Mathematica Pannonica
1/2 (1990), 25 – 43

ON SOME ARITHMETICAL PROPERTIES OF WEIGHTED SUMS OF S-UNITS

K. Győry*

Mathematical Institute, Kossuth Lajos University, H-4010 Debrecen 10, Hungary.

M. Mignotte

Institut de Mathématique, Université Louis Pasteur, F-67084 Strasbourg, France.

T.N. Shorey

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400 005, India.

Received February 1990

AMS Subject Classification: 11 D 57, 11 D 61, 11 D 85, 11 D 72

Keywords: Diophantine equations, sums of S-units, recursive sequences.

Abstract: We prove some new arithmetical properties of sums of the form $\alpha_0 x_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n$ where $\alpha_0, \alpha_1, \cdots, \alpha_n$ are non-zero S-integers and $x_0, x_1, \cdots, x_n$ are S-units in a given algebraic number field K. By using a result of Evertse and Győry [6] on weighted S-unit equations, we derive in §1 a general but ineffective result. In §2, we obtain some effective results for $n = 1$ by means of Baker's method and its p-adic analogue. As

* Supported in part by Grant 273 from the Hungarian National Foundation of Scientific Research.

a consequence, we get some information about the arithmetical properties of the solutions of certain decomposable form equations as well as of the terms of recursive sequences.

1. Ineffective results

Let K be an algebraic number field of degree d with ring of integers $\mathcal{O}_K$ and 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-archimedian valuations, and infinite otherwise. Let S be a finite subset of M_K containing all infinite places. A number $\alpha \in K$ is called an S-integer (resp. an S-unit) if $|\alpha|_v \leq 1$ (resp. $|\alpha|_v = 1$) for every valuation $|\ |_v$ from a place $v \in M_K \setminus S$. The S-integers form a ring which is called the ring of S-integers and is denoted by $\mathcal{O}_S$. The S-units form a multiplicative group which is denoted by $\mathcal{O}_S^*$. For each $\beta \in \mathcal{O}_S \setminus \{0\}$, we write

$$N_S(\beta) = \prod_{v \in S} |\beta|_v$$

which is a positive rational integer called the S-norm of β. If in particular S consists exactly of the infinite places then $N_S(\beta) = |N_{K/Q}(\beta)|$.

Let $n \geq 1$ be an integer. Denote by $\mathbb{P}^n(K)$ the n-dimensional projective space over K, that is the set of all $(n+1)$-tuples $(x_0, x_1, \cdots, x_n)$ with $x_i \in K$, where two tuples are identical if they differ by a non-zero scalar multiple. Further, we denote by $\mathbb{P}^n(\mathcal{O}_S^*)$ the set of $(x_0, x_1, \cdots, x_n)$ with $x_i \in \mathcal{O}_S{}^*$. For given $\underline{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_n) \in (\mathcal{O}_S \setminus \setminus\{0\})^{n+1}$, we consider those $\beta \in \mathcal{O}_S$ which can be represented in the form

$$(1) \qquad \beta = \alpha_0 x_0 + \alpha_1 x_1 + \cdots + \alpha_n x_n \quad \text{with} \quad x_0, x_1, \cdots, x_n \in \mathcal{O}_S^*.$$

Van der Poorten and Schlickewei [8] and Evertse [5], independently, proved that for given non-zero $\beta \in \mathcal{O}_S$, the equation (1) has at most finitely many solutions such that

$$(2) \qquad \sum_{j=1}^{r} \alpha_{i_j} x_{i_j} \neq 0 \text{ for each subset } \{i_1, \cdots, i_r\} \text{ of } \{0, 1, \cdots, n\}.$$

Later, Evertse and Győry [6] proved that there is a constant C depending only on K, S and n but not on $\underline{\alpha}$ such that the number of solutions of (1) having property (2) is at most C. The proofs of these results of [8], [5] and [6] involve the p-adic analogue of the Thue-Siegel-Roth-Schmidt method. Very recently, Everest [2], [3] gave an asymptotic formula for the number of $\underline{x} = (x_0, x_1, \cdots, x_n) \in \mathbb{P}^n(\mathcal{O}_S^*)$ with $N_S(\alpha_0 x_0 + \cdots + \alpha_n x_n) \leq q$ and (2) as $q \to \infty$. Tijdeman and Wang [15] applied the above result of Evertse and Győry [6] to simultaneous weighted sums of elements of finitely generated mulitplicative groups. As another application, we shall deduce the following theorem.

For a rational integer ν with $|\nu| > 1$, we denote by $P(\nu)$ the greatest prime factor of ν and we write $P(0) = P(\pm 1) = 1$. In what follows in **1**, $C_1(\ )$, $C_2(\ ), \cdots$ will denote positive numbers depending only on parameters occuring between parantheses.

Theorem 1. *Let $P > 1$ be an integer. The number of values $N_S(\beta)$ with $\beta \in \mathcal{O}_S$ and $P(N_S(\beta)) \leq P$ for which* (1) *holds is at most $C_1(K, S, P, n)$.*

It is a remarkable fact that C_1 does not depend on the coefficients $\alpha_0, \alpha_1, \cdots, \alpha_n$ in (1). We remark that in general we are not able to make C_1 explicit. This is due to the non-explicit character of the number $C = C(K, S, n)$ mentioned above. Further, we note that in Theorem 1 all β are taken into account which are represented in the form (1) (independently of the fact that (2) holds or not).

