C_1)$, where C_1 is the effective constant of the above proposition that depends only on d and n.

Let $v \in M_{K,\mathrm{fin}}$ and p_v be the positive generator of $\mathfrak{p}_v \cap \mathbb{Z}$. The following lemma provides a tool to remove denominators so as to construct models over $\mathrm{Spec}(\mathcal{O}_K)$ from models which are defined only over an open subset.

Lemma 1.5. *For a in $\mathcal{O}_T$ we define the rational integer*

$$\delta(a) := \prod_{\substack{v \in T, v \nmid \infty \\ |a|_v > 1}} |a|_v.$$

Then $\delta(a)a \in \mathcal{O}_K$.

Proof. We take $w \nmid \infty$ and verify $|\delta(a)a|_w \leq 1$. For $w \notin T$ we have $|\delta(a)|_w \leq 1$ and $|a|_w \leq 1$ and therefore the assertion. If $w \in T$ and $|a|_w \leq 1$, then again $|\delta(a)|_w \leq 1$ and so the assertion follows again. Finally, if $w \in T$ and $|a|_w > 1$, then

$$|\delta(a)|_w = \prod_{\substack{v \in T, p_v = p_w \\ |a|_v > 1}} |\,|a|_v|_w \leq |\,|a|_w|_w \leq |a|_w^{-1}.$$

This concludes the proof. □

We notice that the statement of the lemma would also follow from [11, Proposition 1.6.6] where with extra effort an additional property is proved.

The next lemma allows us to remove class group obstructions in connection with globally minimal models.

Lemma 1.6. *There exists a set of at most $h_K \log(|D_K|)$ finite places v with p_v bounded by $|D_K|^{1/2}$ such that $\mathcal{O}_T$ for $T \subset M_K$ is a principal ideal domain if T contains the set.*

Proof. By [34, Theorem 4, p. 119] we can choose for each class in the class group of K an integral representative $\mathfrak{a}$ with the property that

$$\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) \leq |D_K|^{1/2}$$

and from this we conclude that at most $\log(|D_K|)/(2\log(2))$ prime ideals divide $\mathfrak{a}$. On taking the sum over the class group shows that this gives at most $h_K \log(|D_K|)/(2\log(2))$ prime ideals. Their classes generate the class group. Let $P \subset \mathbb{N}$ be the set of rational primes corresponding to these prime ideals. We define T_0 as the set of v in $M_{K,\text{fin}}$ such that ℓ divides the norm of $\mathfrak{p}_v$ for some $\ell \in P$ and we see that

$$|T_0| \leq d h_K \log(|D_K|)$$

and that the largest rational prime in P is at most $|D_K|^{1/2}$. In the ring $\mathcal{O}_T$ for $T \supseteq T_0$ as in the lemma, ideals corresponding to elements in T_0 become trivial. Their image in the class group of $\mathcal{O}_T$ generate the group and this shows that the class group is trivial. □

We choose a fundamental system $\mathcal{U}$ of T-units and a generator ζ of the torsion subgroup of $\mathcal{O}_T^\times$ and we say that $\Delta \in \mathcal{O}_T^\times$ is reduced if it takes the form $\Delta = \zeta^m \prod_{\varepsilon \in \mathcal{U}} \varepsilon^{n(\varepsilon)}$ with $0 \leq m, n(\varepsilon) \leq 11$. For our geometric lemma below we assume that T contains S, that $\mathcal{O}_T$ is a principal ideal domain and that $2, 3$ are invertible in $\mathcal{O}_T$.

Lemma 1.7. *Let E be an elliptic curve over K with good reduction outside S. There exists a globally minimal Weierstrass model of E over* $\operatorname{Spec}(\mathcal{O}_T)$ *given by an equation of the form $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ with discriminant reduced and in $\mathcal{O}_T^\times$.*

Proof. By assumption the Picard group of $\operatorname{Spec}(\mathcal{O}_T)$ is trivial and then [38, Theorem 9.4.35] provides a globally minimal Weierstrass model $\mathcal{W}$ of E over $\operatorname{Spec}(\mathcal{O}_T)$. We choose $F \in \mathcal{O}_T[X, Y, Z]$ such that $\mathcal{W} = \operatorname{Proj}(\mathcal{O}_T[X, Y, Z]/(F))$. For $v \in M_{K,\text{fin}}$ we take $\mathfrak{p} = \mathfrak{p}_v \in \operatorname{Spec}(\mathcal{O}_T)$ and $\mathcal{W}_\mathfrak{p} = \mathcal{W} \times_{\mathcal{O}_T} \operatorname{Spec}(\mathcal{O}_{T,\mathfrak{p}})$. Since $\mathcal{W}$ is minimal its localization $\mathcal{W}_\mathfrak{p}$ stays minimal. The elliptic curve E has good reduction outside S and since $S \subseteq T$ it follows that E has the same property with respect to T. Therefore the fiber $\mathcal{W}_\mathfrak{p}(\mathfrak{p})$ of $\mathcal{W}_\mathfrak{p}$

at $\mathfrak{p}$ is smooth for all $\mathfrak{p}$ not in T and from [38, Corollary 10.1.23] we deduce that $\Delta_{\mathcal{W}} \in \bigcap_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_T)} \mathcal{O}_{T,\mathfrak{p}}^\times = \mathcal{O}_T^\times$.

By assumption 6 is in $\mathcal{O}_T^\times$ and this implies that there exists a Weierstrass model $\mathcal{W}'$ over $\mathrm{Spec}(\mathcal{O}_T)$ with defining equation $Y^2Z = X^3 + a_4'XZ^2 + a_6'Z^3$ such that the discriminants $\Delta_{\mathcal{W}}$ and $\Delta_{\mathcal{W}'}$ coincide up to a T-unit. This shows that $\mathcal{W}'$ is another globally minimal Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_T)$. We write its discriminant as

$$\Delta_{\mathcal{W}'} = \zeta^{m'} \prod_{\varepsilon\in\mathcal{U}} \varepsilon^{n'(\varepsilon)}$$

with $\mathcal{U}$ the fundamental system of T-units and ζ the root of unity introduced above. Reduction modulo 12 gives

$$\Delta_{\mathcal{W}'} = u^{12}\zeta^m \prod_{\varepsilon\in\mathcal{U}} \varepsilon^{n(\varepsilon)}$$

for some $u \in \mathcal{O}_T^\times$ and with $0 \leq m, n(\varepsilon) \leq 11$. The same arguments as above show that the Weierstrass model defined by $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ with $a_4 = u^{-4}a_4', a_6 = u^{-6}a_6'$ is a globally minimal Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_T)$ and has discriminant $u^{-12}\Delta_{\mathcal{W}'}$ which is reduced and in $\mathcal{O}_T^\times$. □

Observe that even if $\mathcal{O}_K$ is a principal ideal domain, it is a priori not possible to associate to E an equation with coefficients in $\mathcal{O}_K$ and with reduced discriminant as the following example shows. Let $K = \mathbb{Q}$, $S = \{2, 3\}$ and E be the elliptic curve defined by the equation

$$Y^2Z = X^3 - 4XZ^2 + \frac{8}{3}Z^3. \tag{3}$$

The Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_S)$ given by (3) has discriminant $\Delta_{\mathcal{W}} = 2^{10}$ which is reduced. The equation $Y^2Z = X^3 - 324XZ^2 + 1944Z^3$ gives a Weierstrass model of E over $\mathrm{Spec}(\mathbb{Z})$ and its discriminant is $2^{10}3^{12}$ which is not reduced anymore. In conclusion E has no Weierstrass model over $\mathrm{Spec}(\mathbb{Z})$ with reduced discriminant.

We need that $\Delta_{\mathcal{W}}$ is reduced to get a bound for its height in terms of S and K. If an effective Szpiro conjecture on the minimal discriminant of an elliptic curve [71] would be true, the reduction would be obsolete in the case when $\mathcal{O}_K$ is a principal ideal domain.

As a conclusion we see that, even if $K = \mathbb{Q}$, we have to consider solutions a_4, a_6 of (2) in $\mathcal{O}_T$ and not only in $\mathcal{O}_K$. This shows that the results of Baker on the effective resolution of the hyperelliptic equation [3, 5], or more specifically on the Mordell equation [1, 2], are not sufficient to deal with the problem.

With these results we are now ready to prove the main theorem and this will be done in the next section.

1.5 Proof of the main theorem

Let K and S be as in the main theorem. The constants $C_2, C_3, \ldots$ which will be introduced in the proof depend only on the degree d of K and can be computed effectively. For T we take the union of the set of places constructed in Lemma 1.6, the sets S and $M_{K,\infty}$, and the set of places corresponding to prime divisors of 6. The set T is effectively computable and we have to compare the number s and the prime p in the main theorem associated to S with the corresponding quantities t and q for T. Using the bound in Lemma 1.6 we get

$$t \leq ds + dh_K \log(|D_K|) + 2d \quad \textit{and} \quad q \leq p\, |D_K|^{1/2}. \tag{4}$$

We take now an elliptic curve E over K with good reduction outside S and conclude, since T contains S, that our curve E has good reduction outside T. As in [14, Lemma 1] we choose a fundamental system $\mathcal{U}$ of T-units such that

$$h(\varepsilon) \leq C_2^{(t+1)^2} R_T \tag{5}$$

for all $\varepsilon \in \mathcal{U}$ and we fix a generator ζ of the torsion subgroup of $K^\times$.

Our Lemma 1.7 gives a globally minimal Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_T)$ with equation $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ and coefficients a_4, a_6 in $\mathcal{O}_T$ such that $\Delta = \Delta_{\mathcal{W}}$ is reduced. We multiply the equation (2) with 16 and then $(4a_4, 4a_6) \in \mathcal{O}_T \times \mathcal{O}_T$ is a solution of

$$-27Y^2 = X^3 + \Delta. \tag{6}$$

From Lemma 1.5 we see that $\alpha = \delta(\Delta)\Delta \in \mathcal{O}_K$ and clearly $\delta(\Delta)$ is bounded by $H_K(\Delta) = H(\Delta)^d$. Then $x = -4\delta(\Delta)^2 a_4, y = 12\delta(\Delta)^3 a_6$ is a solution of the equation $3Y^2 = X^3 - \delta(\Delta)^5\alpha$. The polynomial $g(X) = X^3 - \delta(\Delta)^5\alpha$ is separable and therefore an application of Proposition 1.4 to $3Y^2 = g(X)$ gives

$$H(x) \leq H(g)^2\, e^\lambda \tag{7}$$

with $\lambda = \lambda_1\lambda_2\lambda_3$ (for the definition of the quantities $\lambda_1, \lambda_2, \lambda_3$ see Proposition 1.4).

Since the degree of g is 3 we get

$$\lambda_1 \leq C_3^{(t+1)^2} q^{108d} (\log q)^{36dt} \tag{8}$$

and for estimating λ_2 and λ_3 we need bounds for $\left|N_{K/\mathbb{Q}}(\Delta_g)\right|$, $H(g)$ and A. In a first step we estimate $H(\Delta)$ and $\delta(\Delta)$ and in a second step the estimates are used to derive upper bounds for $\left|N_{K/\mathbb{Q}}(\Delta_g)\right|$, $H(g)$ and A. In a third step we deduce the upper bounds for λ_2 and λ_3 as stated.

To give an estimate for $H(\Delta)$ we bound from above the T-regulator R_T (defined in [13]). From [13, Lemma 3] we get $R_T \leq R_K h_K (d \log q)^t$ and from [35] we see that $R_K h_K$ is at most $(10d)^{10d} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1}$ which combines to

$$R_T \leq C_4 \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1} (d \log q)^t.$$

The discriminant Δ is reduced and this means that

$$\Delta = \zeta^m \prod_{\varepsilon \in \mathcal{U}} \varepsilon^{n(\varepsilon)}$$

for integers $0 \leq m, n(\varepsilon) < 12$. Height properties together with (5) and the upper bound for R_T lead to

$$H(\Delta) \leq \exp(C_5^{(t+1)^2} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1} (\log q)^t)$$

and we conclude that

$$\delta(\Delta) \leq \exp(C_6^{(t+1)^2} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1} (\log q)^t). \tag{9}$$

The absolute value of the norm from K to $\mathbb{Q}$ of $\Delta_g = -27(\delta(\Delta)^5 \alpha)^2$ is at most equal to $H(\Delta_g)^d$ and can be estimated by $C_7 H(\delta(\Delta)^5 \alpha)^{2d}$. We recall that $\alpha = \delta(\Delta)\Delta$ and therefore

$$H(\alpha) \leq \exp(C_8^{(t+1)^2} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1} (\log q)^t)$$

and then from (9) the inequality

$$\left|N_{K/\mathbb{Q}}(\Delta_g)\right| \leq \exp(C_9^{(t+1)^2} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d-1} (\log q)^t)$$

follows.

In our application of Proposition 1.4 we have $H(g) = H(\delta(\Delta)^5 \alpha)$, $a = 3$ and $A = 3^d$. We put the estimates together and obtain

$$\lambda_2 \leq \exp(C_{10}^{(t+1)^2} \left|D_K\right|^{1/2} (\log \left|D_K\right|)^{d} (\log q)^t) \tag{10}$$

and

$$\lambda_3 \le (C_{11}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)^{55d}. \tag{11}$$

The estimates for λ_1, λ_2 and λ_3 given in (8), (10) and (11) are now used to give an upper bound for $H(x)$, $H(a_4)$ and $H(a_6)$. From (7) we get

$$H(x) \le \exp(\exp(C_{12}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t))$$

and (9) together with the inequality $H(a_4) \le H(x)H(4\delta(\Delta)^2)$ leads to

$$H(a_4) \le \exp(\exp(C_{13}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)). \tag{12}$$

From (6) we see that $H(a_6) \le 59H(a_4)^{3/2}H(\Delta)^{1/2}$ and our estimates for $H(a_4)$ and $H(\Delta)$ give

$$H(a_6) \le \exp(\exp(C_{14}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)). \tag{13}$$

Finally, we replace t and q in (12), (13) by the estimates in (4) and obtain

$$\begin{aligned}\max(h(a_4), h(a_6)) &\le \exp(C_{15}^{(s+h_K \log|D_K|+1)^2} (\log p)^{ds+dh_K \log|D_K|+2d}) \\ &\le \exp(C_{16}(s + h_K \log |D_K| + \log\log p)^2))\end{aligned}$$

as claimed in the theorem. □

1.6 Proof of the corollaries

Once the main theorem is established it is not difficult to deduce the corollaries to the main theorem.

Proof of Corollary 1.1. The main theorem gives a set of places T which, as we may assume, contains with a finite place v all places which are associated to the divisors of $p_v\mathcal{O}_K$ for p_v a generator of $\mathfrak{p}_v \cap \mathbb{Z}$. This can be done without changing the estimates and the rational primes p_v for $v \in T$ then become invertible in $\mathcal{O}_T$.

Let E be an elliptic curve defined over K with good reduction outside S. Then there exists a globally minimal Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_T)$ given by an equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, where the height of $a, b \in \mathcal{O}_T$ is bounded in terms of K and S and where $\Delta_{a,b} = -16(4a^3 + 27b^2) \in \mathcal{O}_T^\times$. From Lemma 1.5 we see that $\alpha = \delta(a)a$ and $\beta = \delta(b)b$ are in $\mathcal{O}_K$ and that $\delta(a)\delta(b) \le (H(a)H(b))^d$. The construction of T implies that all prime divisors of $\delta(a)$ and $\delta(b)$ are invertible in $\mathcal{O}_T$ and this shows that $\delta(a), \delta(b) \in$

$\mathcal{O}_T^\times$. One also sees that $u = \delta(a)\delta(b), a_4 = u^4 a, a_6 = u^6 b$ and $\Delta = u^{12}\Delta_{a,b}$ have logarithmic heights at most $30d \max(h(a), h(b))$. Our main theorem then gives the bound for $\max(h(a_4), h(a_6))$ as stated.

