BOUNDS FOR THE SOLUTIONS OF UNIT EQUATIONS

YANN BUGEAUD (Strasbourg) and KÁLMÁN GYŐRY *) (Debrecen)

1. Introduction

Many diophantine problems can be reduced to (ordinary) unit equations and S-unit equations in two unknowns (for references, see e.g. [15], [24], [11], [16], [25]). Several effective bounds have been established for the heights of the solutions of such equations (see e.g. [24], [11], [25], [3] and the references given there). Except in [3], their proofs involved Baker's method and its p-adic analogue as well as certain quantitative results concerning independent units. The best known estimates for S-unit equations are due to Győry [13] and, for (ordinary) unit equations, to Schmidt [23], Sprindžuk [25] (with non completely explicit constants) and Győry [14] (with explicit constants). These led to a lot of applications.

The purpose of the present paper is to considerably improve (in completely explicit form) the above-mentioned estimates in terms of the cardinality of S and of the parameters involved (degree, unit rank, regulator, class number) of the ground field. To obtain these improvements we use, among other things, some recent improvements of Waldschmidt [26] and Kunrui Yu [27] concerning linear forms in logarithms, some recent estimates of Brindza [5] and Hajdu [18] for fundamental systems of S-units, some upper and lower bounds for S-regulators (cf. Lemma 3 of this paper) and an idea of Schmidt [23]. Further, in our arguments we pay a particular attention to the dependence on the parameters in question. As a consequence of our result, we derive explicit bounds for the solutions of homogeneous linear equations of three terms in S-integers of bounded S-norm. These improve some earlier estimates of Győry [13], [14].

An application of our improvements is given in [17] to decomposable form equations (including Thue equations, norm form equations and discriminant form equations) in S-integers of a number field. Some other applications will be published in two further works.

2. Bounds for the solutions of S-unit equations

We shall use throughout this paper the following standard notation. Let $\mathbf{K}$ be an algebraic number field of degree d with regulator R_K, class number h_K and unit rank r. Denote by O_K the ring of integers of $\mathbf{K}$, and by O_K^* the unit group of O_K. Let S be a finite set of places on $\mathbf{K}$ containing the set of infinite places S_∞. Denote by s the cardinality of S, by t the number of finite places in S, and by P the largest of the rational primes lying below the finite places of S, with the convention that $P = 1$ if $S = S_\infty$, i.e. if $t = 0$. Further, denote by O_S the ring of S-integers, and by O_S^* the group of S-units in $\mathbf{K}$. Then $s - 1 = r + t$ is the rank of O_S^*. The case $s = 1$ being trivial, we assume throughout the paper that $s \geq 2$. We denote by R_S the S-regulator of $\mathbf{K}$ (for its definition, see Section 3). We note that for $S = S_\infty$ (i.e. $t = 0$), we have $O_S = O_K$ and $R_S = R_K$.

For any algebraic number α, we denote by $\mathrm{h}(\alpha)$ the (absolute) height of α (cf. Section 3). There exists a $\delta_{\mathbf{K}} > 0$, depending only on $\mathbf{K}$, such that $d \log \mathrm{h}(\alpha) \geq \delta_{\mathbf{K}}$ for any $\alpha \in \mathbf{K} \setminus \{0\}$ which is not a root of unity (cf. Section 3).

Throughout this paper, we stand the notation $\log^* a$ for $\max\{\log a, 1\}$.

Let α, β be non-zero elements of $\mathbf{K}$ with

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \leq H \quad (H \geq e).$$

Consider the S-unit equation

$$\alpha x + \beta y = 1 \quad \text{in } x, y \in O_S^*. \tag{1}$$

When $S = S_\infty$ (i.e. $t = 0$) then (1) is an (ordinary) unit equation.

*) Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

Theorem. *All solutions x, y of (1) satisfy*

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} < \exp\{c_1 P^d R_S (\log^* R_S)(\log^*(PR_S)/\log^* P)\log H\}, \tag{2}$$

where

$$c_1 = c_1(d, s, \mathbf{K}) = 3^{25}(9d^2/\delta_{\mathbf{K}})^{s+1}\, s^{5s+10}.$$

Further, if in particular $S = S_\infty$ (i.e. $t = 0$), then the bound in (2) can be replaced by

$$\exp\{c_2 R_K (\log^* R_K)\log H\} \tag{3}$$

where

$$c_2 = c_2(d, r, \mathbf{K}) = 3^{r+27}\,(r+1)^{5r+17}\, d^3\, \delta_{\mathbf{K}}^{-(r+1)}.$$

Remark 1. It is clear that the factor $(\log^*(PR_S)/\log^* P)$ in (2) does not exceed $2\log^* R_S$, and if $\log^* R_S \le \log^* P$, then it is at most 2. Further, by Lemma 3 (cf. Section 3), we have

$$R_S \le R_K h_K (d \log^* P)^t. \tag{4}$$

Remark 2. As is known, $R_K h_K$ can be estimated from above in terms of d and D_K, the discriminant of $\mathbf{K}$. Denote by q the number of complex places of $\mathbf{K}$, and put $\Delta = \left(\frac{2}{\pi}\right)^q |D_K|^{1/2}$. If $d \ge 2$, then we have e.g. (cf. [21])

$$R_K h_K \le \Delta(\log\Delta)^{d-1-q}(d - 1 + \log\Delta)^q/(d-1)!. \tag{5}$$

Our theorem provides a considerable improvement of earlier estimates of Kotov and Trelina [19], Győry [13], [14], Schmidt [23] and Sprindžuk [25] for S-unit equations.

