JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Rafael VON KÄNEL

An effective proof of the hyperelliptic Shafarevich conjecture

Tome 26, n° 2 (2014), p. 507-530.

<http://jtnb.cedram.org/item?id=JTNB_2014__26_2_507_0>

Journal de Théorie des Nombres de Bordeaux **26** (2014), 507–530

An effective proof of the hyperelliptic Shafarevich conjecture

par Rafael VON KÄNEL

Résumé. Soit C une courbe hyperelliptique de genre $g \geq 1$ sur un corps de nombres K avec bonne réduction en dehors d'un ensemble fini S de places de K. Nous démontrons que C possède un modèle de Weierstrass sur l'anneau des entiers de K avec hauteur effectivement bornée en termes de g, S et K. En particulier, nous démontrons que pour tout corps de nombres K, tout ensemble fini S de places de K et tout entier $g \geq 1$, on peut déterminer en principe l'ensemble des classes d'isomorphisme de courbes hyperelliptiques de genre g sur K avec bonne réduction en dehors de S.

Abstract. Let C be a hyperelliptic curve of genus $g \geq 1$ over a number field K with good reduction outside a finite set of places S of K. We prove that C has a Weierstrass model over the ring of integers of K with height effectively bounded only in terms of g, S and K. In particular, we obtain that for any given number field K, finite set of places S of K and integer $g \geq 1$ one can in principle determine the set of K-isomorphism classes of hyperelliptic curves over K of genus g with good reduction outside S.

1. Introduction

Let K be a number field, let S be a finite set of places of K and let $g \geq 1$ be an integer. The main goal of this article is to show that for given K, S and g there is an effective constant $\Omega(K, S, g)$ with the following property. If C is a hyperelliptic curve over K of genus g with good reduction outside S, then there is a Weierstrass model of C over $\mathcal{O}_K$,

$$Y^2 = f(X),$$

such that the absolute logarithmic Weil height of the polynomial $f \in \mathcal{O}_K[X]$ is at most $\Omega(K, S, g)$, where $\mathcal{O}_K$ is the ring of integers in K. In particular, this holds for all elliptic and all smooth, projective and geometrically connected genus 2 curves over K, since they are hyperelliptic.

We deduce a completely effective Shafarevich conjecture [29] for hyperelliptic curves over K which generalizes and improves the results for elliptic

Manuscrit reçu le 21 décembre 2012, accepté le 21 mai 2013.

curves over K of Coates [5] and of Fuchs, Wüstholz and the author [10]. In addition, our effective result allows in principle to list all K-isomorphism classes of hyperelliptic curves over K of genus g with good reduction outside S. Such lists already exist for special K, S and g. For example, the case $K = \mathbb{Q}$, $S = \{2\}$ and $g = 2$ was established by Merriman and Smart in [20, 31]. We also mention that the theorem of this paper is used in the proof of [33, Theorem 1] which gives an effective exponential version of Szpiro's discriminant conjecture for hyperelliptic curves over K.

In our proofs we combine the effective reduction theory of Evertse and Győry [8], which is based on the theory of logarithmic forms, with results for Weierstrass models of hyperelliptic curves obtained by Lockhart [19] and by Liu [17]. This method can be exhausted to deal with the corresponding problem for slightly more general curves. Generalizations are motivated by the "effective Mordell Conjecture", which would follow from a version of our main result for arbitrary curves over K of genus at least two. However, we point out that our method certainly does not work in this generality. To conclude the discussion of potential Diophantine applications of our results we mention Levin's paper [16]. In this paper, Levin establishes a link "effective Shafarevich conjecture for hyperelliptic Jacobians $\Rightarrow$ effective Siegel theorem for hyperelliptic curves".

Paršin [23] and Oort [22] proved the qualitative Shafarevich conjecture for hyperelliptic curves over K, and Faltings' finiteness theorems in [9] cover in particular Shafarevich's conjecture for all curves over K of genus at least two. However, it is not known if the proofs of Paršin, Oort and Faltings are effective (i.e. allow in principle to list all K-isomorphism classes of hyperelliptic curves over K of genus g with good reduction outside S). See for example Levin's discussion in [16] or section 3 for certain crucial aspects of the method of Paršin and Oort.

The plan of the paper is as follows: In section 2 we define the geometric objects, as for example Weierstrass models, discriminants and Weierstrass points, to state and discuss the results in section 3. In section 4 we begin with Lemma 4.1. It allows to construct effectively principal ideal domains in K. Then we collect some results for Weierstrass models to prove Proposition 4.1 which gives a Weierstrass model of C with certain minimality properties. In section 5 we go into number theory. We first give some elementary results for binary forms. Then in Proposition 5.1 we apply the theory of logarithmic forms to establish effective estimates for the height of some monic polynomials and binary forms with given discriminant. In section 6 we prove the theorem by the following strategy. We first assume that C has a K-rational Weierstrass point. On using results of Lockhart [19] we obtain a Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_T)$

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

such that the discriminant $\Delta(f)$ of $f \in \mathcal{O}_T[X]$ has minimality properties, for $T \supseteq S$ a controlled finite set of places of K and $\mathcal{O}_T$ the ring of T-integers with units $\mathcal{O}_T^\times$. Then we deduce some T-unit equations

$$x + y = 1, \quad x, y \in \mathcal{O}_T^\times.$$

Győry and Yu [13] applied the theory of logarithmic forms to bound the height of x, y. On using their result we get $\tau \in \mathcal{O}_T$ such that $f(X + \tau)$ has height controlled by $K, S, g, \Delta(f)$ and then by K, S, g, since $\Delta(f)$ has minimality properties. A suitable transformation of $Y^2 = f(X+\tau)$ provides the desired Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_K)$ in this case. In the remaining case where C has no K-rational Weierstrass point we use that hyperelliptic curves and binary forms are closely related. We slightly extend an effective theorem for binary forms of Evertse and Győry [8], which is based on the theory of logarithmic forms, to combine it with a global result of the theory of Weierstrass models of Liu [17]. This gives a Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_T)$ with height bounded and then as in the first case we get the desired model over $\mathrm{Spec}(\mathcal{O}_K)$.

Throughout this paper we shall use the following conventions. The number of curves over K always refers to the number of K-isomorphism classes of these curves. We identify a closed point $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ 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. Geometric preliminaries

In this section we give some definitions to state the results in the next section. Let K be a number field and let $g \geq 1$ be an integer.

A hyperelliptic curve C over K of genus g is a smooth projective and geometrically connected curve $C \to \mathrm{Spec}(K)$ of genus g such that there is a finite morphism $\varphi : C \to \mathbb{P}^1_K$ of degree 2, for $\mathbb{P}^1_K$ the projective line over K. For example, [18, Proposition 7.4.9] gives that all elliptic and all smooth projective and geometrically connected genus two curves over K are hyperelliptic curves over K.

Let $-\mathrm{id}$ be the automorphism of a hyperelliptic curve C of order two induced by a generator of the Galois group corresponding to $\varphi : C \to \mathbb{P}^1_K$. If $g \geq 2$, then a K-rational Weierstrass point of C is a section of $C \to \mathrm{Spec}(K)$ which is fixed by $-\mathrm{id}$ and if $g = 1$, then any section of $C \to \mathrm{Spec}(K)$ is a K-rational Weierstrass point of C.