Let $\mathcal{W}$ be the subscheme of $\mathbb{P}^2_{\mathcal{O}_K} = \mathrm{Proj}(\mathcal{O}_K[X, Y, Z])$ defined by the Weierstrass equation $Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3$ with discriminant $\Delta_{\mathcal{W}} = \Delta \in \mathcal{O}_K \cap \mathcal{O}_T^\times$. The generic fiber of $\mathcal{W}$ over $\mathrm{Spec}(\mathcal{O}_K)$ is K-isomorphic to E and this shows that $\mathcal{W}$ is a Weierstrass model of E over $\mathrm{Spec}(\mathcal{O}_K)$ with the required properties. □

Proof of Corollary 1.2. By assumption we get with the same notation as in the first step of the proof of the main theorem that

$$t \le d(s+2) \quad \textit{and} \quad q \le p. \tag{14}$$

We replace t and q in (12) and (13) by the bounds given in (14). The same arguments as in the proof of Corollary 1.1 then give Corollary 1.2. □

Proof of Corollary 1.3. We put $T = S \cup \{2, 3\} = \mathcal{U}$ and take $\zeta = -1$. From Lemma 1.7 we obtain a globally minimal Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_T)$ defined by $Y^2 Z = X^3 + a_4 X Z^2 + a_6 Z^3$ with $a_4, a_6 \in \mathcal{O}_T = \mathcal{O}_S[1/6]$. Its discriminant $\Delta = \Delta_{\mathcal{W}} = -16(4a_4^3 + 27a_6^2) \in \mathbb{Z}$ can be written as $\pm \prod \ell^{n(\ell)}$ with $0 \le n(\ell) \le 11$ and with $n(\ell) = 0$ unless $\ell \in S$ or $\ell = 2, 3$. We see that $x = -4a_4, y = 4a_6$ gives a solution of

$$27Y^2 = X^3 - \Delta.$$

The discriminant Δ_g of the polynomial $g(X) = X^3 - \Delta$ is $-27\Delta^2$. We apply Proposition 1.4, where now $a = A = 27$ and $H = \max(|\Delta|, 27)$, and get an upper bound for $H(x)$. Since $H(\Delta) = |\Delta| \le q^{11t}$, it follows that $|\Delta_g| = 27|\Delta|^2 \le 27q^{22t}$ and $H \le 27|\Delta| \le 27q^{11t}$. Using these estimates and $\log q \le q$ we get

$$H(x) \le \exp(C_{17}^{(t+1)^2} q^{170+10^3 t})$$

for an effective constant C_{17}. Finally, we replace t and q by the upper bounds given in (14) and obtain

$$\max(H(a_4), H(a_6)) \le \exp(C_{18}^{(s+1)^2} p^{10^3(s+3)}) \tag{15}$$

with an effective constant C_{18}, which completes the proof of the first part of the corollary. From (15) we deduce the remaining parts with the same arguments as used in the proof of Corollary 1.1. □

2 An effective Shafarevich theorem for hyperelliptic curves

2.1 Introduction

Let S be a finite set of places of a number field K. We denote by $\mathcal{O}_K$ the ring of integers in K, by $\mathcal{O}_S$ the ring of S-integers in K and by $\mathcal{O}_S^\times$ the units in $\mathcal{O}_S$. A hyperelliptic curve (C, φ) over K is defined as a pair of a smooth, projective and geometrically connected curve $C \to \operatorname{Spec}(K)$ of genus $g \geq 1$ together with a finite morphism $\varphi : C \to \mathbb{P}^1_K$ of degree 2. Unless stated otherwise we identify (C, φ) with the $\operatorname{Spec}(K)$-scheme C, and we mention that all elliptic curves and all smooth, projective and geometrically connected curves of genus 2 are hyperelliptic curves over the same base scheme. We say that C has good reduction outside S if and only if a minimal regular model of C over $\operatorname{Spec}(\mathcal{O}_S)$ is smooth (see section 2.2).

The first goal of this chapter (see Theorem 2.1) is to show that for given K, S and $g \geq 1$ there exist an effective constant Ω_0 and an effectively computable set of places $T \supseteq S$ of K with the following properties. If C is a hyperelliptic curve over K of genus g with good reduction outside S, then there exists a globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_K$ (defined in section 2.2). It arises from a hyperelliptic equation

$$Y^2 = f(X), \quad \text{with discriminant } \Delta \in \mathcal{O}_T^\times \cap \mathcal{O}_K,$$

such that the absolute logarithmic Weil heights (defined in chapter 1) of the coefficients of $f \in \mathcal{O}_K[X]$ are at most Ω_0.

From this we deduce for example a completely effective Shafarevich theorem (see Corollary 2.2) for hyperelliptic curves. This generalizes and improves the results of chapter 1 and of Coates [15]. An other application leads into the direction of an effective Mordell Conjecture. If C has good reduction outside S one can obtain from our hyperelliptic equation for C with bounded coefficients an effective estimate in terms of K, S and g for the stable Falting's height of the Jacobian $J(C) \to \operatorname{Spec}(K)$ of C (see [17]). Similar bounds for all smooth, projective and geometrically connected curves of genus $g \geq 2$ would imply an effective version of Falting's theorem [24] (Mordell's Conjecture). We note that one part of [24] is already effective due to the work of Masser and Wüstholz [44] and that a discussion of our method in this context is given in section 2.3. Furthermore our method can be exhausted to deal with the corresponding problem for some more general curves.

The second goal (see Theorem 2.3) is to show that if C is a hyperelliptic curve over K of genus $g \geq 1$ with conductor N_C (defined in section 2.2) then C has a Weierstrass scheme $\mathcal{W}(f)$ over $\mathcal{O}_K$ given by

$$Y^2 = f(X) \in \mathcal{O}_K[X]$$

with coefficients having absolute logarithmic Weil heights bounded effectively in terms of K, g and N_C.

In later chapters we get from this second theorem several applications in Diophantine geometry. For instance we shall prove exponential effective versions of Szpiro's Discriminant Conjecture [71] and of Frey's Height Conjecture [25] extended to hyperelliptic curves. Furthermore, we shall discuss some consequences for minimal regular models of a hyperelliptic curve over $\mathrm{Spec}(\mathcal{O}_K)$ and we shall show that the elliptic $\mathbb{Q}$-factors of Jacobian's of modular curves can be determined effectively. The latter will make a quantitative result of Brumer and Silverman [12] completely effective.

The principal ideas of our proof are as follows: We construct out of S a controlled finite set of places $T \supseteq S$ of K such that 2 and the residue characteristics of the finite places in T are in $\mathcal{O}_T^\times$ and that $\mathcal{O}_T$ is a principal ideal domain (see Lemma 2.4).

Suppose that C has good reduction outside S. For technical reasons (see section 2.3) we first consider the case where C has a K-rational Weierstrass point (defined in section 2.2). Since $2 \in \mathcal{O}_T^\times$ and $\mathcal{O}_T$ is a principal ideal domain we get from Lockhart [39] a specific globally T-minimal Weierstrass scheme of C (see Proposition 2.8 (i)), arising from

$$Y^2 = f(X), \text{ such that } f(X) \in \mathcal{O}_T[X] \text{ is monic} \tag{16}$$

with discriminant $\Delta(f) \in \mathcal{O}_T^\times$ effectively controlled in terms of K and T.

By a standard reduction (introduced by Győry) we deduce from our monic f some unit equations to which we then apply an effective theorem of Győry and Yu [29] based on deep results of the theory of logarithmic forms. On using the solutions of the unit equations we get $\tau \in \mathcal{O}_T$ such that $f(X+\tau) \in \mathcal{O}_T[X]$ has effectively bounded height (see Proposition 2.10 (i)). Finally after a suitable change of variables we get in this case the desired Weierstrass scheme over $\mathcal{O}_K$.

It remains to treat the case where C has no K-rational Weierstrass point. From a global result of the theory of Weierstrass schemes of Liu [37] we get a Weierstrass scheme of C arising from a hyperelliptic equation of the shape of (16), where now f is in general not monic but has degree $2g+2$ (see Proposition 2.8 (ii)).

Since hyperelliptic curves of genus g and binary forms of degree $2g+2$ have isomorphic moduli spaces we can use effective results for binary forms with given discriminant. We slightly extend a result of Evertse and Győry [22], based also on the theory of logarithmic forms, and then apply it to the homogenization $F \in \mathcal{O}_T[X, Y]$ of f. This gives an automorphism Φ of $\mathbb{A}^2(\mathcal{O}_T)$ such that the pullback Φ^*F of F along Φ has effectively bounded height (see Proposition 2.10 (ii)). Finally a transformation of $Y^2 = \Phi^*F(X, 1)$ provides the desired Weierstrass scheme over $\mathcal{O}_K$.

The plan of the remaining of chapter 2 is as follows: In section 2.2 we give precise definitions for the geometric objects we shall work with. In section 2.3 we state our results and discuss several aspects of our main theorem and our method. In section 2.4 we first give Lemma 2.4. Then we expose some known results for Weierstrass schemes to prove afterwards Proposition 2.8. In section 2.5 we go into number theory. We list some elementary properties of the absolute logarithmic Weil height and of binary forms. Then we prove two technical lemmas and Proposition 2.10. In section 2.6 we give the proofs of the theorems and the corollary.

Throughout the whole of chapter 2 we shall use the following conventions. We say that two hyperelliptic curves are K-isomorphic if they are isomorphic in the category of Spec(K)-schemes, we often identify a closed point $\mathfrak{p} \in$ Spec$(\mathcal{O}_K)$ with the corresponding finite place v of K and vice versa, we denote by log the principal value of the natural logarithm and we define the maximum of the empty set and the product taken over the empty set as 1.

2.2 Geometric preliminaries

In this section we define precisely what we mean with models, good reduction, Weierstrass schemes, discriminants, conductors and Weierstrass points of hyperelliptic curves.

Let R be a Dedekind domain with group of units $R^\times$ and with quotient field a number field K. Let $C \to$ Spec(K) be a hyperelliptic curve with genus $g \geq 1$. For brevity we write $\mathcal{B} =$ Spec(R).

If $\mathcal{Y}$ is an integral, projective and flat $\mathcal{B}$-scheme of dimension 2 which is regular, then we say that $\mathcal{Y}$ is an arithmetic surface over $\mathcal{B}$. An arithmetic surface $\mathcal{M} \to \mathcal{B}$ is a minimal arithmetic surface if every birational map $\mathcal{Y} \dashrightarrow \mathcal{M}$ of arithmetic surfaces over $\mathcal{B}$ is a birational morphism.

Let $\mathcal{C}$ be a projective, normal and flat $\mathcal{B}$-scheme of dimension 2 with generic fiber $\mathcal{C}_\eta$, where $\mathcal{C}_\eta$ is K-isomorphic to C. We call the pair $(\mathcal{C}, \psi)$ of $\mathcal{C}$ together with a K-isomorphism $\psi : \mathcal{C}_\eta \to C$ a model of C over $\mathcal{B}$. A morphism between two models $(\mathcal{C}, \psi), (\mathcal{C}', \psi')$ of C is a morphism in the category of $\mathcal{B}$-schemes that is compatible with the K-isomorphisms $\psi : \mathcal{C}_\eta \to C$ and $\psi' : \mathcal{C}'_\eta \to C$. For simplicity we suppress ψ and write $\mathcal{C}$ instead of $(\mathcal{C}, \psi)$.

Let $(\mathcal{C}, \psi)$ be a model of C over $\mathcal{B}$. If $\mathcal{C}$ is a regular scheme then it is an arithmetic surface over $\mathcal{B}$ and we call $(\mathcal{C}, \psi)$ a regular model of C over $\mathcal{B}$. If $\mathcal{C}$ is a minimal arithmetic surface we say that $(\mathcal{C}, \psi)$ is a minimal regular model of C over $\mathcal{B}$. It exists and is unique up to an isomorphism of models over $\mathcal{B}$ (see for example [38, Proposition 10.1.8]).

We say that C has good reduction at a closed point in $\mathrm{Spec}(\mathcal{O}_K)$ if there exists a model of C which is smooth over the spectrum of the local ring at this point.

Let S be a finite set of places of K. Then the finite places in S are in bijection with a subset of $\mathrm{Spec}(\mathcal{O}_K)$, denoted also by S. We say that C has good reduction outside S if it has good reduction at all closed points in $\mathrm{Spec}(\mathcal{O}_K)$ which are not in S. This is equivalent to the statement that the minimal regular model of C over $\mathrm{Spec}(\mathcal{O}_S)$ is smooth, where $\mathcal{O}_S$ is the ring of S-integers in K.

To get effective results we shall use the theory of Weierstrass schemes of C over $\mathcal{D}$, where $\mathcal{D}$ is the spectrum of the local ring $\mathcal{O}_\mathfrak{p}$ at an arbitrary $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$. For elliptic curves such a theory is well-known (see for example [38]) and a generalization to hyperelliptic curves is due to Liu [37]. The function field $K(C)$ of C can be written as $K(X)[Y]$ with a relation

$$Y^2 + k(X)Y = f(X), \quad f(X), k(X) \in K[X], \tag{17}$$

where $2g+1 \leq \max\bigl(2\mathrm{deg}\ k(X), \mathrm{deg}\ f(X)\bigr) \leq 2g+2$. We say that (17) is a hyperelliptic equation for C defined over K.

We first assume that $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ is a closed point and we denote by $-\mathrm{id} : C \to C$ a hyperelliptic involution on (C, φ), where $-\mathrm{id}$ is the automorphism of order 2 induced by a generator of the Galois group of $K(C)$ over $\varphi^*(K(\mathbb{P}^1_K))$. We note that $-\mathrm{id}$ is unique if $g \geq 2$. A Weierstrass scheme $\mathcal{W}$ of C over $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ is the normalization of the integral scheme

$$\mathrm{Spec}(\mathcal{O}_\mathfrak{p}[X]) \cup \mathrm{Spec}(\mathcal{O}_\mathfrak{p}[1/X]) \text{ in } C,$$

for $X \in K(C)$ with $K(X)$ fixed by the action of $\langle -\mathrm{id} \rangle$ on $K(C)$. For each such $\mathcal{W}$ there exists $Y \in K(C)$ such that the integral closure of $\mathcal{O}_\mathfrak{p}[X]$ in $K(C)$ is a free $\mathcal{O}_\mathfrak{p}[X]$-module with base $\{1, Y\}$ and such that the rational functions Y and X are related by (17). We say that the Weierstrass scheme $\mathcal{W}$ arises from this hyperelliptic equation.

Let η be the generic point of $\mathrm{Spec}(\mathcal{O}_K)$. A Weierstrass scheme $\mathcal{W} =$

$\mathcal{W}(f,k)$ of C over $\mathrm{Spec}(\mathcal{O}_\eta) = \mathrm{Spec}(K)$ arising from a hyperelliptic equation (17) is defined as the union of the spectra of

$$K[X,Y]/(Y^2 + k(X)Y - f(X)) \text{ and } K[Z,W]/(W^2 + k_1(Z)W - f_1(Z)),$$

where $k_1(Z) = k(1/Z)Z^{g+1}$, $f_1(Z) = f(1/Z)Z^{2g+2}$ and the two open subschemes glue along the principal open subschemes $D(X) \cong D(Z)$ with relations $XZ = 1$ and $Y = X^{g+1}W$. If further $k = 0$ we write $\mathcal{W} = \mathcal{W}(f)$. We note that the curve $C \to \mathrm{Spec}(K)$ is K-isomorphic to any Weierstrass scheme $\mathcal{W}$ of C over $\mathrm{Spec}(K)$ and that there exists a one to one correspondence of Weierstrass schemes of C over $\mathrm{Spec}(K)$ and hyperelliptic equations of C defined over K.