It follows from the above mentioned results of [8] or [5] that the set of values $N_S(\beta)$ with $\beta \in \mathcal{O}_S$ and (1) is not bounded. Theorem 1 implies immediately the following result.

Corollary 1. *$P(N_S(\beta)) \to \infty$ as $N_S(\beta) \to \infty$ with $\beta \in \mathcal{O}_S$ and* (1).

For $n = 1$, we shall give in **2** effective and quantitive versions of this assertion. We note that Corollary 1 can also be deduced from the results of [8] or [5]. We shall now give a consequence of Corollary 1 to decomposable form equations. Let

$$F(\underline{X}) = F(X_1, \cdots, X_m) \in \mathcal{O}_S[X_1, \cdots, X_m]$$

be a decomposable form in $m \geq 2$ variables which factorises into linear forms, say $l_1(\underline{X}), \cdots, l_n(\underline{X})$ over K. For a non-zero element b of $\mathcal{O}_S$, we consider the decomposable form equation

$$F(\underline{x}) = F(x_1, \cdots, x_m) = b \text{ in } x_1, \cdots, x_m \in \mathcal{O}_S. \tag{3}$$

Corollary 2. *Suppose that for some i with $1 \leq i \leq m, X_i$ can be expressed as a linear combination of $l_1(\underline{X}), \cdots, l_n(\underline{X})$. If (3) has infinitely many solutions and if $N_S(x_i)$ is unbounded for the solutions $\underline{x} = (x_1, \cdots, x_m)$ of (3) then, for these solutions, $P(N_S(x_i))$ is also unbounded.*

Important examples to which Corollary 2 can be applied are the full norm form equations, i.e. equations of the form

$$F(\underline{x}) = N(x_1 + \omega_2 x_2 + \cdots + \omega_n x_n) = b \text{ in } x_1, \cdots, x_n \in \mathbb{Z}$$

where $\{1, \omega_2, \cdots, \omega_n\}$ is a basis of $\mathbb{Q}(\omega_2, \cdots, \omega_n)$ over $\mathbb{Q}$. In this case, every X_i can be expressed as a linear combination of the linear factors of F, and if the equation is solvable and $n \geq 3$ or $n = 2$ and $\mathbb{Q}(\omega_2)$ is real, then it has infinitely many solutions $\underline{x} = (x_1, \cdots, x_n)$. Then $\max_i |x_i|$ is obviously unbounded. Moreover, it follows from a recent result of Everest [4] that, for these solutions, $|x_i|$ is unbounded for each i, and hence Corollary 2 implies that $P(x_i)$ is not bounded. For effective and quantitive versions of this assertion with $m = 2$, $n = 2$, see Corollary 4.

We shall now prove Theorem 1. As was mentioned above, the proof will be based on the following result on weighted unit equations. Let $\alpha'_0, \cdots, \alpha'_n \in K \setminus \{0\}$. A solution of the S-unit equation

$$\alpha'_0 x_0 + \cdots + \alpha'_n x_n = 1 \text{ in } x_0, x_1, \cdots, x_n \in \mathcal{O}_S^* \tag{4}$$

is called degenerate if $\alpha'_0 x_0 + \cdots + \alpha'_n x_n$ has a vanishing subsum, and non-degenerate otherwise. Now, we state the following theorem of Evertse and Győry [6].

Lemma 1. *The number of non-degenerate solutions of* (4) *is at most* $C_2(K, S, n)$.

As was mentioned above, the number C_2 cannot be made explicit by means of the method of proof used in [6]. At the last conference on Diophantine approximations in Oberwolfach (March 14-18, 1988), H.P. Schlickewei announced that in the special case when $K = \mathbb{Q}$ and S is generated by s distinct prime numbers, he is able to make explicit

$$C_2(\mathbb{Q}, S, n) = (8(s+1))^{2^{26n+4}(s+1)^6}.$$

Using this explicit value of C_2, in this special case we can make C_1 explicit in Theorem 1.

Proof of Theorem 1. It is enough to deal with the case $\beta \neq 0$. If $\beta \in \mathcal{O}_S \setminus \{0\}$ is represented in the form (1), then it is also represented by a non-empty subsum of $\alpha_0 x_0 + \cdots + \alpha_n x_n$ which has no non-empty vanishing subsum. Since $\alpha_0 x_0 + \cdots + \alpha_n x_n$ has at most 2^{n+1} subsums, it will be sufficient to prove the assertion for those β for which (1) holds and $\alpha_0 x_0 + \cdots + \alpha_n x_n$ has no vanishing subsum.

Let S' be the smallest subset of M_K with $S' \supseteq S$ such that all elements $\beta \in \mathcal{O}_S \setminus \{0\}$ with $P(N_S(\beta)) \leq P$ belong to $\mathcal{O}_{S'}^*$. It is easy to see that S' is finite and depends only on K, S and P. If $\beta \in \mathcal{O}_S \setminus \{0\}$ with $P(N_S(\beta)) \leq P$ is represented in the form (1), then we have

$$1 = \alpha_0(x_0/\beta) + \cdots + \alpha_n(x_n/\beta) \quad \text{where} \quad x_i/\beta \in \mathcal{O}_{S'}^*.$$

