Invent math. 92, 461–477 (1988)

Inventiones mathematicae

On S-unit equations in two unknowns

J.-H. Evertse[1]*, K. Györy[2]**, C.L. Stewart[3]***, and R. Tijdeman[4]

[1] Department of Pure Mathematics, Centre for Mathematics and Computer Science, Kruislaan 413, NL-1098 SJ Amsterdam, The Netherlands
[2] Mathematical Institute, Kossuth Lajos University, H-4010 Debrecen, Hungary
[3] Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
[4] Mathematical Institute, University of Leiden, NL-2333 CA Leiden, The Netherlands

§ 0. Introduction

Let K be an algebraic number field of degree d, with discriminant D_K and ring of integers $\mathcal{O}_K$. Let M_K be the set of places (i.e. equivalence classes of multiplicative valuations) on K. A place v is called finite if v contains only non-archimedean valuations, and infinite otherwise. K has only finitely many infinite places. Let S be a finite subset of M_K, containing all infinite places. A number $\alpha \in K$ is called an S-unit if $|\alpha|_v = 1$ for every valuation $|\ |_v$ from a place $v \in M_K \backslash S$. The S-units form a multiplicative group which is denoted by U_S. We shall deal with the S-unit equation

$$\alpha_1 x + \alpha_2 y = \alpha_3 \quad \text{in } x, y \in U_S, \tag{1}$$

where $\alpha_1, \alpha_2, \alpha_3 \in K^* (= K \backslash \{0\})$. Lang [9] proved that (1) has only finitely many solutions. Denote this number of solutions by $\nu_S(\alpha_1, \alpha_2, \alpha_3)$. We call two triples $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ in $(K^*)^3$ (and their corresponding S-unit equations) S-equivalent if there exist a permutation σ of (1, 2, 3), a $\lambda \in K^*$ and S-units $\varepsilon_1, \varepsilon_2, \varepsilon_3$ such that

$$\beta_i = \lambda \varepsilon_i \alpha_{\sigma(i)} \quad \text{for } i = 1, 2, 3. \tag{2}$$

It is easy to check that if $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$ are S-equivalent, then $\nu_S(\alpha_1, \alpha_2, \alpha_3) = \nu_S(\beta_1, \beta_2, \beta_3)$ (cf. [6] § 1).

Evertse [3] proved that $\nu_S(\alpha_1, \alpha_2, \alpha_3) \leqq 3 \times 7^{d+2s}$ for every $(\alpha_1, \alpha_2, \alpha_3) \in (K^*)^3$ where s denotes the cardinality of S. A general upper bound for ν_S which is polynomial in s does not exist, since a result of Erdös, Stewart and Tijdeman

* Research supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.); *Current address*: see R. Tijdeman
** Research supported in part by Grant 273 from the Hungarian National Foundation for Scientific Research
*** Research supported in part by Grant A 3528 from the Natural Sciences and Engineering Research Council of Canada

[2] implies that in case $K=\mathbb{Q}$ there is a positive constant C and there are sets S of arbitrarily large cardinality for which $\nu_S(1,1,1)>\exp(C(s/\log s)^{1/2})$. On the other hand, for a large class of triples $(\alpha_1,\alpha_2,\alpha_3)$ specified below, Győry [7] derived an upper bound for $\nu_S(\alpha_1,\alpha_2,\alpha_3)$ which is linear in s. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ be the prime ideals corresponding to the finite places in S. For any $\alpha\in K^*$ the principal ideal (α) can be written uniquely as a product of two (not necessarily principal) ideals $\mathfrak{a}'$ and $\mathfrak{a}''$, where $\mathfrak{a}'$ is composed of $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ and $\mathfrak{a}''$ is composed solely of prime ideals different from $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$. We put $N_S(\alpha)=N_{K/\mathbb{Q}}(\mathfrak{a}'')$. Győry proved the following.

For any ε with $0<\varepsilon\leqq 1$ there is an effectively computable number C depending only on ε, K and S such that $\nu_S(\alpha_1,\alpha_2,\alpha_3)\leqq s+3t$ for each triple $(\alpha_1,\alpha_2,\alpha_3)\in(\mathcal{O}_K\setminus\{0\})^3$ with

$$N_S(\alpha_3)\geqq C \quad \text{and} \quad (N_S(\alpha_3))^{1-\varepsilon}\geqq \min(N_S(\alpha_1), N_S(\alpha_2)). \tag{3}$$

If, moreover, $(\log N_S(\alpha_3))^{1-\varepsilon}\geqq\max(\log N_S(\alpha_1), \log N_S(\alpha_2))$, then $\nu_S(\alpha_1,\alpha_2,\alpha_3)\leqq s+t$.

We remark that there are infinitely many S-equivalence classes which have a representative satisfying condition (3) and infinitely many S-equivalence classes which do not have such a representative (cf. [6], § 3).

In this paper we prove that almost all equivalence classes of S-unit equations in two unknowns have remarkably few solutions.

Theorem 1. *Let S be a finite subset of M_K containing all infinite places. Then there exists a finite set $\mathcal{A}$ of triples in $(K^*)^3$ with the following property: for each triple $(\alpha_1,\alpha_2,\alpha_3)\in(K^*)^3$ which is not S-equivalent to any of the triples from $\mathcal{A}$, the number of solutions of* (1) *is at most two.*

For $s>1$, the upper bound 'two' cannot be improved, since there are infinitely many S-equivalence classes of S-unit equations (1) with two solutions (cf. [6], § 1). The proof of Theorem 1 is based on the Main Theorem on S-Unit Equations (Lemma 1) which is proved by the p-adic analogue of the Thue-Siegel-Roth-Schmidt method and is therefore ineffective. Consequently, its proof does not enable one to describe triples $(\alpha_1,\alpha_2,\alpha_3)$ for which (1) has no more than two solutions. The following improvement of Győry's result is based on the effective method of Baker and its p-adic analogue. It provides the upper bound $s+1$ for the number of solutions of all S-unit equations with the exception of a finite set of S-equivalence classes which is, at least in principle, effectively determinable. For any non-zero algebraic number α with minimal polynomial

$$F(X)=a_0\prod_{i=1}^{n}(X-\alpha_i)\in\mathbb{Z}[X], \tag{4}$$

we define the height $h(\alpha)$ of α by

$$h(\alpha)=\left(|a_0|\prod_{i=1}^{n}\max(1,|\alpha_i|)\right)^{1/n}. \tag{5}$$

For given $C\geqq 1$, there are only finitely many $\alpha\in K^*$ with $h(\alpha)\leqq C$, and all these α can be effectively determined.

Theorem 2. *Let S be a finite subset of M_K of cardinality s, containing all infinite places. Suppose that the rational primes corresponding to the finite places in S do not exceed $P(\geqq 2)$. Let $\mathscr{B}$ denote the set of triples $(\beta_1, \beta_2, \beta_3) \in (\mathcal{O}_K \setminus \{0\})^3$ with*

$$\max(h(\beta_1), h(\beta_2), h(\beta_3)) \leqq \exp\{(C_1 s)^{C_2 s} P^{d+1}\},$$

where C_1 and C_2 are certain explicitly computed numbers depending only on d and $|D_K|$. Then for each triple $(\alpha_1, \alpha_2, \alpha_3) \in (K^*)^3$ which is not S-equivalent to any of the triples in $\mathscr{B}$, the number of solutions of (1) *is at most* $s+1$.