Geometric definitions of the discriminant of a hyperelliptic curve can be made by the use of the relative dualizing sheaf of a minimal regular model over a Dedekind scheme (see [33] or [57], [18]). For our purpose we shall need a more explicit definition and in virtue of the constructive Weierstrass model theory (see [37]) we define the discriminant Δ of a Weierstrass scheme $\mathcal{W} \to \mathcal{D}$ of C as follows: If $\mathcal{W} \to \mathcal{D}$ arises from (17), then

$$\Delta = \begin{cases} 2^{4g}\Delta(u) & \text{for deg } u = 2g+2 \\ 2^{4g}\mu_0^2\Delta(u) & \text{otherwise,} \end{cases} \tag{18}$$

where $u = f + k^2/4$ has leading coefficient μ_0 and $\Delta(w)$ is the usual discriminant of a polynomial $w \in K[X]$.

To measure somewhat crudely the arithmetical size of a Weierstrass scheme $\mathcal{W}$ of C over $\mathcal{D}$ we take

$$h(\mathcal{W}) = \max\bigl(h(\Delta), h(u)\bigr),$$

for $h(\Delta)$ and $h(u)$ the absolute logarithmic Weil height (defined in chapter 1) of Δ and the maximum of the absolute logarithmic Weil heights of the coefficients of u respectively.

Let $f_\mathfrak{p}$ be the exponent of the conductor of the Jacobian variety of C over K at a closed point $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ (defined in [40, p. 575]). We take $d_\mathfrak{p} = 1$ in the case where C has bad reduction at $\mathfrak{p}$ and its Jacobian is K-isomorphic to the generic fiber of an abelian scheme over $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ and $d_\mathfrak{p} = 0$ otherwise. Then we define the conductor ideal $\mathfrak{F}_C$ of C as $\mathfrak{F}_C = \prod \mathfrak{p}^{f_\mathfrak{p}+d_\mathfrak{p}}$ with the product taken over all closed points $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ and the conductor N_C of C as

$$N_C = N_{K/\mathbb{Q}}(\mathfrak{F}_C), \tag{19}$$

where $N_{K/\mathbb{Q}}$ is the ideal norm from K into $\mathbb{Q}$. We mention that the positive integer $f_{\mathfrak{p}}$ coincide with the exponent of the conductor at $\mathfrak{p}$ of the l-adic representation (see Serre [58])

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Q}_l}(\mathrm{H}^1_{\text{ét}}(C \times_K \mathrm{Spec}(\overline{K}), \mathbb{Q}_l)),$$

for $\overline{K}$ an algebraic closure of K and for l a rational prime different from the residue characteristic of $\mathfrak{p}$.

We recall that $\mathfrak{p}$ is a closed point of $\mathrm{Spec}(\mathcal{O}_K)$. Let T be an arbitrary finite set of places of K. Then the Weierstrass scheme $\mathcal{W}_{\mathfrak{p}} \to \mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$ of C with discriminant $\Delta_{\mathfrak{p}}$ is a minimal Weierstrass scheme of C over $\mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$, if $\mathrm{ord}_{\mathfrak{p}}\Delta_{\mathfrak{p}}$ is minimal when taken over all Weierstrass schemes of C over $\mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$. The minimal Weierstrass scheme over $\mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$ is for $g \geq 2$ in general not unique (see [37, remarque 5]). We say that a Weierstrass scheme $\mathcal{W} \to \mathcal{D}$ with discriminant Δ is globally T-minimal over $R \subseteq \mathcal{O}_T$ if it arises from a hyperelliptic equation with coefficients in R such that $\mathrm{ord}_{\mathfrak{p}}\Delta = \mathrm{ord}_{\mathfrak{p}}\Delta_{\mathfrak{p}}$ at each closed point $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_T)$. Hence from a morphism $\mathcal{D} \to \mathrm{Spec}(R)$ and a globally T-minimal Weierstrass scheme over R one can get a model of C over $\mathrm{Spec}(R)$, which is, as a model over $\mathcal{D}$, isomorphic to $\mathcal{W}$. For our purpose it suffices to consider Weierstrass schemes of C over $\mathcal{D}$ and we say that a Weierstrass scheme is globally minimal over R if it is globally T_0-minimal over R, where T_0 is the empty set. We conclude the discussion of these schemes with the following explicit criterion for good reduction of C at $\mathfrak{p}$: The curve C has good reduction at $\mathfrak{p}$ if and only if a minimal Weierstrass scheme $\mathcal{W}_{\mathfrak{p}} \to \mathrm{Spec}(\mathcal{O}_{\mathfrak{p}})$ of C is smooth.

A K-rational Weierstrass point of C is a section $P : \mathrm{Spec}(K) \to C$ with $P = -\mathrm{id} \circ P$. Let Σ be the ramification locus of the double covering $\varphi : C \to \mathbb{P}^1_K$. We get that $P \in C(K) \cap \Sigma$ and then we say that the pair $((C, \varphi), P)$ is a pointed hyperelliptic curve. A hyperelliptic equation (17) of C with f monic of degree $2g+1$ and $\deg k \leq g$ is called a Weierstrass equation for C. Lockhart considered in [39] pointed hyperelliptic curves and showed that they admit a Weierstrass equation. The morphisms of pointed hyperelliptic curves over K are those $\mathrm{Spec}(K)$-morphisms of hyperelliptic curves defined over K which are compatible with the K-rational Weierstrass sections of the pointed curves.

Let $Y^2 = f(X)$ and $V^2 = l(U)$ be two hyperelliptic equations of C defined over K with discriminants Δ and Δ' respectively. Then [38, Corollary 7.4.33] gives

$$\Phi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(K), \ \lambda \in K^\times$$

such that

$$U = \Phi X = \frac{\alpha X + \beta}{\gamma X + \delta}, \quad V = \frac{\lambda Y}{(\gamma X + \delta)^{g+1}}$$

and that

$$\Delta' = \lambda^{4(2g+1)}(\det \Phi)^{-2(g+1)(2g+1)}\Delta. \tag{20}$$

Now we are ready to state the results of chapter 2 and this will be done in the next section.

2.3 Statement of the results

In this section we state the theorems and corollaries and then we discuss several aspects of these results and of our method. In the sequel k_0 is an effectively computable absolute constant.

Let S be a finite set of places of a number field K. Let $\mathcal{O}_S$ be the ring of S-integers in K with group of units $\mathcal{O}_S^\times$ and $\mathcal{O}_K$ be the ring of integers in K. Let d be the degree of K and D_K be the absolute value of the field discriminant of K over $\mathbb{Q}$. For $g \geq 1$ we let $\nu = 6(2g+1)(2g)(2g-1)d^2$ and to measure S we take

$$\sigma = s + h_S \text{ and } \ p, \tag{21}$$

for s the number of finite places in S, h_S the class number of $\mathcal{O}_S$ and p the largest residue characteristic of the finite places in S. We now can state the first theorem.

Theorem 2.1. *There is a finite set of places $T \supseteq S$ such that if C is a hyperelliptic curve over K of genus g with good reduction outside S then there is a globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_K$ with $\Delta \in \mathcal{O}_T^\times$. Furthermore,*

- *(i) if C has a K-rational Weierstrass point, then f is monic separable of degree $2g+1$ and $h(\mathcal{W}(f)) \leq (\nu\sigma)^{5\nu\sigma} p^{\nu d s/2} D_K^{\nu h_S/4}$,*
- *(ii) if C has no K-rational Weierstrass point, then f is separable of degree $2g+2$ and $h(\mathcal{W}(f)) \leq (\nu\sigma)^{k_0(2\nu)^3\sigma^4} p^{(3\nu)^3\sigma^4} D_K^{(3\nu)^3\sigma^4}$.*

The proof shows in addition that the set of places T of K in the theorem can be constructed effectively. For example we can take any set of places $T \supseteq S$ of K with the properties that $|T| \leq d\sigma$, that $\mathcal{O}_T$ is a principal ideal domain and that the residue characteristics ℓ of the finite places in T are at most $2pD_K^{1/2}$ and satisfy $2\ell \in \mathcal{O}_T^\times$ (see Lemma 2.4). If $K = \mathbb{Q}$ we can take $T = S \cup \{2\}$.

The above result holds for all elliptic and all smooth, projective and geometrically connected curves of genus 2 over K, since they are hyperelliptic. By adding to T the places of K above 3 we can assume in the elliptic case after a suitable change of variables which does not increase our bounds that $f(X) = X^3 + a_4X + a_6$. Therefore our theorem generalizes the results for elliptic curves over K of Coates, who covered in [15] the case $K = \mathbb{Q}$, and of chapter 1 to arbitrary hyperelliptic curves over K. Our explicit bound (take in part (i) $g = 1$, $K = \mathbb{Q}$) is sharper in all quantities than the explicit one of Coates. Furthermore, the effective bound of chapter 1, which is double exponential and only explicit in terms of S, is reduced to a completely explicit polynomial bound (take in part (i) $g = 1$). For the sake of completeness we also refer to a paper of Smart [67] in which he calculated a complete list of genus 2 curves over $\mathbb{Q}$ with good reduction outside 2.

In view of an effective Mordell Conjecture it is possible, as indicated in the introduction, to bound effectively the stable Faltings heights of the Jacobian's of our curves in terms of K, g and S. De Jong and Rémond establish in a not yet published paper [17] such bounds for cyclic covers of $\mathbb{P}^1_K$ with prime degree and with good reduction outside S. They combine the method introduced by Paršin, which we describe below, with effective methods coming from the theory of logarithmic forms. We remark that the arguments of section 2.5 and 2.6 would also give similar bounds for curves with good reduction outside S, which correspond to function fields $K(X)[Y]$ with a relation $Y^m = f(X)$, for $m \geq 2$ and for f as in Proposition 2.10. Moreover, it seems that our method of constructing a minimal equation for the curve and then applying effective results based on the theory of logarithmic forms, can be used to deduce analogous estimates for Jacobian's of more general curves.

We discuss the methods of the proofs from a technical point of view. Suppose that C has good reduction outside S. To get from Lemma 2.6 a specific Weierstrass scheme of C over a Dedekind domain R we need that R is a principal ideal domain. In our proof we extend S to T such that $\mathcal{O}_T$ is a principal ideal domain. It seems that one can avoid an extension of S by working, after a base change, with $C_L \to \operatorname{Spec}(L)$, for $L = H(K)$ the Hilbert class field of K. But if $K \neq L$ one does not get a Weierstrass scheme over $\operatorname{Spec}(K)$.

In 1972 Paršin [52] introduced an other approach to get a specific Weierstrass scheme over a finite extension of K. We sketch a reformulation of Oort [51]: There exists a finite extension $W \supseteq K$, unramified over K at all places of W that do not extend a place in T, such that $C(W)$ contains the $2g + 2$ Weierstrass points of C. With the help of a fixed K-rational Weierstrass point we embed $C_W \to \operatorname{Spec}(W)$ in its Jacobian $J(C_W) \to \operatorname{Spec}(W)$ which extends to a smooth abelian scheme $\mathcal{J} \to \mathrm{Spec}(\mathcal{O})$, where $\mathcal{O}$ denotes the integral closure of $\mathcal{O}_T$ in W. Then on using that the images of Weierstrass points are 2-torsion points of $\mathcal{J}$ one can deduce a Weierstrass equation for $C_W \to \mathrm{Spec}(W)$ with coefficients in $\mathcal{O}$ and discriminant Δ invertible in $\mathcal{O}$. But as before this approach gives in general no equation over K.

We now motivate the separation of the statements in (i) and (ii) depending on whether a K-rational Weierstrass point of C exists or not. The globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ from Proposition 2.8 has the property that f has degree $2g+2$ if and only if we are in part (ii). But only if deg $f = 2g+2$ we get from the $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ of Proposition 2.10, which is not necessarily a translation, a Weierstrass scheme of C over $\mathcal{O}_T$. On the other hand in part (i) we can reduce the problem directly to solve a unit equation. This has the advantage that it leads to explicit estimates in (i), which depend directly on the recently in [29] established and at the moment best bounds for unit equations. The method of (i) only works if f is monic and thus can not be applied to the arbitrary f of (ii).

From our theorem we deduce a completely effective Shafarevich theorem for hyperelliptic curves of given genus. We recall that k_0 is an effectively computable absolute constant and that S is a finite set of places of a number field K. Let $g \geq 1$ be an integer and let ν, σ, p, d and D_K be as above (see (21)).

Corollary 2.2. *The K-isomorphism classes of hyperelliptic curves of genus g over K with good reduction outside S can be determined effectively and their number is at most*

$$\exp((\nu\sigma)^{k_0(2\nu)^3\sigma^4} p^{(3\nu)^3\sigma^4} D_K^{(3\nu)^3\sigma^4}).$$

In particular we get that the number of isomorphism classes of pointed hyperelliptic curves over K of genus g with good reduction outside S is at most

$$\exp\bigl((\nu\sigma)^{6\nu\sigma} p^{\nu ds/2} D_K^{\nu h_S/4}\bigr).$$

We next give an interpretation of Theorem 2.1 in terms of bad reduction. Instead of describing, for fixed K, S and $g \geq 1$, the hyperelliptic curves over K of genus g with good reduction outside S we now take an arbitrary hyperelliptic curve C over K of genus $g \geq 1$ and describe it by the bad reduction set $S_C \subset \mathrm{Spec}(\mathcal{O}_K)$ where C has not good reduction. As the applications in the following chapters indicate this new interpretation seems more convenient from a theoretical point of view. For simplicity we write S for S_C and to measure this set we take

$$\sigma = s + h_S, \;\; N_C \text{ and } \;\; p$$

for s the number of finite places in S, h_S the class number of $\mathcal{O}_S$, N_C the conductor of C and p the largest rational prime divisor of N_C. Let d and D_K be the degree and the absolute value of the field discriminant of K over $\mathbb{Q}$ respectively. As above we take $\nu = 6(2g+1)(2g)(2g-1)d^2$.

Theorem 2.3. *Suppose C is a hyperelliptic curve defined over K of genus $g \geq 1$ with bad reduction set S. Then there is a Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_K$ such that*

(i) if C has a K-rational Weierstrass point, then f is monic separable of degree $2g+1$ and $h(\mathcal{W}(f)) \leq (2^d D_K^{h_S/2} N_C)^{\nu^2}$,

(ii) if C has no K-rational Weierstrass point, then f is separable of degree $2g+2$ and $h(\mathcal{W}(f)) \leq (\nu\sigma)^{k_0(2\nu)^3\sigma^4} p^{(3\nu)^3\sigma^4} D_K^{(3\nu)^3\sigma^4}$.

From this we get an effective estimate for $h(\mathcal{W}(f))$ in terms of K, g and N_C, since s and p are at most N_C and $h_S \leq h_K$. In forthcoming work we will deduce several Diophantine applications from this (see the discussion in section 2.1).

In the last part of this section we discuss the constants. For the Diophantine applications given later it is important that the dependence on S_C of the bound in Theorem 2.3 is as sharp as possible. This motivated to use, instead of p and σ, the more precise measure N_C of S_C for some estimates. As a consequence for hyperelliptic curves with a K-rational Weierstrass point we get that the shape of the bounds in the applications are best possible in view of the actual state of the art in the theory of logarithmic forms. The appearance of k_0 in the estimates can be justified as follows. There exists no result that gives for an arbitrary binary form $F \in \mathcal{O}_T[X,Y]$ with nonzero discriminant Δ_F an element $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that $h(\Phi^* F)$ is explicitly bounded in terms of K, T, $h(\Delta_F)$ and the degree of F (see section 2.5). Effective results exist but to make them explicit one is forced into lengthy computations of constants. We omit the latter and to get bounds as explicit as possible we use the actual best effective result of [22] which leads to explicit bounds in the above terms and effectively computable absolute constants c_6, c_7. Then, as a consequence of explicitly computing the constants in every step of our proofs we derived the relation

$$k_0 = c_6 c_7.$$

We note that throughout the whole chapter 2 the constants are calculated according to Baker's philosophy: “Although some care has been taken to obtain numerical constants reasonably close to the best that can be acquired with the present method of proof, there is, nevertheless, little doubt that the numbers on the right of the above inequalities can be reduced to a certain extent by means of minor refinements. In particular it will be seen that several of the numbers occurring in our estimates have been freely rounded off in order that the final conclusion should assume a simple form, and so some obvious improvements are immediately obtainable."