Hence, it follows from Lemma 1 that there exists a subset U_0 of $(\mathcal{O}_{S'}^*)^{n+1}$ of cardinality at most $C_3(K, S', n) \leq C_4(K, S, P, n)$ with the following property: If $\beta \in \mathcal{O}_S \setminus \{0\}$ with $P(N_S(\beta)) \leq P$ such that

$$\beta = \alpha_0 x_0 + \cdots + \alpha_n x_n \text{ and } \alpha_0 x_0 + \cdots + \alpha_n x_n \text{ has no vanishing subsum,} \tag{5}$$

then $(x_0, \cdots, x_n) = \eta(x_0^0, \cdots, x_n^0)$ for some $\eta \in \mathcal{O}_{S'}^*$, and $(x_0^0, \cdots, x_n^0) \in U_0$. Fix such a tuple $(x_0^0, \cdots, x_n^0) \in U_0$ and suppose that $\beta' \in \mathcal{O}_S \setminus \{0\}$ with $P(N_S(\beta')) \leq P$ is another element such that

$$\begin{cases} \beta' = \alpha_0 x_0' + \cdots + \alpha_n x_n' \text{ holds, } \alpha_0 x_0' + \cdots + \alpha_n x_n' \\ \qquad \text{has no vanishing subsum and } (x_0', \cdots, x_n') = \\ \qquad = \eta'(x_0^0, \cdots, x_n^0) \text{ with some } \eta' \in \mathcal{O}_{S'}^*. \end{cases} \tag{6}$$

Then, it follows that $(x_0', \cdots, x_n') = \eta'/\eta(x_0, \cdots, x_n)$ and hence we have $\eta'/\eta \in \mathcal{O}_S^*$. But this, together with (5) and (6), implies that $\beta' = (\eta'/\eta)\beta$ and so $N_S(\beta') = N_S(\beta)$. Consequently, the number of values $N_S(\beta)$ with $\beta \in \mathcal{O}_S \setminus \{0\}$ for which (1), (2) and $P(N_S(\beta)) \leq P$ hold does not exceed the cardinality of U_0 which is bounded above by $C_4(K, S, P, n)$. $\diamondsuit$

Proof of Corollary 2. Suppose that

$$X_i = c_{i_1} l_{i_1}(\underline{X}) + \cdots + c_{i_k} l_{i_k}(\underline{X}) \tag{7}$$

for some distinct $i_i, \cdots, i_k$ and $c_{i_1}, \cdots, c_{i_k} \in K \setminus \{0\}$. By assumption, (3) has infinitely many solutions $\underline{x} = (x_1, \cdots, x_m)$ and $N_S(x_i)$ is unbounded for these solutions. Then it follows from (3) that, for these solutions, $l_{i_j}(\underline{x})$ can assume only finitely many values apart from a factor from $\mathcal{O}_S^*$, $j = 1, \cdots, k$. Consequently, there is a subset χ of solutions $\underline{x} = (x_1, \cdots, x_m)$ of (3) with unbounded $N_S(x_i)$ such that, for each of these solutions, $l_{i_j}(\underline{x}) = \delta_{i_j} u_{i_j}$ with some fixed $\delta_{i_j} \in K \setminus \{0\}$ and with $u_{ij} \in \mathcal{O}_S^*, j = 1, \cdots, k$. There is a $t \in \mathrm{N}$ for which $\alpha_{i_j} := t c_{i_j} \delta_{i_j} \in \mathcal{O}_S \setminus \{0\}$ for $j = 1, \cdots, k$. Now (7) implies that

$$t x_i = \alpha_{i_1} u_{i_1} + \cdots + \alpha_{i_k} u_{i_k}. \tag{8}$$

For $k = 1$, this gives

$$N_S(x_i) N_S(t) = N_S(t x_i) = N_S(\alpha_{i_1})$$

which implies that $N_S(x_i)$ is bounded. For $k \geq 2$, Corollary 1 can be applied to (8). Then Corollary 1 together with the unboundedness of $N_S(x_i)$ implies that $P(N_S(t x_i))$ is unbounded, whence $P(N_S(x_i))$ is also unbounded. $\diamondsuit$

2. Effective results

In this section, we consider the effective versions of Corollary 1 for $n = 1$ and some of their consequences. Let K, $\mathcal{O}_K$, d, S, $\mathcal{O}_S$ and $\mathcal{O}_S^*$

have the same meaning as in **1**. For given $\underline{\alpha} = (\alpha_0, \alpha_1) \in (\mathcal{O}_S \setminus \{0\})^2$, consider now those $\beta \in \mathcal{O}_S \setminus \{0\}$ which can be represented in the form

$$\beta = \alpha_0 x_0 + \alpha_1 x_1 \quad \text{with} \quad x_0, x_1 \in \mathcal{O}_S^*. \tag{9}$$

Then it follows from an effective result of Győry ([7], Lemma 6) on S-unit equations that

$$P(N_S(\beta)) > C_5 \mathrm{loglog} N_S(\beta) \tag{10}$$

provided that $N_S(\beta) > C_6$, where C_5, C_6 are effectively computable positive numbers depending only on K, S and $\underline{\alpha}$. The proof of the above mentioned result of [7] involves Baker's theory on linear forms in logarithms and its p-adic analogue. By using the same theory as well as its p-adic analogue we shall prove the following improvement of (10).

For a rational integer ν with $|\nu| > 1$, we denote by $Q(\nu)$ the greatest square free factor of ν and we set $Q(0) = Q(\pm 1) = 1$.