For $t>0$, Theorem 2 implies Győry's result stated above. For let $(\alpha_1, \alpha_2, \alpha_3) \in (\mathcal{O}_K \setminus \{0\})^3$ be a triple satisfying (3) for some $\varepsilon > 0$ and some number C which will be chosen later. For any triple $(\beta_1, \beta_2, \beta_3) \in (\mathcal{O}_K \setminus \{0\})^3$ which is S-equivalent to $(\alpha_1, \alpha_2, \alpha_3)$ we have

$$\{\max(h(\beta_1), h(\beta_2), h(\beta_3))\}^d \geqq \frac{N_S(\alpha_3)}{\min(N_S(\alpha_1), N_S(\alpha_2))}. \tag{6}$$

This can be proved easily by observing that the right hand side of (6) does not change if $\alpha_1, \alpha_2, \alpha_3$ are multiplied by the same number in K^* or by different S-units, that the left-hand side of (6) is invariant under permutations of $\beta_1, \beta_2, \beta_3$, and that for each β in $\mathcal{O}_K \setminus \{0\}$

$$1 \leqq N_S(\beta) \leqq |N_{K/\mathbb{Q}}(\beta)| \leqq (h(\beta))^d.$$

By combining (6) with (3) we obtain that

$$\max(h(\beta_1), h(\beta_2), h(\beta_3)) \geqq C^{\varepsilon/d}$$

for each triple $(\beta_1, \beta_2, \beta_3) \in (\mathcal{O}_K \setminus \{0\})^3$ which is S-equivalent to $(\alpha_1, \alpha_2, \alpha_3)$. Together with Theorem 2 this implies that (1) has at most $s+1$ solutions if C is sufficiently large.

By combining Theorem 2 with an explicit upper bound for the heights of the solutions of (1), derived by Győry [7] (see also Lemma 7 in this paper) we obtain that any triple $(\beta_1, \beta_2, \beta_3) \in (K^*)^3$ for which $\beta_1 x' + \beta_2 y' = \beta_3$ has more than $s+1$ solutions in S-units x', y', is S-equivalent to a triple $(\alpha_1, \alpha_2, \alpha_3) \in (\mathcal{O}_K \setminus \{0\})^3$ such that the solutions of (1) have heights which do not exceed an effectively computable number independent of $\alpha_1, \alpha_2, \alpha_3$. More precisely we have the following result.

Theorem 3. *Let K, S, s, P have the same meaning as in Theorem 2. Let $(\beta_1, \beta_2, \beta_3) \in (K^*)^3$ be a triple for which the equation $\beta_1 x' + \beta_2 y' = \beta_3$ in S-units x', y' has at least $s+2$ solutions. Then there is a triple $(\alpha_1, \alpha_2, \alpha_3) \in (\mathcal{O}_K \setminus \{0\})^3$, S-equivalent to $(\beta_1, \beta_2, \beta_3)$, such that all solutions (x, y) of* (1) *satisfy*

$$\max(h(x), h(y)) \leqq \exp\{(C_3 s)^{C_4 s} P^{2d+2}\},$$

where C_3 and C_4 are effectively computable numbers depending only on d and $|D_K|$.

The special case $K=\mathbb{Q}$ of Theorem 1 has been considered in [6] § 5. On the other hand, it is possible to generalize Theorem 1 to the case that K is any subfield of $\mathbb{C}$ and U_S is any finitely generated multiplicative subgroup of $\mathbb{C}^*$, or that U_S is just a subgroup of finite rank of $\mathbb{C}^*$. For the proofs it suffices to replace the Main Theorem on S-Unit Equations as we use it (Lemma 1) by the version due to van der Poorten and Schlickewei [14] in the first instance and the version of Laurent [12] in the second.

Suppose that we want to extend our results to S-unit equations

$$\alpha_1 x_1 + \ldots + \alpha_n x_n = \alpha_{n+1} \quad \text{in } x_1, \ldots, x_n \in U_S, \tag{7}$$

where $(\alpha_1, \ldots, \alpha_{n+1}) \in (K^*)^{n+1}$ with $n>2$. If U_S is infinite an equation of this type may have infinitely many solutions such that some non-empty proper subsum of $\alpha_1 x_1 + \ldots + \alpha_n x_n$ vanishes. Such solutions will be called degenerate. For example, let $\alpha_1, \ldots, \alpha_{n-1} \in K^*$ such that $\alpha_1 x_1' + \ldots + \alpha_{n-1} x_{n-1}' = 0$ for some $x_1', \ldots, x_{n-1}' \in U_S$. Then, for any $\varepsilon \in U_S$, Eq. (7) with $\alpha_{n+1} = \alpha_n$ has the degenerate solution $x_1 = \varepsilon x_1'$, $x_2 = \varepsilon x_2'$, $\ldots$, $x_{n-1} = \varepsilon x_{n-1}'$, $x_n = 1$. However, as we shall show in § 5, the number of non-degenerate solutions can also be large. We shall prove that for $K=\mathbb{Q}$ and for any sufficiently large integer s there is a set S of cardinality s and infinitely many S-inequivalent $n+1$-tuples $(\alpha_1, \ldots, \alpha_{n+1}) \in (\mathbb{Q}^*)^{n+1}$ for which the number of non-degenerate solutions of the S-unit Equation (7) is at least $\exp((4+o(1))\,(s/\log s)^{1/2})$ as $s \to \infty$. Thus the constant two in Theorem 1 and the number $s+1$ in Theorem 2 must be replaced by a number at least as large as $\exp((4+o(1))\,(s/\log s)^{1/2}$ as $s \to \infty$. On the other hand, recently Evertse and Györy [5] have shown that apart from finitely many S-inequivalent $n+1$-tuples $(\alpha_1, \ldots, \alpha_{n+1}) \in (K^*)^{n+1}$, the solutions of (7) are contained in at most $2^{(n+1)!}$ proper linear subspaces of K^n. For $n=2$, this gives a weaker version of our Theorem 1 with the upper bound 2^6 instead of 2.

For more background material and applications of results on S-unit equations, we refer the reader to our survey paper [6] in the Proceedings of the L.M.S. Conference on Transcendence Theory at Durham, England. At this conference, held in July, 1986, Theorem 1 was established.

§ 1. Proof of Theorem 1

Let n be an integer with $n \geqq 1$. Points in the vector space K^{n+1} are denoted by $X=(X_0, X_1, \ldots, X_n)$. If we identify pairwise linearly dependent non-zero points in K^{n+1}, we obtain the n-dimensional projective space $\mathbb{P}^n(K)$. Points in $\mathbb{P}^n(K)$, so-called projective points, are denoted by $X=(X_0 : X_1 : \ldots : X_n)$, where the homogeneous coordinates are in K and are determined up to a multiplicative constant in K. We denote the subset of $\mathbb{P}^n(K)$ of projective points with all the homogeneous coordinates in U_S by $\mathbb{P}^n(U_S)$. We shall apply the Main Theorem on S-Unit Equations which was first stated by van der Poorten and Schlickewei [14]. Evertse formulated his version of this theorem in terms of (c, d, S)-admissible points. Since $\mathbb{P}^n(U_S)$ consists precisely of all $(1, 0, S)$-admissible points, we may use the following statement.

Lemma 1. (Evertse, [4, Theorem 1]). *There are only finitely many projective points* $X=(X_0:X_1:\ldots:X_n)\in\mathbb{P}^n(U_S)$ *such that*

$$X_0+X_1+\ldots+X_n=0 \tag{8}$$

with

$$X_{i_0}+X_{i_1}+\ldots+X_{i_m}\neq 0$$

for each proper, non-empty subset $\{i_0, i_1, \ldots, i_m\}$ *of* $\{0, 1, \ldots, n\}$.