For $\alpha \in \mathbf{K}\setminus\{0\}$, the ideal generated by α can be uniquely written in the form $\mathfrak{a}_1 \cdot \mathfrak{a}_2$ where the ideal $\mathfrak{a}_1$ (resp. $\mathfrak{a}_2$) is composed of prime ideals outside (resp. inside) S. Then the S-norm of α, denoted by $\mathrm{N}_S(\alpha)$, is defined as $\mathrm{N}(\mathfrak{a}_1)$. In the particular case $S = S_\infty$, we have $\mathrm{N}_{S_\infty}(\alpha) = |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\alpha)|$. Further, $\mathrm{N}_S(\alpha)$ is a positive integer for every $\alpha \in O_S \setminus \{0\}$.

In some applications, it is more convenient to consider the following equation instead of (1) :

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 0 \quad \text{in } x_i \in O_S\setminus\{0\} \text{ with } \mathrm{N}_S(x_i) \le N \text{ for } i = 1, 2, 3, \tag{6}$$

where $\alpha_1, \alpha_2, \alpha_3 \in \mathbf{K}\setminus\{0\}$ with $\max_{1\le i\le 3} \mathrm{h}(\alpha_i) \le H$ $(H \ge e)$.

Let $c_3 = c_3(d, r, \mathbf{K}) = r^{r+1}\,\delta_{\mathbf{K}}^{-(r-1)}/2$ and let $c_1 = c_1(d, s, \mathbf{K})$, $c_2 = c_2(d, r, \mathbf{K})$ denote the numbers specified in the Theorem. Then we have

Corollary. *For every solution x_1, x_2, x_3 of (6) there is an $\varepsilon \in O_S^*$ such that*

$$\begin{aligned}\max_{1\le i\le 3} \mathrm{h}(\varepsilon x_i) < \exp\{&3c_1 c_3 P^d R_S (\log^* R_S)(\log^*(PR_S)/\log^* P)\cdot \\ &(R_K + t h_K \log^* P + \log(HN))\}.\end{aligned} \tag{7}$$

Further, if $S = S_\infty$, then the bound in (7) can be replaced by

$$\exp\{3c_2 c_3 R_K(\log^* R_K)(R_K + \log(HN))\}.$$

Our Corollary considerably improves the earlier bounds of Győry [13], [14] concerning equation (6).

3. Bounds for S-units and S-regulators

Keeping the notations of Section 2, denote by $M_{\mathbf{K}}$ the set of places on $\mathbf{K}$. In every place v we choose a valuation $|\,.\,|_v$ in the following way : if v is infinite and corresponds to an embedding $\sigma : \mathbf{K} \to \mathbf{C}$ then we put, for every $\alpha \in \mathbf{K}$,

$$|\alpha|_v = |\sigma(\alpha)|^{d_v},$$

where $d_v = 1$ or 2 according as $\sigma(\mathbf{K})$ is contained in $\mathbf{R}$ or not; if v is a finite place corresponding to the prime ideal $\mathfrak{p}$ in $\mathbf{K}$ then we put $|0|_v = 0$ and, for $\alpha \in \mathbf{K} \setminus \{0\}$,

$$|\alpha|_v = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}.$$

The (absolute) height of an algebraic number α contained in $\mathbf{K}$ is defined by

$$\mathrm{h}(\alpha) = \Big(\prod_{v \in \mathrm{M}_K} \max(1, |\alpha|_v)\Big)^{1/d}.$$

This height is independent of the choice of $\mathbf{K}$. If the algebraic number α is of degree n with minimal polynomial $a_0(X-\alpha_1)\ldots(X-\alpha_n) \in \mathbf{Z}[X]$ over $\mathbf{Z}$, then, by ([20], page 54), we have

$$\mathrm{h}(\alpha) = \Big(|a_0| \prod_{i=1}^{n} \max(1, |\alpha_i|)\Big)^{1/n}. \tag{8}$$

There is a positive constant $\delta_{\mathbf{K}}$, depending only on $\mathbf{K}$, such that for every non-zero algebraic number $\alpha \in \mathbf{K}$ which is not a root of unity we have $\log \mathrm{h}(\alpha) \geq \delta_{\mathbf{K}}/d$ (we recall that d denotes the degree of $\mathbf{K}$). Further, if α is not an algebraic integer then (8) implies that $\log \mathrm{h}(\alpha) \geq \log 2/d$. Hence we have $\delta_{\mathbf{K}} \leq \log 2$.

It is easy to see that we can take

$$\delta_{\mathbf{K}} = \frac{\log 2}{r+1} \quad \text{for } \; d = 1, 2,$$

where r denotes the unit rank of $\mathbf{K}$. Further, it follows from results of Blanksby and Montgomery [2] and of Dobrowolski [7], [8] that both

$$\delta_{\mathbf{K}} = \frac{1}{53 d \log 6d} \quad \text{and} \quad \delta_{\mathbf{K}} = \frac{1}{1201}\left(\frac{\log\log d}{\log d}\right)^3$$

are appropriate choices for $d \geq 3$. For large d, the factor $1/1201$ can be replaced by a larger one (see e.g. [9]).