Finally, we remark that in view of our theoretical applications we tried to polish the dependence of the bounds on S (or S_C). But on going through our arguments one can improve with little effort the dependence on other parameters of interest as for example the discriminant D_K or the degree d of K.

2.4 Minimal Weierstrass schemes with special properties

In this section we first show that one can construct effectively a set of places T out of S such that $\mathcal{O}_T$ is a principal ideal domain, where S is a finite set of places of a number field K. Then, after stating a known result for hyperelliptic curves C over K, we prove Lemma 2.7 which describes a relation between the structure of Weierstrass schemes and the existence of a K-rational Weierstrass point of C. In the last part we give the proof of Proposition 2.8. It shows that each C with good reduction outside S has a globally T-minimal Weierstrass scheme over $\mathcal{O}_T$ with discriminant controlled effectively in terms of K and T.

We recall that h_S is the class number of the ring of S-integers $\mathcal{O}_S$, that $\mathcal{O}_K$ denotes the ring of integers in K, and that D_K is the absolute value of the discriminant of K over $\mathbb{Q}$. Let s, N_S and p be the number of finite places in S, the product taken over the finite places $v \in S$ of the number of elements in the residue field of v and the largest rational prime divisor of N_S respectively. Then let t, N_T and q be the corresponding quantities associated to a finite set of places T of K. The next lemma allows us to remove class group obstructions in connection with globally minimal Weierstrass schemes. We thank at this place Sergej Gorchinskiy for improving the upper bound for t in Lemma 1.6 to the following estimate in

Lemma 2.4. *There exists a set $T \supseteq S$ such that $\mathcal{O}_T$ is a principal ideal domain and that the following inequalities $N_T \leq N_S D_K^{(h_S-1)/2}$, $q \leq \max(p, D_K^{1/2})$ and $t \leq s + h_S - 1$ hold.*

Proof. For the class group of a Dedekind domain R we write $Cl(R)$ and we note that a localization $R \hookrightarrow R'$ gives a surjective morphism $Cl(R) \to Cl(R')$ of abelian groups. Hence $Cl(\mathcal{O}_K)$ surjects onto $Cl(\mathcal{O}_S)$ and we assume that $\bar{\mathfrak{a}}$ is a non-trivial element of $Cl(\mathcal{O}_S)$. Thus [34, Theorem 4, p. 119] gives a non-principal ideal $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_S) \hookrightarrow \mathrm{Spec}(\mathcal{O}_K)$ such that $\mathfrak{p}$ divides an integral representative of $\bar{\mathfrak{a}}$ and that the residue field of $\mathfrak{p}$ has at most $D_K^{1/2}$ elements. Since $\mathfrak{p}$ is not a principal $\mathcal{O}_S$-ideal its class in $Cl(\mathcal{O}_S)$ is a non-trivial element in the kernel of the surjective morphism $Cl(\mathcal{O}_S) \to Cl(\mathcal{O}_{S\cup\{\mathfrak{p}\}})$. This implies that the class number of the latter is at most $h_S - 1$. Then, after repeating this argument at most $h_S - 1$ times, we conclude that there exists a set of places $T \supseteq S$ of K with the required properties. □

The following lemma is used in the proof of Proposition 2.8 to bound the absolute Weil height of the discriminant of a Weierstrass scheme. Let d be the degree of K over $\mathbb{Q}$ and let n_T be the product taken over the finite places $v \in T$ of the logarithm of the number of elements in the residue field of v.

Lemma 2.5. *There exists a fundamental system Σ of T-units with*

$$h(\epsilon) \leq (10\,|\Sigma|!)^2 (dD_K)^d n_T, \quad \epsilon \in \Sigma.$$

Proof. Let R_T and R_K be the T-regulator and the regulator of K respectively. From [29, Remark 3] we get $R_T \leq R_K h_K n_T$ and since $R_K h_K$ is at most $(2d)^{d-1} D_K^{1/2} \max(1, \log D_K)^{d-1}/(d-1)!$ (see [35, Theorem 6.5]) this leads to

$$R_T \leq (2d)^{d-1} D_K^{1/2} \max(1, \log D_K)^{d-1} n_T/(d-1)!\ . \tag{22}$$

Then the lemma follows from [29, Lemma 2] which gives a fundamental system Σ of T-units with absolute logarithmic Weil heights bounded by $40(|\Sigma|!)^2 \max(1, \log d) R_T$. □

Let C be a hyperelliptic curve of genus $g \geq 1$ defined over K and let R be a Dedekind domain with quotient field K and with group of units $R^\times$. The following lemma is a direct consequence of [37, Proposition 2], where the latter is a global result obtained by Liu in his pioneering paper [37] on Weierstrass models of C over discrete valuation rings.

Lemma 2.6. *Suppose that R is a principal ideal domain and that a minimal regular model of C over* $\mathrm{Spec}(R)$ *is smooth. Then there exists a Weierstrass scheme $\mathcal{W}(f,k)$ of C with $f, k \in R[X]$ and with discriminant $\Delta \in R^\times$.*

We next discuss a relation between K-rational Weierstrass points and Weierstrass schemes $\mathcal{W} \to \mathcal{D}$ (defined in section 2.2) of C. This will be used in the proof of part (ii) of the proposition below.

Lemma 2.7. *If C has no K-rational Weierstrass point and if $\mathcal{W} \to \mathcal{D}$ is a Weierstrass scheme of C arising from $Y^2 = f(X)$, then f has degree $2g + 2$.*

Proof. We take C as in the lemma. If $\mathcal{W} \to \mathcal{D}$ is a Weierstrass scheme of C arising from $Y^2 = f(X)$ then f has degree $2g + 1$ or $2g + 2$. We assume that f has degree $2g + 1$ and deduce a contradiction. Let $\alpha_i \in K$ be the coefficients of f, where $\alpha_0 \neq 0$ denotes the leading coefficient. Then the change of coordinates $X = \alpha_0 U$, $Y = \alpha_0^{g+1} V$ together with (20) gives a Weierstrass equation

$$V^2 = U^{2g+1} + \alpha_0^{-(2g+2)}(\alpha_1 U^{2g} + \ldots + \alpha_{2g+1})$$

for C such that the polynomial on the right-hand side has nonzero discriminant. Then [39, Theorem 1.7] implies that this Weierstrass equation defines a regular affine curve over $\mathrm{Spec}(K)$. Therefore the closure of an embedding of this affine curve into the projective space $\mathbb{P}_K^{g+2}$ is a hyperelliptic curve $C' \to \mathrm{Spec}(K)$ with a K-rational Weierstrass point (for details we refer to [39, p. 731]). It follows that $K(C') = K(C)$ and then that the curves C and C' are K-isomorphic which leads to a contradiction to our assumption that C has no K-rational Weierstrass point. We conclude that $\deg f = 2g+2$. □

For our proposition below we assume that a finite set of places T of K contains S, that $\mathcal{O}_T$ is a principal ideal domain and that 2 is invertible in $\mathcal{O}_T$. Let Σ be a fundamental system of T-units and let ζ be a generator of the torsion part of the T-units $\mathcal{O}_T^\times$. We write $\mathcal{U} = (\Sigma, \zeta)$ and then we say that $\epsilon \in \mathcal{O}_T^\times$ is $\mathcal{U}$-reduced if it takes the form $\epsilon = \zeta^r \prod_{\epsilon \in \Sigma} \epsilon^{r(\epsilon)}$, $0 \leq r, r(\epsilon) < 4(g + 1)(2g + 1)$. Let t be the number of finite places in T, let n_T be the product taken over the finite places $v \in T$ of the logarithm of the number of elements in the residue field of v and we recall that d denotes the degree of K over $\mathbb{Q}$.

Proposition 2.8. *If $\mathcal{U}$ is as above and if C is a hyperelliptic curve over K of genus $g \geq 1$ with good reduction outside S, then there is a globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_T$ such that $\Delta \in \mathcal{O}_T^\times$ is $\mathcal{U}$-reduced. Furthermore,*

(i) if C has a K-rational Weierstrass point, then $f \in \mathcal{O}_T[X]$ is separable and monic of degree $2g + 1$,

(ii) if C has no K-rational Weierstrass point, then $f \in \mathcal{O}_T[X]$ is separable of degree $2g + 2$.

There is a $\mathcal{U}$ as above such that further $h(\Delta(f)) \leq (50g(t+d)!)^2(2dD_K)^{2d} n_T$.

Proof. We now take a hyperelliptic curve C over K of genus $g \geq 1$ with good reduction outside S. Since T contains S we conclude that our curve C has a forteriori good reduction outside T.

(i) We first suppose that C has a K-rational Weierstrass point P and to simplify notation we shall write C for the pointed hyperelliptic curve (C, P). In a first step we construct a globally T-minimal Weierstrass scheme of C over $\mathcal{O}_K[1/2] \subseteq \mathcal{O}_T$ with discriminant invertible in $\mathcal{O}_T$. Let $\mathfrak{a}$ be an integral representative of the Weierstrass class (see [39, Definition 2.7]) of C. Since $\mathcal{O}_T$ is a principal ideal domain we get a T-integer α and a fractional ideal $\mathfrak{a}_T$ of K, which is composed only of primes in T, such that $\mathfrak{a} = \alpha\mathfrak{a}_T$. After multiplying this ideal equation with a suitable T-unit in $\mathcal{O}_K$ we see that there is an integral representative $\mathfrak{b}$ of the Weierstrass class of C which is composed only of primes in T. An application of [39, Proposition 2.8] to $\mathfrak{b}$ and C gives rational functions U, V in $K(C) = K(U)[V]$ and polynomials $l, m \in \mathcal{O}_K[U]$ such that l is monic of degree $2g + 1$, the degree of m is at most g, and the Weierstrass scheme $\mathcal{W}(l, m)$ has discriminant Δ' with

$$\Delta'\mathcal{O}_K = \mathfrak{b}^{4g(2g+1)}\mathfrak{D}_C,$$

for $\mathfrak{D}_C$ the minimal discriminant ideal of C (see [39, Definition 2.5]). To see that $\Delta' \in \mathcal{O}_T^\times$ we let $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_T)$ be an arbitrary closed point. Since our curve C has good reduction outside T we get that a minimal Weierstrass scheme $\mathcal{W}_\mathfrak{p} \to \operatorname{Spec}(\mathcal{O}_\mathfrak{p})$ of C is smooth. In particular this implies that the special fiber of $\mathcal{W}_\mathfrak{p}$ is smooth over the spectrum of the residue field at $\mathfrak{p}$ and therefore $\mathfrak{p}$ does not divide the discriminant of $\mathcal{W}_\mathfrak{p}$. We conclude that $\mathfrak{D}_C$ is invertible in $\mathcal{O}_T$ and then the above representation of $\Delta'\mathcal{O}_K$ shows $\Delta' \in \mathcal{O}_T^\times$. The equations

$$W = U, \quad Z = V + m(U)/2$$

induce an isomorphism between $\mathcal{W}(l, m)$ and the Weierstrass scheme $\mathcal{W}(u)$ of C, where $u = l + m^2/4$. Furthermore, the discriminant of $\mathcal{W}(u)$ equals Δ' and since $2 \in \mathcal{O}_T^\times$, deg $m \leq g$ we see that $u \in \mathcal{O}_T[W]$ is monic with degree $2g + 1$.

In a second step we reduce the discriminant. Since $\Delta' \in \mathcal{O}_T^\times$ there exist integers $a, a(\epsilon)$ such that Δ' takes the form $\Delta' = \zeta^a \prod \epsilon^{a(\epsilon)}$ with the product taken over $\epsilon \in \Sigma$. By reducing the exponents $a, a(\epsilon)$ modulo $4g(2g + 1)$ we can rewrite the above equation as $\Delta' = \omega^{-4g(2g+1)}\zeta^r \prod_{\epsilon\in\Sigma} \epsilon^{r(\epsilon)}$ with integers $0 \leq r, r(\epsilon) < 4g(2g + 1)$ and $\omega \in \mathcal{O}_T^\times$. From

$$X = \omega^2 W, \quad Y = \omega^{2g+1} Z$$

we see that the Weierstrass scheme $\mathcal{W}(f)$ of C, where $f(X) = \omega^{4g+2}u(X/\omega^2)$, has $\mathcal{U}$-reduced discriminant $\Delta = \omega^{4g(2g+1)}\Delta'$ and is isomorphic to $\mathcal{W}(u)$.

Furthermore, the properties of u imply that $f \in \mathcal{O}_T[X]$ is monic and has degree $2g+1$. Hence we conclude that the Weierstrass scheme $\mathcal{W}(f)$ of C has the required properties.

(ii) We now assume that C has no K-rational Weierstrass point. Since our curve C has good reduction outside T there exists a minimal regular model of C over $\text{Spec}(\mathcal{O}_T)$ which is smooth. Then an application of Lemma 2.6 with $R = \mathcal{O}_T$ to C gives a Weierstrass scheme $\mathcal{W}(l,m)$ of C with discriminant $\Delta' \in \mathcal{O}_T^\times$ and with $l, m \in \mathcal{O}_T[U]$. As in (i) we get that the equation $u = l + m^2/4$ in $\mathcal{O}_T[U]$ induces an isomorphism between $\mathcal{W}(l,m)$ and $\mathcal{W}(u)$. Our assumption made in (ii) combined with Lemma 2.7, applied to $\mathcal{W}(u)$, shows that u has degree $2g+2$ and then we see that Δ' is also the discriminant of $\mathcal{W}(u)$. Next we reduce, in the same way as in (i), with a suitable $\omega \in \mathcal{O}_T^\times$ and with $X = \omega^2 W, Y = \omega^{2g+2} Z$ the exponents of Δ' modulo $4(g+1)(2g+1)$. This gives $f \in \mathcal{O}_T[X]$ of degree $2g+2$ such that $\mathcal{W}(f)$ is isomorphic to $\mathcal{W}(u)$ and such that the discriminant Δ of $\mathcal{W}(f)$ is $\mathcal{U}$-reduced. Since Δ is invertible in $\mathcal{O}_T$ we see that the Weierstrass scheme $\mathcal{W}(f)$ of C has the desired properties.

To prove the last statement of the proposition we choose $\mathcal{U} = (\Sigma, \zeta)$ such that Σ is a fundamental system of T-units with heights bounded as in Lemma 2.5. Then the first part of the proposition provides a globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_T$ with $\mathcal{U}$-reduced discriminant $\Delta \in \mathcal{O}_T^\times$ such that f has the properties of (i) or (ii). Since Δ is $\mathcal{U}$-reduced it takes the form $\zeta^r \prod_{\epsilon \in \Sigma} \epsilon^{r(\epsilon)}$ for integers $0 \le r, r(\epsilon) < 4(g+1)(2g+1)$. Therefore the bound in Lemma 2.5 together with the estimates $|\Sigma| \le t+d-1$ and $h(\Delta(f)) \le 4g + h(\Delta)$ leads to

$$h(\Delta(f)) \le 24g^2(10(t+d)!)^2(2dD_K)^{2d} n_T + 4g.$$

We conclude that this $\mathcal{U}$ is suitable for the last statement and this completes the proof of the proposition. □

2.5 Binary forms and monic polynomials with given discriminant

In the first part of this section we collect some results which we shall use in the proof of Proposition 2.10. We state elementary properties of binary forms and we give a lemma relating polynomials in $K[X]$ with their homogenizations in $K[X,Y]$, where in this section K is a number field, T is an arbitrary finite set of places of K and $\mathcal{O}_K$ is the ring of integers in K. In the second part we prove Proposition 2.10 which gives effective bounds for the height of pullbacks of binary forms and monic polynomials.

