ACTA ARITHMETICA
148.2 (2011)

An effective Shafarevich theorem for elliptic curves

by

Clemens Fuchs, Rafael von Känel and
Gisbert Wüstholz (Zürich)

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 [Sh] 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 [Co] got for the special case $K = \mathbb{Q}$ and $2, 3 \in S$ an effective constant C 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 $\max(|g_2|, |g_3|) \le C$. 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 [BrSi] 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 [EvSi]. Later in 1999 this upper bound for N was improved by Poulakis [Po]. He used an estimate for the number of solutions of the unit equation $x + y = 1$ obtained in [Ev] to establish his explicit upper bound for N.

After Baker stated in [Ba1] his groundbreaking effective lower bounds for linear forms in logarithms of algebraic numbers the existence of an effective

2010 *Mathematics Subject Classification*: Primary 11G05, 11D25, 14H52; Secondary 14D20, 14G40.
Key words and phrases: elliptic curves, Weierstrass models, number fields, good reduction, Shafarevich's theorem, Mordell equation, Baker's method.

DOI: 10.4064/aa148-2-5

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 [MaWü], Holzapfel [Ho] and Serre [Se2, Se1]. For the sake of completeness we also refer to a paper of Cremona and Lingham from 2007 (cf. [CrLi]) 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 $\mathbb{P}^2(\mathbb{C})$ 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 in this paper we shall consider an elliptic curve as a geometric object. The precise definition and also the notions of Weierstrass model and good reduction will be introduced in Section 2 below.

The main goal of this paper 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 C depending only on quantities (specified in Section 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

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

here h is the absolute logarithmic Weil height of K which will be defined in Section 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 paper is as follows: We start in Section 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 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 4 we slightly extend the result of Bugeaud [Bu, 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 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 6 we prove 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 $K = \mathbb{Q}$.

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 [De]) a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \tag{2.1}$$

$a_i \in K$, 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 (2.1).

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 $\mathcal{W} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(K)$ to E is called a *Weierstrass model* of E over $\mathrm{Spec}(R)$ 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 $\mathrm{Spec}(R_\mathfrak{p})$. 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 there exists a smooth Weierstrass model of E over $\mathrm{Spec}(R_{\mathfrak{p}})$, and it has *good reduction outside a subset* S *of* $\mathrm{Spec}(R)$ if it has good reduction at all $\mathfrak{p}$ not in S.

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, $M_{K,\mathrm{fin}}$ 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 $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ we let $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ be the order of $\mathfrak{p}$ in the principal ideal (α) defined by α and we put $\mathrm{ord}_v(\alpha) = \mathrm{ord}_{\mathfrak{p}_v}(\alpha)$. The places $v \in M_{K,\mathrm{fin}}$ define absolute values $|\alpha|_v$ on K if we put $|\alpha|_v = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}_v)^{-\mathrm{ord}_v(\alpha)}$ for $\alpha \neq 0$ and $|0|_v = 0$.

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

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

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 $H(f) = H(\beta_1, \dots, \beta_n)$. 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 $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ 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 $p = \max(3, p_1, \dots, p_s)$ 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 (cf. [BoGu, Theorem 1.5.13]), $\mathcal{O}_S^\times$ is finitely generated and has rank $s + d - 1$.

We denote by D_K the discriminant and by h_K the class number of K. In what follows $C_1, \dots, C_5$ 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*

$$h(\mathcal{W}) \leq \exp(\exp(C_1(s + h_K \log |D_K| + \log\log p)^2)).$$

There are various ways to attach a height to an elliptic curve. One possibility is to follow Silverman [Si2] and 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 a 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 these 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 [Si1]). 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 4.4 together 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

$$-27a_6^2 = 4a_4^3 + \frac{1}{16}\Delta_{\mathcal{W}} \tag{3.1}$$

with $\Delta_{\mathcal{W}} \in \mathcal{O}_T^\times$ and using an improved version of a result of Bugeaud [Bu] given in Proposition 4.1 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 the fact that T is effective in terms of S. The proposition requires that the coefficients of the equation in (3.1) 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 [Si3, 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 any more, and this establishes an extension to arbitrary number fields K of the result of Coates.