Let $R \subseteq K$ be a Dedekind domain with field of fractions K. The function field $K(C)$ of C takes the form $K(C) = K(X)[Y]$, where

$$Y^2 + f_2(X)Y = f(X), \quad f(X), f_2(X) \in R[X] \tag{2.1}$$

and $2g+1 \leq \max(2\deg f_2(X), \deg f(X)) \leq 2g+2$, for $\deg w(X)$ the degree of any $w(X) \in R[X]$. We say that (2.1) is a hyperelliptic equation of C over R. The normalization $\mathcal{W}(f, f_2)$ of the $\mathrm{Spec}(R)$-scheme $\mathrm{Spec}(R[X]) \cup \mathrm{Spec}(R[1/X])$ in $K(C)$ is called a Weierstrass model of C over $\mathrm{Spec}(R)$. This generalizes the well-known definition of Weierstrass models of elliptic curves over $\mathrm{Spec}(R)$, see [18, p.442] or [30, p.42]. To ease notation we write $\mathcal{W}(f)$ for $\mathcal{W}(f, f_2)$ if $f_2 = 0$ and we define somewhat crudely the height $h(\mathcal{W}(f))$ of $\mathcal{W}(f)$ as the absolute logarithmic height (see [3, 1.6.1]) of $f \in R[X]$. We define the discriminant Δ of $\mathcal{W}(f, f_2)$ by

$$\Delta = \begin{cases} 2^{4g}\Delta(f_0) & \text{for } \deg f_0 = 2g+2 \\ 2^{4g}\alpha_0^2\Delta(f_0) & \text{otherwise,} \end{cases}$$

where $f_0 = f + f_2^2/4$ has leading coefficient α_0 and discriminant $\Delta(f_0)$. This discriminant allows to study the reductions of C. More precisely, let $\mathfrak{p} \in \mathrm{Spec}(R)$ be closed and let $R_\mathfrak{p}$ be its local ring. As usual we define that the curve C has good reduction at v if C is the generic fiber of a smooth proper scheme over $\mathrm{Spec}(R_\mathfrak{p})$. This is equivalent to the existence of a smooth Weierstrass model of C over $\mathrm{Spec}(R_\mathfrak{p})$. We note that a Weierstrass model of C over $\mathrm{Spec}(R_\mathfrak{p})$ with discriminant Δ is smooth if and only if $v(\Delta) = 0$. The curve C has good reduction outside a set of places S of K if it has good reduction at all finite places v of K which are not in S.

We remark that our explicit definition of Δ is not intrinsic. However, in [33] we shall show that the more sophisticated discriminant of Deligne and Saito [28, p.155] for arithmetic surfaces over $\mathrm{Spec}(R_\mathfrak{p})$ of generic fiber C can be controlled in terms of Δ.

3. Statement of the results

In this section we state the theorem and the corollary. We also discuss several aspects of our results and methods. In the sequel c denotes an effective absolute constant.

Let K be a number field. We denote by $\mathcal{O}_K$ its ring of integers, by d its degree over $\mathbb{Q}$ and by D_K the absolute value of its discriminant over $\mathbb{Q}$. Let $g \geq 1$ be an integer and write

$$\nu = 6(2g+1)(2g)(2g-1)d^2.$$

Let S be a finite set of places of K. We denote by $\mathcal{O}_S$ the ring of S-integers of K and by $\mathcal{O}_S^\times$ its unit group. Let h_S be the class number of $\mathcal{O}_S$ and let h_K be the class number of $\mathcal{O}_K$. We remark that $h_S \leq h_K$ and we write $\lambda_S = \log_2 h_S$. To measure S we take

$$\sigma = s + \lambda_S + 1, \quad p \quad \text{and} \quad N_S = \prod N(v) \tag{3.1}$$

with the product taken over the finite places $v \in S$, for s the number of finite places in S, p the maximum of the residue characteristics of the finite places in S and $N(v)$ the number of elements in the residue field of v. Now we can state our main result.

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

(i) if C has a K-rational Weierstrass point, then f is monic separable of degree $2g+1$ and $h(\mathcal{W}(f)) \leq (\nu\sigma)^{5\nu\sigma} N_S^{\nu/2} D_K^{\nu(\lambda_S+1)/4}$,

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

The proof shows in addition that we can take in the theorem any set of places $T \supseteq S$ of K with the following properties: T contains at most $d\sigma$ finite places, $\mathcal{O}_T$ is a principal ideal domain, the residue characteristics ℓ of the finite places of T are at most $\max(2, p, \sqrt{D_K})$ and satisfy $2\ell \in \mathcal{O}_T^\times$, and $N_T \leq (2N_S D_K^{\lambda_S/2})^d$. Such sets T exist and they can be determined effectively. For example if $K = \mathbb{Q}$, then we can take $T = S \cup \{2\}$.

The above result holds for all elliptic and all smooth projective and geometrically connected genus 2 curves 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

$$f(X) = X^3 + a_4 X + a_6.$$

Therefore the theorem generalizes the results for elliptic curves over K of Coates, who covered in [5] the case $K = \mathbb{Q}$, and of [10] to arbitrary hyperelliptic curves over K. Since $N_S \leq p^{ds}$, we see that 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 bounds in [10], which are double exponential and only explicit in terms of S, are reduced to fully explicit polynomial bounds (take in part (i) $g = 1$). We continue the discussion of the bounds below the corollary.

From our theorem we derive a completely effective Shafarevich conjecture [29] for hyperelliptic curves over number fields. The qualitative finiteness statement was proven by Shafarevich for elliptic curves, by Paršin [23] for genus 2 curves and by Oort [22] for arbitrary hyperelliptic curves of genus $g \geq 2$, and Merriman and Smart [20, 31] used [8] to compile a list of all genus 2 curves over $\mathbb{Q}$ with good reduction outside $\{2\}$, see also the survey article of Poonen [25, Section 11]. In principle, the following corollary allows to compile such lists in much more general situations. We recall that c denotes an effective absolute constant.

Corollary. *The K-isomorphism classes $H_{K,S,g}$ of hyperelliptic curves of genus $g \geq 1$ over K with good reduction outside S can be determined effectively and their number $N(K,S,g)$ satisfies*

$$N(K,S,g) \leq \exp((\nu\sigma)^{c(2\nu)^3\sigma^4} p^{(3\nu)^3\sigma^4} D_K^{(3\nu)^3\sigma^4}).$$

In particular, this is an effective finiteness theorem of Shafarevich type for hyperelliptic curves over K of genus one with no K-rational point. This corollary for more general genus one curves with no K-rational point would give the effective finiteness of the Tate-Shafarevich group of elliptic curves over K. The proof of the corollary shows in addition that the number of curves in $H_{K,S,g}$ with a K-rational Weierstrass point is at most

$$\exp\big((\nu\sigma)^{6\nu\sigma} N_S^{\nu/2} D_K^{\nu(\lambda_S+1)/4}\big).$$

Let $N(K,S,E)$ be the number of elliptic curves in $H_{K,S,1}$. Brumer and Silverman [4] proved $N(\mathbb{Q},S,E) \leq c_1 N_S^{c_2}$ for absolute constants c_1, c_2 (see also Helfgott and Venkatesh [14] for an improved c_2). For $g \geq 2$ one can derive a similar estimate on combining the geometric ideas of this paper with Evertse's [7]. It leads to

$$\max(N(K,S,E), N(K,S,g)) \leq c_3 N_S^{c_4},$$

for c_3 a constant depending only on K, g and c_4 an effective constant depending only on g. We plan to give the details in a future article.

We now explain the separation of the theorem in (i) and (ii) depending on whether a K-rational Weierstrass point of C exists or not. In part (i) we can reduce the problem directly to solve unit equations. This has the advantage that it leads to explicit estimates in (i), which depend directly on the at the moment best bounds for unit equations. But the method of (i) only works for monic polynomials and thus can not be applied in our proof of (ii). Therein we get from Proposition 4.1 (ii) a Weierstrass model $\mathcal{W}(f)$ with f not necessarily monic.

Next we discuss our results in view of the nice paper [6] of de Jong and Rémond. Let C be a smooth, projective and geometrically connected curve over K of genus g, with good reduction outside S. We denote by $h_F(J)$ the absolute stable Faltings height of the Jacobian $J = \mathrm{Pic}^0(C)$ of C. If there exists a finite morphism $C \to \mathbb{P}^1_K$ of prime degree which is geometrically a cyclic cover, then [6] gives an effective upper bound for $h_F(J)$ in terms of K, S and g. A motivation for such results is given by Rémond [26]. On using Kodaira's construction, he showed that an effective upper bound for $h_F(J)$, in terms of K, S and g, would imply the effective Mordell Conjecture. To prove their result, de Jong and Rémond generalize the method of Paršin [23] and Oort [22] which worked before only for hyperelliptic curves. They replace therein the qualitative finiteness theorem for unit equations of

Siegel-Mahler by its effective analogue of Győry and Yu [13]. This gives an affine plane model of C with bounded height, which then allows to estimate $h_F(J)$ by combining results of Bost, David and Pazuki [24] and of Rémond [27]. On the other hand, our method relies on the effective reduction theory of Evertse and Győry [8] and on results for Weierstrass models of hyperelliptic curves obtained by Lockhart [19] and by Liu [17]. Hence, we conclude that the method of de Jong and Rémond and our method are rather different. We point out that the main new feature of our method is that it allows to prove the following: Any hyperelliptic curve C has a Weierstrass model, with height effectively bounded in terms of K, S, g, which is defined over $\mathcal{O}_K$. This immediately implies an effective Shafarevich theorem for hyperelliptic curves in the classical sense, i.e. which allows to determine effectively the K-isomorphism classes in question. On the other hand, the method of Paršin, Oort, de Jong and Rémond (only) gives that any hyperelliptic curve C has a Weierstrass model, with height effectively bounded in terms of K, S, g, which is defined over a field extension L of K. Although L can be controlled, it is not clear if this weaker statement can be used to deduce our Theorem. Further, it is not clear if the method of Paršin, Oort, de Jong and Rémond allows to determine effectively the K-isomorphism classes of hyperelliptic curves over K of genus g, with good reduction outside S; their method (only) allows to effectively determine the smaller set of $\bar{K}$-isomorphism classes, where $\bar{K}$ denotes an algebraic closure of K.