Theorem 2. *There are effectively computable positive numbers C_7, C_8, depending only on K, S and $\underline{\alpha}$, such that if* (9) *and $N_S(\beta) > C_7$ hold then*

$$Q(N_S(\beta)) > \exp\{C_8 \frac{(\mathrm{loglog} N_S(\beta))^2}{\mathrm{logloglog} N_S(\beta)}\}. \tag{11}$$

It follows from a well-known result (cf. [9]) that, for large $N_S(\beta)$,

$$\log Q(N_S(\beta)) \leq 1.02 P(N_S(\beta)).$$

This, together with (11), implies

$$P(N_S(\beta)) > C_9 \frac{(\mathrm{loglog} N_S(\beta))^2}{\mathrm{logloglog} N_S(\beta)}$$

with some effectively computable positive number $C_9 = C_9(K, S, \underline{\alpha})$.

For some applications, it will be more convenient to consider (9) and state Theorem 2 in a slightly different form. In what follows, $C_{10}(\ )$, $C_{11}(\ ), \cdots$ will denote effectively computable positive numbers depending only on parameters occuring between parantheses. For brevity, we write $N(\beta)$ for $N_{K/\mathbb{Q}}(\beta), \beta \in K$. We denote by $\mathcal{L}$ the multiplicative semigroup $\mathcal{O}_S^* \cap \mathcal{O}_K$, by $\overline{|\alpha|}$ the maximum of the absolute values of the conjugates of an algebraic number α, and by $H(\alpha)$ the (usual) height of α (i.e. maximum of the absolute values of the coefficients of the minimal defining polynomial of α over $\mathbf{Z}$). There is a positive integer a with $a \le C_{10}(\underline{\alpha})$ such that $a\alpha_i \in \mathcal{O}_K$ and $\overline{|a\alpha_i|} \le C_{11}(\underline{\alpha})$ for $i = 0, 1$. Further, for each pair x_0, x_1 satisfying (9), there is an $x \in \mathcal{L}$ such that $x\, x_i \in \mathcal{L}$ for $i = 0, 1$. Hence, we may assume without loss of generality that, in (9), $\underline{\alpha} = (\alpha_0, \alpha_1) \in (\mathcal{O}_K \setminus \{0\})^2$, $\beta \in \mathcal{O}_K \setminus \{0\}$ and

$$\beta = \alpha_0 x_0 + \alpha_1 x_1 \quad \text{with} \quad x_0, x_1 \in \mathcal{L}. \tag{9'}$$

Further, it is easy to see that we may also assume that

$$\min(\mathrm{ord}_{\wp}(x_0), \mathrm{ord}_{\wp}(x_1)) \le C_{12}(K, S) \tag{12}$$

for every prime ideal $\wp$ in $\mathcal{O}_K$. Since $|N(\beta)| \ge N_S(\beta)$ and, for large $N_S(\beta), Q(N_S(\beta)) \ge C_{13} Q(N(\beta))$ with some $C_{13} = C_{13}(K, S, \underline{\alpha})$, Theorem 2 immediatly follows from the following.

Theorem 3. *Suppose that $\beta \in \mathcal{O}_K \setminus \{0\}$ is represented in the form* (9') *with* (12) *and $|N(\beta)| > e^{e^e}$. Then*

$$\log |Q(N(\beta))| \ge C_{14} \frac{(\mathrm{loglog}|N(\beta)|)^2}{\mathrm{logloglog}|N(\beta)|} \tag{13}$$

where C_{14} is an effectively computable positive number depending only on K, S and $\underline{\alpha}$.

Theorem 3 with $K = \mathbf{Q}$ is due to Shorey [11]. Theorem 3 and Theorem 4 below will be proved in **3**. To formulate Theorem 4, we write in (9')

$$X = \max(\overline{|x_0|}, \overline{|x_1|}, e) \tag{14}$$

and

$$P_1 = P(N_{K/Q}(\beta)).$$

Further, we set

$$D = \begin{cases} 2 & \text{if } d = 1, \\ d & \text{if } d > 1. \end{cases} \tag{15}$$

The following result is an analogue of Corollary 1.2 of [13] which was established in the case $K = \mathbb{Q}$.

Theorem 4. *There are effectively computable positive numbers C_{15}, C_{16}, depending only on K, S and $\underline{\alpha}$, such that if (9') and (12) hold then*

$$(16) \quad \log(\prod_{\sigma} \max(|x_0^{(\sigma)}|, |x_1^{(\sigma)}|)) \leq C_{15} P_1^{D+1}(\log\log X)/\log(P_1+1)$$

where the product is taken over all the embeddings of K in C *and*

$$(17) \qquad \log H(\frac{x_1}{x_0}) \leq C_{16} P_1^{D+1}(\log\log X)/\log(P_1+1).$$

We establish now some consequences of Theorem 3 and 4. Let u_0, u_1, r and s be algebraic numbers such that

$$u_m = ru_{m-1} + su_{m-2} \ \text{ for } \ m = 2, 3, \cdots.$$

We assume that the companion polynomial $X^2 - rX - s$ to the sequence $\{u_m\}_{m=0}^{\infty}$ has distinct non-zero roots α and β such that α/β is not a root of unity. Then, it is easy to see (cf. [13], Ch. B) that

$$(18) \qquad u_m = a\alpha^m + b\beta^m \ \text{ for } \ m = 0, 1, 2, \cdots$$

where

$$a = \frac{u_0\beta - u_1}{\beta - \alpha}, \ b = \frac{u_1 - u_0\alpha}{\beta - \alpha}.$$