COROLLARY 3.1 (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*

$$h(\mathcal{W}) \le \exp(\exp(C_2(s + h_K \log|D_K| + \log\log p)^2)).$$

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 3.2. *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* $\mathrm{Spec}(\mathcal{O}_T)$ *and a Weierstrass model $\mathcal{W}'$ of E over* $\mathrm{Spec}(\mathcal{O}_K)$, *both smooth over* $\mathrm{Spec}(\mathcal{O}_T)$, *such that their logarithmic heights are bounded by*

$$\exp(C_3^{(s+1)^2}|D_K|^{d+2}(\log p)^{d(s+2)}).$$

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 3.3 (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* $\mathrm{Spec}(\mathcal{O}_S[1/6])$ *and a Weierstrass model $\mathcal{W}'$ of E over* $\mathrm{Spec}(\mathbb{Z})$, *both smooth over* $\mathrm{Spec}(\mathcal{O}_S[1/6])$, *such that their heights satisfy*

$$\max(H(\mathcal{W}), H(\mathcal{W}')) \le \exp(C_4^{(s+1)^2} p^{10^3(s+3)}).$$

Coates showed in [Co] 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

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

The bound in Corollary 3.3 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

$$N(\mathbb{Q},S) \le \exp(C_5^{(s+1)^2} p^{10^3(s+3)})$$

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

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 [Bu, 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 4.1. *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 $n \ge 3$. We set $A = \max(|N_{K/\mathbb{Q}}(a)|, 3)$ 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*

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

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

$$\lambda_1 = c_1^{(t+1)^2} q^{4n^3 d} (\log q)^{4n^2 dt},$$
$$\lambda_2 = |D_K|^{15n^2/2} A^{3n^2} |N_{K/\mathbb{Q}}(\Delta_g)|^{12n},$$
$$\lambda_3 = (\log |AD_K N_{K/\mathbb{Q}}(\Delta_g)|)^{6n^2 d} \log\log H.$$

The constant c_1 is effective and depends only on d and n.

Proof. Since all conditions of [Bu, 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 [Bu] 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 [Bu].

In a first step we work out the dependence on t of the constant c_{12} in [Bu, Lemma 4]. Following the proof and using the same arguments as in the proof of the main theorem of [BuGy] 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 by 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 replaced 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 replaced by $\exp(k_1(t+1)^2)$ and the statement follows with $c_1 = k_1$, where this c_1 is the one of the statement in this proposition. ∎

We remark that the above arguments imply, more generally, that the effective constant of the first bound of Bugeaud [Bu, 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 let 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 4.2. *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 $|\delta(a)a|_w \le 1$. For $w \notin T$ we have $|\delta(a)|_w \le 1$ and $|a|_w \le 1$ and therefore the assertion. If $w \in T$ and $|a|_w \le 1$, then again $|\delta(a)|_w \le 1$ and so the assertion follows in this case. Finally, if $w \in T$ and $|a|_w > 1$, then

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

This concludes the proof. ∎

We notice that the statement of the lemma would also follow from [BoGu, 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 4.3. *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 [La, 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

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

and from this we conclude that at most $(\log|D_K|)/(2\log 2)$ prime ideals divide $\mathfrak{a}$. 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 $M_{K,\mathrm{fin}}$ such that l divides the norm of $\mathfrak{p}_v$ for some $l \in P$ and we see that

$$|T_0| \le d h_K \log|D_K|$$

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 images 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 $0 \le m, n(\varepsilon) \le 11$. 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 4.4. *Let* E *be an elliptic curve over* K *with good reduction outside* S*. There exists a globally minimal Weierstrass model of* E *over* $\mathrm{Spec}(\mathcal{O}_T)$ *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 $\mathrm{Spec}(\mathcal{O}_T)$ is trivial and then [Li, Theorem 9.4.35] provides a globally minimal Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_T)$. Pick $F \in \mathcal{O}_T[X,Y,Z]$ with $\mathcal{W} = \mathrm{Proj}(\mathcal{O}_T[X,Y,Z]/(F))$. For $v \in M_{K,\mathrm{fin}}$ we take $\mathfrak{p} = \mathfrak{p}_v \in \mathrm{Spec}(\mathcal{O}_T)$ and $\mathcal{W}_\mathfrak{p} = \mathcal{W} \times_{\mathcal{O}_T} \mathrm{Spec}(\mathcal{O}_{T,\mathfrak{p}})$. 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 [Li, 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 $0 \le m, n(\varepsilon) \le 11$. 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

$$Y^2Z = X^3 - 4XZ^2 + \frac{8}{3}Z^3. \tag{4.1}$$

The Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_S)$ given by (4.1) 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 any more. 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 [Sz] were 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 (3.1) 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 [Ba4, Ba5], or more specifically on the Mordell equation [Ba2, Ba3], 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.