We recall that s denotes the cardinality of S. For $v \in S$, denote by $|\,.\,|_v$ the corresponding valuation normalized as above. Let $v_1, \ldots, v_{s-1}$ be a subset of S, and let $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ be a fundamental system of S-units in $\mathbf{K}$. Denote by R_S the absolute value of the determinant of the matrix $(\log|\varepsilon_i|_{v_j})_{i,j=1,\ldots,s-1}$. It is easy to verify that R_S is a positive number which is independent of the choice of $v_1, \ldots, v_{s-1}$ and of the fundamental system of S-units $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$. R_S is called the S-regulator of $\mathbf{K}$. If in particular $S = S_\infty$, then we have $R_S = R_K$.

There are several quantitative results in the literature for units and S-units of small height; for references, see e.g. [24], [5] and [18]. The following lemma is in fact due to Hajdu [18]. It is an extended version of an earlier theorem of Brindza [5]. For convenience of the reader, we give here a proof for Lemma 1 with a slightly better value for c_4 than in [18].

Put

$$c_4 = c_4(d, s) = \big((s-1)!\big)^2/(2^{s-2} d^{s-1})$$

and

$$c_5 = c_5(d, s, \mathbf{K}) = c_4 \left(\frac{\delta_{\mathbf{K}}}{d}\right)^{2-s}, \; c_6 = c_6(d, s, \mathbf{K}) = c_4 d^{s-1} \delta_{\mathbf{K}}^{-1}.$$

Lemma 1. *There exists in $\mathbf{K}$ a fundamental system $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ of S-units with the following properties :*

$$\prod_{i=1}^{s-1} \log \mathrm{h}(\varepsilon_i) \leq c_4 R_S; \tag{i}$$

$$\log \mathrm{h}(\varepsilon_i) \leq c_5 R_S, \quad i = 1, \ldots, s-1; \tag{ii}$$

(iii) the absolute values of the entries of the inverse matrix of $(\log|\varepsilon_i|_{v_j})_{i,j=1,\dots,s-1}$ *do not exceed* c_6.

Proof of Lemma 1. We shall combine some arguments from the proofs of [5] and [18]. For $\alpha \in \mathbf{K}\setminus\{0\}$ put

$$\underline{v}(\alpha) = (\log|\alpha|_{v_1}, \dots, \log|\alpha|_{v_{s-1}}).$$

The lattice Λ in $\mathbf{R}^{s-1}$ spanned by the vectors $\underline{v}(\eta)$ with $\eta \in O_S^*$ has determinant R_S.

The function $F : \mathbf{R}^{s-1} \to \mathbf{R}$ defined by

$$F(\underline{x}) = |x_1| + \dots + |x_{s-1}|$$

for $\underline{x} = (x_1, \dots, x_{s-1}) \in \mathbf{R}^{s-1}$ is a symmetric convex distance function (cf. [6], Ch. IV), i.e. it is non-negative, continuous, $F(\alpha\underline{x}) = \alpha F(\underline{x})$ $(\alpha \geq 0$ real) and $F(\underline{x}+\underline{y}) \leq F(\underline{x}) + F(\underline{y})$ for $\underline{x}$, $\underline{y} \in \mathbf{R}^{s-1}$. Denote by V_F the volume of the bounded set $\{\underline{x} \in \mathbf{R}^{s-1} \mid F(\underline{x}) < 1\}$. It is easy to check that $V_F = 2^{s-1}/(s-1)!$. By a theorem of Minkowski (cf. [6], Ch. VIII) the successive minima $\lambda_1, \dots, \lambda_{s-1}$ of Λ with respect to F have the property

$$\lambda_1 \dots \lambda_{s-1} \leq 2^{s-1} R_S / V_F = (s-1)! R_S. \tag{9}$$

Further, there are multiplicatively independent S-units $\eta_1, \dots, \eta_{s-1}$ for which

$$F(\underline{v}(\eta_i)) = \lambda_i, \quad i = 1, \dots, s-1. \tag{10}$$

It follows (cf. [6], p. 135, Lemma 8) that there exists a fundamental system $\{\varepsilon_1, \dots, \varepsilon_{s-1}\}$ of S-units such that

$$F(\underline{v}(\varepsilon_i)) \leq \max\left\{1, \frac{i}{2}\right\} F(\underline{v}(\eta_i)), \quad i = 1, \dots, s-1. \tag{11}$$

However, for every $\eta \in O_S^*$, we have $\prod_{v\in S} |\eta|_v = 1$, hence

$$\log \mathrm{h}(\eta) = \frac{1}{d}\sum_{v\in S} \max\{0, \log|\eta|_v\} = \frac{1}{2d}\sum_{v\in S} \big|\log|\eta|_v\big|,$$

which implies that

$$\frac{1}{2d} F(\underline{v}(\eta)) \leq \log \mathrm{h}(\eta) \leq \frac{1}{d} F(\underline{v}(\eta)). \tag{12}$$

Hence, by (12), (11), (10) and (9), we have

$$\begin{aligned}\prod_{i=1}^{s-1} \log \mathrm{h}(\varepsilon_i) &\leq \frac{1}{d^{s-1}} \prod_{i=1}^{s-1} F(\underline{v}(\varepsilon_i)) \leq \frac{(s-1)!}{2^{s-2} d^{s-1}} \prod_{i=1}^{s-1} F(\underline{v}(\eta_i)) \\ &\leq \big((s-1)!\big)^2 R_S / (2^{s-2} d^{s-1})\end{aligned} \tag{13}$$

which proves (i).