Then $\{u_m\}_{m=0}^{\infty}$ is called a non-degenerate binary recursive sequence of algebraic numbers. There exists an effectively computable number C_{14} depending only on the sequence $\{u_m\}_{m=0}^{\infty}$ such that

$$u_m \neq 0 \ \text{ for } \ m \geq C_{17}.$$

Let $K = \mathbb{Q}(u_0, u_1, \alpha, \beta)$. Observe that $u_m \in K$ for $m \geq 0$. We write

$$N_{K/\mathbb{Q}}(u_m) = \frac{A_m}{B_m} \ \text{ for } \ m \geq C_{17}$$

where A_m and $B_m > 0$ are relatively prime rational integers. Then, as an immediate consequence of Theorem 4, we derive the following result which extends a result of Stewart [14].[1]

Corollary 3. *Let $\{u_m\}_{m=0}^{\infty}$ be a non-degenerate binary recursive sequence of algebraic numbers. Let α and β be roots of the companion polynomial of the sequence $\{u_m\}_{m=0}^{\infty}$. Let $K = \mathbb{Q}(u_0, u_1, \alpha, \beta)$ and let D be given by* (15). *Then, there exists an effectively computable number $C_{18} > 0$ depending only on the sequence $\{u_m\}_{m=0}^{\infty}$ such that*

$$P(A_m) \geq C_{18} m^{1/D+1} \quad \text{if} \quad m \geq C_{18}. \tag{19}$$

Proof of Corollary 3. Let k be the least positive integer such that ka, kb, $k\alpha$ und $k\beta$ are algebraic integers. By considering the sequence $\{k^{m+1}u_m\}_{m=0}^{\infty}$, there is no loss of generality in assuming that a, b, α and β are elements of $\mathcal{O}_K$. We write

$$([\alpha^h], [\beta^h]) = [\pi] \quad \text{with} \quad \pi \in \mathcal{O}_K$$

and

$$\alpha_1 = \pi^{-1}\alpha^h, \ \beta_1 = \pi^{-1}\beta^h$$

where h denotes the class number of K. Then α_1, $\beta_1 \in \mathcal{O}_K$ satisfy $([\alpha_1], [\beta_1]) = [1]$ and α_1/β_1 is not a root of unity. Putting $m = m_1 h + m_2$ with $m_1, m_2 \in \mathbb{Z}$, $0 \leq m_2 < h$ and $a_1 = \alpha^{m_2} a$, $b_1 = \beta^{m_2} b$ in (18), we see that

$$\pi^{-m_1} u_m = a_1 \alpha_1^{m_1} + b_1 \beta_1^{m_1}. \tag{20}$$

Now we apply (17) to the right hand side of (20) to complete the proof of Corollary 3. ◇

Remark. For a non-degenerate binary recursive sequence $\{u_m\}_{m=0}^{\infty}$ with u_0, u_1, r, $s \in \mathbb{Z}$, Shorey [11] showed that

$$\log Q(u_m) \geq C_{19} (\log m)^2 (\operatorname{loglog} m)^{-1} \quad \text{if} \quad m \geq C_{20}, \tag{21}$$

---

[1] In the proofs of [14] and [12] on lower bounds for $P(u_m)$ and $P(u_m/u_n)$, we need to replace the assertions of van der Poorten by the theorems of Yu on p-adic linear forms in logarithms. In view of this, d should be replaced by D in these estimates. A similar remark applies to [13, Chapters 2,3].

where $C_{19} > 0$ and C_{20} are effectively computable numbers depending only on the sequence $\{u_m\}_{m=0}^{\infty}$. In fact, Shorey [11] proved the estimate (21) for $\frac{[u_m,u_n]}{(u_m,u_n)}$ with $m > n$ and $u_n \neq 0$. We note that our Theorem 3 above is an extension of (21).

Next, we derive from Theorems 3 and 4 the following result which is an effective and quantitive version of Corollary 2 with $m = 2$. Compare this with Theorem 5.2 of [13].

Corollary 4. *Let $\Delta > 0$ be a rational integer. Suppose that a, b, c are rational integers satisfying $ac \neq 0$ and $b^2 - 4ac \neq 0$. Let x and y be non-zero rational integers satisfying*

$$P(ax^2 + bxy + cy^2) \leq \Delta. \tag{22}$$

Then we have

(a) *There exists an effectively computable number $C_{21} > 0$ depending only on a, b, c and Δ such that*

$$P(x) \geq C_{21}(\log|x|)^{1/3}, \quad P(y) \geq C_{21}(\log|y|)^{1/3}. \tag{23}$$

(b) *There exists an effectively computable number $C_{22} > 0$ depending only on a, b, c and Δ such that*

$$\log Q(x) \geq C_{22}\frac{(\mathrm{loglog}x')^2}{\mathrm{logloglog}x'}, \ \log Q(y) \geq C_{22}\frac{(\mathrm{loglog}y')^2}{\mathrm{logloglog}y'}, \tag{24}$$

where $x' = \max(|x|, e^e)$ and $y' = \max(|y|, e^e)$.

Let α be a real algebraic number of degree 2. For $n \geq 0$, we write p_n/q_n for the n-th convergent in the continued fraction expansion of α. It is clear that the assumptions of Corollary 4 are satisfied with $x = p_n$, $y = q_n$. Therefore, the estimates (23) and (24) with $x = p_n$, $y = q_n$ are valid. In fact, this particular case of Corollary 4 is a consequence of the estimates (19) and (21) on the greatest prime factor and the greatest square free factor of a non-degenerate binary recursive sequence.