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 4.3, 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 4.3 we get

$$t \le ds + dh_K \log|D_K| + 2d \quad \text{and} \quad q \le p|D_K|^{1/2}. \tag{5.1}$$

We now take 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 [BuGy, Lemma 1] we choose a fundamental system $\mathcal{U}$ of T-units such that

$$h(\varepsilon) \le c_2^{(t+1)^2} R_T \tag{5.2}$$

for all $\varepsilon \in \mathcal{U}$, where R_T denotes the T-regulator (defined in [Bu]), and we fix a generator ζ of the torsion subgroup of $K^\times$.

Our Lemma 4.4 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 equation (3.1) with 16 and find that $(4a_4, 4a_6) \in \mathcal{O}_T \times \mathcal{O}_T$ is a solution of

$$-27Y^2 = X^3 + \Delta. \tag{5.3}$$

From Lemma 4.2 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 4.1 to $3Y^2 = g(X)$ gives

$$H(x) \le H(g)^2\, e^{\lambda} \tag{5.4}$$

with $\lambda = \lambda_1\lambda_2\lambda_3$ (for the definition of the quantities $\lambda_1, \lambda_2, \lambda_3$ see Proposition 4.1).

Since the degree of g is 3 we get

$$\lambda_1 \le c_3^{(t+1)^2} q^{108d} (\log q)^{36dt} \tag{5.5}$$

and to estimate λ_2 and λ_3 we need bounds for $|N_{K/\mathbb{Q}}(\Delta_g)|$, $H(g)$ 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 $|N_{K/\mathbb{Q}}(\Delta_g)|$, $H(g)$ 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. From [Bu, Lemma 3] we get $R_T \le R_K h_K (d\log q)^t$ and from [Le] we see that $R_K h_K$ is at most $(10d)^{10d}|D_K|^{1/2}(\log|D_K|)^{d-1}$, which combines to

$$R_T \le c_4 |D_K|^{1/2} (\log|D_K|)^{d-1} (d\log q)^t.$$

The discriminant Δ is reduced and this means that

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

for integers $0 \le m, n(\varepsilon) < 12$. Height properties together with (5.2) and the upper bound for R_T lead to

$$H(\Delta) \le \exp(c_5^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^{d-1} (\log q)^t)$$

and we conclude that

$$\delta(\Delta) \le \exp(c_6^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^{d-1} (\log q)^t). \tag{5.6}$$

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

$$H(\alpha) \le \exp(c_8^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^{d-1} (\log q)^t)$$

and then (5.6) yields

$$|N_{K/\mathbb{Q}}(\Delta_g)| \le \exp(c_9^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^{d-1} (\log q)^t).$$

In our application of Proposition 4.1 we have $H(g) = H(\delta(\Delta)^5\alpha)$, $a = 3$ and $A = 3^d$. We put the estimates together to obtain

$$\lambda_2 \le \exp(c_{10}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t), \tag{5.7}$$

$$\lambda_3 \le (c_{11}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)^{55d}. \tag{5.8}$$

The estimates for λ_1, λ_2 and λ_3 given in (5.5), (5.7) and (5.8) are now used to give an upper bound for $H(x)$, $H(a_4)$ and $H(a_6)$. From (5.4) we get

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

and (5.6) together with the inequality $H(a_4) \le H(x) H(4\delta(\Delta)^2)$ leads to

$$H(a_4) \le \exp(\exp(c_{13}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)). \tag{5.9}$$

From (5.3) we see that $H(a_6) \le 59 H(a_4)^{3/2} H(\Delta)^{1/2}$ and our estimates for $H(a_4)$ and $H(\Delta)$ give

$$H(a_6) \le \exp(\exp(c_{14}^{(t+1)^2} |D_K|^{1/2} (\log |D_K|)^d (\log q)^t)). \tag{5.10}$$

Finally, we replace t and q in (5.9), (5.10) by the estimates in (5.1) and obtain

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

as claimed in the theorem. ∎

6. Proof of the corollaries. Once the Main Theorem is established it is not difficult to deduce the corollaries.

Proof of Corollary 3.1. 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 4.2 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 $u = \delta(a)\delta(b)$, $a_4 = u^4a$, $a_6 = u^6b$ 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 $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ 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 3.2. By assumption, with the same notation as in the first step of the proof of the Main Theorem, we get

$$t \le d(s+2) \quad \text{and} \quad q \le p. \tag{6.1}$$

We replace t and q in (5.9) and (5.10) by the bounds given in (6.1). The same arguments as in the proof of Corollary 3.1 then give Corollary 3.2. ∎