(ii) follows immediately from (i) and $\log \mathrm{h}(\varepsilon_i) \geq \delta_{\mathbf{K}}/d$, for $i = 1, \dots, s-1$.

We now prove (iii). Put $E = (\log|\varepsilon_i|_{v_j})_{i,j=1,\dots,s-1}$ and $e_{ij} = \det(E_{ij})/\det(E)$ where E_{ij} denotes the matrix obtained from E by omitting the i-th row and j-th column. It follows from (13) and Hadamard's inequality that

$$\begin{aligned}|\det(E_{ij})| &\leq \prod_{\substack{p=1\\p\neq i}}^{s-1} \sqrt{\sum_{\substack{q=1\\q\neq j}}^{s-1} (\log|\varepsilon_p|_{v_q})^2} \leq \prod_{\substack{p=1\\p\neq i}}^{s-1} F(\underline{v}(\varepsilon_p)) \\ &\leq c_4 R_S / F(\underline{v}(\varepsilon_i)).\end{aligned}$$

Together with (12), $|\det(E)| = R_S$ and $\log \mathrm{h}(\varepsilon_i) \geq \delta_{\mathbf{K}}/d$ this implies

$$|e_{ij}| \leq c_4 \delta_{\mathbf{K}}^{-1} d^{s-1}$$

which completes the proof. □

The next lemma has various versions in the literature (for references, see e.g. [15], [24], [10], [18]). Our lemma is an explicit version of Lemma 10 of [10].

Let $c_3 = c_3(d, r, \mathbf{K})$ denote the constant specified in the Corollary.

Lemma 2. *For every $\alpha \in O_S \setminus \{0\}$ and every integer $n \geq 1$ there exists an S-unit ε such that*

$$\mathrm{h}(\varepsilon^n \alpha) \leq \mathrm{N}_S(\alpha)^{1/d} \exp\{n(c_3 R_K + t h_K \log^* P)\}. \tag{14}$$

Proof. First consider the case when $S = S_\infty$. So let $\alpha \in O_K \setminus \{0\}$ and put $M = |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\alpha)|$. Let $S_\infty = \{v_1, \ldots, v_{r+1}\}$ and $L(\alpha) = \max_{1 \leq i \leq r} |\log|\alpha|_{v_i}|$. Then there are multiplicatively independent units $\eta_1, \ldots, \eta_r$ in O_K such that $L(\eta_1)\ldots L(\eta_r) \leq R_K$ (cf. [14]). On the other hand, we have $L(\eta_j) \geq \dfrac{d}{r} \log \mathrm{h}(\eta_j) \geq \dfrac{\delta_{\mathbf{K}}}{r}$, whence $L(\eta_j) \leq r^{r-1}\, \delta_{\mathbf{K}}^{-(r-1)}\, R_K$ for each j.

Consider the system of linear equations

$$\sum_{j=1}^{r} X_j \log|\eta_j|_{v_i} = -\log\left(M^{-d_{v_i}/d}|\alpha|_{v_i}\right), \quad i = 1, \ldots, r+1,$$

in $X_1, \ldots, X_r$. It has a unique solution $x_1, \ldots, x_r$ in $\mathbf{R}$. For $1 \leq j \leq r$, there exist $b_j \in \mathbf{Z}$ and $\rho_j \in \mathbf{R}$ with $|\rho_j| \leq n/2$ such that $x_j = nb_j + \rho_j$. Putting $\eta_1^{b_1} \ldots \eta_r^{b_r} = \varepsilon$, we infer that

$$\begin{aligned}
\left|\log\left(M^{-d_{v_i}/d}|\alpha\varepsilon^n|_{v_i}\right)\right| &= \left|\sum_{j=1}^{r} \rho_j \log|\eta_j|_{v_i}\right| \\
&\leq \frac{nr}{2} \max_{1 \leq j \leq r} \left|\log|\eta_j|_{v_i}\right| \leq \frac{nr}{2} \cdot r \max_{1 \leq j \leq r} L(\eta_j) \\
&\leq n c_3 R_K, \qquad i = 1, \ldots, r+1,
\end{aligned} \tag{15}$$

which implies (14).

The general case of our Lemma follows from the case $S = S_\infty$ as in the proof of Lemma 10 of [10]. $\square$

Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ the prime ideals in $\mathbf{K}$ corresponding to the finite places in S. We recall that P denotes the largest of the rational primes lying below of these prime ideals.

The following lemma is an improvement of some estimates of Pethő [22] and Hajdu [18] for R_S. It should, however, be remarked that Pethő's estimate was established in a more general situation, for some S-orders instead of O_S.

Lemma 3. *If $t > 0$, then we have*

$$R_S \leq R_K h_K \prod_{i=1}^{t} \log \mathrm{N}(\mathfrak{p}_i) \leq R_K h_K (d \log^* P)^t \tag{16}$$

and

$$R_S \geq R_K \prod_{i=1}^{t} \log \mathrm{N}(\mathfrak{p}_i) \geq c_7 (\log 2)(\log^* P), \tag{17}$$

where $c_7 = 0.2052$.