We now consider additional aspects of our method. Theorem (i) together with [6, Remarque] shows that if J is the Jacobian of a hyperelliptic curve over K of genus g, with a K-rational Weierstrass point and with good reduction outside S, then

$$h_F(J) \leq 2^{2^{22}9^g} (\nu\sigma)^{5\nu\sigma} N_S^{\nu/2} D_K^{\nu(\lambda_S+1)/4}. \tag{3.2}$$

This bound depends polynomially on the important quantity N_S (see below), while the estimate of [6] is of the form $\exp(c(K,g)(\log N_S)^2)$ for $c(K,g)$ an effective constant depending only on K and g. In addition, our method gives bounds of the form (3.2) for Jacobians of curves over K which correspond to function fields $K(X)[Y]$ with a relation $Y^m = f(X)$, for $m \geq 2$ an integer and for f as in Proposition 5.1 (i); see the discussion at the end of the paper. Moreover, on exhausting our method further generalizations should be possible in view of the general results from the effective reduction theory of Evertse and Győry. However, it is clear that substantially new ideas are required to deal with arbitrary Jacobian varieties.

Finally, we explain the shape of the estimates. They depend ultimately on the theory of logarithmic forms and we refer to Baker and Wüstholz [1] in which the state of the art of this theory is documented. We conducted some effort to obtain in (i) a bound which in terms of S is polynomial in

σ^σ and N_S. This leads immediately to an estimate in terms of S which is polynomial in N_S and that is what we need for the applications given in [33]. Of course, on accepting a worse dependence on S one could improve the dependence on d, D_K or on g. As a consequence of calculating the constants explicitly in every step of our proofs we obtained

$$c = c_6 c_7,$$

for the effective absolute constants c_6, c_7 of [8, Theorem 3]. We note that throughout this paper 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 in 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."

4. Weierstrass models with minimality properties

In this section we start with a lemma which allows to construct effectively principal ideal domains in any number field K. Then, after collecting some known results for hyperelliptic curves C over K, we give Lemma 4.3. It describes a relation between Weierstrass models and the existence of a K-rational Weierstrass point of C. In the last part we prove Proposition 4.1 which gives a Weierstrass model of C with certain minimality properties.

Let S be a finite set of places of K. We denote by $\mathcal{O}_S$ the ring of S-integers in K and by h_S its class number, and we write $\lambda_S = \log_2 h_S$. Let s, N_S and p be as in (3.1) and for any finite set of places T of K let t, N_T and q be the corresponding quantities. Let $\mathcal{O}_K$ be the ring of integers in K and let D_K be the absolute value of the discriminant of K over $\mathbb{Q}$.

The next lemma allows us later to remove class group obstructions in connection with the existence of certain Weierstrass models. We thank Sergej Gorchinskiy for improving the upper bound for t in [10, Lemma 4.3] to $t \leq s + h_S - 1$, and we thank the referee for further improving $t \leq s + h_S - 1$ to the estimate in Lemma 4.1.

Lemma 4.1. *There is a set of places $T \supseteq S$ of K such that $N_T \leq N_S D_K^{\lambda_S/2}$, $q \leq \max(p, \sqrt{D_K})$, $t \leq s + \lambda_S$ and that $\mathcal{O}_T$ is a principal ideal domain.*

Proof. Let $Cl(R)$ denote the class group of a Dedekind domain $R \subset K$. If $h_S = 1$, then we take $T = S$. We do induction and we now assume that the statement is true for any finite set of places S' of K with corresponding class number $h_{S'}$ at most $h_S/2$. Let $\pi : Cl(\mathcal{O}_K) \to Cl(\mathcal{O}_S)$ be the canonical surjective homomorphism and for a non-trivial $\bar{\mathfrak{a}} \in Cl(\mathcal{O}_S)$ we take $\bar{\mathfrak{b}} \in Cl(\mathcal{O}_K)$ with $\pi(\bar{\mathfrak{b}}) = \bar{\mathfrak{a}}$. Minkowski's theorem gives a representative $\mathfrak{b} \subset \mathcal{O}_K$ of $\bar{\mathfrak{b}}$ such that the residue field of any $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)$ which divides $\mathfrak{b}$ has at most $\sqrt{D_K}$ elements. Since $\bar{\mathfrak{a}}$ is non-trivial and π is a homomorphism there exists such a $\mathfrak{p}$ with $\pi(\bar{\mathfrak{p}})$ non-trivial, where $\bar{\mathfrak{p}}$ is the ideal class of $\mathfrak{p}$. We write $S' = S \cup \{\mathfrak{p}\}$ and then we see that the class number $h_{S'}$ of $\mathcal{O}_{S'}$ is at most $h_S - 1$, since $\pi(\bar{\mathfrak{p}})$ lies in the kernel of the canonical surjective homomorphism $Cl(\mathcal{O}_S) \to Cl(\mathcal{O}_{S'})$. Thus, on using that $h_{S'}$ divides h_S, we deduce that $h_{S'} \le h_S/2$. Finally, an application of the induction hypothesis with S' gives a set of places T of K with the desired properties. □

Let C be a hyperelliptic curve of genus g defined over K. 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 [17, Proposition 2].

Lemma 4.2. *Suppose R is a principal ideal domain and C has good reduction at all closed points in* $\operatorname{Spec}(R)$. *Then there exists a Weierstrass model of C over* $\operatorname{Spec}(R)$ *with discriminant in $R^\times$.*

Let $V^2 = l(Z)$ and $Y^2 = f(X)$ be two hyperelliptic equations of C over K with discriminant Δ' and Δ respectively. Then [17, p.4581] gives

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

such that

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

and that

$$\Delta = \lambda^{4(2g+1)} (\det \phi)^{-2(g+1)(2g+1)} \Delta', \tag{4.1}$$

where $\mathrm{GL}_2(K)$ are the invertible 2×2-matrices with entries in K and $\det \phi$ denotes the determinant of $\phi \in \mathrm{GL}_2(K)$.

Next, we discuss a relation between K-rational Weierstrass points and Weierstrass models of C over $\operatorname{Spec}(R)$. We are grateful to Professor Qing Liu who pointed out that the following Lemma 4.3 is well-known (see for example the results at the bottom of [17, p.4579]).

Lemma 4.3. *Suppose $\mathcal{W}(f)$ is a Weierstrass model of C over* $\operatorname{Spec}(R)$. *If C has no K-rational Weierstrass point, then $f \in R[X]$ has degree* $2g + 2$.

Let S and T be finite sets of places of K. Let Σ be a generating system of the free part of the units $\mathcal{O}_T^\times$ of the ring of T-integers $\mathcal{O}_T$ and let ζ be a generator of the torsion part of $\mathcal{O}_T^\times$. We write $\mathcal{U} = (\Sigma, \zeta)$ and we say that $\epsilon \in \mathcal{O}_T^\times$ is $\mathcal{U}$-reduced if it takes the form $\epsilon = \zeta^r \prod_{\epsilon \in \Sigma} \epsilon^{r(\epsilon)}$, for integers $0 \le r, r(\epsilon) < 4(g+1)(2g+1)$. Let n_T be the product $\prod \log N(v)$ taken over the finite places $v \in T$ for $N(v)$ the number of elements in the residue field of v and let d be the degree of K over $\mathbb{Q}$. Let $h(\alpha)$ be the absolute logarithmic height (see [3, 1.6.1]) of $\alpha \in K$.