First we discuss some properties of binary forms. Let $n \geq 1$, $q \in \mathbb{Q}$, $f \in K[X]$ with roots $\alpha_1, \ldots, \alpha_n$ and let α, β be algebraic over $\mathbb{Q}$. For the readers convenience we recall some properties of the absolute multiplicative Weil height H on K (defined in chapter 1). We get

$$H(\alpha\beta) \leq H(\alpha)H(\beta), \quad H(\alpha^q) = H(\alpha)^{|q|},$$
$$H(f) \leq n\prod_{i=1}^{n} H(\alpha_i)^n, \quad H(\alpha_i) \leq (4H(f))^{n+1}$$

$(1 \leq i \leq n)$ and $H(\alpha_1 + \ldots + \alpha_n) \leq nH(\alpha_1)\cdots H(\alpha_n)$ (see for example [22, Lemma 1]). For an arbitrary polynomial in $K[X,Y]$ we define its height, denoted also by H, as the maximum of the heights of its coefficients and we denote by $h = \log H$ the absolute logarithmic Weil height on $K[X,Y]$.

Over a finite field extension of K we get that the binary form $G(X,Y) = \sum_{0 \leq i \leq n} \beta_i X^{n-i} Y^i \in K[X,Y]$ factors as $\prod_{1 \leq j \leq n}(\rho_j X - \xi_j Y)$ and then the discriminant of G is defined as

$$\Delta(G) = \prod_{1 \leq i < j \leq n} (\rho_i \xi_j - \rho_j \xi_i)^2.$$

The discriminant $\Delta(G)$ has the properties (see [22, p. 169]) that $\Delta(G) \in \mathbb{Z}[\beta_0, \ldots, \beta_n]$ and $\Delta(\alpha G) = \alpha^{2n-2}\Delta(G)$. The pullback $\Psi^* G$ of G by $\Psi \in \mathrm{GL}_2(K)$ can be written as

$$\Psi^* G(X,Y) = G(\alpha X + \beta Y, \gamma X + \delta Y) \text{ for } \Psi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

and has discriminant $\Delta(\Psi^* G) = (\det \Psi)^{n(n-1)}\Delta(G)$.

Next we prove some elementary results for binary forms which we did not find in the literature in the form we need them in the proof of the proposition below. Suppose that $f(X) = \alpha_0 X^n + \ldots + \alpha_n \in K[X]$ has degree $n \geq 1$. We write the monic polynomial

$$\alpha_0^{-1} f(X) = \prod_{1 \leq j \leq n} (X - \gamma_j) \in K[X]$$

as a product taken over k of irreducible and monic $f_k(X) \in K[X]$ and we denote by F and F_k the homogenizations in $K[X,Y]$ of f and f_k respectively. Let $\rho : K \to \mathrm{GL}_2(K)$ be the representation given by

$$\tau \mapsto \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}.$$

Then $(\tau, f) \mapsto \tau^* f$ with $\tau^* f(X) = \rho(\tau)^* F(X, 1)$ defines an action of K on $K[X]$. We recall that T is an arbitrary finite set of places of K, that $\mathcal{O}_T$ denotes the T-integers in K and that $\mathcal{O}_T^\times$ are the units in $\mathcal{O}_T$. If G is a binary form with no multiple factors, then we denote by $d_T(G)$ and $(G)_T$ the T-discriminant and the $\mathcal{O}_T$-ideal of G respectively. Let $|\mathfrak{a}|_T$ be the T-norm of an $\mathcal{O}_T$-ideal $\mathfrak{a}$ of K. For these definitions see for example [22, p. 173].

Lemma 2.9. *The discriminant of F and f are equal and the binary forms $F_k \in K[X, Y]$ are irreducible and satisfy $\prod_k F_k = \alpha_0^{-1} F$. If $F \in \mathcal{O}_T[X, Y]$ is monic with $\Delta(F) \in \mathcal{O}_T^\times$, then $d_T(F) = \mathcal{O}_T$.*

Proof. The leading coefficient $\alpha_0 \in K^\times$ of F is the product of the elements ρ_j, thus all ρ_j are nonzero and then with $F(X, 1) = f(X)$ we get

$$F(X, Y) = \prod_{1 \le j \le n} \rho_j (X - \frac{\xi_j}{\rho_j} Y) = \alpha_0 \prod_{1 \le j \le n} (X - \gamma_j Y),$$

which implies $\Delta(F) = \Delta(f)$. We write F_k as a product taken over l of irreducible and monic binary forms $F_{kl} \in K[X, Y]$. Let n_k and n_{kl} be the degree of F_k and F_{kl} respectively. The polynomial $F_k(X, 1)$ has degree n_k, hence all $F_{kl}(X, 1) \in K[X]$ have also degree $n_{kl} \ge 1$ respectively. Thus the properties of $f_k \in K[X]$ show that $f_k(X) = F_{kl}(X, 1)$ for some l, which implies that $F_k = F_{kl}$ is irreducible. We observe that $\prod_k f_k$ has the same coefficients as $\alpha_0^{-1} F$ which implies the second statement. The $\mathcal{O}_T$-ideal $(F)_T^{-1}$ consists of the elements $\alpha \in K$ such that $\alpha F \in \mathcal{O}_T[X, Y]$. This gives for our monic $F \in \mathcal{O}_T[X, Y]$ that $(F)_T^{-1} = \mathcal{O}_T$ and then our assumption $\Delta(F) \in \mathcal{O}_T^\times$ leads to $d_T(F) = \mathcal{O}_T$. □

Based on the effective resolution of T-unit equations we now give a proposition which allows us later to construct Weierstrass schemes with effectively bounded height. In the sequel k_0 is an effectively computable absolute constant. Let N_T be the product taken over the finite places $v \in T$ of the number of elements in the residue field of v. Let t be the number of finite places in T and let q be the largest residue characteristic of the finite places in T. As before d and D_K denote the degree of K and the absolute value of the field discriminant of K over $\mathbb{Q}$ respectively. For an arbitrary set of places $S \subseteq T$ let $\mathcal{O}_S$ be the ring of S-integers and for an integer n we define $\mu = 3n(n-1)(n-2)d$.

Proposition 2.10. *Suppose $f \in \mathcal{O}_S[X]$ has degree $n \ge 3$ and discriminant $\Delta(f) \in \mathcal{O}_T^\times$ and let F be the homogenization of f in $\mathcal{O}_U[X, Y]$. Then the following two statements hold.*

(i) If f is monic, then there is a unipotent translation $\rho(\tau) \in \mathrm{SL}_2(\mathcal{O}_S)$ such that $h(\tau^* f) \le nh(\Delta(f)) + (N_T D_K^{1/3})^{\mu}(\mu(t+1))^{4\mu(t+1)}$.

(ii) In general there exists an element $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ which satisfies that $h(\Phi^* F) \le 22nh(\Delta(F)) + q^{2n^8 d(t^2+1)^2} D_K^{2n^8(t+1)}(n(t+d))^{k_0 n^8 d(t^2+1)^2}$.

Proof. (i) We start with some notation. Since $n \ge 3$ we can choose pairwise different roots α, β, γ of f. For $L = K(\alpha, \beta, \gamma)$ the quantities D_L, l, U, R_U and u denote the absolute value of the discriminant of L over $\mathbb{Q}$, the degree $[L : \mathbb{Q}]$, the places of L which lie above T together with the infinite places of L, the U-regulator of L and the number of finite places in U respectively. For brevity we write $m = n(n-1)(n-2)$.

First we show that $H(\alpha - \gamma)$ is bounded explicitly in terms of n, K, T and $H(\Delta(f))$. The roots of our monic $f \in \mathcal{O}_U[X]$ are U-integral and $\Delta(f)$ is a U-unit. This shows that all factors of $\Delta(f)$ are T-units, in particular $\alpha - \beta$, $\beta - \gamma$ and $\alpha - \gamma$. Therefore we get a U-unit equation

$$\frac{(\alpha-\beta)}{(\alpha-\gamma)} + \frac{(\beta-\gamma)}{(\alpha-\gamma)} = 1.$$

An application of [29, Theorem 1] to the solutions of this U-unit equation gives a constant $\Omega_U = \exp(7\kappa_T R_U N_T^m \max(1, \log R_U))$, for $\kappa_T = c_1(md, m(t+d))$ defined in [29, Theorem 1], such that

$$H\left(\frac{\gamma-\alpha}{\alpha-\beta}\right) \le \Omega_U. \tag{23}$$

The term Ω_U depends on R_U for which we now derive an upper bound in terms of K, n and T. For n_U defined similarly as n_T with U in place of T we deduce $n_U \le ((l/d)^t n_T)^{l/d}$ and then (22), with L and U in place of K and T respectively, leads to

$$R_U \le (2l)^{l-1} D_L^{1/2} \max(1, D_L)^{l-1}((l/d)^t n_T)^{l/d}.$$

To get a sharp estimate for D_L in terms of T we first show that $(D_{L/K})_T = \mathcal{O}_T$, where $D_{L/K}$ is the relative discriminant of L over K. We consider for $\kappa \in \{\alpha, \beta, \gamma\}$ the field $M = K(\kappa)$, we write $f(X)$ as a product of irreducible monic polynomials $f_k(X) \in K[X]$ and we let F and F_k be the homogenizations in $K[X,Y]$ of f and f_k respectively. Lemma 2.9 implies that $F = \prod_k F_k$ can be associated to a system of fields which contains the field M and then [22, Lemma 15] shows

$$d_T(F) \subseteq (D_{M/K})_T,$$

for $D_{M/K}$ the relative discriminant of M over K. Thus our assumption that $\Delta(f) \in \mathcal{O}_T^\times$ together with Lemma 2.9 shows that $(D_{M/K})_T$ is trivial. Let $\mathfrak{D}_{L/K}$ and $\mathfrak{D}_{M/K}$ be the relative different of L and M over K respectively. The multiplicativity of differents in towers together with [68, Lemma 6] leads to $\mathfrak{D}_{L/K} | \prod_\kappa \mathfrak{D}_{M/K}$ and taking the norm from L into K gives

$$D_{L/K} | \prod_\kappa D_{M/K}^{[L:M]}.$$

Thus we deduce that $(D_{L/K})_T = \mathcal{O}_T$, since all $(D_{M/K})_T$ are trivial and then the arguments of [22, p. 194] show

$$D_L \leq (D_K N_T)^{l/d} (l/d)^{lt}.$$

This together with the above upper bound for R_U and the estimate $l/d \leq n(n-1)(n-2) = m$ gives $R_U \leq c_K c_T$, for

$$c_K = D_K^{m/2} (3m^3 d^2 \max(1, \log D_K))^{md-1},$$

$$c_T = (N_T^{1/2} n_T)^m (\max(t,1) m^{2t} \max(1, \log N_T))^{md-1}.$$

Then we replace in the definition of Ω_U the term R_U by $c_K c_T$ and denote by Ω the resulting term. Hence we get $\Omega_U \leq \Omega$ and since the roots α, β, γ of f were chosen arbitrarily it follows from (23) that $H(\Delta(f)(\alpha-\beta)^{-n(n-1)}) \leq (2\Omega^2)^{n(n-1)}$. This leads to $H(\alpha-\beta)^{n(n-1)} \leq H(\Delta(f))(2\Omega^2)^{n(n-1)}$ which together with (23) gives

$$H(\alpha-\gamma) \leq 2\Omega^3 H(\Delta(f))^{1/(n(n-1))}. \tag{24}$$

To construct $\tau \in \mathcal{O}_U$ such that $H(\alpha-\tau)$ is bounded in terms of Ω, n and $H(\Delta(f))$ we shall use [22, Lemma 6]. The latter says that if $\mathfrak{a}$ is an integral $\mathcal{O}_U$-ideal and $\beta_0 \in \mathcal{O}_U$, then there is an $\alpha_0 \in \mathcal{O}_K$ such that $\alpha_0 - \beta_0 \in \mathcal{O}_U$ and such that $H(\alpha_0) \leq d D_K^{1/2} |\mathfrak{a}|_T$. The trace $\mathrm{Tr}(f)$ of $f \in \mathcal{O}_U[X]$ is an element in $\mathcal{O}_U$ and then an application of [22, Lemma 6] with $\beta_0 = \mathrm{Tr}(f)$ and $\mathfrak{a} = n\mathcal{O}_U$ gives $\eta \in \mathcal{O}_K$, $\tau \in \mathcal{O}_U$ such that $\eta = \mathrm{Tr}(f) - n\tau$ and that $H(\eta) \leq \Omega$. Thus $n(\alpha-\tau) = \sum_\delta (\alpha-\delta) + \eta$, with the sum taken over the roots δ of f, combined with (24) leads to

$$H(\alpha-\tau) \leq \Omega^{3n} H(\Delta(f))^{1/n}.$$

We now use several times the estimates $m \geq 6$, $\max(1, \log(c_K c_T)) \leq 3(c_K c_T)^{1/12}$ and $\max(1, \log x) \leq 3x^{1/3}$ for $x \geq 1$ to simplify the form of the final bound. Since $\tau^* f(X) = \prod(X - (\alpha-\tau))$ with the product taken over the roots α of f, we deduce from the above estimate together with

$$\Omega = \exp\bigl(7\kappa_T N_T^m c_K c_T \max(1, \log(c_K c_T))\bigr)$$

an upper bound for $h(\tau^* f)$ as stated in (i).

(ii) An application of [22, Theorem 3] to F gives $\Gamma \in \mathrm{SL}_2(\mathcal{O}_T)$, $\epsilon \in \mathcal{O}_T^\times$ and effective absolute constants c_6, c_7 such that $H(\epsilon(\Gamma^* F)) \leq \Omega$, with

$$\log \Omega = (4n)^{-4}(c_6(d+t)n)^{c_7 dn^8(t+1)^2} q^{2dn^8(t+1)^2} D_K^{2n^8(t+1)}. \tag{25}$$

We now construct with ϵ and Γ an element $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that $\Phi^* F$ has bounded height. From [29, Lemma 3] and [35, Theorem 6.5] we deduce that there exist T-units ϵ_1 and ϵ_2 such that $\epsilon = \epsilon_1 \epsilon_2^n$ and such that $H(\epsilon_1)$ is bounded from above by a term not exceeding Ω. If $\Psi = \epsilon_2 \Gamma$ and $G = \Psi^* F$ then we see that G takes the form $\epsilon_1^{-1}\epsilon(\Gamma^* F)$ which implies

$$H(G) \leq \Omega^2.$$

Furthermore, if $g(X) = G(X,1)$ then Lemma 2.9 implies that $H(\Delta(G)) = H(\Delta(g)) = H(\prod(\xi - \rho))$, where the product is taken over all roots ξ, ρ of $g(X)$ with $\xi \neq \rho$ and this leads to

$$H(\Delta(G)) \leq 2^{n(n-1)}(4H(G))^{2(n+1)(n(n-1))}.$$

Observe that $\Psi^{-1} \in \mathrm{GL}_2(\mathcal{O}_T)$, $F = (\Psi^{-1})^* G$ and that $\det(\Psi^{-1})^{n(n-1)} = \Delta(F)\Delta(G)^{-1}$. Thus the upper bounds for $H(\Delta(G))$ and $H(G)$ give

$$H(\det(\Psi^{-1})) \leq \Omega^{3n} H(\Delta(F))^{1/(n(n-1))}.$$

An application of [22, Lemma 7] to the transpose of Ψ^{-1} gives $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that the maximum $H(\Psi^{-1}\Phi)$ of the multiplicative Weil heights of the standard coordinates of $\Psi^{-1}\Phi$ is at most $\Omega H(\det(\Psi^{-1}))^8$. Since the pullback * induces a right-action of the group $\mathrm{GL}_2(\mathcal{O}_T)$ on the set of binary forms defined over K we see that $\Phi^* F = (\Psi^{-1}\Phi)^* G$.

