On the number of solutions of linear equations in units of an algebraic number field.

Autor(en): **Györy, K.**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **54 (1979)**

PDF erstellt am: **28.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-41597

Comment. Math. Helvetici 54 (1979) 583–600 Birkhäuser Verlag, Basel

On the number of solutions of linear equations in units of an algebraic number field

K. Győry

1. Introduction

Let $\mathbf{K}$ be an algebraic number field of degree n over the field $\mathbf{Q}$ of rational numbers, and let r denote the number of fundamental units in $\mathbf{K}$. As is well-known, many diophantine problems lead to equations of the form

$$\alpha_1 x_1 + \alpha_2 x_2 = \beta \tag{1}$$

where the coefficients α_1, α_2, β are non-zero algebraic integers and the variables x_1, x_2 are units in $\mathbf{K}$ (see e.g. Siegel [22], [23], Skolem [25], Nagell [15], [17], Mordell [14], Baker [1], [3], Sprindžuk [26], [27], the author [7], [9] and the references mentioned there). We may suppose that in (1) $m = |N_{K/Q}(\beta)| \geq m_k = |N_{K/Q}(\alpha_k)|$ for $k = 1, 2$. It follows from a general theorem of Siegel [22] concerning the Thue equation that the number N of solutions of (1) is finite (and these solutions can be effectively determined by Baker's method, cf. [3]). This result on the finiteness of N has various generalizations, see e.g. Mahler [13] and Lang [11]. From the point of view of some applications of (1) it is crucial to have a good upper bound for N. The best known bound for N is $3^{2r}c'(n)$ when $m \geq \min_k c''(n, \alpha_k)$. It can be deduced from a recent theorem of Choodnovsky ([4], Theorem 2.1, (2)) on the number of solutions of the Thue equation. In [4] $c'(n)(\geq 1)$ and $c''(n, \alpha_k)$ are effectively computable in terms of n and α_k but they are not explicitly computed.

In this paper we give a direct proof for estimating N which enables us to considerably improve the above quoted estimate. Using Baker's method we prove that if m is sufficiently large relative to $\min(m_1, m_2)$ and certain parameters of $\mathbf{K}$ then $N \leq r+1$. This upper bound is best possible for $r \leq 1$. Further, for small values of m our result does not remain valid in general.

We prove our main result in a more general form, for the number of solutions of (1) in S-units x_1, x_2 of $\mathbf{K}$. Our theorem has several applications which will be published in separate papers. It implies e.g. [10] that in our Theorem 1(a) in [6] there exists no so-called exceptional polynomial $f(x)$. The explicit and good dependence on r in our bound is particularly useful in certain applications.

2. The main result

Throughout this paper $\mathbf{K}$ will denote an algebraic number field of degree $n \geq 1$ with ring of integers $\mathbf{Z}_K$. Let R_K and h_K be the regulator and the class number of $\mathbf{K}$. Let $R_K^* = \max(R_K, e)$ and let r be the number of fundamental units in $\mathbf{K}$. Denote by S a finite set of normalized valuations $|\cdots|_v$ of $\mathbf{K}$ containing the set S_∞ of the archimedean valuations. For $\alpha \in \mathbf{K}$ put $\|\alpha\|_v = |\alpha|_v^{n_v}$ where $n_v = [\mathbf{K}_v : \mathbf{Q}_v]$. Suppose that the non-archimedean valuations of S belong to the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and that these prime ideals lie above rational primes not exceeding P (≥ 2). U_S will denote the group of S-units in $\mathbf{K}$. U_S obviously coincides with the group U_K of units in $\mathbf{K}$ for $S = S_\infty$.

Let α_1, α_2 and β be non-zero algebraic integers in $\mathbf{K}$ with $m_k = \prod_{v \in S} \|\alpha_k\|_v$, $k = 1$, 2 and $m = \prod_{v \in S} \|\beta\|_v$. Consider the equation

$$\alpha_1 x_1 + \alpha_2 x_2 = \beta \tag{2}$$

in S-units x_1, x_2 of $\mathbf{K}$. We may suppose without loss of generality that $m \geq \max(m_1, m_2)$. It follows from a theorem of Parry [19] on the Thue-Mahler equation that the number of solutions of (2) is finite and can be estimated from above in terms of $\mathbf{K}$, S, α_1, α_2 and β.[(1)]

In this paper we derive an upper bound for the number of solutions of (2) in a more direct way, without using the Thue–Mahler equation. This new approach enables us to establish a much more precise result on the equation (2).