Proposition 4.1. *Suppose $T \supseteq S$ and $\mathcal{O}_T$ is a principal ideal domain with $2 \in \mathcal{O}_T^\times$. Let $\mathcal{U}$ be as above and let C be a hyperelliptic curve over K of genus g with good reduction outside S. There is a Weierstrass model $\mathcal{W}(f)$ of C over* $\mathrm{Spec}(\mathcal{O}_T)$ *with $\mathcal{U}$-reduced discriminant $\Delta \in \mathcal{O}_T^\times$ such that*

(i) *if C has a K-rational Weierstrass point, then f is separable and monic of degree $2g+1$,*

(ii) *if C has no K-rational Weierstrass point, then f is separable of degree $2g+2$.*

Moreover, there is a $\mathcal{U}$ as above such that any $\mathcal{U}$-reduced $\Delta \in \mathcal{O}_T^\times$ satisfies

$$h(\Delta) \leq (50g(t+d)!)^2 (dD_K)^d n_T.$$

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 fortiori good reduction outside T.

(i) We suppose that C has a K-rational Weierstrass point. In a first step we construct a Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_T)$ with discriminant invertible in $\mathcal{O}_T$. Let $\mathfrak{a} \subseteq \mathcal{O}_K$ be a representative of the Weierstrass class (see [19, Definition 2.7]) of C. Since $\mathcal{O}_T$ is a principal ideal domain we get $\alpha \in \mathcal{O}_K$ and a fractional ideal $\mathfrak{a}_T$ of $\mathcal{O}_K$ in K, which is composed only of primes in T, such that $\mathfrak{a} = \alpha\mathfrak{a}_T$. After multiplying this ideal equation by a suitable T-unit in $\mathcal{O}_K$ we see that there is a representative $\mathfrak{b} \subseteq \mathcal{O}_K$ of the Weierstrass class of C which is composed only of primes in T. An application of [19, Proposition 2.8] gives a Weierstrass model $\mathcal{W}(l, l_2)$ of C over $\mathrm{Spec}(\mathcal{O}_K)$ with discriminant Δ' and with the following properties. The degree of l_2 is at most g, l is monic of degree $2g+1$ and

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

for $\mathfrak{D}_C$ the minimal discriminant ideal of C (see [19, Definition 2.5]). To see that $\Delta' \in \mathcal{O}_T^\times$ we let $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_T)$ be any closed point and we denote by $\mathcal{O}_\mathfrak{p}$ its local ring. Since our curve C has good reduction outside T we get a Weierstrass model $\mathcal{W}$ of C over $\mathrm{Spec}(\mathcal{O}_\mathfrak{p})$ which is smooth. In particular this shows that the special fiber of $\mathcal{W}$ is smooth over the spectrum of the residue field at $\mathfrak{p}$. Therefore $\mathfrak{p}$ does not divide the discriminant of $\mathcal{W}_\mathfrak{p}$ and thus does not divide the minimal discriminant $\mathfrak{D}_C$ as well. Then the above representation of $\Delta'\mathcal{O}_K$ and our choice of $\mathfrak{b}$ give that Δ' is not divisible by $\mathfrak{p}$. This proves that $\Delta' \in \mathcal{O}_T^\times$. Since $2 \in \mathcal{O}_T^\times$ we see that the base change of $\mathcal{W}(l, l_2)$ to $\mathrm{Spec}(\mathcal{O}_T)$ takes the form of a Weierstrass model $\mathcal{W}(l_0)$ of C over $\mathrm{Spec}(\mathcal{O}_T)$ with discriminant Δ', for $l_0 = l + l_2^2/4$. We recall that l is monic of degree $2g+1$ and that l_2 has degree at most g. This shows that l_0 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

$$\Delta' = \omega^{-4g(2g+1)}\zeta^r \prod_{\epsilon\in\Sigma} \epsilon^{r(\epsilon)}, \quad 0 \le r, r(\epsilon) < 4g(2g+1)$$

with $\omega \in \mathcal{O}_T^\times$ and integers $r, r(\epsilon)$. For $f(X) = \omega^{4g+2} l_0(X/\omega^2)$ let $\mathcal{W}(f)$ be the corresponding Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_T)$. By (4.1) it has $\mathcal{U}$-reduced discriminant $\omega^{4g(2g+1)}\Delta' \in \mathcal{O}_T^\times$ and the properties of l_0 imply that f is monic with degree $2g+1$.

(ii) We now assume that C has no K-rational Weierstrass point. Since our curve C has good reduction outside T it has good reduction at all closed points in $\mathrm{Spec}(\mathcal{O}_T)$. Then an application of Lemma 4.2 with $R = \mathcal{O}_T$ gives a Weierstrass model $\mathcal{W}(l, l_2)$ of C over $\mathrm{Spec}(\mathcal{O}_T)$ with discriminant $\Delta' \in \mathcal{O}_T^\times$. As in (i) we get a Weierstrass model $\mathcal{W}(l_0)$ of C over $\mathrm{Spec}(\mathcal{O}_T)$ with discriminant Δ', where $l_0 = l + l_2^2/4$. Our assumption and Lemma 4.3 show that l_0 has degree $2g+2$. Next we reduce, in the same way as in (i), with a suitable $\omega \in \mathcal{O}_T^\times$ the exponents of Δ' modulo $4(g+1)(2g+1)$. Let $f(X) = \omega^{4g+4} l_0(X/\omega^2)$ and then we see that the Weierstrass model $\mathcal{W}(f)$ of C over $\mathrm{Spec}(\mathcal{O}_T)$ has the desired properties.

It remains to prove the last statement. We claim that for any finite set of places S' of K there is a generating system Σ' of the free part of $\mathcal{O}_{S'}^\times$ with

$$h(\epsilon) \le (10\,|\Sigma'|!)^2 (dD_K)^d n_{S'}, \quad \epsilon \in \Sigma', \tag{4.2}$$

for $|\Sigma'|$ the cardinality of Σ'. To see this let $R_{S'}$ be the S'-regulator, R_K the regulator of K and h_K the class number of K. From [13, Remark 3] we get that $R_{S'} \le R_K h_K n_{S'}$ and [15, Theorem 6.5] shows that

$$R_K h_K \le \sqrt{D_K}\max(2d, d\log D_K)^{d-1}/(d-1)!.$$

Hence we deduce

$$R_{S'} \le D_K^{1/2}\max(2d, d\log D_K)^{d-1} n_{S'}/(d-1)!. \tag{4.3}$$

Then the claim follows, since [13, Lemma 2] gives a generating system Σ' of the free part of $\mathcal{O}_{S'}^\times$ such that

$$h(\epsilon) \le (10\,|\Sigma'|!)^2 \max(1, \log d) R_{S'}, \epsilon \in \Sigma'.$$

We choose $\mathcal{U} = (\Sigma, \zeta)$ such that Σ is a generating system of the free part of $\mathcal{O}_T^\times$ with heights bounded as above. Since $\Delta \in \mathcal{O}_T^\times$ 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 above bound for $h(\epsilon)$ together with $|\Sigma| = t + d - 1$ leads to the last statement. This completes the proof of the proposition. □

To apply this proposition in our proof we shall extend S to a set T such that $\mathcal{O}_T$ is a principal ideal domain. By Lemma 4.1 this can be done in a controlled way with the disadvantage inherent that then T depends on K.

We now briefly discuss two further ideas and we let C be as in the proposition above. The first idea is to use the Hilbert class field $H(K)$ of K. This field is controlled in terms of K and it seems that one can avoid an extension of S by working with the base change of C to $H(K)$ to get an equation over $H(K)$ with minimality properties.

The second idea is due to Paršin [23]. There is a smallest finite extension $L \supseteq K$ such that the base change C_L of C to L has $2g+2$ L-rational Weierstrass points. With the help of a fixed L-rational Weierstrass point we embed C_L in its Jacobian over L which extends to an abelian scheme $\mathcal{J} \to \mathrm{Spec}(\mathcal{O})$, where $\mathcal{O}$ denotes the integral closure of $\mathcal{O}_S[1/2]$ in L. Then on using that the Weierstrass points give 2-torsion points on $\mathcal{J}$ we get a Weierstrass model of C_L over a localization of $\mathrm{Spec}(\mathcal{O})$. Its discriminant and also L can be controlled in terms of K, S, g, since all places of L that extend a closed point in $\mathrm{Spec}(\mathcal{O}_S[1/2])$ are unramified over K.