Proof. O_S^*/O_K^* is a free abelian group of rank t which is isomorphic to the multiplicative group of principal ideals in $\mathbf{K}$ generated by the elements of O_S^*. This latter group is a subgroup of finite index, say i_S, of the multiplicative group generated by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ and we have $i_S \leq h_K$. Hence, as is known (see e.g. [4], pp. 85 and 125), this subgroup has a basis of the form

$$(\varepsilon_i) = \mathfrak{p}_i^{a_{ii}} \mathfrak{p}_{i+1}^{a_{i,i+1}} \ldots \mathfrak{p}_t^{a_{it}}, \quad i = 1, \ldots, t,$$

with rational integers a_{ij} such that $a_{ii} > 0$ for $i = 1, \ldots, t$ and that $a_{11} \ldots a_{tt} = i_S$. It follows now that if $\{\varepsilon_{t+1}, \ldots, \varepsilon_{t+r}\}$ is a fundamental system of units in O_K then $\{\varepsilon_1, \ldots, \varepsilon_t, \ldots, \varepsilon_{t+r}\}$ is a fundamental system of S-units in $\mathbf{K}$. Consequently, it is easy to see that

$$R_S = \left|\det(\log|\varepsilon_i|_{v_j})_{i,j=1,\ldots,r+t}\right| = R_K i_S \prod_{i=1}^{t} \log \mathrm{N}(\mathfrak{p}_i) \tag{18}$$

which gives (16). Inequalities (17) follow from (18) and the estimate $R_K \geq c_7$ of Friedman [12]. $\square$

4. Estimates for linear forms in logarithms

In our proofs, we shall use the best known estimates, due to Waldschmidt [26] and Kunrui Yu [27] respectively, for linear forms in logarithms in the complex and in the p-adic case. We shall formulate them in a more convenient form for our purpose.

Let $\alpha_1, \ldots, \alpha_n$ ($n \geq 2$) be non-zero algebraic numbers and let $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$. Put $[\mathbf{K} : \mathbf{Q}] = d$. Let $A_1, \ldots, A_n$ be real numbers such that

$$\log A_i \geq \max\Big\{\log \mathrm{h}(\alpha_i), \frac{|\log \alpha_i|}{3.3d}, \frac{1}{d}\Big\}, \quad i = 1, \ldots, n, \tag{19}$$

where log denotes the principal value of the logarithm. Let $b_1, \ldots, b_n$ be rational integers and put $B = \max\{\,|b_1|, \ldots, |b_n|, 3\}$. Further, set

$$\Lambda = \alpha_1^{b_1} \ldots \alpha_n^{b_n} - 1.$$

In Proposition 1, it will be convenient to make the following technical conditions :

$$B \geq \log A_n \exp\{4(n+1)(7 + 3\log(n+1))\} \tag{20}$$

and

$$7 + 3\log(n+1) \geq \log d. \tag{21}$$

Proposition 1 is a consequence of Corollary 10.1 of Waldschmidt [26].

Proposition 1. (M. Waldschmidt [26]). *If $\Lambda \neq 0$, $b_n = 1$ and (20), (21) hold, then*

$$|\Lambda| \geq \exp\Big\{-c_8(n) d^{n+2} \log A_1 \ldots \log A_n \, \log\Big(\frac{2nB}{\log A_n}\Big)\Big\}, \tag{22}$$

where $c_8(n) = 1500 \cdot 38^{n+1}(n+1)^{3n+9}$.

We remark that a recent explicit estimate of Baker and Wüstholz [1] for linear forms in logarithms would give here a smaller value for $c_8(n)$ in terms of n. However, the lower bound in (22) is better in terms of A_n which is essential for our present applications.

Proof. We denote by log the principal value of the logarithm. Setting $\alpha_0 = -1$, there is a $b_0 \in \mathbf{Z}$ such that $|b_0| \leq |b_1| + \ldots + |b_{n-1}| + 2 \leq nB$ and that

$$\log\big(\alpha_1^{b_1} \ldots \alpha_n^{b_n}\big) = \sum_{j=1}^{n} b_j \log \alpha_j + b_0 \log \alpha_0 := \Omega,$$

where $b_n = 1$. It suffices to deal with the case when $|\Lambda| \leq 1/3$. Since $|\log z| \leq 2|z-1|$ for any $z \in \mathbf{C}$ with $|z-1| \leq 1/3$, we get

$$|\Lambda| \geq |\Omega|/2. \tag{23}$$

After some calculations and under the conditions (20), (21), Corollary 10.1 of [26] implies the following inequality with the choice $E = e, f = 1/(3.3d)$ and $g = 2$:

$$|\Omega| \geq 2\exp\Big\{-c_8(n) d^{n+2} \log A_1 \ldots \log A_n \, \log\Big(\frac{2nB}{\log A_n}\Big)\Big\}.$$

Together with (23) this implies (22). $\square$

In Proposition 2, let $v = v_{\mathfrak{p}}$ be a finite place on $\mathbf{K}$, corresponding to the prime ideal $\mathfrak{p}$ of $\mathbf{K}$. Let p denote the rational prime lying below $\mathfrak{p}$, and denote by $|\,.\,|_v$ the non-archimedian valuation normalized as in Section 3. Instead of (19), assume now that $A_1, \ldots, A_n$ are real numbers such that

$$\log A_i \geq \max\{\log \mathrm{h}(\alpha_i), |\log \alpha_i|/(10d), \log p\}, \quad i = 1, \ldots, n. \tag{24}$$

The following proposition is a simple consequence of the main result of Kunrui Yu [27].