Proof of Corollary 4. There is no loss of generality in assuming that $a = 1$. Let α and β be non-zero distinct algebraic integers satisfying

$$x^2 + bxy + cy^2 = (x - \alpha y)(x - \beta y). \tag{25}$$

We set $K = \mathbb{Q}(\alpha)$. Then $D = 2$. Let $\wp_1, \cdots, \wp_t$ be the set of all prime ideals in K which divide rational primes not exceeding $N(\alpha\beta)\Delta$ and we write $\mathcal{L}$ for the set of all non-zero elements of $\mathcal{O}_K$ which have no prime ideal divisor different from $\wp_1, \cdots, \wp_t$. Then we observe from (22) and (25) that $\beta(x - \alpha y)$, $\alpha(x - \beta y)$, $(x - \alpha y)$ and $(-x + \beta y)$ are elements of $\mathcal{L}$. Furthermore, we observe that

$$(\beta - \alpha)x = \beta(x - \alpha y) + \alpha(-x + \beta y) \tag{26}$$

and

$$(\beta - \alpha)y = (x - \alpha y) + (-x + \beta y). \tag{27}$$

(a) We apply Theorem 4 with $\alpha_0 = \alpha_1 = 1$, $x_0 = \beta(x - \alpha y)$ and $x_1 = \alpha(-x + \beta y)$. For this, we observe from (26) that X given by (14) satisfies $2X \geq |(\beta - \alpha)x|$. Now, we derive from (16) that $P(x) \geq C_{21}(\log|x|)^{1/3}$. Similarly, the estimate for $P(y)$ follows from (27).
(b) We apply Theorem 3 with $x_0 = \beta(x - \alpha y)$, $x_1 = \alpha(-x + \beta y)$, as well as $x_0 = x - \alpha y$, $x_1 = -x + \beta y$, to obtain (24). $\diamondsuit$

3. Proofs of Theorems 3 and 4

We keep the notation of §2. In what follows, $C_{23}, C_{24}, \cdots$ will denote effectively computable positive numbers which, unless otherwise stated, depend only on K, S and $\underline{\alpha}$. First we prove Theorem 3. Suppose that $\beta \in \mathcal{O}_K \setminus \{0\}$ is represented in the form (9') with $\underline{\alpha} = (\alpha_1, \alpha_2) \in (\mathcal{O}_K \setminus \{0\})^2$, $x_0, x_1 \in \mathcal{L}$ and (12). We may assume that $|N(\beta)| > C_{23}$ with C_{23} sufficiently large. Further, we can write (cf. [13], Ch. A)

$$x_i = \rho_i \eta_1^{a_{i,1}} \cdots \eta_r^{a_{i,r}} \pi_1^{b_{i,1}} \cdots \pi_s^{b_{i,s}} \quad \text{for} \quad i = 0, 1, \tag{28}$$

where $a_{i,1}, \cdots, a_{i,r} \in \mathbb{Z}$, $b_{i,1}, \cdots, b_{i,s}$ are non-negative rational integers for $i = 0, 1$,

$$\max(\overline{|\rho_1|}, \overline{|\rho_2|}, \overline{|\eta_1|}, \cdots, \overline{|\eta_r|}, \overline{|\pi_1|}, \cdots, \overline{|\pi_s|}) \leq C_{24}(K, S), \tag{29}$$

$\{\eta_1, \cdots, \eta_r\}$ is a maximal system of independent units in $\mathcal{O}_K$ and the principal ideals $[\pi_1], \cdots, [\pi_s]$ are the h-th powers of the prime ideals in $\mathcal{O}_K$ corresponding to the finite places in S. Here h denotes the class number of K.

Theorem 3 is an immediate consequence of the following result.

Lemma 2. *Let $\beta \in \mathcal{O}_K \setminus \{0\}$ be represented in the form* (9') *with the properties* (12), (28), (29) *and $|N(\beta)| > C_{23}$. Further, suppose that*

$$\log P(N(\beta)) \leq (\mathrm{loglog}|N(\beta)|)^2. \tag{30}$$

Then, there exists $C_{25} > 0$ such that

$$\sum_{\substack{p | N(\beta) \\ p \geq (\log |N(\beta)|)^{C_{25}}}} 1 \geq C_{25} \frac{\mathrm{loglog}|N(\beta)|}{\mathrm{logloglog}|N(\beta)|}$$

where p runs through rational primes.

Proof. We may assume that

$$\sum_{\substack{p | N(\beta) \\ p \geq (\log |N(\beta)|)^{\epsilon}}} 1 < \epsilon \frac{\mathrm{loglog}|N(\beta)|}{\mathrm{logloglog}|N(\beta)|}, \tag{31}$$

where ϵ is an effectively computable positive number with $\epsilon \leq 1$ which depends only on K, S and $\underline{\alpha}$ and which will be chosen suitably later. Thus, we allow C_{23} to depend also on ϵ.