Probably, one can use these ideas to improve the estimates in some special cases as for example when C is semi-stable over K. But it is clear that in general both approaches give no equation for C over K.

5. Binary forms and monic polynomials with given discriminant

In the first part of this section we collect some elementary results for binary forms over any number field K. In the second part we prove Proposition 5.1. It gives effective bounds for the height of certain binary forms and monic polynomials over K of given discriminant.

Let $n \geq 1$ be an integer. Over a field extension of K 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 $\prod_{1\leq j\leq n}(\zeta_j X - \xi_j Y)$ and we define the discriminant $\Delta(G)$ of G by

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

It has the properties (see [8, p.169]) that $\Delta(G) \in \mathbb{Z}[\beta_0,\ldots,\beta_n]$ and that $\Delta(\alpha G) = \alpha^{2n-2}\Delta(G)$, for $\alpha \in K$. The pullback ψ^*G of G by $\psi \in \mathrm{GL}_2(K)$ can be written as

$$\psi^*G(X,Y) = G(\alpha X + \beta Y, \gamma X + \delta Y) \text{ for } \psi = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{GL}_2(K)$$

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

Suppose that $f(X) = \alpha_0 X^n + \ldots + \alpha_n \in K[X]$ is separable of 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 T be a finite set of places of K and let $\mathcal{O}_T$ be the ring of T-integers in K with units $\mathcal{O}_T^\times$. For any $A \in K[X,Y]$ we let $(A)_T$ be the $\mathcal{O}_T$-submodule of K generated by the coefficients of A and if $G \neq 0$ we define

$$d_T(G) = \frac{(\Delta(G))_T}{(G)_T^{2n-2}}.$$

We now prove some elementary results for which we did not find a suitable reference.

Lemma 5.1. *The discriminant of F and of f are equal. 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 $\alpha_0 \in K \setminus \{0\}$ of F is the product of the elements ζ_j, thus all ζ_j are nonzero and then with $F(X,1) = f(X)$ we get

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

which implies $\Delta(F) = \Delta(f)$. On using that $F_k(X,1)$ is irreducible in $K[X]$ we deduce that F_k is irreducible in $K[X,Y]$. We observe that $\prod_k f_k$ has the same coefficients as $\alpha_0^{-1} F$ and this implies that $\prod_k F_k = \alpha_0^{-1} F$. The fractional ideal $(F)_T^{-1}$ of $\mathcal{O}_T$ in K 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 that $\Delta(F) \in \mathcal{O}_T^\times$ leads to $d_T(F) = \mathcal{O}_T$. □

Next we give Proposition 5.1 which allows us later to construct Weierstrass models with effectively bounded height. Its proof is based on the theory of logarithmic forms. More precisely, in part (i) we use ideas of Győry and we apply a result of Győry and Yu [13]. Part (ii) is an application of Győry and Evertse [8]. To state the proposition we have to introduce some notation. In the sequel c is an effective absolute constant.

For any subset T_0 of T let $\mathcal{O}_{T_0}$ be the ring of T_0-integers and let $\rho : \mathcal{O}_{T_0} \to \mathrm{GL}_2(K)$ be the representation given by

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

We say that $\phi \in \rho(\mathcal{O}_{T_0})$ is a unipotent translation and we define $\phi^* f(X) = (\phi^* F)(X, 1)$. For any Dedekind domain $R \subseteq K$ we denote by $\mathrm{SL}_2(R)$ the 2×2-matrices with entries in R and with determinant one.

As before let $N_T = \prod N(v)$ and $n_T = \prod \log N(v)$ with the products taken over the finite places $v \in T$ and for $N(v)$ 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 maximum of the rational prime divisors of N_T.

Let d be the degree of K over $\mathbb{Q}$, let D_K be the absolute value of the discriminant of K over $\mathbb{Q}$ and for any $n \geq 3$ let

$$\mu(n, d) = 3n(n-1)(n-2)d.$$

Let h be the absolute logarithmic height (see [3, 1.6.1]) and let $H = \exp(h)$ be the absolute multiplicative height. We now can state the following proposition.

Proposition 5.1. *Suppose $f \in \mathcal{O}_{T_0}[X]$ has degree $n \geq 3$ and discriminant $\Delta(f) \in \mathcal{O}_T^\times$. Let F be the homogenization of f in $\mathcal{O}_{T_0}[X, Y]$ and write $\mu = \mu(n, d)$.*

(i) *If f is monic, then there is a unipotent translation $\phi \in \mathrm{SL}_2(\mathcal{O}_{T_0})$ such that $h(\phi^* f) \leq h(\Delta(f)) + (N_T D_K^{1/3})^{\mu}(\mu(t+1))^{4\mu(t+1)}$.*

(ii) *In general there is a $\phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that $h(\phi^* F) \leq 32 h(\Delta(F)) + q^{2n^8 d(t^2+1)^2} D_K^{2n^8(t+1)} (n(t+d))^{cn^8 d(t^2+1)^2}$.*

Proof. In the proof we shall use well-known results in [3, Chapter 1] for the height H without mentioning it.

(i) We start with some notation. Since $n \geq 3$ and $\Delta(f) \neq 0$ we can choose pairwise different roots α, β, γ of f and we write $L = K(\alpha, \beta, \gamma)$. 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. We note that $l \leq dm$ for $m = n(n-1)(n-2)$.

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

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

An application of [13, Theorem 1] gives

$$\Omega_U = \exp(7\kappa_T R_U N_T^m \max(1, \log R_U)),$$

for $\kappa_T = c_1(md, m(t+d))$ defined in [13, Theorem 1], such that

$$H\left(\frac{\gamma - \alpha}{\alpha - \beta}\right) \leq \Omega_U. \tag{5.1}$$

In what follows we shall use that κ_T and thus Ω_U are sufficiently big, see [13, Theorem 1]. 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 $n_U \leq ((l/d)^t n_T)^{l/d}$ and then (4.3), with L and U in place of K and S' respectively, leads to

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

To estimate D_L we first show that $\mathfrak{D}_{L/K}\mathcal{O}_T = \mathcal{O}_T$, where $\mathfrak{D}_{L/K}$ is the relative discriminant ideal of L over K. For any fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ in K let $(\mathfrak{a})_T = \mathfrak{a}\mathcal{O}_T$, where $\mathcal{O}_K$ denotes the ring of integers in K. We consider for $\kappa \in \{\alpha, \beta, \gamma\}$ the field $M = K(\kappa)$, we write $f(X)$ as a product taken over k of irreducible monic $f_k(X) \in K[X]$ and we let F and F_k be the homogenizations in $K[X, Y]$ of f and f_k respectively. Lemma 5.1 implies that $F = \prod_k F_k$ can be associated to a system of fields which contains the field M and then [8, Lemma 15] shows

$$d_T(F) \subseteq (\mathfrak{D}_{M/K})_T,$$

for $\mathfrak{D}_{M/K}$ the relative discriminant ideal of M over K. Thus our assumptions that f is monic with $\Delta(f) \in \mathcal{O}_T^\times$ together with Lemma 5.1 show that $(\mathfrak{D}_{M/K})_T$ 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 [32, Lemma 6] leads to $\prod_\kappa \mathfrak{d}_{M/K} \subseteq \mathfrak{d}_{L/K}$ and taking the ideal norm from L into K gives

$$\prod_\kappa \mathfrak{D}_{M/K}^{[L:M]} \subseteq \mathfrak{D}_{L/K}.$$

Thus we deduce that $(\mathfrak{D}_{L/K})_T = \mathcal{O}_T$, since all $(\mathfrak{D}_{M/K})_T$ are trivial. Then the arguments of [8, p.194] show $D_L \leq (D_K N_T)^{l/d} (l/d)^{lt}$ and this together with the above upper bound for R_U gives $R_U \leq c_K c_T$, for