THEOREM. *Let* $\mathbf{K}$, S, α_1, α_2 *and* β *be as above. Suppose that*

$$\log m > \varepsilon^{-1} \log\left(\frac{2}{\varepsilon}\right)(25(r+s+3)n)^{20(r+2)+13s} P^n R_K$$

$$\cdot (R_K + h_K \log P)^s (R_K + s h_K \log P)[s(R_K + h_K \log P) + 1] \log(R_K^*(1 + s h_K P)) \tag{3}$$

and that $\min_k (m_k) \leq m^{1-\varepsilon}$ *for some* ε *with* $0 < \varepsilon \leq 1$. *Then the number of solutions of* (2) *in* S*-units* x_1, x_2 *of* $\mathbf{K}$ *is not greater than* $r + 4s + 1$.

---

[1] In case $\mathbf{K} = \mathbf{Q}$ better and explicit estimates can be deduced from a result of Lewis and Mahler [12].

Remark. If in our theorem $\max_k (\log m_k) \le (\log m)^{1-\varepsilon}$ with some ε, $0<\varepsilon\le 1$, and $m > C(\varepsilon, n, R_K, h_K, s, P)$ (where C can be expressed explicitly in terms of ε, n, R_k, h_K, s and P) then the number of solutions of (2) is at most $r+2s+1$. Further, if in particular $\mathbf{K}=\mathbf{Q}$ and $s\ge 1$, this bound can be improved to $2s$. For $s=1$ this result is best possible.

In case $S=S_\infty$ our theorem implies the following

COROLLARY. *Let* $\mathbf{K}$, α_1, α_2 *and* β *be defined as above. If*

$$\log |N_{K/Q}(\beta)| > \varepsilon^{-1} \log \left(\frac{2}{\varepsilon}\right)(25(r+3)n)^{20(r+2)} R_K^2 \log R_K^* \tag{4}$$

and $\min_k |N_{K/Q}(\alpha_k)| \le |N_{K/Q}(\beta)|^{1-\varepsilon}$ *for some* ε *with* $0<\varepsilon\le 1$, *then the number of solutions of* (2) *in units* x_1, x_2 *of* $\mathbf{K}$ *is not greater than* $r+1$.

It is easily verified that for number fields $\mathbf{K}$ of unit rank $r\le 1$ the bound $r+1$ is already best possible.

Nagell proved [16] that for every $n\ge 5$ there exists a number field $\mathbf{K}$ of degree n such that $x_1+x_2=1$ has at least $3(2n-3)$ solutions in units x_1, x_2 of $\mathbf{K}$. In other words, if m is small or $\beta=\alpha_1=\alpha_2$ our theorem is not true in general. In these cases we can derive an explicit upper bound for the number of solutions of (2) by using our Lemma 6, but this bound depends on r, s, R_K, h_K and P.

Finally we mention an application of our Corollary. Newman showed [18] that if $[\mathbf{K}:\mathbf{Q}]=n\ge 4$ and in $\mathbf{K}$ there is an arithmetic progression η, $\eta+\beta, \ldots, \eta+k\beta$ consisting of units then $k\le n-1$. When β satisfies (4) and $r<n-2$, our Corollary improves Newman's estimate to $k\le r+1$.

3. Lemmas

In order to prove our theorem we need some lemmas. We keep the notations of Section 2. We suppose that there are r_1 real conjugate fields to $\mathbf{K}$ and $2r_2$ complex conjugates to $\mathbf{K}$ and that they are chosen in the usual manner: if α is in $\mathbf{K}$ then $\alpha^{(j)}$ is real for $j=1,\ldots,r_1$ and $\alpha^{(j+r_2)}=\overline{\alpha^{(j)}}$ for $j=r_1+1,\ldots,r_1+r_2$. Let $e_j=1$ if $1\le j\le r_1$ and $e_j=2$ if $r_1+1\le j\le r_1+r_2$.