Denote by $\mathcal{P}$ the set of all prime ideals in $\mathcal{O}_K$, and put

$$\mathcal{P}_1 = \{\wp \in \mathcal{P} | \wp | p \text{ for some positive rational prime} \\ p < (\log |N(\beta)|)^{\epsilon}\} \tag{32}$$

and

$$\mathcal{P}_2 = \{\wp \in \mathcal{P} | \wp | p \text{ for some rational prime } p \text{ with} \\ (\log |N(\beta)|)^{\epsilon} \leq p \leq \exp\{(\mathrm{loglog}|N(\beta)|)^2\}\}. \tag{33}$$

Then $\wp \in \mathcal{P}_1 \cup \mathcal{P}_2$ for each prime ideal divisor $\wp$ of β. The product of h ideals from any fixed ideal class (modulo the group of principal ideals) is a principal ideal. Hence β can be written in the form

$$\beta = \beta_1 \cdot \beta_2 \quad \text{with} \quad \beta_1, \beta_2 \in \mathcal{O}_K \tag{34}$$

so that all prime ideal divisors of β_1 belong to $\mathcal{P}_1$ and β_2 is divisible by at most $h(h-1)$ prime ideals (with multiplicities) from $\mathcal{P}_1$. Further, this, together with (30) and (31), implies

$$\beta = \rho_2' {\gamma_1'}^{d_1} \cdots {\gamma_t'}^{d_t}$$

where ρ_2' is a unit in $\mathcal{O}_K, \gamma_1', \cdots, \gamma_t'$ are non-units in $\mathcal{O}_K$ and $d_1, \cdots, d_t$ are non-negative rational integers such that

$$t \leq C_{26}\epsilon \frac{\text{loglog}|N(\beta)|}{\text{logloglog}|N(\beta)|} + C_{27} \tag{35}$$

and

$$\log |N(\gamma_j')| \leq C_{28}(\text{loglog}|N(\beta)|)^2 \quad \text{for} \quad j = 1, \cdots, t.$$

Consequently, we apply Lemma A.15 of [13] to find associates $\gamma_1, \cdots, \gamma_t$ of $\gamma_1', \cdots, \gamma_t'$, respectively, such that

$$\log \overline{|\gamma_j|} \leq C_{29}(\text{loglog}|N(\beta)|)^2 \quad \text{for} \quad j = 1, \cdots, t. \tag{36}$$

Further, on multiplying both sides of (9') by an appropriate unit and applying again Lemma A.15 of [13] to x_0 and x_1, there is no loss of generality in assuming that

$$\beta_2 = \gamma_1^{d_1} \cdots \gamma_t^{d_t}, \tag{37}$$

$$\log \overline{|\beta_1|} \leq C_{30} \log |N(\beta_1)| \tag{38}$$

and (12), (28), (29) hold. Also, observe that

$$d_j \leq (\log |N(\beta_2)|)/\log 2 \leq 2 \log |N(\beta)| \quad \text{for} \quad j = 1, \cdots, t. \tag{39}$$

Let in (28),

$$V =: \max_{\substack{1\le j\le r\\ i=0,1}} |a_{i,j}|,\ W =: \max_{\substack{1\le j\le r\\ i=0,1}} b_{i,j}, \tag{40}$$

and we put

$$U =: \max(V, W). \tag{41}$$

In view of $|N(\beta)| > C_{23}$, we have $U > C_{31}$ with some C_{31} sufficiently large. We apply an estimate of Yu ([16], Theorem 1') on p-adic linear forms in logarithms to derive from (9'), (28), (29), (12), (40) and (41) that

$$\operatorname{ord}_{\wp}(\beta) \le C_{32} P^D (\log U)/\log p, \tag{42}$$

where $\wp$ is a prime ideal in $\mathcal{P}_1 \cup \mathcal{P}_2$ dividing a rational prime p. Now, we apply (42), (32) and Theorem 9 of [9] to derive that

$$\log |N(\beta_1)| \le (\log |N(\beta)|)^{C_{33}\epsilon} \log U$$

whence, by (38),

$$\log \overline{|\beta_1|} \le C_{30} (\log |N(\beta)|)^{C_{33}\epsilon} \log U. \tag{43}$$

Let $\wp$ be a prime ideal divisor of π_1 in O_K. We apply again Theorem 1' of Yu [16] on p-adic linear forms in logarithms to $\beta - \alpha_1 x_1$ to derive from (9'), (28), (29), (12), (40), (41), (39), (36) and (35) that

$$b_{0,1} \le (\log |N(\beta)|)^{C_{34}\epsilon} (\log U)^2. \tag{44}$$

Repeated applications of estimates for p-adic linear forms in logarithms provide the estimate (44) for all $b_{i,j}$ with $i = 0, 1$ and $j = 1, \cdots, s$. Thus

$$W \le (\log |N(\beta)|)^{C_{34}\epsilon} (\log U)^2. \tag{45}$$

If $U \le W^2$, then we observe from (45) that

$$W \le (\log |N(\beta)|)^{2C_{34}\epsilon}, U \le (\log |N(\beta)|)^{4C_{34}\epsilon}$$

which, together with (9'), (28), (29) and $|N(\beta)| > C_{23}$, implies that $\log|N(\beta)| \leq (\log|N(\beta)|)^{8C_{34}\epsilon}$ which is not possible if $\epsilon < (8C_{34})^{-1}$. Thus, we assume that

$$U > W^2. \tag{46}$$

Then, by (41), (9'), (28), (29) and $|N(\beta)| > C_{23}$,

$$U = V \quad \text{and} \quad U \geq (\log|N(\beta)|)^{1/2}. \tag{47}$$

There is no loss of generality in assuming that $|a_{0,1}| = V$. We write from (28) that, for each embedding σ of K in $\mathbb{C}$,

$$\sum_{j=1}^{r} a_{0,j} \log|\eta_j^{(\sigma)}| = -\log|\rho_0^{(\sigma)}| + \log|x_0^{(\sigma)}| - \sum_{j=1}^{t} b_{0,j}|\pi_j^{(\sigma)}|.$$