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

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

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 root $\gamma \neq \alpha, \beta$ of f was chosen arbitrarily it follows from (5.1) 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 gives

$$H(\alpha - \beta) \leq 2\Omega^2 H(\Delta(f))^{1/(n(n-1))}. \tag{5.2}$$

In a second step we approximate the trace $\mathrm{Tr}(f)$ of f by a suitable $\tau \in \mathcal{O}_{T_0}$ such that if α is a root of f, then $H(\alpha - \tau)$ is bounded explicitly in terms of Ω, n and $H(\Delta(f))$. Our assumption $f \in \mathcal{O}_{T_0}[X]$ provides that $\mathrm{Tr}(f) \in \mathcal{O}_{T_0}$ and then an application of [8, Lemma 6] gives $\eta \in \mathcal{O}_K$, $\tau \in \mathcal{O}_{T_0}$

such that $\eta = \mathrm{Tr}(f) - n\tau$ and that $H(\eta) \le \Omega$. Thus for any root α of f we get

$$n(\alpha - \tau) = \sum (\alpha - \beta) + \eta,$$

with the sum taken over the roots β of f, which together with (5.2) leads to

$$H(\alpha - \tau) \le \Omega^{2n} H(\Delta(f))^{1/n}.$$

For $\phi = \rho(\tau)$ in $\mathrm{SL}_2(\mathcal{O}_{T_0})$ we get $\phi^* f(X) = \prod (X - (\alpha - \tau))$ with the product taken over the roots α of f. Then we deduce from the above estimate for $h(\alpha - \tau)$, which holds for all roots α of f, together with

$$\Omega = \exp\big(7\kappa_T N_T^m c_K c_T \log(c_K c_T)\big)$$

and the definitions of c_K, κ_T, c_T an upper bound for $h(\phi^* f)$ as stated in (i). To simplify the form of the final bound we used the estimates $m \ge 6$, $\log x \le 3x^{1/3}$ for $x \ge 1$, $n_T \le N_T$ and $\log(c_K c_T) \le 3(c_K c_T)^{1/12}$.

(ii) From [8, Theorem 3] we get $\psi_0 \in \mathrm{SL}_2(\mathcal{O}_T)$, $\epsilon \in \mathcal{O}_T^\times$ and effective absolute constants $c_6 \ge 3$, $c_7 \ge 1$ such that $H(\epsilon(\psi_0^* F)) \le \Omega$, where

$$\log \Omega = (7n)^{-2} (c_6(d+t)n)^{c_7 d n^8 (t+1)^2} q^{2dn^8(t+1)^2} D_K^{2n^8(t+1)}. \tag{5.3}$$

We now construct with ϵ and ψ_0 an element $\phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that $\phi^* F$ has bounded height. From [13, Lemma 3] 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, which is at most Ω by [15, Theorem 6.5]. If $\psi = \epsilon_2^{-1}\psi_0$ and $G = \psi^* F$, then we see that G takes the form $\epsilon_1^{-1}\epsilon(\psi_0^* F)$ which implies

$$H(G) \le \Omega^2. \tag{5.4}$$

For $g(X) = G(X,1)$ we get from Lemma 5.1 that $H(\Delta(G)) = H(\Delta(g))$ and this leads to $H(\Delta(G)) \le 2^{3n(n-1)} H(G)^{2n-2}$. Then (5.4) implies

$$H(\det(\psi^{-1})) \le \Omega^2 H(\Delta(F))^{1/(n(n-1))},$$

since $\det(\psi^{-1})^{n(n-1)} = \Delta(F)\Delta(G)^{-1}$ by $F = (\psi^{-1})^* G$. An application of [8, Lemma 7] with the transpose of $\psi^{-1} \in \mathrm{GL}_2(\mathcal{O}_T)$ gives $\phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that the maximum $H(\psi^{-1}\phi)$ of the absolute multiplicative heights of the standard coordinates of $\psi^{-1}\phi$ is at most $\Omega H(\det(\psi^{-1}))^8$. Thus the upper bound for $H(\det(\psi^{-1}))$ implies

$$H(\psi^{-1}\phi) \le \Omega^{17} H(\Delta(F))^{8/(n(n-1))}. \tag{5.5}$$

In the last step we derive an upper bound for $H(\phi^* F)$ in terms of n, Ω and $H(\Delta(F))$. Let (α_i) be the coefficients of G and let

$$\psi^{-1}\phi = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Since the pullback * induces a right-action of the group $\mathrm{GL}_2(K)$ on the set of binary forms over K we get that $\phi^*F = (\psi^{-1}\phi)^*G$ which shows

$$\phi^*F(X,Y) = \sum_{i=0}^{n} \alpha_i(\alpha X + \beta Y)^{n-i}(\gamma X + \delta Y)^i.$$

We deduce that

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

and we see that the i-th factor of the product on the right-hand side is at most $2^{3n}H(\alpha_i)H(\psi^{-1}\phi)^{2n}$. Hence (5.4) and (5.5) give

$$H(\phi^*F) \leq \Omega^{(7n)^2}H(\Delta)^{32}$$

and then (ii) follows from (5.3) with $c = c_6c_7$. This completes the proof of the proposition. □

For any monic and separable $f \in K[X]$ of degree $n \geq 3$ we let T_0 be the smallest set of places of K such that $f \in \mathcal{O}_{T_0}[X]$. For T we take the smallest set of places of K containing T_0 such that $\Delta(f) \in \mathcal{O}_T^\times$. Then we see that (i) gives a unipotent translation $\phi \in \mathrm{SL}_2(\mathcal{O}_{T_0})$ such that

$$h(\phi^*f) \leq h(\Delta(f)) + (N_T D_K^{1/3})^{\mu}(\mu(t+1))^{4\mu(t+1)},$$

for $\mu = \mu(n,d)$. The quantities t and N_T can be bounded effectively in terms of $\Delta(f)$ and T_0 such that the resulting bound improves in all parameters the actual best effective estimates (see [11, Thm 7], [2], [12] and the references therein) and makes them completely explicit. For example we can reduce the exponent $(dn!)^2((n!d)!)$ of N_T and D_K, which would follow from [11, Thm 7], to $\mu \leq 6n^3d$. Moreover, it is shown in [11] that an effective estimate for $h(\phi^*f)$ has several applications in algebraic number theory. These can now be stated with sharper and fully explicit bounds. Finally, we mention that Evertse and Győry informed the author that they are writing a book which will inter alia allow to improve Proposition 5.1 and which will give explicitly the effective absolute constants c_6, c_7 and $c = c_6c_7$ in the above proof.

6. Proofs

For an outline of the principal ideas of the following proof we refer to the introduction. Let K be a number field of degree d over $\mathbb{Q}$ and denote by $\mathcal{O}_K$ its ring of integers. Let D_K be the absolute value of the discriminant of K over $\mathbb{Q}$, let S be a finite set of places of K and let $g \geq 1$ be an integer. As before we let h be the absolute logarithmic height (see [3, 1.6.1]).

Proof of the Theorem. We take a hyperelliptic curve C of genus g defined over K, with good reduction outside S, as in the theorem. First, we recall some notation. For any finite place v of K, we denote by $N(v)$ the cardinality of the residue field of v. Let s be the number of finite places in S, write $N_S = \prod N(v)$ with the product taken over the finite places $v \in S$ and let p be the maximum of the rational prime divisors of N_S; and for any finite set of places T of K we denote by t, N_T and q the corresponding quantities. If ℓ is a rational prime, then there exist at most d finite places of K of residue characteristic ℓ and if T contains all finite places of K of residue characteristic ℓ, then ℓ is invertible in the ring of T-integers $\mathcal{O}_T$. Thus, on using Lemma 4.1, we see that there exists a finite set of places T of K with the following properties. The set T contains the set S, $\mathcal{O}_T$ is a principal ideal domain, 2 and all residue characteristics of the finite places in T are in the group of units $\mathcal{O}_T^\times$ of $\mathcal{O}_T$,

$$(6.1)\quad t \le d(s+\lambda_S+1) = d\sigma,\ N_T \le (2N_S D_K^{\lambda_S/2})^d \ \text{ and } q \le \max(2, p, D_K^{1/2}).$$

Here $\lambda_S = \log_2 h_S$ for h_S the class number of $\mathcal{O}_S$.