Proof of Theorem 1. Since $(\alpha_1, \alpha_2, \alpha_3)$ and $(\alpha_1/\alpha_3, \alpha_2/\alpha_3, 1)$ are S-equivalent, we may assume without loss of generality that $\alpha_3=1$. Suppose

$$\alpha_1 x+\alpha_2 y=1 \tag{9}$$

has three distinct solutions (x_1, y_1), (x_2, y_2), (x_3, y_3) in $(U_S)^2$. Then we obtain, after eliminating α_1 and α_2,

$$x_1 y_2-x_2 y_1+x_2 y_3-x_3 y_2+x_3 y_1-x_1 y_3=0. \tag{10}$$

Note that the expression on the left-hand side does not change value if we interchange all x's and y's or if we permute the subscripts $\{1, 2, 3\}$ consistently. Furthermore,

$$x_1 y_2\neq x_2 y_1, \qquad x_2 y_3\neq x_3 y_2, \qquad x_3 y_1\neq x_1 y_3, \tag{11}$$

since the solutions of (9) are distinct. We shall show that there are only finitely many possibilities for x_2/x_1 and y_2/y_1. By the preceding considerations it suffices to prove this claim in each of the following cases:

(a) no proper, non-empty subsum of the left-hand side of (10) vanishes,
(b1) $x_1 y_2+x_2 y_3=0$, $x_2 y_1+x_3 y_2-x_3 y_1+x_1 y_3=0$,
(b2) $x_1 y_2-x_3 y_2=0$, $x_2 y_1-x_2 y_3-x_3 y_1+x_1 y_3=0$,
(c1) $x_1 y_2-x_2 y_1+x_2 y_3=0$, $x_3 y_2-x_3 y_1+x_1 y_3=0$,
(c2) $x_1 y_2+x_2 y_3+x_3 y_1=0$, $x_2 y_1+x_3 y_2+x_1 y_3=0$,
(c3) $x_1 y_2+x_2 y_3-x_1 y_3=0$, $x_2 y_1+x_3 y_2-x_3 y_1=0$.

Case (a). By Lemma 1 there are only finitely many projective points $(x_1 y_2:x_2 y_1:x_2 y_3:x_3 y_2:x_3 y_1:x_1 y_3)\in\mathbb{P}^5(U_S)$. Hence there are only finitely many possibilities for x_2/x_1 and y_2/y_1.

Case (b1). No subsum of $x_2 y_1+x_3 y_2-x_3 y_1+x_1 y_3$ can vanish by (11), $x_2\neq x_3$, $y_1\neq 0$, $x_3\neq 0$, $y_1\neq y_2$. By Lemma 1 there are only finitely many projective points $(x_1 y_2:x_2 y_3)\in\mathbb{P}^1(U_S)$ and $(x_2 y_1:x_3 y_2:x_3 y_1:x_1 y_3)\in\mathbb{P}^3(U_S)$. Hence there are only finitely many possibilities for $x_1 y_2/x_2 y_3$, y_2/y_1, $x_2 y_1/x_1 y_3$, whence for $x_2 y_3/x_1 y_1$, $x_2 y_1/x_1 y_3$, whence for x_2^2/x_1^2, whence for x_2/x_1.

Case (b2). This is impossible, since $y_2\neq 0$, $x_1\neq x_3$.

Case (c1). By Lemma 1 there are only finitely many projective points $(x_1 y_2:x_2 y_1:x_2 y_3)\in\mathbb{P}^2(U_S)$ and $(x_3 y_2:x_3 y_1:x_1 y_3)\in\mathbb{P}^2(U_S)$. Hence there are only finitely many possibilities for y_2/y_1, $x_1 y_2/x_2 y_1$, whence for x_2/x_1.

Case (c2). By Lemma 1 there are only finitely many projective points $(x_1 y_2 : x_2 y_3 : x_3 y_1) \in \mathbb{P}^2(U_S)$ and $(x_2 y_1 : x_3 y_2 : x_1 y_3) \in \mathbb{P}^2(U_S)$. Hence there are only finitely many possible values for $x_2 y_3/x_1 y_2$, $x_1 y_2/x_3 y_1$, $x_3 y_2/x_2 y_1$, $x_2 y_1/x_1 y_3$, whence for $x_2^2 y_1/x_1^2 y_2$, $x_1 y_2^2/x_2 y_1^2$, whence for x_2^3/x_1^3 and y_2^3/y_1^3, whence for x_2/x_1 and y_2/y_1.

Case (c3). By Lemma 1 there are only finitely many projective points $(x_1 y_2 : x_2 y_3 : x_1 y_3) \in \mathbb{P}^2(U_S)$ and $(x_2 y_1 : x_3 y_2 : x_3 y_1) \in \mathbb{P}^2(U_S)$. Hence there are only finitely many possibilities for x_2/x_1 and y_2/y_1.

We conclude that there are indeed only finitely many possibilities for x_2/x_1 and y_2/y_1. Since (x_1, y_1) and (x_2, y_2) satisfy (9), we have

$$\alpha_1 x_1 = \frac{(y_2/y_1)-1}{y_2/y_1 - x_2/x_1}, \qquad \alpha_2 y_1 = \frac{(x_2/x_1)-1}{x_2/x_1 - y_2/y_1}$$

Hence there are only finitely many possibilities for α_1 and α_2 up to multiplicative factors from U_S.

Remark. Up to multiplicative factors from U_S, there are only finitely many elements of K^* which can be represented as sums of two S-units in two essentially different ways. This is an immediate consequence of Lemma 1. It means that in Theorem 1 'two' can be replaced by 'one' when $\alpha_1 = \alpha_2$ and solutions (x, y) and (y, x) are not distinguished.

§ 2. Valuations and heights

Since the algebraic number field K has degree d, it has d different $\mathbb{Q}$-isomorphisms into $\mathbb{C}$, $\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \sigma_{r_1+r_2+1}, \ldots, \sigma_{r_1+2r_2} = \sigma_d$ say, where σ_i maps K into $\mathbb{R}$ for $i = 1, \ldots, r_1$, σ_i maps K into $\mathbb{C}$ for $i = r_1+1, \ldots, d$ and $\overline{\sigma_{r_1+j}(\alpha)} = \sigma_{r_1+r_2+j}(\alpha)$ for $\alpha \in K$ and $j \in \{1, \ldots, r_2\}$. K has exactly $r_1 + r_2$ infinite places, and each infinite place v contains exactly one valuation of the type $|\sigma_{i(v)}(\ )|$ where $i(v) \in \{1, \ldots, r_1 + r_2\}$. In each infinite place v we choose the valuation

$$|\ |_v = |\sigma_{i(v)}(\ )|^{d_v/d}, \tag{12}$$

where $d_v = 1$ if $1 \leqq i(v) \leqq r_1$ and $d_v = 2$ if $r_1 + 1 \leqq i(v) \leqq r_1 + r_2$.