In the last step we use elementary height properties of polynomials in several variables to get an upper bound for $H(\Phi^* F)$ in terms of n, $H(G)$ and $H(\Psi^{-1}\Phi)$. Let $\mathcal{H}$ be the exponential of the affine height introduced in [31, p. 225]. We observe that $H \leq \mathcal{H} \leq H^{n+1}$ and for

$$\Psi^{-1}\Phi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

we write $\Phi^* F(X,Y) = \sum_{i=0}^n \alpha_i (\alpha X + \beta Y)^{n-i}(\gamma X + \delta Y)^i$, where α_i are the coefficients of G. Then from [31, Proposition B.7.2] we deduce

$$\mathcal{H}(\Phi^* F) \leq \ (n+1)\prod_{i=0}^n \mathcal{H}(\alpha_i(\alpha X + \beta Y)^{n-i}(\gamma X + \delta Y)^i)$$

and also that the i-th factor of the product on the right-hand side is at most

$$2^{3(n+1)}\mathcal{H}(\alpha_i)\mathcal{H}(\alpha X+\beta Y)^{n-i}\mathcal{H}(\gamma X+\delta Y)^i.$$

The inequality $\mathcal{H}\leq H^{n+1}$ shows that $\mathcal{H}(\alpha X+\beta Y)^{n-i}\mathcal{H}(\gamma X+\delta Y)^i$ is bounded from above by $H(\Psi^{-1}\Phi)^{n(n+1)}$ and this leads to

$$H(\Phi^*F)\leq (n+1)(2^3H(G)H(\Psi^{-1}\Phi)^n)^{(n+1)^2}.$$

Therefore statement (ii) follows with $k_0=c_6c_7$ from (25) combined with the above estimates for $H(\Psi^{-1}\Phi)$ and $H(G)$. This completes the proof of the proposition. □

For an arbitrary monic and separable $f\in\mathcal{O}_T[X]$ of degree $n\geq 3$ we let U be the smallest set of places of K which contains T and all the prime divisors of $\Delta(f)$. Then we see that the proof of part (i) gives a unipotent translation $\rho(\tau)\in\mathrm{SL}_2(\mathcal{O}_T)$ such that

$$h(\tau^*f)\leq nh(\Delta(f))+(N_UD_K^{1/3})^\mu(\mu(u+1))^{4\mu(u+1)},$$

for u the number of finite places in U and N_U defined as N_T with U in the place of T. The quantities u and N_U can be bounded effectively in terms of $\Delta(f)$ and T such that the resulting bound improves the actual best effective estimates for monic polynomials with coefficients in $\mathcal{O}_T$ (see [26] and the references in [9] and [27]) and makes them completely explicit. For example we reduced the exponent $n^2(n!)^2d$ of N_U in [26, Theorem 7] to $\mu\leq 6n^3d$. Moreover, it is shown in [26] that such an estimate for $h(\tau^*f)$ has several applications in algebraic number theory which now can be stated with sharper and fully explicit bounds.

We get that k_0 is the product of the effectively computable absolute constants c_6 and c_7 of [22, Theorem 3] and we mention that in course of the proof of Theorem 2.3 (i) we derive with a similar method an other version of the first part of the proposition.

2.6 Proofs

For an outline of the principal ideas of the following proof we refer to the introduction. Let K be a number field with degree d, let D_K be the absolute value of the discriminant of K over $\mathbb{Q}$ and let $M_{\mathrm{fin}}(\alpha)$ denote the set of finite places of $\mathbb{Q}(\alpha)$, where α is an algebraic number over $\mathbb{Q}$.

Proof of Theorem 2.1. We now take a hyperelliptic curve C of genus $g \geq 1$ defined over K with good reduction outside a finite set of places S of K as in the theorem. Lemma 2.4 gives a finite set of places T of K with the properties that T contains the set S, that the ring of T-integers $\mathcal{O}_T$ is a principal ideal domain and that 2 and the residue characteristics of the finite places in T are in the group of units $\mathcal{O}_T^\times$ of $\mathcal{O}_T$. We have to compare the number s of finite places in S, the product N_S taken over the finite places $v \in S$ of the number of elements in the residue field of v and the largest rational prime divisor p of N_S with the corresponding quantities t, N_T and q for T. Lemma 2.4 gives

$$t \leq d(s + h_S) = d\sigma, \;\; N_T \leq (2N_S D_K^{(h_S-1)/2})^d \;\text{ and } q \leq \max(2, p, D_K^{1/2}), \quad (26)$$

for h_S the class number of $\mathcal{O}_S$.

To prove statement (i) we assume that C has a K-rational Weierstrass point. Then an application of Proposition 2.8 (i) to our curve C and the set T gives a globally T-minimal Weierstrass scheme $\mathcal{W}(l)$ of C such that l is monic of degree $2g+1$ with coefficients in $\mathcal{O}_T$ and such that the absolute logarithmic Weil height of $\Delta(l) \in \mathcal{O}_T^\times$ is at most

$$(50g(t+d)!)^2(2dD_K)^{2d}n_T.$$

An application of Proposition 2.10 (i) gives a unipotent translation $\rho(\tau) \in \mathrm{SL}_2(\mathcal{O}_T)$ such that τ^*l has coefficients in $\mathcal{O}_T$ with discriminant $\Delta(\tau^*l) = \Delta(l)$ and that

$$\max\big(h(\Delta(\tau^*l)), h(\tau^*l)\big) \leq 2(\mu(t+1))^{4\mu(t+1)}(N_T D_K^{1/3})^\mu, \quad (27)$$

for $\mu = 3(2g+1)(2g)(2g-1)d = \nu/(2d)$.

In the remaining part of the proof of (i) we show that $\mathcal{W}(\tau^*l)$ extends to a globally T-minimal Weierstrass scheme of C over $\mathcal{O}_K$ with the desired properties. To simplify notation we write

$$n = 2g+1, \quad \eta = 1. \quad (28)$$

Let α be a coefficient of $\tau^*l \in \mathcal{O}_T[X]$. By Lemma 1.5 we see that the positive rational integer

$$\delta(\alpha) = \prod_{w \in M_{\mathrm{fin}}(\alpha)} \max\big(1, |\alpha|_w\big), \quad (29)$$

is at most $H(\alpha)^d$ and satisfies that $\delta(\alpha)\alpha \in \mathcal{O}_K$. The residue characteristic of a finite place in T is invertible in $\mathcal{O}_T$ and only the finite places w of $\mathbb{Q}(\alpha)$

with $\operatorname{ord}_w(\alpha) \leq -1$ contribute to the right-hand side of (29). Since $\alpha \in \mathcal{O}_T$ this shows that

$$\omega = \prod \delta(\alpha) \in \mathcal{O}_T^\times$$

with the product taken over the coefficients α of τ^*l and that $\omega \leq H(\tau^*l)^{d(n+1)}$. By construction we get that $\mathcal{W}(\tau^*l)$ is a globally T-minimal Weierstrass scheme of C over $\mathcal{O}_T$ with discriminant $\Delta' \in \mathcal{O}_T^\times$. The equations $U = \omega^2 X$, $V = \omega^n Y$ induce an isomorphism between the Weierstrass schemes $\mathcal{W}(\tau^*l)$ and $\mathcal{W}(f)$, where the latter is indeed a Weierstrass scheme of C that arises from

$$V^2 = f(U) = \omega^{2n}\tau^*l(U/\omega^2) \in \mathcal{O}_K[U]$$

with discriminant Δ. Then we see that $\Delta \in \mathcal{O}_T^\times \cap \mathcal{O}_K$ and $f \in \mathcal{O}_K[U]$ satisfy $H(\Delta) \leq \omega^{4(g+1-\eta)(2g+1)}H(\Delta')$ and $H(f) \leq \omega^{2n}H(\tau^*l)$ respectively. We now replace N_T and t in (27) by the estimates given in (26) and then we conclude from the above estimates combined with the upper bound for ω that the globally T-minimal Weierstrass scheme $\mathcal{W}(f)$ of C over $\mathcal{O}_K$ has the required properties. This completes the proof of part (i) of Theorem 2.1.

We now prove statement (ii). By assumption the curve C has no K-rational Weierstrass point. Thus Proposition 2.8 (ii), applied to C and T, gives a Weierstrass scheme $\mathcal{W}(l)$ of C with discriminant $\Delta \in \mathcal{O}_T^\times$ such that $l \in \mathcal{O}_T[X]$ has degree $2g+2$ and that the absolute Weil height of $\Delta(l) \in \mathcal{O}_T^\times$ is effectively bounded in terms of K, T and g. Then an application of Proposition 2.10 (ii) to the homogenization $L \in \mathcal{O}_T[X,Y]$ of l gives

$$\Phi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_T)$$

and an effectively computable absolute constant k_0 such that

$$h(\Phi^*L) \leq 2q^{2n^8 d(t^2+1)^2} D_K^{2n^8(t+1)} (n(t+d))^{k_0 n^8 d(t^2+1)^2}, \tag{30}$$

for $n = 2g+2$. Let $\Phi^*l(X) = \Phi^*L(X,1)$ and since $\Phi \in \mathrm{SL}_2(\mathcal{O}_T)$ we get from Lemma 2.9 that $\Delta(\Phi^*l) = \Delta(l)$.

We next show that $\mathcal{W}(\Phi^*l)$ is a Weierstrass scheme of C. The group $\mathrm{SL}_2(\mathcal{O}_T)$ acts on the non-constant rational functions of $K(C)$ by fractional linear transformations, hence we get a non-constant rational function $U = \Phi^{-1}X \in K(C)$. Therefore $V = Y(\gamma U + \delta)^{g+1}$ is non-constant in $K(C)$ and then we can rewrite the equation $Y^2 = l(X)$ as

$$\frac{V^2}{(\gamma U + \delta)^{2g+2}} = l(\frac{\alpha U + \beta}{\gamma U + \delta}).$$

After multiplying both sides of this equation by $(\gamma U+\delta)^{2g+2}$ we obtain

$$V^2=\sum_{i=0}^{2g+2}\alpha_i(\alpha U+\beta)^{2g+2-i}(\gamma U+\delta)^i=L(\alpha U+\beta,\gamma U+\delta)=\Phi^*l(U)$$

with α_i the coefficients of l. This shows that $\mathcal{W}(\Phi^*l)$ is indeed a Weierstrass scheme of C.

Then (30) together with the arguments of the proof of part (i) (where now $n=2g+2$, $\eta=0$ in (28) and where now Φ^*l plays the role of τ^*l) gives statement (ii). This completes the proof of Theorem 2.1. □

We shall use the notation introduced in course of the proof of Theorem 2.1 to prove our second theorem in this chapter.

Proof of Theorem 2.3. Let $\mu=\nu/(2d)$, let r be the radical of the integer N_T and let ω be the number of rational prime divisors of r. We observe that $t\leq d\omega$ and that explicit versions of the prime number theorem in [56] lead to $\omega^\omega\leq r^3$. From this we deduce

$$(\mu(t+1))^{4\mu(t+1)}\leq(2\mu)^{4\mu}N_T^{5(\mu d)^2/2-\mu}. \tag{31}$$

A hyperelliptic curve C over K of genus g has good reduction outside its bad reduction set S_C. Therefore the arguments of the proof of Theorem 2.1 give the statement, where now in (i) we combine (27) with the estimate (31). □

It remains to prove Corollary 2.2. Let S be a finite set of places of a number field K and let h_S, s, p, d and D_K be the quantities defined in (21). We denote by $N_{\mathcal{H}}=N_{\mathcal{H}}(K,S,g)$ the number of K-isomorphism classes of hyperelliptic curves of genus g defined over K with good reduction outside S.

Proof of Corollary 2.2. Theorem 2.1 shows that there is an explicit constant $\Omega=\Omega(K,S,g,k_0)$, for k_0 an effectively computable absolute constant, with the following property. Every hyperelliptic curve C over K of genus g with good reduction outside S gives a polynomial $f\in\mathcal{O}_K[X]$ of degree at most $2g+2$ with absolute multiplicative Weil height H at most Ω.

If two such curves give the same f, then their function fields are described by the hyperelliptic equation $Y^2=f(X)$ and we see that these curves are K-isomorphic. This implies that $N_{\mathcal{H}}$ is bounded from above by the number of polynomials $f \in K[X]$ with $H(f) \leq \Omega$. Thus an explicit Northcott theorem [11, Theorem 1.6.8] yields

$$N_{\mathcal{H}} \leq (5\Omega)^{10d^2g}$$

and then (27) leads to an upper bound for Ω which shows that the estimate of Corollary 2.2 holds as stated.

The polynomials in $K[X]$ with bounded degree and absolute height can be determined effectively (for details we refer to the discussions in [11]). Thus the effective upper bound given in the theorem implies that the K-isomorphism classes of hyperelliptic curves over K of genus g with good reduction outside S can be determined effectively. This completes the proof of Corollary 2.2. □

3 Some applications

3.1 Introduction

In this section we first generalize Szpiro's Discriminant Conjecture to arbitrary hyperelliptic curves C over a number field K. Then we prove an exponential version of this conjecture and we deduce an effective upper bound for the Arakelov degree of an elliptic curve over K in terms of its conductor. Further, if C is elliptic or has genus 2, then we derive an effective estimate for the geometric discriminant of C in terms of the conductor. We get the same estimate also for the number of singular points on the geometric special fibers of the minimal regular model of C over the ring of integers in K.

Next we introduce quasi-minimal Weierstrass schemes of an arbitrary hyperelliptic curve C over a number field K which has a K-rational Weierstrass point. Then we generalize the Height Conjecture of Frey for elliptic curves to the more general curves C and we prove an effective exponential version of this conjecture. From this we deduce new results for modular Jacobians.

3.2 On Szpiro's Discriminant Conjecture

Let C be a hyperelliptic curve of genus $g \geq 1$ defined over a number field K. We denote by $\mathcal{O}_K$ the ring of integers of K. For a closed point $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$ we denote by $\mathcal{W}_\mathfrak{p}$ a minimal Weierstrass scheme of C over the local ring $\mathcal{O}_\mathfrak{p}$ at $\mathfrak{p}$ and we denote by $\Delta_\mathfrak{p}$ its minimal discriminant (defined in chapter 2). The positive integer $n_\mathfrak{p} = \operatorname{ord}_\mathfrak{p}\Delta_\mathfrak{p}$ is independent of the choice of $\mathcal{W}_\mathfrak{p}$ and then we define the minimal discriminant ideal of C as $\mathfrak{D}_C = \prod \mathfrak{p}^{n_\mathfrak{p}}$ with the product taken over all closed points $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$. Let

$$\Delta_C = N_{K/\mathbb{Q}}(\mathfrak{D}_C) \tag{32}$$

and let N_C be the conductor of C (defined in (19)). We now generalize Szpiro's Discriminant Conjecture [71, Conjecture 1] to arbitrary hyperelliptic curves over K.

Conjecture 3.1. *There exist constants c, κ, depending only on K and $g \geq 1$, such that if C is a hyperelliptic curve defined over K of genus g, then*

$$\Delta_C \leq c N_C^\kappa.$$

We give some motivation for this conjecture. For hyperelliptic curves with a K-rational Weierstrass point Lockhart stated in [39] an even stronger conjecture and he showed in [39, Proposition 4.3] that the *abc*-Conjecture of

Masser and Oesterlé for number fields [41] implies Conjecture 3.1 for a special class of hyperelliptic curves over K. Furthermore, Nguyen [48] proved a complex function field analogue of Conjecture 3.1 for hyperelliptic fibrations. The following result gives an effective exponential version of Conjecture 3.1.