To prove statement (i) we can assume that C has a K-rational Weierstrass point. Proposition 4.1 (i) gives a Weierstrass model $\mathcal{W}(l)$ of C over $\operatorname{Spec}(\mathcal{O}_T)$ with discriminant $\Delta' \in \mathcal{O}_T^\times$ and with the following properties. The polynomial l is monic of degree $2g+1$ and its discriminant $\Delta(l) = 2^{-4g}\Delta' \in \mathcal{O}_T^\times$ satisfies

$$h(\Delta(l)) \le 2(50g(t+d)!)^2(dD_K)^d N_T.$$

Then we get from Proposition 5.1 (i) a unipotent translation $\phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that

$$(6.2)\qquad h(\phi^* l) \le 2(\mu(t+1))^{4\mu(t+1)}(N_T D_K^{1/3})^\mu,$$

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

In the next step we modify $\mathcal{W}(\phi^* l)$ to get a Weierstrass model of C over $\operatorname{Spec}(\mathcal{O}_K)$ with the desired properties. To simplify notation we write

$$(6.3)\qquad n = 2g+1, \quad \eta = 1.$$

Let α be a coefficient of $\phi^* l$. We denote by $N(w)$ the cardinality of the residue field of a finite place w of $\mathbb{Q}(\alpha)$ and we define $|\alpha|_w = N(w)^{-w(\alpha)}$, where $w(\alpha)$ is the order in α of the prime ideal which corresponds to w. On taking the product over the finite places w of $\mathbb{Q}(\alpha)$ we see that

$$(6.4)\qquad \delta(\alpha) = \prod \max(1, |\alpha|_w) \in \mathbb{N}$$

is at most $H(\alpha)^d$ and that $\delta(\alpha)\alpha \in \mathcal{O}_K$ by [10, Lemma 4.2]. 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 $\mathrm{ord}_w(\alpha) \leq -1$ contribute to the right-hand side of (6.4). Since $\phi^* l$ has coefficients in $\mathcal{O}_T$ this shows that

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

where the product is taken over the coefficients α of $\phi^* l$. For

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

let $\mathcal{W}(f)$ be the corresponding Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_K)$. By (4.1) it has discriminant $\omega^{4(g+1-\eta)(2g+1)} \Delta' \in \mathcal{O}_T^\times$ and we see that

$$h(\mathcal{W}(f)) \leq 4dn^2 h(\phi^* l). \tag{6.5}$$

On replacing N_T and t in (6.2) by the estimates given in (6.1) we conclude from (6.5) that $\mathcal{W}(f)$ has the required properties. This completes the proof of Theorem (i).

To prove statement (ii) we can assume that C has no K-rational Weierstrass point. Proposition 4.1 (ii) gives a Weierstrass model $\mathcal{W}(l)$ of C over $\mathrm{Spec}(\mathcal{O}_T)$ with discriminant $\Delta' \in \mathcal{O}_T^\times$ such that l has degree $2g+2$ and discriminant $\Delta(l) = 2^{-4g} \Delta' \in \mathcal{O}_T^\times$ which satisfies

$$h(\Delta(l)) \leq 2(50g(t+d)!)^2 (dD_K)^d n_T.$$

Then an application of Proposition 5.1 (ii) to the two variable homogenization L of l gives

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

and an effective absolute constant c such that

$$h(\phi^* L) \leq 2q^{2n^8 d(t^2+1)^2} D_K^{2n^8(t+1)} (n(t+d))^{cn^8 d(t^2+1)^2}, \tag{6.6}$$

for $n = 2g+2$.

We now use the close relation between hyperelliptic curves and binary forms. Suppose that $\mathcal{W}(l)$ arises from $V^2 = l(Z)$. The group $\mathrm{SL}_2(\mathcal{O}_T)$ acts on the non-constant rational functions in $K(C)$ by fractional linear transformations. We get a non-constant rational function $X = \phi^{-1} Z \in K(C)$. Therefore $Y = V(\gamma X + \delta)^{n/2}$ is non-constant and it is in $K(C)$, since $n/2$ is an integer. Then we can rewrite $V^2 = l(Z)$ as

$$\frac{Y^2}{(\gamma X + \delta)^n} = l(\frac{\alpha X + \beta}{\gamma X + \delta}).$$

Multiplying both sides of this equation by $(\gamma X + \delta)^n$ gives

$$Y^2 = \sum_{i=0}^{n} \alpha_i (\alpha X + \beta)^{n-i} (\gamma X + \delta)^i = \phi^* l(X)$$

for (α_i) the coefficients of l and this implies that $\mathcal{W}(\phi^* l)$ is a Weierstrass model of C over $\mathrm{Spec}(\mathcal{O}_T)$. Lemma 5.1 shows that $\Delta(\phi^* L) = \Delta(\phi^* l)$ and $\Delta(L) = \Delta(l)$ which gives $\Delta(\phi^* l) = \Delta(l)$, since ϕ is in $\mathrm{SL}_2(\mathcal{O}_T)$. Therefore

$\mathcal{W}(\phi^* l)$ has discriminant $\Delta' \in \mathcal{O}_T^\times$. Then $h(\mathcal{W}(\phi^* l)) = h(\phi^* L)$ and (6.6) together with the arguments of the proof of part (i) (where now $n = 2g+2$, $\eta = 0$ in (6.3)) lead to Theorem (ii). To simplify the form of the final bound we used here the estimate $g(6dg)^2 \leq \nu$. This completes the proof of the theorem. □

It remains to prove the corollary. We denote by N the number of K-isomorphism classes of hyperelliptic curves of genus g defined over K with good reduction outside S.

Proof of the Corollary. The theorem shows that there is an explicit constant $\Omega = \Omega(K, S, g, c)$, for c an effective absolute constant, with the following property. Any 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 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 is bounded from above by the number of polynomials $f \in K[X]$ of degree at most $2g+2$ that satisfy $H(f) \leq \Omega$. Thus the proof of [3, 1.6.8] yields

$$N \leq (5\Omega)^{10d^2 g}$$

and then (6.2) and (6.6) lead to an upper bound for Ω which shows that the estimate of the corollary holds as stated.

The polynomials in $K[X]$ with bounded degree and bounded absolute height can be determined effectively (for details we refer to the discussions in [3]). 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 the corollary. □

To conclude this article we demonstrate how our method can be used to deal with more general curves. Let C be a smooth, projective and geometrically connected curve over K of genus g, with good reduction outside S. We denote by $h_F(J)$ the absolute stable Faltings height of the Jacobian $J = \mathrm{Pic}^0(C)$ of C. Let L be a finite field extension of K. We denote by D_L the absolute value of the discriminant of L over $\mathbb{Q}$ and by $d_L = [L : \mathbb{Q}]$ the degree of L over $\mathbb{Q}$. Let T be a finite set of places of L. We denote by $\mathcal{O}_T^\times$ the group of units of the ring of T-integers $\mathcal{O}_T$ of L and we define $N_T = \prod N(v)$ with the product taken over all finite places $v \in T$, where $N(v)$ is the number of elements of the residue field of v.

Proposition 6.1. *There exists an effective constant λ, depending only on D_L, d_L, N_T and g, with the following property. Assume the function field* *of* $C \times_K L$ *takes the form* $L(X)[Y]$*, where*

$$Y^m = f(X), \quad m \in \mathbb{Z}_{\geq 2},$$

for $f \in \mathcal{O}_T[X]$ *a monic separable polynomial of degree at least* 3 *with* $\Delta(f) \in \mathcal{O}_T^\times$*. Then it holds*

$$h_F(J) \leq \lambda.$$

Proof. In the sequel $\lambda_1, \lambda_2, \ldots$ denote effective constants depending only on D_L, d_L, N_T and g. Let n be the degree of f, and let l be the least common multiple of m and n. We write $l = m'm$ and $l = n'n$ with positive integers m' and n'. The Riemann-Hurwitz formula implies

$$\max(m, n) \leq l \leq \lambda_1. \tag{6.7}$$

Let ζ be a generator of the torsion part of $\mathcal{O}_T^\times$. An application of (4.2) with $S' = T$ and $K = L$ gives a generating system $\Sigma = \Sigma'$ of the free part of $\mathcal{O}_T^\times$ such that