For each $\alpha \in K^*$ we have

$$(\alpha) = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}(\alpha)},$$

where (α) denotes the ideal generated by α, $\mathfrak{p}$ runs through the set of prime ideals of $\mathcal{O}_K$, and the exponents $\operatorname{ord}_{\mathfrak{p}}(\alpha)$ are integers of which at most finitely many are non-zero. If v is the finite place corresponding to the prime ideal $\mathfrak{p}$, then we put

$$|\alpha|_v = (N_{K/\mathbb{Q}}(\mathfrak{p}))^{-\operatorname{ord}_{\mathfrak{p}}(\alpha)/d} \quad \text{if } \alpha \neq 0, \qquad |0|_v = 0. \tag{13}$$

The valuations $|\ |_v (v \in M_K)$ chosen above satisfy the product formula

$$\prod_{v\in M_K} |\alpha|_v = 1 \qquad \text{for } \alpha\in K^*. \tag{14}$$

The set of infinite places on K is denoted by S_∞. If S is any finite subset of M_K containing S_∞, then we have

$$N_S(\alpha) = \left(\prod_{v\in S} |\alpha|_v\right)^d \qquad \text{for } \alpha\in K, \tag{15}$$

where $N_S(\alpha)$ has the same meaning as in the Introduction. In particular, $N_{S_\infty}(\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$. Finally we have

$$N_S(\alpha) = 1 \qquad \text{for each } S\text{-unit } \alpha. \tag{16}$$

If h is the height defined in (5), then (cf. [11], p. 54)

$$h(\alpha) = \prod_{v\in M_K} \max(1, |\alpha|_v) \qquad \text{for } \alpha\in K^*. \tag{17}$$

We shall use frequently that

$$h(\alpha^{-1}) = h(\alpha), \qquad h(\alpha\beta) \leqq h(\alpha)\, h(\beta) \qquad \text{for } \alpha, \beta\in K^*. \tag{18}$$

In the literature two other heights frequently appear, namely $H(\alpha)$, which is the maximum of the absolute values of the coefficients of the minimal polynomial of α over $\mathbb{Z}$, and $|\overline{\alpha}|$, which is the maximum of the absolute values of the conjugates of α over $\mathbb{Q}$. We have

$$|\overline{\alpha}|^{1/n} \leqq h(\alpha) \leqq |\overline{\alpha}| \tag{19}$$

if α is a non-zero algebraic integer of degree n, and

$$\tfrac{1}{2} H(\alpha)^{1/n} \leqq h(\alpha) \leqq (n+1)^{1/(2n)} H(\alpha)^{1/n} \tag{20}$$

if α is a non-zero algebraic number of degree n. (19) is obvious, while the proof of (20) can be found, for instance, in [11], p. 60, Theorem 2.8.

§ 3. Lemmas for the proofs of Theorems 2 and 3

We shall use the same notation as in the previous sections. In particular, s is the cardinality of S and the rational primes corresponding to the finite places in S do not exceed $P(\geqq 2)$. Let t denote the number of finite places in S, and define r such that $r+1$ is equal to the number of infinite places on K. Thus $s=r+t+1$. It is well known that the group U_S of S-units has rank $r+t=s-1$. In the remainder of the paper, $c_1, c_2, \ldots,$ will denote effectively computable numbers >1, which depend only on d and the absolute value of the discriminant D_K of K. We shall use frequently the fact that the class number h_K of K and the regulator R_K of K can be estimated from above by effectively computable numbers depending only on d and $|D_K|$. This follows from an upper bound for $h_K R_K$ derived by Siegel [16] and a lower bound for R_K due to Zimmert [17].

In the next three lemmas some estimates for S-units are given. We recall that d_v and the valuations $|\ |_v$ were introduced in (12) and (13).

Lemma 2. *If $r \geqq 1$, then there exist multiplicatively independent units $\eta_1, \dots, \eta_r$ in $\mathcal{O}_K$ with the following properties:*

(i) $\max_j h(\eta_j) \leqq c_1$;

(ii) *every unit η in $\mathcal{O}_K$ can be written as $\eta = \eta' \eta_1^{a_1} \dots \eta_r^{a_r}$ with $a_1, \dots, a_r \in \mathbb{Z}$ and $h(\eta') \leqq c_2$;*

(iii) *for each $v_0 \in S_\infty$, the entries of the inverse of the matrix $(\log|\eta_j|_v)_{\substack{1 \leqq j \leqq r \\ v \in S_\infty \setminus \{v_0\}}}$ have absolute values at most c_3.*

Proof. Lemma 2 has been proved e.g. in [8] Lemma 2 and in [15] Corollaries A.4 and A.5, however with $|\overline{\eta_j}|$ and $|\overline{\eta'}|$ instead of $h(\eta_j)$, $h(\eta')$, respectively. In view of (19) we may replace $|\overline{\eta_j}|$, $|\overline{\eta'}|$ by $h(\eta_j)$ and $h(\eta')$, respectively.

Let $\eta_1, \dots, \eta_r$ be a fixed system of independent units in $\mathcal{O}_K$ with the properties specified in Lemma 2, and denote by U the multiplicative group generated by them.

Lemma 3. *Let $\alpha \in K^*$ with $|N_{K/\mathbb{Q}}(\alpha)| = M$. Then there exists an $\eta \in U$ such that*

$$c_4^{-1} M^{d_v/d^2} \leqq |\eta \alpha|_v \leqq c_5 M^{d_v/d^2} \quad \text{for every } v \in S_\infty.$$

Proof. This follows e.g. from [8], Lemma 3 or [15], Lemma A.15, together with (12).

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ be the prime ideals corresponding to the finite places in S. Each of these prime ideals has norm at most P^d. Together with Lemma 3 this proves that there are $\pi_1, \dots, \pi_t \in \mathcal{O}_K$ with

$$(\pi_j) = \mathfrak{p}_j^{h_K} \quad \text{and} \quad h(\pi_j) \leqq c_6 P^{h_K} \quad \text{for } j = 1, \dots, t. \tag{21}$$

We fix elements $\pi_1, \dots, \pi_t$ in $\mathcal{O}_K$ with property (21). The number $\alpha \in K$ is called an S-integer if $|\alpha|_v \leqq 1$ for all $v \notin S$ (i.e. $v \in M_K \setminus S$). The S-integers form a ring which is denoted by $\mathcal{O}_S$. The group of units of $\mathcal{O}_S$ is just U_S. The next lemma is a straightforward consequence of Lemmas 2 and 3.

Lemma 4. *Every $\alpha \in \mathcal{O}_S$ can be written in the form*

$$\alpha = \alpha' \eta_1^{a_1} \dots \eta_r^{a_r} \pi_1^{b_1} \dots \pi_t^{b_t} \tag{22}$$

with appropriate rational integers a_i, b_j and with $\alpha' \in \mathcal{O}_K$ such that $\pi_j \nmid \alpha'$ for $j = 1, \dots, t$ and

$$c_7^{-1} N_S(\alpha)^{d_v/d^2} \leqq |\alpha'|_v \leqq c_8 P^{d_v t h_K/d} N_S(\alpha)^{d_v/d^2} \quad \text{for } v \in S_\infty. \tag{23}$$

Remark. It is clear that in (22) $\alpha/\alpha' \in U_S$.