Theorem 3.2. *There exist effective constants c_1, κ_1, depending only on K and $g \geq 1$, such that if C is a hyperelliptic curve defined over K of genus g with a K-rational Weierstrass point, then*

$$\log \Delta_C \leq c_1 N_C^{\kappa_1}.$$

If C has no K-rational Weierstrass point, then we still get an effective estimate for $\log \Delta_C$ in terms of K, g and N_C. We omit to work out explicitly this estimate since it would be exponential in terms of N_C.

Let d be the degree of K over $\mathbb{Q}$, let D_K be the absolute value of the field discriminant of K over $\mathbb{Q}$ and let h_K be the class number of K. In the above theorem we can take for example

$$\kappa_1 = \nu^2 = (6(2g+1)(2g)(2g-1)d^2)^2, \quad c_1 = (2^d D_K^{h_K/2})^{\kappa_1}. \tag{33}$$

The dependence of these constants on the terms d, D_K, h_K and g can be sharpened to a certain extent (see the discussion in chapter 2). But to get rid of the logarithm in the above theorem our method needs at least bounds for linear forms in logarithms which are equivalent (see Baker [6]) to the *abc*-Conjecture for $\mathbb{Q}$.

We mention that for elliptic curves over $\mathbb{Q}$ the *abc*-Conjecture implies Szpiro's Discriminant Conjecture and that Stewart and Yu [69, Theorem 1] proved an exponential version of the *abc*-Conjecture for $\mathbb{Q}$. It seems (see the standard links in [49] and the references there) that these results can not be combined to cover our theorem in the case of elliptic curves over $\mathbb{Q}$. On the other hand, the arguments in [49] together with our theorem give a version of the *abc*-Conjecture for number fields that is essentially of the same shape as the main results in [69], [28].

Proof of Theorem 3.2. We take a hyperelliptic curve C of genus $g \geq 1$ defined over K of conductor N_C as in the theorem. An application of Theorem 2.3 to C gives a Weierstrass scheme $\mathcal{W}$ of C over $\mathcal{O}_K$ with discriminant $\Delta \in \mathcal{O}_K$ such that $h(\Delta)$ is bounded effectively in terms of N_C, g and K. We assume that a closed point $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$ divides $\mathfrak{D}_C$ with an exponent $n_\mathfrak{p}$. The scheme $\mathcal{W}$ arises from a hyperelliptic equation for C defined over $\mathcal{O}_K \subset \mathcal{O}_\mathfrak{p}$ and then the minimality property of $\mathfrak{D}_C$ shows $n_\mathfrak{p} \leq \operatorname{ord}_\mathfrak{p}(\Delta)$. Thus we see that $\Delta_C \leq N_{K/\mathbb{Q}}(\Delta)$ which implies

$$\log \Delta_C \leq h(\Delta).$$

Hence the estimate of Theorem 2.3 for $h(\Delta)$ leads to the upper bound for Δ_C as stated. This completes the proof of Theorem 3.2. □

For elliptic curves over K we now give an interpretation of our theorem in terms of Arakelov geometry.

Corollary 3.3. *The Arakelov degree of the direct image of the relative dualizing sheaf of a minimal regular model over* $\mathrm{Spec}(\mathcal{O}_K)$ *with generic fiber an elliptic curve E over K is at most*

$$(2^d D_K^{h_K})^{(6d)^4} N_E^{(6d)^4}.$$

Proof. Let $\deg_{\mathrm{Ar}}(\omega_E)$ be the Arakelov degree of the direct image of the relative dualizing sheaf of a minimal regular model over $\mathrm{Spec}(\mathcal{O}_K)$ with generic fiber an elliptic curve E over K. If E has semi-stable reduction over $\mathrm{Spec}(\mathcal{O}_K)$, then a result of Szpiro [72, Theorem] gives

$$12\deg_{\mathrm{Ar}}(\omega_E) = \log \Delta_E.$$

Furthermore, the arguments of Ullmo (see [73, p. 1049]) show that this equality holds also in the non-semistable case. Therefore Theorem 3.2 implies the statement. □

The definition of the minimal discriminant ideal of a hyperelliptic curve is intrinsic but unnatural in the sense that a generalization to an arbitrary smooth, projective and geometrically connected curve X of genus $g \geq 1$ over K fails. Following Deligne [19], we now define a discriminant also for these more general curves X. Let $\mathcal{X}$ be a minimal regular model of X over $\mathrm{Spec}(\mathcal{O}_K)$, let $\mathfrak{p}$ be a closed point in $\mathrm{Spec}(\mathcal{O}_K)$, and let $S = \mathrm{Spec}(\mathcal{O}_\mathfrak{p})$. The morphism $\rho : \mathcal{X} \times_{\mathcal{O}_K} S \to S$, obtained by base change to S, gives a minimal regular model of X over S and a result of Mumford [47, Theorem 5.10] provides an isomorphism

$$\det R\rho_*(\omega_{\mathcal{X}/S}^{\otimes 2}) \otimes K \to (\det R\rho_*\omega_{\mathcal{X}/S})^{\otimes 13} \otimes K,$$

for $\omega_{\mathcal{X}/S}$ the relative dualizing sheaf of $\mathcal{X}$ over S. This isomorphism gives a canonical non-zero rational section δ of the invertible $\mathcal{O}_S$-module

$$\mathcal{L} = (\det R\rho_*\omega_{\mathcal{X}/S})^{\otimes 13} \otimes \det R\rho_*(\omega_{\mathcal{X}/S}^{\otimes 2})^{\otimes -1}.$$

Then the normalized valuation $\delta_\mathfrak{p}$ of δ, defined by $\mathcal{O}_S \cdot \delta = \mathfrak{p}^{\delta_\mathfrak{p}}\mathcal{L}$, and the number of irreducible components $m_\mathfrak{p}$ of the geometric special fiber of ρ are independent of the choice of $\mathcal{X}$. Since only finitely many fibers of $\mathcal{X}$ are not smooth, we can define

$$\delta_X = \prod N_{K/\mathbb{Q}}(\mathfrak{p})^{\delta_\mathfrak{p}}, \ m_X = \sum (m_\mathfrak{p} - 1)$$

with product and sum taken over the closed points of $\operatorname{Spec}(\mathcal{O}_K)$. The positive rational integers δ_X and m_X are invariants of X.

We now can state our corollary. It is a consequence of Theorem 3.2 and results of Bloch, Liu, Ogg and Saito.

Corollary 3.4. *Suppose C is a smooth, projective and geometrically connected curve over K of genus $1 \le g \le 2$. If C has a K-rational Weierstrass point, then $\log \delta_C$ and m_C are at most $c_1 N_C^{\kappa_1}$.*

If C is hyperelliptic over K of genus $g \le 2$ and has no K-rational Weierstrass point, then we get an effective estimate for $\log \delta_C$ and m_C which is exponential in the conductor N_C.

It seems possible to derive from Theorem 3.2 similar results also for arbitrary hyperelliptic curves C with genus $g \ge 3$ over K. The strategy is as follows. For the discriminant $\Lambda_\mathfrak{p}$ of C introduced by Kausz [33] one can show that $\Lambda_\mathfrak{p} \le n_\mathfrak{p}$ (see the proof of [37, Proposition 2 (d)]). Hence it suffices to estimate $\delta_\mathfrak{p}$ effectively in terms of $\Lambda_\mathfrak{p}$. A result of Maugeais [45] implies for curves C with stable reduction over $\operatorname{Spec}(\mathcal{O}_K)$ that $\delta_\mathfrak{p} \le \Lambda_\mathfrak{p}$ which then leads to $\log \delta_C \le c_1 N_C^{\kappa_1}$. But the general case remains an interesting project.

Conjecture 3.1 implies that the invariants $m_\mathfrak{p}$, $\delta_\mathfrak{p}$ of the curves C in the above corollary are bounded only in terms of K.

For our proof of Corollary 3.4 we need to introduce some further notation. We fix an algebraic closure $\overline{K}$ of K. Let $\mathfrak{p}$ be a closed point in $\operatorname{Spec}(\mathcal{O}_K)$ with residue field k and we write $S = \operatorname{Spec}(\mathcal{O}_\mathfrak{p})$. We denote by $X_{\overline{K}}$ and $X_{\overline{k}}$ the geometric generic and geometric special fiber of $\rho : \mathcal{X} \to S$ respectively. Following Saito, we define

$$\operatorname{Art}_\mathfrak{p}(X) = \chi(X_{\overline{K}}) - \chi(X_{\overline{k}}) - \delta,$$

where χ is the Euler characteristic for the étale topology and where δ is the Swan conductor associated to a l-adic representation (defined in ([58])). For brevity we shall write $\operatorname{Art}_\mathfrak{p} = \operatorname{Art}_\mathfrak{p}(X)$.

Proof of Corollary 3.4. Let $\mathfrak{p}$ be an arbitrary closed point in $\operatorname{Spec}(\mathcal{O}_K)$ with residue field k.

We first suppose that C has genus one. By assumption C has a K-rational point O and then we write E for the elliptic curve (C, O) over K. Observe that any two K-rational points of E are related by a K-isomorphism (a translation) of C. Hence our definition of $n_{\mathfrak{p}}$ coincides with the order of $\mathfrak{p}$ in the usual minimal discriminant ideal of an elliptic curve and then Saito's results [57, Corollary 2] and [57, Theorem 1] state

$$n_{\mathfrak{p}} = -\mathrm{Art}_{\mathfrak{p}} \text{ and } \delta_{\mathfrak{p}} = -\mathrm{Art}_{\mathfrak{p}}$$

respectively. We take $m = 1$ in Bloch's result [10, Lemma 1.2 (i)] (see also Ogg's formula [50]) which gives

$$-\mathrm{Art}_{\mathfrak{p}} = m_{\mathfrak{p}} + f_{\mathfrak{p}} - 1, \tag{34}$$

and then Theorem 3.2 gives the desired upper bound for m_E and δ_E.

For the second part we now assume that C has genus 2. To apply results of Liu [36] and Saito [57] we work over the strict henselisation $\mathcal{O}$ of $\mathcal{O}_{\mathfrak{p}}$. If $S' = \mathrm{Spec}(\mathcal{O})$, then $\rho' : \mathcal{X} \times_S S' \to S'$ gives a minimal regular model of $C' = C \times_K L$ over S', for $L \supset K$ the field of fractions of $\mathcal{O} \supset \mathcal{O}_{\mathfrak{p}}$. Let $\Delta_{\min}$ and $\Delta'_{\min}$ be the minimal discriminants at $\mathfrak{p}$ of C and C' respectively, introduced by Liu in [36, Definition 1], and let $\mathrm{Art}'_{\mathfrak{p}}$ and $\delta'_{\mathfrak{p}}$ be the Artin conductor and the discriminant of C' respectively. Then we get

$$\mathrm{Art}_{\mathfrak{p}} = \mathrm{Art}'_{\mathfrak{p}}, \quad \delta'_{\mathfrak{p}} = \delta_{\mathfrak{p}} \tag{35}$$

and we observe that the residue field of the henselian ring $\mathcal{O}$ is algebraically closed. Hence over $\mathcal{O}$ we can use [36, Theorème 1] and [36, Theorème 2]. The former result shows that $-\mathrm{Art}'_{\mathfrak{p}} \leq \mathrm{ord}_{\mathfrak{p}}\Delta'_{\min}$ and the latter result gives that $\mathrm{ord}_{\mathfrak{p}}\mathfrak{D}_{C'} = \mathrm{ord}_{\mathfrak{p}}\Delta'_{\min} + 10\big(\mathrm{ord}_{\mathfrak{p}}\Delta'_{\min} + \mathrm{Art}'_{\mathfrak{p}}\big)$. This leads to

$$-\mathrm{Art}'_{\mathfrak{p}} \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}_{C'}.$$

Saito [57, Theorem 1] gives $-\mathrm{Art}'_{\mathfrak{p}} = \delta'_{\mathfrak{p}}$ which together with (35) implies that $-\mathrm{Art}_{\mathfrak{p}} = \delta_{\mathfrak{p}}$. Then the above estimate for $-\mathrm{Art}'_{\mathfrak{p}}$ combined with (35) shows

$$\delta_{\mathfrak{p}} = -\mathrm{Art}'_{\mathfrak{p}} \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}_{C'} = \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}_C.$$

As in (34) we get $-\mathrm{Art}_{\mathfrak{p}} = m_{\mathfrak{p}} + f_{\mathfrak{p}} - 1$. We conclude the inequalities $m_{\mathfrak{p}} \leq \delta_{\mathfrak{p}} + 1 \leq \mathrm{ord}_{\mathfrak{p}}\mathfrak{D}_C + 1$ and then the stated estimate for $\log \delta_C$ and m_C follows from Theorem 3.2. This completes the proof of Corollary 3.4. □

3.3 On the Height Conjecture

Let C be a hyperelliptic curve of genus $g \geq 1$ over a number field K. In this section we shall always assume that C has a K-rational Weierstrass point P (see the discussions after Theorem 3.6). To simplify the notation we shall write C for the pair (C, P) and then also $\mathfrak{D}_C$ for $\mathfrak{D}_{(C,P)}$, where the latter is the minimal discriminant of (C, P) defined in [39].

To state our results we now define quasi-minimal Weierstrass schemes of C over the ring of integers $\mathcal{O}_K$ of K. When $\mathcal{O}_K$ is not a principal ideal domain these schemes substitute the globally minimal Weierstrass schemes of C over $\mathcal{O}_K$ (defined in chapter 2). They provide a link between arithmetic and geometric properties of hyperelliptic curves (see the applications discussed in chapter 0). Our curve C has a Weierstrass equation

$$Y^2 + k(X)Y = f(X), \tag{36}$$

where $f \in \mathcal{O}_K[X]$ is monic of degree $2g + 1$ and where $k \in \mathcal{O}_K[X]$ has degree at most g. Let $\mathcal{W}(f, k)$ be a Weierstrass scheme of C, arising from a Weierstrass equation (36), with discriminant Δ. We say that $\mathcal{W}(f, k)$ is a quasi-minimal Weierstrass scheme of C over $\mathcal{O}_K$ if $N_{K/\mathbb{Q}}(\Delta)$ is minimal when taken over all discriminants of Weierstrass equations (36) for C. The curve C has always a quasi-minimal Weierstrass scheme over $\mathcal{O}_K$ and a globally minimal Weierstrass scheme of C over $\mathcal{O}_K$ is, a forteriori, quasi-minimal over $\mathcal{O}_K$.

As in chapter 2 we denote by $h(\mathcal{W}(f, k))$ the height of $\mathcal{W}(f, k)$ and by N_C the conductor of C.

Conjecture 3.5. *There are constants c, κ, depending only on K and $g \geq 1$, with the following property. If C is a hyperelliptic curve defined over K of genus g with a K-rational Weierstrass point, then there is a quasi-minimal Weierstrass scheme $\mathcal{W}(f, k)$ of C over $\mathcal{O}_K$ with*

$$H(\mathcal{W}(f, k)) \leq c N_C^{\kappa}.$$

From [63] we see that this conjecture generalizes Conjecture 0.2 to hyperelliptic curves C over K with a K-rational Weierstrass point. A motivation for this conjecture is the next theorem which gives an effective exponential version. Furthermore, for elliptic curves Frey proved in [25] a function field version of this conjecture. Let c_1, κ_1 be the explicit constants given in (33).