$$h(\epsilon) \leq \lambda_2, \quad \epsilon \in \Sigma. \tag{6.8}$$

Here we used that the cardinality $|\Sigma|$ of Σ, which appears in the upper bound (4.2), satisfies $|\Sigma| = t + d_L - 1 \leq \lambda_3$, where t denotes the number of finite places in T. Our assumption provides $\Delta = \Delta(f) \in \mathcal{O}_T^\times$. Thus there exist integers $a, a(\epsilon)$ such that Δ takes the form $\Delta = \zeta^a \prod_{\epsilon \in \Sigma} \epsilon^{a(\epsilon)}$. On reducing the exponents $a, a(\epsilon)$ modulo $l(n-1)$, we can rewrite the above equation as $\Delta = \omega^{-l(n-1)} \zeta^r \prod_{\epsilon \in \Sigma} \epsilon^{r(\epsilon)}$ with $\omega \in \mathcal{O}_T^\times$ and integers $0 \leq r, r(\epsilon) < l(n-1)$. We define $U = \omega^{n'} X$ and $V = \omega^{m'} Y$, and we write $f_\omega(U) = \omega^l f(U/\omega^{n'}) \in L[U]$. It follows that

$$V^m = f_\omega(U) \tag{6.9}$$

defines an affine plane model of $C_L = C \times_K L$. Further, we observe that $f_\omega \in \mathcal{O}_T[U]$ is monic, since $f \in \mathcal{O}_T[X]$ is monic and $\omega \in \mathcal{O}_T$, and the discriminant Δ_ω of f_ω satisfies $\Delta_\omega = \omega^{l(n-1)} \Delta = \zeta^r \prod_{\epsilon \in \Sigma} \epsilon^{r(\epsilon)}$. Therefore the inequalities $0 \leq r(\epsilon) < l(n-1)$, (6.7), (6.8) and $|\Sigma| \leq \lambda_3$ imply

$$h(\Delta_\omega) \leq \lambda_4. \tag{6.10}$$

The monic polynomial $f_\omega \in \mathcal{O}_T[U]$ is separable, with discriminant $\Delta_\omega \in \mathcal{O}_T^\times$. Moreover, f_ω has degree $n \geq 3$ and therefore we see that f_ω and T satisfy all conditions of Proposition 5.1 (i). Hence, an application of Proposition 5.1 (i) with $f = f_\omega$ and $T_0 = T$ gives a unipotent translation $\phi \in \mathrm{SL}_2(\mathcal{O}_T)$ such that $f^* = \phi^* f_\omega$ satisfies

$$h(f^*) \leq \lambda_5 + h(\Delta_\omega). \tag{6.11}$$

Here we used in addition (6.7) to estimate n which appears in the upper bound of Proposition 5.1 (i). The definition of $\phi^* f_\omega$ gives $\tau \in \mathcal{O}_T$ such that $W = U - \tau$ satisfies $f^*(W) = f_\omega(U)$, and then (6.9) shows that $V^m = f^*(W)$ defines an affine plane model of C_L.

Let $h_\theta(J)$ be the theta height of J, defined in [27, p.760]. On using Rémond [27, Théorème 1.3 and 1.5], we obtain an explicit estimate for $h_\theta(J)$ in terms of $h(f^*)$, m, n and g. Further, a result of Bost-David-Pazuki implies an explicit upper bound for $h_F(J)$ in terms of $h_\theta(J)$ and g, see [24]. Then (6.7), (6.10) and (6.11) lead to $h_F(J) \leq \lambda_6$ as desired. □

Proposition 6.1 provides a tool to prove new cases of the "effective Shafarevich conjecture": Suppose there exists a finite field extension L of K and a finite set of places T of L such that the function field of $C \times_K L$ satisfies the condition of Proposition 6.1 and such that N_T, D_L and d_L can be effectively controlled in terms of K, S and g. Then Proposition 6.1 gives an effective constant λ', depending only on K, S and g, such that $h_F(J) \leq \lambda'$.

Acknowledgements: It is a great pleasure to thank Gisbert Wüstholz and Clemens Fuchs for their excellent support during my PhD studies and for their helpful comments which improved the exposition of the above text. Many thanks go to Philipp Habegger, Sergey Gorchinskiy and Professor Alexei Paršin for answering several mathematical questions, to Professor Bjorn Poonen for his suggestion to look at [20, 31], to Professor Qing Liu for an interesting remark, and to the referee for useful comments which clarified certain discussions and for a comment which allowed to replace in the upper bounds $h_S - 1$ by $\log_2 h_S$. In addition, the author would like to thank Gisbert Wüstholz for financial support during spring semester 2011. This material is based upon work supported by the National Science Foundation under agreement No. DMS-0635607.

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, New Mathematical Monographs, **9**, Cambridge University Press, Cambridge, (2007).

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

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

[4] A. Brumer and J. H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91**, 1, (1996), 95–102.

[5] 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.

[6] R. de Jong and G. Rémond, *Conjecture de Shafarevitch effective pour les revêtements cycliques*, Algebra Number Theory **5**,8 (2011), 1133–1143.

[7] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75**, 3 (1984), 561–584.

[8] J.-H. Evertse and K. Győry, *Effective finiteness results for binary forms with given discriminant*, Compositio Math., **79**, 2 (1991), 169–204.

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

[10] C. Fuchs, R. von Känel, and G. Wüstholz, *An effective Shafarevich theorem for elliptic curves*, Acta Arith., **148**, 2 (2011), 189–203.

[11] 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.

[12] ———, *Polynomials and binary forms with given discriminant*, Publ. Math. Debrecen, **69**, 4, (2006), 473–499.

[13] K. Győry and K. Yu, *Bounds for the solutions of S-unit equations and decomposable form equations*, Acta Arith., **123**, 1 (2006), 9–41.

[14] H. A. Helfgott and A. Venkatesh, *Integral points on elliptic curves and 3-torsion in class groups*, J. Amer. Math. Soc., **19**, 3 (2006), 527–550.

[15] H. W. Lenstra, Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. (N.S.), **26**,2 (1992), 211–244.

[16] A. Levin, *Siegel's theorem and the Shafarevich conjecture*, J. Théor. Nombres Bordeaux, **24**, 3 (2012), 705–727.

[17] Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc., **348**, 11 (1996), 4577–4610.

[18] ———, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, **6**, Oxford University Press, Oxford, (2002), Oxford Science Publications.

[19] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer., Math. Soc., **342**, 2 (1994), 729–752.

[20] J. R. Merriman and N. P. Smart, *Curves of genus* 2 *with good reduction away from* 2 *with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc., **114**, 2 (1993), 203–214, Corrigenda: [21].

[21] ———, *Corrigenda: "Curves of genus* 2 *with good reduction away from* 2 *with a rational Weierstrass point"*, Math. Proc. Cambridge Philos. Soc., **118**, 1 (1995), 189.

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

[23] 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.

[24] F. Pazuki, *Theta height and Faltings height*, Bull. Soc. Math. France, **140**, 1 (2012), 19–49.

[25] B. Poonen, *Computational aspects of curves of genus at least* 2, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., Springer, Berlin, **1122**, (1996) pp. 283–306.

[26] G. Rémond, *Hauteurs thêta et construction de Kodaira*, J. Number Theory, **7**8, 2 (1999), 287–311.
[27] ———, *Nombre de points rationnels des courbes*, Proc. Lond. Math. Soc. (3), **101**, 3 (2010), 759–794.
[28] T. Saito, *Conductor, discriminant, and the Noether formula of arithmetic surfaces*, Duke Math. J., **5**7, 1 (1988), 151–173.
[29] I.R. Shafarevich, *Algebraic number fields*, Proc. Internat. Congr. Mathematicians, Stockholm, Inst. Mittag-Leffler, Djursholm, (1962), 163–176.
[30] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, **106**, Springer, Dordrecht, (2009).
[31] N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75**, 2 (1997), 271–307.
[32] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math., **23**, (1974), 135–152.
[33] R. von Känel, *On Szpiro's Discriminant Conjecture*, Internat. Math. Res. Notices, (2013), 1–35, Available online: doi: 10.1093/imrn/rnt079.

Rafael von Känel
IHÉS
35 Route de Chartres
91440 Bures-sur-Yvette
France
E-mail: rvk@ihes.fr
URL: www.ihes.fr/~rvk