Proof. Let $\alpha\in\mathcal{O}_S$. Then $(\alpha)=\mathfrak{a}''\mathfrak{p}_1^{d_1}\dots\mathfrak{p}_t^{d_t}$, where $\mathfrak{a}''$ is an integral ideal relatively prime with $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ and $d_1,\dots,d_t$ are rational integers. Define rational integers $b_j, b'_j (j=1,\dots,t)$ by $d_j=h_K b_j+b'_j$ and $0\leqq b'_j<h_K$. Then the ideal $\mathfrak{b}:=\mathfrak{a}''\mathfrak{p}_1^{b'_1}\dots\mathfrak{p}_t^{b'_t}$ is principal, with norm M, say. Using the fact that $N_{K/\mathbb{Q}}(\mathfrak{a}'')=N_S(\alpha)$ and that each prime ideal $\mathfrak{p}_j$ has norm at most P^d, it follows that

$$N_S(\alpha)\leqq M\leqq P^{tdh_K}N_S(\alpha).$$

Together with Lemma 3 and Lemma 2 (ii) this shows that $\mathfrak{b}$ has a generator α' for which $\pi_j\nmid\alpha'$ for $j=1,\dots,t$ and (22) and (23) hold. □

We recall that two triples $(\alpha_1,\alpha_2,\alpha_3)$, $(\beta_1,\beta_2,\beta_3)$ in $(K^*)^3$ are called S-equivalent if there are $\lambda\in K^*$, S-units $\varepsilon_1,\varepsilon_2,\varepsilon_3$ and a permutation σ of (1, 2, 3) such that

$$\beta_i=\lambda\varepsilon_i\alpha_{\sigma(i)}\quad \text{for } i=1,2,3.$$

The next lemma shows that each S-equivalence class contains a triple with certain specified properties.

Lemma 5. *Each S-equivalence class contains a triple $(\alpha_1,\alpha_2,\alpha_3)$ with the following properties:*

(i) $\alpha_1,\alpha_2,\alpha_3\in\mathcal{O}_K\setminus\{0\}$;
(ii) $N_S(\alpha_1)\leqq N_S(\alpha_2)\leqq N_S(\alpha_3)$;
(iii) $\prod_{v\notin S}\max(|\alpha_1|_v,|\alpha_2|_v,|\alpha_3|_v)\geqq c_9^{-1}$;
(iv) $c_7^{-1}N_S(\alpha_i)^{d_v/d^2}\leqq|\alpha_i|_v\leqq c_8 P^{d_v t h_K/d}N_S(\alpha_i)^{d_v/d^2}$ *for* $i=1,2,3$ *and* $v\in S_\infty$.
(v) $P^{-h_K}<|\alpha_i|_v\leqq 1$ *for* $i=1,2,3$ *and* $v\in S\setminus S_\infty$.

We shall call such triples S-normalized.

Proof. Let $(\beta_1,\beta_2,\beta_3)\in(K^*)^3$. We shall prove that $(\beta_1,\beta_2,\beta_3)$ is S-equivalent with an S-normalized triple. We suppose that $N_S(\beta_1)\leqq N_S(\beta_2)\leqq N_S(\beta_3)$. This can be achieved by permuting β_1,β_2 and β_3. Let $\mathfrak{d}$ be the inverse of the ideal generated by β_1,β_2, and β_3. Then there exists a $\delta\in\mathfrak{d}$ with $|N_{K/\mathbb{Q}}(\delta)|\leqq|D_K|^{1/2}N_{K/\mathbb{Q}}(\mathfrak{d})$ (cf. [10], p. 119 for a sharper estimate). Put $\beta'_i=\delta\beta_i$ for $i=1,2,3$. Then $\beta'_i\in\mathcal{O}_K\setminus\{0\}$ for $i=1,2,3$, $N_S(\beta'_1)\leqq N_S(\beta'_2)\leqq N_S(\beta'_3)$ and

$$\begin{aligned}N_{K/\mathbb{Q}}((\beta'_1,\beta'_2,\beta'_3))&=N_{K/\mathbb{Q}}(\delta)\,N_{K/\mathbb{Q}}((\beta_1,\beta_2,\beta_3))\\&\leqq|D_K|^{1/2}N_{K/\mathbb{Q}}(\mathfrak{d})\,N_{K/\mathbb{Q}}((\beta_1,\beta_2,\beta_3))=|D_K|^{1/2}.\end{aligned}\tag{24}$$

Moreover, by (13),

$$\begin{aligned}N_{K/\mathbb{Q}}((\beta'_1,\beta'_2,\beta'_3))&=\Big(\prod_{v\notin S_\infty}\max(|\beta'_1|_v,|\beta'_2|_v,|\beta'_3|_v)\Big)^{-d}\\&\geqq\Big(\prod_{v\notin S}\max(|\beta'_1|_v,|\beta'_2|_v,|\beta'_3|_v)\Big)^{-d}.\end{aligned}$$

Together with (24) this implies that

$$\prod_{v \notin S} \max(|\beta'_1|_v, |\beta'_2|_v, |\beta'_3|_v) \geqq c_9^{-1}.$$

Hence the triple $(\beta'_1, \beta'_2, \beta'_3)$ satisfies (i), (ii), (iii). By Lemma 4 there are S-units $\varepsilon_1, \varepsilon_2, \varepsilon_3$ such that for $\alpha_i = \varepsilon_i \beta'_i$ we have $\alpha_i \in \mathcal{O}_K \setminus \{0\}$, $\pi_j \nmid \alpha_i$ for $i = 1, 2, 3, j = 1, \ldots, t$, and

$$c_7^{-1} N_S(\beta'_i)^{d_v/d^2} \leqq |\alpha_i|_v \leqq c_8 P^{d_v t h_K/d} N_S(\beta'_i)^{d_v/d^2} \text{ for } v \in S_\infty. \tag{25}$$

Thus (i) holds. (v) follows from $\pi_j \nmid \alpha_i$ and (i), while (25) and $N_S(\beta'_i) = N_S(\alpha_i)$ for $i = 1, 2, 3$ imply (iv). Since $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are S-units, $\alpha_1, \alpha_2, \alpha_3$ also satisfy (ii) and (iii). □

The main tools in the proofs of Theorems 2 and 3 are lower bounds for linear forms in logarithms, both in the archimedean and the p-adic case.

Lemma 6. *Let $v \in S$. Let $\gamma_1, \ldots, \gamma_k \in K^*$ with $h(\gamma_i) \leqq A_i$ $(3 \leqq A_1 \leqq \ldots \leqq A_k)$ for $i = 1, \ldots, k$ and let $b_1, \ldots, b_k$ be rational integers with $\max_i |b_i| \leqq B (B \geqq 3)$. Put*

$$\Lambda = \gamma_1^{b_1} \ldots \gamma_k^{b_k} - 1, \qquad \Omega = \prod_{i=1}^{k} \log A_i, \qquad \Omega' = \prod_{i=1}^{k-1} \log A_i.$$

Then either $\Lambda = 0$ or

$$|\Lambda|_v \geqq \exp\{-(c_{10} k)^{c_{11} k} \Omega \log \Omega' \log B\} \qquad \text{if } v \text{ is infinite}$$

and

$$|\Lambda|_v \geqq \exp\{-(c_{12} k)^{c_{13} k} P^d (\log P) \Omega (\log B)^2\} \qquad \text{if } v \text{ is finite.}$$

Proof. This follows easily from results of Baker [1] (in case that v is infinite) and van der Poorten [13] (in case that v is finite), by taking (20) into consideration. □

The next lemma gives an effective upper bound for the heights of the solutions of the S-unit Equation (1). It is an easy consequence of a result of Győry [7].

Lemma 7. *Let $\alpha_1, \alpha_2, \alpha_3$ be non-zero elements of $\mathcal{O}_K$ with $\max_i h(\alpha_i) \leqq A (A \geqq 3)$ and let $x, y \in U_S$ such that*

$$\alpha_1 x + \alpha_2 y = \alpha_3.$$

Then $\max(h(x), h(y)) \leqq \exp\{(c_{14} s)^{c_{15} s} P^{d+1/2} \log A\}$.