Proof of Corollary 3.3. We put $T = S \cup \{2, 3\} = \mathcal{U}$ and take $\zeta = -1$. From Lemma 4.4 we obtain a globally minimal Weierstrass model $\mathcal{W}$ of E over $\mathrm{Spec}(\mathcal{O}_T)$ defined by $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ 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 $\pm\prod l^{n(l)}$ with $0 \le n(l) \le 11$ and with $n(l) = 0$ unless $l \in S$ or $l = 2, 3$. 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 4.1, 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 (6.1) to obtain

$$\max(H(a_4), H(a_6)) \le \exp(c_{18}^{(s+1)^2} p^{10^3(s+3)}) \tag{6.2}$$

with an effective constant c_{18}, which completes the proof of the first part of the corollary. From (6.2) we deduce the remaining parts with the same arguments as used in the proof of Corollary 3.1. ∎

Acknowledgements. The authors thank Sergey Gorchinskiy for his interesting comments on a preliminary version of the paper.

References

[Ba1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 13 (1966), 204–216; *II*, ibid. 14 (1967), 102–107; *III*, ibid. 14 (1967), 220–228; *IV*, ibid. 15 (1968), 204–216.

[Ba2] —, *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.

[Ba3] —, *Contributions to the theory of Diophantine equations. II. The Diophantine equation* $y^2 = x^3 + k$, ibid., 193–208.

[Ba4] —, *The Diophantine equation* $y^2 = ax^3 + bx^2 + cx + d$, J. London Math. Soc. 43 (1968), 1–9.

[Ba5] —, *Bounds for the solutions of the hyperelliptic equation*, Math. Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[BoGu] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Math. Monogr. 4, Cambridge Univ. Press, Cambridge, 2007.

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

[Bu] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Compos. Math. 107 (1997), 187–219.

[BuGy] Y. Bugeaud and K. Győry, *Bounds for the solutions of unit equations*, Acta Arith. 74 (1996), 67–80.

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

[CrLi] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. 16 (2007), 303–312.

[De] P. Deligne, *Courbes elliptiques: formulaire d'après J. Tate*, in: Modular Functions of One Variable, IV (Antwerp, 1972), Lecture Notes in Math. 476, Springer, Berlin, 1975, 53–73.

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

[EvSi] 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), 237–248.

[Ho] R.-P. Holzapfel, *The Ball and Some Hilbert Problems*, Birkhäuser, Basel, 1995.

[La] S. Lang, *Algebraic Number Theory*, 2nd ed., Grad. Texts in Math. 110, Springer, New York, 1994.

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

[Li] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxf. Grad. Texts Math. 6, Oxford Univ. Press, Oxford, 2006.

[MaWü] D. W. Masser and G. Wüstholz, *Some effective estimates for elliptic curves*, in: Arithmetic of Complex Manifolds (Erlangen, 1988), Lecture Notes in Math. 1399, Springer, Berlin, 1989, 103–109.

[Po] D. Poulakis, *The number of solutions of the Mordell equation*, Acta Arith. 88 (1999), 173–179; Corrigendum, ibid. 92 (2000), 387–388.

[Se1] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Benjamin, New York, 1968.

[Se2] —, *Lectures on the Mordell–Weil Theorem*, 3rd ed., Vieweg, Wiesbaden, 1997.

[Sh] I. R. Shafarevich, *Algebraic number fields*, in: Proc. Internat. Congr. of Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, 163–176 (in Russian); English transl.: Amer. Math. Soc. Transl. (2) 31, Amer. Math. Soc., Providence, RI, 1963, 25–39.

[Si1] J. H. Silverman, *Heights and elliptic curves*, in: Arithmetic Geometry (Storrs, 1984), Springer, New York, 1986, 253–265.

[Si2] —, *Elliptic curves of bounded degree and height*, Proc. Amer. Math. Soc. 105 (1989), 540–545.

[Si3] —, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[Sz] L. Szpiro, *Propriétés numériques du faisceau dualisant relatif*, Astérisque 86 (1981), 44–78.

Clemens Fuchs, Rafael von Känel, Gisbert Wüstholz
Department of Mathematics
ETH Zürich
Rämistrasse 101
8092 Zürich, Switzerland
E-mail: clemens.fuchs@math.ethz.ch
rafael.vonkaenel@math.ethz.ch
gisbert.wuestholz@math.ethz.ch

Received on 11.6.2010
and in revised form on 28.12.2010 (6416)