Proposition 2. (Kunrui Yu [27]). *Let*

$$\Phi = c_9(n)\big(d/\sqrt{\log p}\big)^{2(n+1)} p^d \log A_1 \ldots \log A_n \ \log(10nd\log A),$$

where $c_9(n) = 22000(9.5(n+1))^{2(n+1)}$ *and* $A = \max\{A_1, \ldots, A_n, e\}$. *If* $\Lambda \neq 0$ *then*

$$|\Lambda|_v \geq \exp\big\{-d(\log p)\Phi\log(dB)\big\}.$$

Further, if $b_n = 1$ *and* $A_n \geq A_i$ *for* $i = 1, \ldots, n-1$, *then* A *can be replaced by* $\max\{A_1, \ldots, A_{n-1}, e\}$ *and for any* δ *with* $0 < \delta \leq 1$, *we have*

$$|\Lambda|_v \geq \exp\big\{-d(\log p)\max\{\Phi\log(\delta^{-1}\Phi/\log A_n), \delta B\}\big\}.$$

Proof. This is a reformulation of the result presented in the introduction of Kunrui Yu [27]. □

Remark 6. We remark that, in Propositions 1 and 2, the condition $\mathbf{K} = \mathbf{Q}(\alpha_1, \ldots, \alpha_n)$ can be removed. It is enough to assume that $\mathbf{K}$ is an algebraic number field of degree d which contains $\alpha_1, \ldots, \alpha_n$. This observation will be needed in Section 5.

5. Proofs of the Theorem and the Corollary

Proof of the Theorem. Let x, y be an arbitrary but fixed solution of

$$\alpha x + \beta y = 1 \quad \text{in} \ \ x, y \in O_S^*. \tag{1}$$

We assume that $\mathrm{h}(x) \geq \mathrm{h}(y)$. Let $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ be a fundamental system of S-units in $\mathbf{K}$ satisfying the properties specified in Lemma 1. Then we can write

$$y = \zeta\varepsilon_1^{b_1} \ldots \varepsilon_{s-1}^{b_{s-1}} \tag{25}$$

with a root of unity ζ in $\mathbf{K}$ and with rational integers $b_1, \ldots, b_{s-1}$. Put $B = \max\big\{|b_1|, \ldots, |b_{s-1}|, 3\big\}$ and $S = \{v_1, \ldots, v_s\}$. Then (25) implies

$$\log|y|_{v_j} = \sum_{i=1}^{s-1} b_i \log|\varepsilon_i|_{v_j}, \qquad j = 1, \ldots, s-1,$$

whence, by (iii) of Lemma 1 and (12), we get

$$B \leq c_6 \sum_{j=1}^{s-1}\big|\log|y|_{v_j}\big| \leq 2dc_6\ \log\mathrm{h}(y) \leq 2dc_6\ \log\mathrm{h}(x) \tag{26}$$

with the $c_6 = c_6(d, s, \mathbf{K})$ specified in Lemma 1.

Let $v \in S$ for which $|x|_v$ is minimal. Setting $\alpha_s = \zeta\beta$ and $b_s = 1$, we deduce from (1) that

$$|\alpha x|_v = |\varepsilon_1^{b_1} \ldots \varepsilon_{s-1}^{b_{s-1}}\alpha_s^{b_s} - 1|_v. \tag{27}$$

We shall derive a lower bound for $|\alpha x|_v$.

First assume that v is infinite. In order to apply Proposition 1, put

$$\begin{aligned} \log A_i &= \delta_{\mathbf{K}}^{-1}\ \log\mathrm{h}(\varepsilon_i), \qquad i = 1, \ldots, s-1, \\ \log A_s &= \delta_{\mathbf{K}}^{-1}\ \log H. \end{aligned} \tag{28}$$

It is easy to check that

$$7 + 3\log(s+1) \geq \log d.$$

Further, we may assume that

$$B \geq \log A_s \exp\big\{4(s+1)(7+3\log(s+1))\big\}. \tag{29}$$

Indeed, (1) implies that

$$\mathrm{h}(x) \leq 2H^2 \mathrm{h}(y). \tag{30}$$

Further, it follows from (25) and (ii) of Lemma 1 that

$$\mathrm{h}(y) \leq \prod_{i=1}^{s-1} \mathrm{h}(\varepsilon_i)^{|b_i|} \leq \exp\{(s-1)c_5 R_S B\}. \tag{31}$$

Hence, if (29) does not hold, we get at once a bound for $\mathrm{h}(x)$ which is better than that in the Theorem.

We have $|\,.\,|_v = |\sigma(\,.\,)|^{d_v}$ for some $\sigma : \mathbf{K} \to \mathbf{C}$. Applying σ to equation (1) and then omitting σ everywhere, we may assume that $|\,.\,|_v = |\,.\,|^{d_v}$. On applying now Proposition 1 to (27) and using (i) of Lemma 1, we derive that

$$|\alpha x|_v \geq \exp\Big\{-c_{10} R_S \log H \, \log\Big(\frac{c_{11} B}{\log H}\Big)\Big\}, \tag{32}$$

where $c_{10} = d_v\, c_8(s)\, c_4 d^{s+2}\, \delta_{\mathbf{K}}^{-s}$ and $c_{11} = 2s\delta_{\mathbf{K}}$.