Proof. Let x_3 be an S-unit such that $x x_3$, $y x_3$ and x_3 are all algebraic integers and put $x_1 = x x_3$ and $x_2 = y x_3$. Then $\alpha_1 x_1 + \alpha_2 x_2 = \alpha_3 x_3$. By a result of Győry [7] there are $\kappa \in U_S \cap \mathcal{O}_K$ and $\rho_1, \rho_2, \rho_3 \in \mathcal{O}_K$ such that

$$x_i = \kappa \rho_i \qquad \text{for } i = 1, 2, 3,$$

and

$$\max_i |\overline{\rho_i}| \leqq \exp\{(c_{16}s)^{c_{17}s} P^d (\log P)^{t+5} \log A'\},$$

where $A' = \max(3, |\overline{\alpha_1}|, |\overline{\alpha_2}|, |\overline{\alpha_3}|)$. We may now deduce Lemma 7 from this result by employing (19), the inequalities

$$h(x) = h\left(\frac{x_1}{x_3}\right) = h\left(\frac{\rho_1}{\rho_3}\right) \leqq h(\rho_1)\, h(\rho_3),$$

and

$$h(y) = h\left(\frac{x_2}{x_3}\right) = h\left(\frac{\rho_2}{\rho_3}\right) \leqq h(\rho_2)\, h(\rho_3),$$

which hold in view of (18), and the estimate $(\log P)^{t+5} \leqq P^{1/2}(c_{18}s)^{c_{19}s}$ which applies for appropriate constants c_{18} and c_{19}. □

§ 4. Proofs of Theorems 2 and 3

We shall use the same notation as in the previous sections. In particular, $c_{20}, c_{21}, \ldots$ are explicitly computable numbers, depending on d and $|D_K|$ only.

Proof of Theorem 2. Let $(\beta_1, \beta_2, \beta_3) \in (K^*)^3$ be an S-normalized triple for which the equation $\beta_1 x + \beta_2 y = \beta_3$ in S-units x, y has at least $s+2$ solutions. Put $m = \max(h(\beta_1), h(\beta_2), h(\beta_3))$. We shall prove that

$$m \leqq \exp\{(c_{20}s)^{c_{21}s} P^{d+1}\}. \tag{26}$$

This proves Theorem 2, since by Lemma 5, each triple in $(K^*)^3$ is S-equivalent to an S-normalized triple.

Put $\beta'_1 = \beta_1/\beta_3$, $\beta'_2 = \beta_2/\beta_3$. By assumption, the equation

$$\beta'_1 x + \beta'_2 y = 1 \quad \text{in} \quad x, y \in U_S$$

has $s+2$ different solutions $(x_0, y_0), (x_1, y_1), \ldots, (x_{s+1}, y_{s+1})$, say, ordered such that

$$\prod_{v \in S} \max(1, |\beta'_1 x_0|_v) \leqq \prod_{v \in S} \max(1, |\beta'_1 x_1|_v) \leqq \ldots \leqq$$
$$\leqq \prod_{v \in S} \max(1, |\beta'_1 x_{s+1}|_v). \tag{27}$$

First we show that for $i = 1, \ldots, s+1$, there is a place $w(i)$ in S with

$$|\beta'_1 x_i|_{w(i)} \leqq P^{c_{22}/s} m^{-1/(c_{23}s^2)}. \tag{28}$$

This estimate will play a key role in our proof. To prove (28) we distinguish two cases: (a) $N_S(\beta'_1) \leqq m^{-d/4}$ and (b) $N_S(\beta'_1) > m^{-d/4}$.

We note that the case (a) can essentially be found in Győry [7]. The new aspect of Theorem 2 and its proof is that we can now prove (28), hence the theorem, in case (b). Further, we shall obtain a slight improvement of Győry [7] in case (a) by treating infinite and finite places uniformly.

Suppose first that $N_S(\beta'_1)\leqq m^{-d/4}$. Then, by the fact that x_i is an S-unit for $i=1,\dots,s+1$, and by (16), (15), we have $\prod_{v\in S}|\beta'_1 x_i|_v\leqq m^{-1/4}$ for $i=1,\dots,s+1$. But this implies at once that for each i in $\{1,\dots,s+1\}$ there is a $w(i)\in S$ with $|\beta'_1 x_i|_{w(i)}\leqq m^{-1/(4s)}$.

Now suppose that $N_S(\beta'_1)>m^{-d/4}$. Then also $N_S(\beta'_2)>m^{-d/4}$, by Lemma 5 (ii). Let $i\geqq 1$ and take $v\in M_K\backslash S$. By $\beta'_1 x_j+\beta'_2 y_j=1$ for $j=0, 1,\dots,s+1$, we have

$$|\beta'_1(x_i-x_0)|_v=|\beta'_2(y_0-y_i)|_v,$$

whence

$$|\beta'_1(x_i-x_0)|_v\leqq\min(|\beta'_1|_v,|\beta'_2|_v)\qquad\text{for } v\in M_K\backslash S.$$

Together with the product formula (14) this implies that

$$\prod_{v\in S}|\beta'_1(x_i-x_0)|_v\geqq A, \tag{29}$$

where

$$A=\{\prod_{v\notin S}\min(|\beta'_1|_v,|\beta'_2|_v)\}^{-1}.$$

By applying the product formula and (15) we obtain

$$\begin{aligned}A&=(\prod_{v\notin S}|\beta'_1\beta'_2|_v)^{-1}\prod_{v\notin S}\max(|\beta'_1|_v,|\beta'_2|_v)\\&=N_S(\beta'_1\beta'_2)^{1/d}\prod_{v\notin S}\max\left(\left|\frac{\beta_1}{\beta_3}\right|_v,\left|\frac{\beta_2}{\beta_3}\right|_v\right).\end{aligned}$$

Another application of the product formula yields that

$$A=N_S(\beta'_1\beta'_2)^{1/d}N_S(\beta_3)^{1/d}\prod_{v\notin S}\max(|\beta_1|_v,|\beta_2|_v). \tag{30}$$

In view of $\beta_1 x_0+\beta_2 y_0=\beta_3$ we have $|\beta_3|_v\leqq\max(|\beta_1|_v,|\beta_2|_v)$ for $v\in M_K\backslash S$. Hence by Lemma 5 (iii),

$$\prod_{v\notin S}\max(|\beta_1|_v,|\beta_2|_v)=\prod_{v\notin S}\max(|\beta_1|_v,|\beta_2|_v,|\beta_3|_v)\geqq c_9^{-1}. \tag{31}$$

By Lemma 5 (iv), (v) and the fact that $P\geqq 2$ and $N_S(\beta_i)\geqq 1$ for $i=1, 2, 3$ we have

$$|\beta_i|_v\geqq P^{-c_{24}}\max(1,|\beta_i|_v)\qquad\text{for } i=1,2,3\quad\text{and}\quad v\in S.$$

Therefore, by (15) and Lemma 5 (ii), we have, for $i=1, 2, 3$,

$$N_S(\beta_3)\geqq N_S(\beta_i)\geqq P^{-c_{24}ds}\{\prod_{v\in S}\max(1,|\beta_i|_v)\}^d=P^{-c_{24}ds}\{h(\beta_i)\}^d.$$

Hence

$$N_S(\beta_3)\geqq P^{-c_{24}ds}m^d.$$

Together with (15), (30) and (31) and $N_S(\beta_2')\geqq N_S(\beta_1')\geqq m^{-d/4}$ this yields

$$A\geqq P^{-c_{25}s}m^{1/2}.$$

By combining this with (29) we obtain

$$\prod_{v\in S}|\beta_1'(x_i-x_0)|_v\geqq P^{-c_{25}s}m^{1/2} \quad \text{for } i=1,\dots,s+1. \tag{32}$$