As usual, $\overline{|\alpha|}$ will denote the maximum of the absolute values of the conjugates of an algebraic number α. We denote by $H(\alpha)$ the height (in the usual sense) of α.

LEMMA 1. *If $r \geq 1$, then there exist independent units $\eta_1, \ldots, \eta_r$ in* **K** *such that*

$$\prod_{i=1}^{r} \max(\log \overline{|\eta_i|}, 1) < c_1 R_K \tag{5}$$

and the absolute values of the elements of the inverse matrix of $(e_j \log|\eta_i^{(j)}|)_{1 \leq i,j \leq r}$ do not exceed c_2, where

$$c_1 = \left(\frac{6m^2}{\log n}\right)^r \quad \textit{and} \quad c_2 = \frac{6r!n^2}{\log n}.$$

Proof. This is a special case of Lemma 2 of [9]. It follows from the work [24] of Siegel (combining his argument with a recent result of Dobrowolski [5]).

If $r \geq 1$, let $\eta_1, \ldots, \eta_r$ be fixed units in $\mathbf{Z}_K$ with the properties specified in Lemma 1 and let U denote the multiplicative group generated by $\eta_1, \ldots, \eta_r$. In case $r = 0$ let $U = \{1\}$ and $c_1 = c_2 = 1$.

LEMMA 2. *Let α be a non-zero element in* **K** *with $|N_{K/Q}(\alpha)| = M$. There exists a unit $\varepsilon \in U$ such that*

$$|\log|M^{-1/n}(\alpha\varepsilon)^{(j)}|| \leq \frac{c_1 r}{2} R_K, \qquad j = 1, \ldots, n. \tag{6}$$

Proof. This is a special case of Lemma 3 in [9].

Let $\alpha_1, \ldots, \alpha_m$ be $m \geq 2$ non-zero algebraic numbers in **K** with heights respectively not exceeding $A_1, \ldots, A_m$ (with $\log\log A_i \geq 1$). We further suppose that $A_1 \leq A_2 \leq \cdots \leq A_m = A'$ and we set

$$\Omega' = (\log A_1) \cdots (\log A_{m-1}), \qquad c_3 = (25(m+1)n)^{10(m+1)}$$

and $T = c_3 \Omega' \log \Omega'$. Write

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_{m-1} \log \alpha_{m-1} - \log \alpha_m$$

where $b_1, \ldots, b_{m-1}$ are rational integers with absolute values at most B and all the logarithms have their principal values.

LEMMA 3 (A. J. van der Poorten and J. H. Loxton). *If* $\Lambda \neq 0$ *and for some* $\delta > 0$

$$|\Lambda| < e^{-\delta B},$$

then $B < \delta^{-1} T \log(\delta^{-1} T) \log A'$ *or* $B < c_3^{-1/2} T \log(c_3^{-1/2} T) \log A'$ *according as* $\delta \leq c_3^{-1/2} T$ *or* $\delta > c_3^{-1/2} T$.

Proof. This deep result is Theorem 3 in [21]. It is an explicit form of Theorem 2 of Baker [2].

We shall use the following consequence of Lemma 3. Put

$$c_4 = (25(m+2)n)^{10(m+2)} \quad \text{and} \quad T' = c_4 \Omega' \log \Omega'.$$

With the above notation we have

LEMMA 4. *If* $0 < \delta < 2mc_4^{-1/2} T'$ *and*

$$0 < |\alpha_1^{b_1} \cdots \alpha_{m-1}^{b_{m-1}} \alpha_m^{-1} - 1| < e^{-\delta B}$$

then $B < 4e\delta^{-1} T' \log(4em\delta^{-1} T') \log A'$.