Since $|x|_v$ is minimal, we have

$$\mathrm{h}(x) = \mathrm{h}(1/x) \leq |x|_v^{-(s-1)/d}. \tag{33}$$

Hence it follows from (32), (26) and $|\alpha|_v \leq H^d$ that

$$\frac{\log \mathrm{h}(x)}{\log H} \leq \frac{2(s-1)}{d} c_{10} R_S \log\Big(\frac{c_{12} \log \mathrm{h}(x)}{\log H}\Big),$$

where $c_{12} = 2d\, c_6\, c_{11}$. This gives

$$\mathrm{h}(x) \leq \exp\{c_{13} R_S (\log^* R_S) \log H\} \tag{34}$$

with

$$c_{13} = 3^{s+26} d^3\, \delta_{\mathbf{K}}^{-s}\, s^{5s+12}.$$

We remark that in the particular case $S = S_\infty$, i.e. when $t = 0$, (34) implies the second part of the Theorem.

Next assume that v is finite. To apply Proposition 2, we put now

$$\begin{aligned} \log A_i &= \delta_{\mathbf{K}}^{-1} \log \mathrm{h}(\varepsilon_i) + \log^* P, \qquad i = 1, \ldots, s-1, \\ \log A_s &= \delta_{\mathbf{K}}^{-1} \log H + \log^* P. \end{aligned} \tag{35}$$

Using (i) of Lemma 1, we get

$$\begin{aligned} \log A_1 \ldots \log A_{s-1} &\leq \prod_{i=1}^{s-1} \big(\delta_{\mathbf{K}}^{-1} \, \log \mathrm{h}(\varepsilon_i)\big) \left(\sum_{j=0}^{s-1} \binom{s-1}{j} (d \log^* P)^j - (d \log^* P)^{s-1} \right) + (\log^* P)^{s-1} \\ &\leq (\log^* P)^{s-2} (c_{14} R_S + \log^* P) \end{aligned}$$

with $c_{14} = (s/d)\, \big((s-1)!\big)^2\, \delta_{\mathbf{K}}^{-(s-1)}$. Together with the second ineqality of Lemma 3 this gives

$$\log A_1 \ldots \log A_{s-1} \leq 2c_{14} R_S (\log^* P)^{s-2}. \tag{36}$$

We distinguish two cases. First assume that $\log H < c_5 R_S$. Then, by Lemmas 1 and 3, we have

$$\log A := \max_{1 \le i \le s} \log A_i \le c_{15} R_S \tag{37}$$

with $c_{15} = c_5 \delta_{\mathbf{K}}^{-1} + (c_7 \log 2)^{-1}$. We apply now to (27) the first part of Proposition 2. Putting

$$\Phi = c_{16} \frac{P^d}{(\log^* P)^{s+1}} \log A_1 \ldots \log A_s \ \log(10sd \log A)$$

with $c_{16} = c_9(s)\,(d^2/\log 2)^{s+1}$, we infer that

$$|\alpha x|_v \ge \exp\{-d(\log^* P)\Phi \log(dB)\}, \tag{38}$$

whence, by (33), (26) and $|\alpha|_v \le H^d$,

$$\log \mathrm{h}(x) \le 2(s-1)(\log^* P)\ \Phi\ \log(c_{17} \log \mathrm{h}(x))$$

follows with $c_{17} = 2d^2 c_6$. Together with (36), (37) and $\log H < c_5 R_S$ this gives

$$\mathrm{h}(x) \le \exp\big\{c_{18} P^d R_S (\log^* R_S)(\log^*(P R_S)/\log^* P) \log H\big\} \tag{39}$$

where

$$c_{18} = 3^{26}(18 d^2/\delta_{\mathbf{K}})^{s+1}\, s^{4s+7}.$$

Next assume that $\log H \ge c_5 R_S$. Then, by Lemmas 1 and 3, we have $A_s \ge A_i$ for $i = 1, \ldots, s-1$ and

$$\log A := \max_{1 \le i \le s-1} \log A_i \le c_{15} R_S. \tag{40}$$

Consider now the above defined Φ with this value of $\log A$. First we give an upper bound for $\mathrm{h}(x)$ in terms of Φ.

If $B < \Phi(\log^* P)/(c_5 R_S)$ then (30), (31) and (35) imply that

$$\mathrm{h}(x) \le 2H^2 \exp\{(s-1)\Phi \log^* P\} < \exp\{s\,\Phi \log^* P\}. \tag{41}$$

Assume now that $B \ge \Phi(\log^* P)/(c_5 R_S)$. We apply the second part of Proposition 2 to (27). Putting $\delta = \Phi(\log^* P)/(B c_5\, R_S)$ we obtain

$$|\alpha x|_v \ge \exp\Big\{-d(\log^* P)\Phi \log\Big(\frac{B c_5\, R_S}{\log^* P\ \log A_s}\Big)\Big\}.$$

Hence, proceeding again as above, we deduce that

$$\frac{\log \mathrm{h}(x)}{\log^* P\ \log A_s} \le 2(s-1)(\Phi/\log A_s)\ \log\left(\frac{c_{19}\, R_S \log \mathrm{h}(x)}{\log^* P\ \log A_s}\right)$$

with $c_{19} = 2d\, c_6\, c_5$. From this we infer as above that

$$\mathrm{h}(x) \le \exp\big\{c_{20} \Phi (\log^* P) \log^*(P R_S)\big\} \tag{42}$$

where $c_{20} = 19(s-1)\log(c_{16})$.