Theorem 3.6. *Suppose C is a hyperelliptic curve over K of genus $g \geq 1$ with a K-rational Weierstrass point. Then there is a quasi-minimal Weierstrass scheme $\mathcal{W}(f,k)$ of C over $\mathcal{O}_K$ with*

$$h(\mathcal{W}(f,k)) \leq c_1 N_C^{\kappa_1}.$$

Our method combined with a modification of Lemma 3.7 gives also an effective estimate in terms of K, g and N_C for quasi-minimal Weierstrass schemes of hyperelliptic curves without a K-rational Weierstrass point. These modifications are only of technical nature but the resulting bounds are so big that the technical effort will not be worth it.

We briefly discuss how our theorem leads to an effective upper bound, of the same shape as in the theorem, for the absolute Faltings height h_{abs} of the Jacobian over K of an arbitrary hyperelliptic C over K. The crucial point is that h_{abs} is stable under finite field extensions and that the field of definition $L = K(P)$ of one of the $2g+2$ Weierstrass points P of C can be controlled effectively in terms of g, K and N_C. Hence we can apply our theorem to the hyperelliptic curve $C \times_K \operatorname{Spec}(L)$ which has a L-rational Weierstrass point and then by results of Bost-David we can compare effectively h_{abs} with $h(\mathcal{W}(f,k))$ (see [17]). In particular this gives an effective upper bound, of the shape as in the theorem, for the relative Faltings height h_{rel} of the Jacobians over K of semi-stable hyperelliptic curves over K.

The arguments of the last section indicate that the exponential versions of the *abc*-Conjecture of Stewart-Yu and Győry do not imply directly our theorem in the elliptic case.

Before we go into the proof of Theorem 3.6 we expose briefly the principal ideas. A lemma together with Theorem 3.2 gives a Weierstrass scheme $\mathcal{W}(f_0)$ of C over $\mathcal{O}_K$ with discriminant Δ_0 such that $h(\Delta_0) \leq c_1 N_C^{\kappa_1}$. Proposition 2.10 then gives a unipotent translation $\rho(\tau) \in \mathrm{SL}_2(\mathcal{O}_K)$ such that $\mathcal{W}(\tau^* f_0)$ has height bounded as stated. Finally we show that $\tau^* f_0$ takes the form $f + k^2/4$, for $\mathcal{W}(f,k)$ a quasi-minimal Weierstrass scheme of C over $\mathcal{O}_K$.

Proof of Theorem 3.6. We start with the following lemma which allows to control the discriminant of quasi-minimal Weierstrass schemes.

Lemma 3.7. *If $\mathcal{W}(f,k)$ is a quasi-minimal Weierstrass scheme of C over $\mathcal{O}_K$ with discriminant Δ, then $N_{K/\mathbb{Q}}(\Delta) \leq D_K^{2g(2g+1)} \Delta_C$.*

Proof. From [34, Theorem 4, p. 119] we get an integral ideal $\mathfrak{a}$ in the Weierstrass class of C (defined in [39, p. 737]) with $N_{K/\mathbb{Q}}(\mathfrak{a}) \leq D_K^{1/2}$. Then [39, Proposition 2.8] gives a Weierstrass scheme of C with discriminant Δ', arising from a Weierstrass equation (36) of C, such that

$$\Delta'\mathcal{O}_K = \mathfrak{a}^{4g(2g+1)}\mathfrak{D}_C. \tag{37}$$

Since $\mathcal{W}(f,k)$ is a quasi-minimal Weierstrass scheme of C over $\mathcal{O}_K$, we get $N_{K/\mathbb{Q}}(\Delta) \leq N_{K/\mathbb{Q}}(\Delta')$. Then the above equality of ideals together with the upper bound for the norm of $\mathfrak{a}$ leads to

$$N_{K/\mathbb{Q}}(\Delta) \leq D_K^{2g(2g+1)}\Delta_C,$$

which completes the proof of the lemma. □

Let $\mathcal{W}(l,m)$ be a quasi-minimal Weierstrass scheme of C over $\mathcal{O}_K$ with discriminant Δ'. From [22, Lemma 10] we get $\epsilon \in \mathcal{O}_K^\times$ such that

$$h(\epsilon^{4g(2g+1)}\Delta') \leq \log N_{K/\mathbb{Q}}(\Delta') + 12g^2(6d^3)^d R_K. \tag{38}$$

We now consider the Weierstrass scheme $\mathcal{W}(f_0)$ of C over $\mathcal{O}_K$ with discriminant $\Delta_0 = (2\epsilon)^{4g(2g+1)}\Delta'$, where

$$f_0(X) = (2\epsilon)^{4g+2}\big(l(\frac{X}{4\epsilon^2}) - \frac{1}{4}m(\frac{X}{4\epsilon^2})^2\big).$$

Lemma 3.7 gives $N_{K/\mathbb{Q}}(\Delta') \leq D_K^{2g(2g+1)}\Delta_C$ and then Theorem 3.2 together with (38) implies

$$h(\Delta_0) \leq \frac{1}{2(2g+1)}c_1 N_C^{\kappa_1},$$

where we obtained the factor $\frac{1}{2(2g+1)}$ on using in (38) an upper bound for R_K in terms of d and D_K (see [35]) and on calculating the constants in Theorem 2.3 and Theorem 3.2 more precisely.

Let $N_T = \prod N_{K/\mathbb{Q}}(\mathfrak{p})$ with the product taken over the prime ideals $\mathfrak{p}$ which divide Δ_0. The integers Δ_0 and $2^{4g(2g+1)}\Delta'$ coincide up to unit in $\mathcal{O}_K$, therefore (37) shows $N_T \leq 2^d D_K^{1/2} N_C$. Thus an application of Proposition 2.10 (i) gives a unipotent translation $\rho(\tau) \in \mathrm{SL}_2(\mathcal{O}_K)$ such that

$$h(\tau^* f_0) \leq \frac{1}{2}c_1 N_C^{\kappa_1} + nh(\Delta(f_0)).$$

We define $f(X) = \epsilon^{4g+2}l(\epsilon^{-2}X + \tau)$ and $k(X) = \epsilon^{4g+2}m(\epsilon^{-2}X + \tau)$ and then we see from the above estimates for $h(\Delta_0)$ and $h(\tau^* f_0)$ that the quasi-minimal Weierstrass scheme $\mathcal{W}(f,k)$ of C over $\mathcal{O}_K$ has the desired properties. This completes the proof of Theorem 3.6. □

We next deduce some consequences for modular Jacobians. Let $N \geq 1$ be an integer and let $X_0(N)$ be the projective modular curve over $\mathbb{Q}$ that classifies isomorphism classes of elliptic curves with a cyclic subgroup of order N. We denote by $J_0(N) \to \mathrm{Spec}(\mathbb{Q})$ the Jacobian variety of $X_0(N)$. Let $h_{\mathrm{rel}}(E)$ denote the relative Faltings height of an elliptic curve E over $\mathbb{Q}$.

Corollary 3.8. *If E is an elliptic $\mathbb{Q}$-factor of $J_0(N)$, then*

$$h_{\mathrm{rel}}(E) \leq (2N)^{6^4}.$$

This makes the quantitative result of Brumer and Silverman [12] completely effective and it shows in particular that the elliptic $\mathbb{Q}$-factors of $J_0(N)$ can be determined effectively. We note that Conjecture 3.5 gives the above statement without the logarithm and that the *abc*-Conjecture [41] gives for all $\epsilon > 0$ a constant $C(\epsilon)$, which depends only on ϵ, such that

$$\exp(h_{\mathrm{rel}}(E)) \leq C(\epsilon) N^{1/2+\epsilon}.$$

Proof of Corollary 3.8. Deligne and Rapoport constructed explicitly in [20] a minimal regular model of $X_0(N)$ which is smooth over $\mathrm{Spec}(\mathbb{Z}[1/N])$. Hence $X_0(N)$ has good reduction at all the rational primes not dividing N. Then $J_0(N)$ is the generic fiber of an abelian scheme $\mathcal{J}$ which is smooth over $\mathrm{Spec}(\mathbb{Z}[1/N])$ (see Milne [46, Corollary 12.3]). Therefore the minimal regular model of an elliptic factor E of $J_0(N)$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/N])$. This implies that the conductor N_E of E is at most N and then the upper bound given in Theorem 3.6 together with an explicit version of a comparison result in [63] leads to the desired estimate. This concludes the proof of Corollary 3.8. □

References

[1] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London Ser. A **263** (1967/1968), 173–191.

[2] ———, *Contributions to the theory of Diophantine equations. II. The Diophantine equation $y^2 = x^3 + k$*, Philos. Trans. Roy. Soc. London Ser. A **263** (1967/1968), 193–208.

[3] ———, *The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$*, J. London Math. Soc. **43** (1968), 1–9.

[4] ———, *Linear forms in the logarithms of algebraic numbers. I, II, III, IV*, Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid. 14 (1967), 220-228 **15** (1968), 204–221.

[5] ———, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

[6] ———, *Logarithmic forms and the abc-conjecture*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 37–44.

[7] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.

[8] ———, *Logarithmic forms and Diophantine geometry*, New Mathematical Monographs, vol. 9, Cambridge University Press, Cambridge, 2007.

[9] A. Bérczes, J.-H. Evertse, and K. Győry, *Diophantine problems related to discriminants and resultants of binary forms*, Diophantine geometry, CRM Series, vol. 4, Ed. Norm., Pisa, 2007, pp. 45–63.

[10] S. Bloch, *de Rham cohomology and conductors of curves*, Duke Math. J. **54** (1987), no. 2, 295–308.

[11] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[12] A. Brumer and J. H. Silverman, *The number of elliptic curves over* **Q** *with conductor N*, Manuscripta Math. **91** (1996), no. 1, 95–102.

[13] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compositio Math. **107** (1997), no. 2, 187–219.

[14] Y. Bugeaud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. **74** (1996), no. 1, 67–80.

[15] J. Coates, *An effective p-adic analogue of a theorem of Thue. III. The diophantine equation $y^2 = x^3 + k$*, Acta Arith. **16** (1969/1970), 425–435.

[16] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312.

[17] R. de Jong and G. Rémond, *Conjecture de Shafarevitch pour les revêtements cycliques*, Preprint, 1–8.

[18] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 53–73. Lecture Notes in Math., Vol. 476.

[19] ______, *Le déterminant de la cohomologie*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 93–177.

[20] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[21] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584.

[22] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compositio Math. **79** (1991), no. 2, 169–204.

[23] J.-H. Evertse and J. H. Silverman, *Uniform bounds for the number of solutions to $Y^n = f(X)$*, Math. Proc. Cambridge Philos. Soc. **100** (1986), no. 2, 237–248.

[24] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

[25] G. Frey, *Links between solutions of $A - B = C$ and elliptic curves*, Number theory (Ulm, 1987), Lecture Notes in Math., vol. 1380, Springer, New York, 1989, pp. 31–62.

[26] K. Győry, *Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely domains*, J. Reine Angew. Math. **346** (1984), 54–100.

[27] ______, *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen **69** (2006), no. 4, 473–499.

[28] ______, *On the abc conjecture in algebraic number fields*, Acta Arith. **133** (2008), no. 3, 281–295.

[29] K. Győry and K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith. **123** (2006), no. 1, 9–41.

[30] M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), no. 2, 419–450.

[31] ______, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

[32] R.-P. Holzapfel, *The ball and some Hilbert problems*, Lectures in Mathematics ETH Zürich, Birkhäuser Verlag, Basel, 1995.

[33] I. Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, Compositio Math. **115** (1999), no. 1, 37–69.

[34] S. Lang, *Algebraic number theory*, second ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[35] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.) **26** (1992), no. 2, 211–244.

[36] Q. Liu, *Conducteur et discriminant minimal de courbes de genre* 2, Compositio Math. **94** (1994), no. 1, 51–79.

[37] ______, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610.

[38] ______, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002, Oxford Science Publications.

[39] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342** (1994), no. 2, 729–752.

[40] P. Lockhart, M. Rosen, and J. H. Silverman, *An upper bound for the conductor of an abelian variety*, J. Algebraic Geom. **2** (1993), no. 4, 569–601.

[41] D. W. Masser, *On abc and discriminants*, Proc. Amer. Math. Soc. **130** (2002), no. 11, 3141–3150.

[42] D. W. Masser and G. Wüstholz, *Some effective estimates for elliptic curves*, Arithmetic of complex manifolds (Erlangen, 1988), Lecture Notes in Math., vol. 1399, Springer, Berlin, 1989, pp. 103–109.

[43] ———, *Estimating isogenies on elliptic curves*, Invent. Math. **100** (1990), no. 1, 1–24.

[44] ———, *Periods and minimal abelian subvarieties*, Ann. of Math. (2) **137** (1993), no. 2, 407–458.

[45] S. Maugeais, *Relèvement des revêtements p-cycliques des courbes rationnelles semi-stables*, Math. Ann. **327** (2003), no. 2, 365–393.

[46] J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.

[47] D. Mumford, *Stability of projective varieties*, Enseignement Math. (2) **23** (1977), no. 1-2, 39–110.

[48] K. V. Nguyen, *Non-semistable Arakelov bound and hyperelliptic Szpiro ratio for function fields*, Proc. Amer. Math. Soc. **127** (1999), no. 11, 3125–3130.

[49] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Astérisque (1988), no. 161-162, Exp. No. 694, 4, 165–186 (1989), Séminaire Bourbaki, Vol. 1987/88.

[50] A. P. Ogg, *Elliptic curves and wild ramification*, Amer. J. Math. **89** (1967), 1–21.

[51] F. Oort, *Hyperelliptic curves over number fields*, Classification of algebraic varieties and compact complex manifolds, Springer, Berlin, 1974, pp. 211–218. Lecture Notes in Math., Vol. 412.

[52] A. N. Paršin, *Minimal models of curves of genus* 2*, and homomorphisms of abelian varieties defined over a field of finite characteristic*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 67–109.

[53] D. Poulakis, *The number of solutions of the Mordell equation*, Acta Arith. **88** (1999), no. 2, 173–179.

[54] ______, *Corrigendum to the paper: "The number of solutions of the Mordell equation" [Acta. Arith.* **88** *(1999), no. 2, 173–179]*, Acta Arith. **92** (2000), no. 4, 387–388.

[55] M. Raynaud, *Hauteurs et isogénies*, Astérisque (1985), no. 127, 199–234, Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84).

[56] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[57] T. Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J. **57** (1988), no. 1, 151–173.

[58] J.-P. Serre, *Facteurs locaux des fonctions zêta des variétes algébriques*, Séminaire DPP, vol. 19, (1969-1970).

[59] ______, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[60] ______, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997.

[61] ______, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998.

[62] I.R. Shafarevich, *Algebraic number fields*, Proc. Internat. Congr. Mathematicians, Stockholm, Inst. Mittag-Leffler, Djursholm, 1962, pp. 163–176.

[63] J. H. Silverman, *Heights and elliptic curves*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 253–265.

[64] ______, *Elliptic curves of bounded degree and height*, Proc. Amer. Math. Soc. **105** (1989), no. 3, 540–545.

[65] ______, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743.

[66] ______, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[67] N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307.

[68] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (1974), 135–152.

[69] C. L. Stewart and K. Yu, *On the abc conjecture. II*, Duke Math. J. **108** (2001), no. 1, 169–181.

[70] L. Szpiro, *Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux*, Astérisque, vol. 86, Société Mathématique de France, Paris, 1981.

[71] ———, *Discriminant et conducteur des courbes elliptiques*, Astérisque (1990), no. 183, 7–18, Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[72] ———, *Sur les propriétés numériques du dualisant relatif d'une surface arithmétique*, The Grothendieck Festschrift, Vol. III, Progr. Math., vol. 88, Birkhäuser Boston, Boston, MA, 1990, pp. 229–246.

[73] E. Ullmo, *Points entiers, points de torsion et amplitude arithmétique*, Amer. J. Math. **117** (1995), no. 4, 1039–1055.

[74] R. von Känel, *On the Modular Degree Conjecture*, Preprint.

[75] ———, *Some applications of the Height Conjecture*, Preprint.