This, together with (47), (29) and (46), implies (cf. also [13], Ch. A) that

$$U = V \leq C_{35}(\log\overline{|x_0|} + U^{1/2}).$$

Therefore, in view of (47) and $|N(\beta)| > C_{23}$

$$\log\overline{|x_0|} \geq C_{36}U. \tag{48}$$

On the other hand, we see from (28) and (46) that

$$\log|N(x_0)| \leq C_{37}W < C_{37}U^{1/2}. \tag{49}$$

By (46), we have $d \geq 2$. Further, in view of (48), (49), (47) and $|N(\beta)| > C_{23}$ we may assume that there exists an embedding σ of K in C such that

$$\log|x_0^{(\sigma)}| \leq -\frac{C_{36}}{d}U. \tag{50}$$

Now, apply Theorem 2 of Baker [1] on linear forms in logarithms to obtain from (9'), (28), (29), (34), (37), (43), (36), (39), (35), (41) and (47) that

$$\log|(\alpha_0 x_0)^{(\sigma)}| = \log|\beta^{(\sigma)} - (\alpha_1 x_1)^{(\sigma)}| \geq \tag{51}$$

$$\geq (\log |N(\beta)|)^{C_{38}\epsilon} (\log U)^2.$$

Finally, we combine (50) and (51) to derive that

$$U \leq (\log |N(\beta)|)^{2C_{38}\epsilon}$$

which, in view of (47), is not possible if $\epsilon < (4C_{38})^{-1}$. Finally, we set $\epsilon = \min((8C_{34})^{-1}, (4C_{38})^{-1}, 1)$ and $C_{25} = \epsilon/2$ to complete the proof of Lemma 2. $\diamondsuit$

Proof of Theorem 4. Suppose that $\beta \in O_K \setminus \{0\}$ and $x_0, x_1 \in \mathcal{L}$ satisfying (9') and (12). Then, as we have seen above, we may also assume that (28) and (29) hold. Let V, W, U and X be defined by (40), (41) and (14), respectively. Then, using some arguments from the above proof, it is easy to see that

$$U = \max(V, W) \leq C_{39} \log X. \tag{52}$$

We apply Theorem 2 of Baker [1] on linear forms in logarithms to derive form (9'), (12), (28), (29) and (52) that

$$|N(\beta)| \geq C_{40}(\prod_{\sigma} \max(|\alpha_0 x_0)^{(\sigma)}|, |(\alpha_1 x_1)^{(\sigma)}|)(\log X)^{-C_{41}}, \tag{53}$$

where the product is taken over all the embeddings σ of K in $\mathbb{C}$. On the other hand, it follows from (42), (52) and Theorem 9 of [9] that

$$\log |N(\beta)| \leq C_{42} P_1^{D+1} (\text{loglog} X)/\log(P_1 + 1). \tag{54}$$

We combine (53) and (54) to derive (16). Finally, (17) follows from (16) and Lemma C of [10]. $\diamondsuit$

Acknowledgements. Some results of this paper were obtained during the first author's stay at the University of Strasbourg, in 1987. The first author thanks Professor M. Mignotte and the University of Strasbourg for their hospitality.

References

[1] BAKER, A.: The theory of linear forms in logarithms, *Transcendence Theory: Advances and Applications* (Academic Press, London, 1977), 1 – 27.

[2] EVEREST, G.R.: A Hardy-Littlewood approach to the S-unit equation, *Compositio Math.* **70** (1989), 101 – 118.

[3] EVEREST, G.R.: Counting the values taken by sums of S-units, to appear.

[4] EVEREST, G.R.: On the solutions of the norm form equation, to appear.

[5] EVERTSE, J.-H.: On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225 - 244.

[6] EVERTSE, J.-H. and GYŐRY, K.: On the numbers of solutions of weighted unit equations, *Compositio Math.* **66** (1988), 329 – 354.

[7] GYŐRY, K.: On the number of solutions of linear equations in units of an algebraic number field, *Comment. Math. Helv.* **54** (1979), 583 – 600.

[8] VAN DER POORTEN, A.J. and SCHLICKEWEI, H.P.: The growth conditions for recurrence sequences, *Macquarie Univ. Math. Rep. 82-0041*, North Ryde, Australia, 1982.

[9] ROSSER, J.B. and SCHOENFELD, L.: Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64 – 94.

[10] SHOREY, T.N., VAN DER POORTEN, A.J., TIJDEMAN, R. and SCHINZEL, A.: Applications of the Gel'fond-Baker method to Diophantine equations, *Transcendence Theory: Advances and Applications* (Academic Press, London, 1977), 59 – 77.

[11] SHOREY, T.N.: The greatest square free factor of a binary recursive sequence, *Hardy-Ramanujan Journal* **6** (1983), 23 – 36.

[12] SHOREY, T.N.: Linear forms in members of a binary recursive sequence, *Acta. Arith.* **43** (1984), 317 – 331.

[13] SHOREY, T.N. and TIJDEMAN, R.: Exponential diophantine equations, *Cambridge Tracts in Mathematics* **87** (1986), Cambridge University Press.

[14] STEWART, C.L.: On divisors of terms of linear recurrence sequences, *J. Reine Angew. Math.* **333** (1982), 12 – 31.

[15] TIJDEMAN, R. and LIANXIANG WANG.: Simultaneous weighted sums of elements of finitely generated multiplicative groups, *Proc. Koninklijke Ned. Akad. Wet., Mathematics* **91** (1988), 205 – 209.

[16] KUNRUI YU, Linear forms in p-adic logarithms II, *Compositio Math.* **74** (1990), 15 – 113.