The right hand side of (42) is greater than that of (41). Lemma 3, (35) and $\log H \ge c_5 R_S$ imply that $\log A_s < c_{21} \log H$ with $c_{21} = (c_5\, c_7 \log 2)^{-1} + \delta_{\mathbf{K}}^{-1}$. Hence, estimating from above Φ, we obtain in both cases that

$$\mathrm{h}(x) \le \exp\big\{c_{18} P^d R_S (\log^* R_S)(\log^*(P R_S)/\log^* P) \log H\big\}, \tag{43}$$

with the constant c_{18} defined above. However, it is easy to verify that both c_{13} in (34) and c_{18} in (39) and (43) are less than $c_1 = c_1(d, s, \mathbf{K})$ specified in the Theorem. This completes the proof of our assertion. $\square$

Proof of the Corollary. Let x_1, x_2, x_3 be a solution of (6). Then, by Lemma 2, there are $\varepsilon_i \in O_S^*$ such that

$$\mathrm{h}(\varepsilon_i x_i) \leq N^{1/d} \exp\{c_3 R_K + t h_K \log^* P\} \tag{44}$$

with the constant c_3 specified in Lemma 2. Putting

$$\alpha = \frac{\alpha_1(\varepsilon_1 x_1)}{\alpha_3(\varepsilon_3 x_3)}, \quad \beta = \frac{\alpha_2(\varepsilon_2 x_2)}{\alpha_3(\varepsilon_3 x_3)},$$

$x = -\varepsilon_3/\varepsilon_1$, $y = -\varepsilon_3/\varepsilon_2$ is a solution of equation (1).

We have

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \leq \exp\big\{2c_3(R_K + t h_K \log^* P + \log(HN))\big\}.$$

Now our Theorem provides an explicit upper bound for $\max\{\mathrm{h}(x), \mathrm{h}(y)\}$. Together with (44), this implies (7) with the choice $\varepsilon = -\varepsilon_3$. $\square$

Acknowledgements : Most of the arguments used in the present paper were found independently by the two authors. The first named author would like to thank Professor Maurice Mignotte for his constant encouragements.

REFERENCES

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

[2] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), 355-369.

[3] E. Bombieri, *Effective diophantine approximation on G_m*, Ann. Scuola Norm. Sup. Pisa (IV) 20 (1993), 61-89.

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London, 2nd ed., 1967.

[5] B. Brindza, *On the generators of S-unit groups in algebraic number fields*, Bull. Austral. Math. Soc. 43 (1991), 325-329.

[6] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Die Grundlehren der mathematischen Wissenschaften, Band 99, Springer Verlag, Berlin, 1959.

[7] E. Dobrowolski, *On the maximal modulus of conjugates of an algebraic integer*, Bull. Acad. Polon. Sci. 26 (1978), 291-292.

[8] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta. Arith. 34 (1979), 391-401.

[9] A. Dubickas, *On a conjecture of A. Schinzel and H. Zassenhaus*, Acta Arith. 63 (1993), 15-20.

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

[11] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *S-unit equations and their applications*, in "New Advances in Transcendence Theory" (A. Baker ed.), pp. 110-174. Cambridge University Press, 1988.

[12] E. Friedman, *Analytic formulas for regulators of number fields*, Invent. Math. 98 (1989), 599-622.

[13] K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. 54 (1979), 583-600.

[14] K. Győry, *On the solutions of linear diophantine equations in algebraic integers of bounded norm*, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. 22/23 (1980), 225-233.

[15] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's papers in pure and applied mathematics, No. 56, Kingston, Canada, 1980.

[16] K. Győry, *Some recent applications of S-unit equations*, Journées arithmétiques de Genève 1991, (D. F. Coray, Y.-F. S. Pétermann eds.), Astérisque, 209. Soc. Math. France, 1992, pp. 17-38.

[17] K. Győry, *Bounds for the solutions of decomposable form equations*, to appear.

[18] L. Hajdu, *A quantitative version of Dirichlet's S-unit theorem in algebraic number fields*, Publ. Math. Debrecen 42 (1993), 239-246.

[19] S. V. Kotov and L. A. Trelina, *S-ganze Punkte auf elliptischen Kurven*, J. Reine Angew. Math. 306 (1979), 28-41.

[20] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, Berlin, 1983.

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

[22] A. Pethő, *Beiträge zur Theorie der S-Ordnungen*, Acta. Math. Acad. Sci. Hungar. 37 (1981), 51-57.

[23] W. M. Schmidt, *Integer points on curves of genus* 1, Compositio Math. 81 (1992), 33-59.

[24] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[25] V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Math. 1559, Springer Verlag, 1993.

[26] M. Waldschmidt, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. 45 (1993), 176-224.

[27] Kunrui Yu, *Linear forms in p-adic logarithms* III, Compositio Math. 91 (1994), 241-276.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG (FRANCE)

e-mail : bugeaud@pari.u-strasbg.fr

Kálmán Győry
Institute of Mathematics
Kossuth Lajos University
4010 DEBRECEN (HUNGARY)