Using

$$|\beta_1'(x_i-x_0)|_v\leqq 2\max(1,|\beta_1' x_0|_v)\max(1,|\beta_1' x_i|_v) \quad \text{for } v\in S,$$

we obtain, in view of (27),

$$\prod_{v\in S}|\beta_1'(x_i-x_0)|_v\leqq 2^s\{\prod_{v\in S}\max(1,|\beta_1' x_0|_v)\}\{\prod_{v\in S}\max(1,|\beta_1' x_i|_v)\}$$
$$\leqq 2^s\{\prod_{v\in S}\max(1,|\beta_1' x_i|_v)\}^2.$$

Together with (32) this yields

$$\prod_{v\in S}\max(1,|\beta_1' x_i|_v)\geqq P^{-c_{26}s}m^{1/4}. \tag{33}$$

We may assume that

$$m>P^{4c_{26}s}, \tag{34}$$

since otherwise (26) holds for appropriate c_{20}, c_{21}. Now (33) implies that there is a $v(i)\in S$ with

$$|\beta_1' x_i|_{v(i)}\geqq P^{-c_{26}}m^{1/(4s)}.$$

Further, since $\prod_{v\in S}|\beta_1' x_i|_v\geqq 1$, there is a $w(i)\in S$ with

$$|\beta_1' x_i|_{w(i)}\leqq P^{c_{26}/s}m^{-1/(4s^2)}.$$

This implies (28) for sufficiently large c_{22}.

By using (28) we now prove that for appropriate i, j $(i\neq j)$ and w, $|1-y_i/y_j|_w$ is quite small in terms of m. Then, a standard application of Baker's inequality and its p-adic analogue will yield a lower bound for $|1-y_i/y_j|_w$ in terms of m which immediately provides inequality (26).

By the box principle, there are distinct i,j in $\{1,\dots,s+1\}$ with $w(i)=w(j)=w$, say. Hence

$$|\beta_1' x_i|_w\leqq P^{c_{22}/s}m^{-1/(c_{23}s^2)}, \quad |\beta_1' x_j|_w\leqq P^{c_{22}/s}m^{-1/(c_{23}s^2)}. \tag{35}$$

While proving (26) we assume that

$$m\geqq(4^{s^2}P^{c_{22}s})^{2c_{23}} \tag{36}$$

which is obviously no restriction. Then $|\beta'_1 x_i|_w \leqq \frac{1}{2}$ and $|\beta'_1 x_j|_w \leqq \frac{1}{2}$. Together with (35) and $\beta'_1 x_i + \beta'_2 y_i = \beta'_1 x_j + \beta'_2 y_j = 1$ this shows that

$$|\beta'_2 y_j|_w \geqq \tfrac{1}{2}, \quad |\beta'_2(y_i - y_j)|_w = |\beta'_1(x_j - x_i)|_w \leqq 2P^{c_{22}/s} m^{-1/(c_{23}s^2)}.$$

By combining this with (36) we obtain

$$\left|1 - \frac{y_i}{y_j}\right|_w = \frac{|\beta'_2(y_i - y_j)|_w}{|\beta'_2 y_j|_w} \leqq m^{-1/(2c_{23}s^2)} \leqq m^{-1/(c_{27}s^2)}. \tag{37}$$

Further, $y_i/y_j \neq 1$, since (x_i, y_i) and (x_j, y_j) are distinct solutions. By Lemma 4 and $y_i/y_j \in U_S$, there are rational integers $a_1, \ldots, a_r, b_1, \ldots, b_t$ such that

$$\frac{y_i}{y_j} = z \prod_{k=1}^{r} \eta_k^{a_k} \prod_{l=1}^{t} \pi_l^{b_l}, \tag{38}$$

where $\eta_1, \ldots, \eta_t$ satisfy the conditions of Lemma 2, $\pi_1, \ldots, \pi_t$ satisfy the conditions of (21) and

$$z \in \mathcal{O}_K, \quad h(z) \leqq c_{28} P^{c_{29}s}. \tag{39}$$

By combining this with Lemma 6, (38), Lemma 2 (i) and (21) we obtain

$$\left|1 - \frac{y_i}{y_j}\right|_w \geqq \exp\{-(c_{30}s)^{c_{31}s} P^{d+1/4} (\log 2B)^2\}, \tag{40}$$

where $B = \max(3, |a_1|, \ldots, |a_r|, |b_1|, \ldots, b_t|)$.

We shall now estimate B from above. By (18) and Lemma 7 we have

$$h\left(\frac{y_i}{y_j}\right) \leqq h(y_i)\, h(y_j) \leqq \exp\{(c_{32}s)^{c_{33}s} P^{d+1/2} \log(4m)\}. \tag{41}$$

For $l = 1, \ldots, t$, let v_l be the finite place in S for which $|\pi_l|_{v_l} < 1$. By (38), the product formula, (17) and (18) we have

$$\begin{aligned} 2^{|b_l|/d} &\leqq \max(|\pi_l^{b_l}|_{v_l}, |\pi_l^{-b_l}|_{v_l}) = \max\left(\left|\frac{y_i}{y_j} z^{-1}\right|_{v_l}, \left|\frac{y_i}{y_j} z^{-1}\right|_{v_l}^{-1}\right) \\ &= \max\left(\prod_{v \neq v_l} \left|\frac{y_j}{y_i} z\right|_v, \left|\frac{y_j}{y_i} z\right|_{v_l}\right) \\ &\leqq \prod_{v \in M_K} \max\left(1, \left|\frac{y_j}{y_i} z\right|_v\right) = h\left(\frac{y_j}{y_i} z\right) \leqq h\left(\frac{y_j}{y_i}\right) h(z), \end{aligned}$$

for $l = 1, \ldots, t$. Put $B' = \max_{1 \leqq l \leqq t} |b_l|$. Together with (39) and (41) this yields

$$B' \leqq (c_{34}s)^{c_{35}s} P^{d+3/4} \log(4m). \tag{42}$$

Note that, by (38) and (18),

$$h(\eta_1^{a_1}\dots\eta_r^{a_r})=h\left(\frac{y_i}{y_j}z^{-1}\prod_{l=1}^{t}\pi_l^{-b_l}\right)$$
$$\leqq h\left(\frac{y_i}{y_j}\right)h(z)\left(\prod_{l=1}^{t}h(\pi_l)\right)^{B'}.$$

Together with (41), (39), (21) and (42) this implies

$$h(\eta_1^{a_1}\dots\eta_r^{a_r})\leqq\exp\{(c_{36}s)^{c_{37}s}P^{d+1}\log(4m)\}.$$

By (17) and (18) we have $h(\alpha)\geqq|\alpha|_v$, $h(\alpha)\geqq|\alpha|_v^{-1}$ for $\alpha\in\mathcal{O}_K\backslash\{0\}$, $v\in M_K$. Hence

$$\left|\sum_{i=1}^{r}a_i\log|\eta_i|_v\right|\leqq(c_{36}s)^{c_{37}s}P^{d+1}\log(4m)\qquad\text{for } v\in S_\infty.$$

Together with Lemma 2 (iii) this yields

$$\max_{1\leqq k\leqq r}|a_k|\leqq(c_{38}s)^{c_{39}s}P^{d+1}\log(4m).$$

By combining this with (42) we obtain

$$2B\leqq(c_{40}s)^{c_{41}s}P^{d+1}\log(4m).$$

A substitution of this into (40) yields that

$$\left|1-\frac{y_i}{y_j}\right|_w\geqq\exp\{-(c_{42}s)^{c_{43}s}P^{d+1/2}\{\log\log(4m)\}^2\}.$$

By comparing this with (37) we obtain

$$\frac{\log(4m)}{\{\log\log(4m)\}^2}\leqq(c_{44}s)^{c_{45}s}P^{d+1/2}.$$

It is easy to check that this implies (26). □

Proof of Theorem 3. Let $(\beta_1,\beta_2,\beta_3)\in(K^*)^3$ and suppose that the equation $\beta_1x'+\beta_2y'=\beta_3$ in x', $y'\in U_S$ has at least $s+2$ solutions. Then there exists, by Theorem 2, a triple $(\alpha_1,\alpha_2,\alpha_3)\in(\mathcal{O}_K\backslash\{0\})^3$, S-equivalent to $(\beta_1,\beta_2,\beta_3)$ such that

$$\log\{\max(h(\alpha_1),h(\alpha_2),h(\alpha_3))\}\leqq(C_1s)^{C_2s}P^{d+1}$$

with the C_1 and C_2 specified in Theorem 2. By combining this with Lemma 7, we obtain that each pair of S-units (x,y) with $\alpha_1x+\alpha_2y=\alpha_3$ satisfies

$$\max(h(x),h(y))\leqq\exp\{(C_3s)^{C_4s}P^{2d+2}\},$$

where C_3 and C_4 are effectively computable positive numbers depending only on d and $|D_K|$.

§ 5. An example of an S-unit equation in more than two variables with many solutions

At the end of the Introduction we mentioned that for the case of unit equations in $n>2$ variables there do not exist such small upper bounds for the numbers of solutions as those of Theorems 1 and 2 for the case $n=2$. In this section we shall prove this claim by showing that for $K=\mathbb{Q}$ and for any sufficiently large integer s there is a set S of cardinality s and infinitely many pairwise S-inequivalent $n+1$-tuples $(\alpha_1, \ldots, \alpha_{n+1}) \in (\mathbb{Q}^*)^{n+1}$ for which (7) has at least $\exp((4+o(1))\,(s/\log s)^{1/2})$ non-degenerate solutions as $s \to \infty$.

To see this, observe that, by Theorem 3 of [2], for s sufficiently large there is a set W of $s-1$ prime numbers, and a positive integer c such that the equation $x_1 - x_2 = c$ has at least $\exp((4+o(1))\,(s/\log s)^{1/2})$ solutions in positive integers x_1 and x_2 all of whose prime factors are from W. Let S consist of the infinite place together with those places associated with a prime number from W. Next let $q_1, q_2 \ldots$ be a sequence of prime numbers such that q_1 is larger than all of the prime numbers in W and also larger than $c+n-3$ and such that

$$q_{i+1} > q_i + c + n - 3 \qquad \text{for } i = 1, 2, \ldots.$$

Then, for $j = 1, 2, \ldots,$ the S-unit equation

$$x_1 - x_2 + q_j x_3 + x_4 + \ldots + x_n = c + q_j + n - 3$$

has at least $\exp((4+o(1))\,(s/\log s)^{1/2})$ solutions in S-units, since we may take $x_3 = \ldots = x_n = 1$ and choose x_1 and x_2 so that $x_1 - x_2 = c$. Among them at most $2n$ solutions are degenerate, since in any vanishing subsum x_1 does not occur, $-x_2$ has to occur and the number of possible values for x_2 in a vanishing subsum is at most $2n$. Observe by (2) that if $(\alpha_1, \ldots, \alpha_{n+1})$ and $(\beta_1, \ldots, \beta_{n+1})$ are S-equivalent $n+1$-tuples then there is a permutation σ of $\{1, \ldots, n+1\}$ such that for all pairs (i,j) with $1 \leqq i \leqq n$, $1 \leqq j \leqq n$ we have

$$\frac{\beta_i}{\beta_j} = \varepsilon_{i,j} \frac{\alpha_{\sigma(i)}}{\alpha_{\sigma(j)}}$$

with $\varepsilon_{i,j}$ an S-unit. Let $k > l \geqq 1$. If the $n+1$-tuples $(\beta_1, \ldots, \beta_{n+1}) = (1, -1, q_k, 1, \ldots, 1, c+q_k+n-3)$ and $(\alpha_1, \ldots, \alpha_{n+1}) = (1, -1, q_l, 1, \ldots, 1, c+q_l+n-3)$ are S-equivalent then

$$q_k = \varepsilon \frac{\alpha_{\sigma(3)}}{\alpha_{\sigma(j)}} \beta_j \tag{43}$$

where ε is an S-unit, $\beta_j \in \{1, -1, c+q_k+n-3\}$ and $\alpha_{\sigma(3)}, \alpha_{\sigma(j)}$ are from $\{1, -1, q_l, c+q_l+n-3\}$. But by construction the q_k-adic value of the right-hand side of (43) is 1 which is a contradiction. Thus $(1, -1, q_k, 1, \ldots, 1, c+q_k+n-3)$ and $(1, -1, q_l, 1, \ldots, 1, c+q_l+n-3)$ are S-inequivalent for $k \neq l$.

Acknowledgement. We thank the referee for his suggestions and comments.

References

1. Baker, A.: The theory of linear forms in logarithms. Transcendence theory: advances and applications, pp. 1–27. London: Academic Press 1977
2. Erdös, P., Stewart, C.L., Tijdeman, R.: Some diophantine equations with many solutions. Compos. Math. to appear
3. Evertse, J.-H.: On equations in S-units and the Thue-Mahler equation. Invent Math. **75**, 561–584 (1984)
4. Evertse, J.-H.: On sums of S-units and linear recurrences. Compos. Math. **53**, 225–244 (1984)
5. Evertse, J.-H., Györy, K.: On the numbers of solutions of weighted unit equations. Compos. Math. (to appear)
6. Evertse, J.-H., Györy, K., Stewart, C.L., Tijdeman, R.: S-unit equations and their applications. New advances in transcendence theory. Cambridge University Press (to appear)
7. Györy, K.: On the number of solutions of linear equations in units of an algebraic number field. Comment. Math. Helv. **54**, 583–600 (1979)
8. Györy, K.: On the solutions of linear diophantine equations in algebraic integers of bounded norm. Ann. Univ. Budapest Eötvös, Sect. Math. **22–23**, 225–233 (1979–80)
9. Lang, S.: Integral points on curves. Publ. Math. Inst. Hautes Etudes Sci. **6**, 27–43 (1960)
10. Lang, S.: Algebraic number theory. Reading, Mass: Addison-Wesley 1970
11. Lang, S.: Fundamentals of diophantine geometry. New York: Springer 1983
12. Laurent, M.: Equations diophantiennes exponentielles. Invent. Math. **78**, 299–327 (1984)
13. Poorten, A.J., van der: Linear forms in logarithms in the p-adic case. Transcendence theory: advances and applications, pp. 29–57. London: Academic Press 1977
14. Poorten, A.J., van der, Schlickewei, H.P.: The growth conditions for recurrence sequences. Macquarie Univ. Math. Rep. 82-0041, North. Ryde, Australia, 1982
15. Shorey, T.N., Tijdeman, R.: Exponential diophantine equations. Cambridge University Press 1986
16. Siegel, C.L.: Abschätzung von Einheiten. Nachr. Akad. Wiss. Gött., II, Math.-Phys. Kl 71–86, 1969
17. Zimmert, R.: Ideale kleiner Norm in Idealklassen und eine Regulatorabschätzung. Invent. Math. **62**, 367–380 (1981)

Oblatum 12-V-1987 & 3-XII-1987