Proof. Lemma 4 can be deduced from Lemma 3 by a well-known argument. Let $b_m = -1$. By taking the principal values of the logarithms we get

$$\log(\alpha_1^{b_1} \cdots \alpha_m^{b_m}) = \sum_{i=1}^{m} b_i \log \alpha_i + b_0 \log(-1)$$

where $|b_0| \leq |b_1| + \cdots + |b_m| \leq mB$. Since $|\log z| \leq 2|z-1|$ for $|z-1| \leq \frac{1}{3}$, it is clear that Lemma 4 is a direct consequence of Lemma 3.

Let $\mathfrak{p}$ be a prime ideal of $\mathbf{K}$ lying above the rational prime p. Following van der Poorten [20], we write $e_\mathfrak{p}$ for the ramification index of $\mathfrak{p}$ and $f_\mathfrak{p}$ for its residue class degree, so $N_{\mathbf{K}/\mathbf{Q}}(\mathfrak{p}) = p^{f_\mathfrak{p}}$. Let $g_\mathfrak{p} = [\frac{1}{2} + e_\mathfrak{p}/(p-1)]$ and $G_\mathfrak{p} = p^{f_\mathfrak{p} g_\mathfrak{p}}(p^{f_\mathfrak{p}} - 1)$. Let $\alpha_1, \ldots, \alpha_m, \Omega'$ and A' be defined as in Lemma 3 and write $c_5 = (16(m+1)n)^{12(m+1)}$, $T^* = c_5 G_\mathfrak{p} \Omega' \log \Omega'$.

LEMMA 5 (A. J. van der Poorten). *If* $0 < \delta^* < 1$ *and there exist rational integers* $b_1, \ldots, b_{m-1}$ *with absolute values at most* B *such that*

$$\infty > \operatorname{ord}_\mathfrak{p}(\alpha_1^{b_1} \cdots \alpha_{m-1}^{b_{m-1}} \alpha_m^{-1} - 1) > \delta^* B$$

then $B < (\delta^*)^{-1} T^* \log((\delta^*)^{-1} T^*) \log A'$.

Proof. This is Theorem 4 of van der Poorten [20].

We remark that $G_p \le p^n$ if $p > 3$ and $G_p \le p^{2n}$ if $p \le 3$.

Let S be defined as in Section 2 and put $G_S = \max_{1\le i\le s} G_{p_i}$ for $s \ge 1$ and $G_S = 1$ for $s = 0$. Denote by $\mathcal{N}$ the set of algebraic integers α in $\mathbf{K}$ satisfying

$$|N_{K/Q}(\alpha)| \le N.$$

With the notation introduced above we have the following

LEMMA 6. *Let α_1, α_2, α_3 be non-zero algebraic integers in $\mathbf{K}$ with $\max_{1\le k\le 3} \overline{|\alpha_k|} \le A$. If x_1, x_2 and x_3 are non-zero algebraic integers in $\mathbf{K}$ satisfying*

$$\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_3 = 0 \quad \textit{and} \quad x_1, x_2, x_3 \in \mathcal{N}(U_S \cap \mathbf{Z}_K) \tag{7}$$

then for some $\sigma \in U_S \cap \mathbf{Z}_K$ and $\rho_k \in \mathbf{Z}_K$ we have

$$x_k = \sigma \rho_k, \qquad k = 1, 2, 3 \tag{8}$$

and

$$\begin{aligned} \max_{1\le k\le 3} \overline{|\rho_k|} < \exp\{ & c_6 G_s (\log P)[s(R_K + h_K \log P) \log(1 + sR_K h_K) + 1] \\ & \cdot R_K((s+1)R_K + sh_K \log P) \\ & \qquad \times (R_K + h_K \log P)^s [\log R_K^* + s \log(1 + R_K h_K \log P)]^2 \\ & \cdot [R_K + sh_K \log P + \log(AN)]\}, \end{aligned} \tag{9}$$

where $c_6 = (25(r+s+3)n)^{19r+13s+2rs+36}$.

As is known, this statement, with weaker estimates, was earlier implicitly proved in several papers. In the special case $s = 0$ we obtained in [9] a slightly better result. Our Lemma 6 has several applications. By using this lemma we can improve, for example, our estimates established in [8].

Put $p_i^{h_K} = (\pi_i)$ with some $\pi_i \in \mathbf{Z}_K$ for $i = 1, \ldots, s$. As will be apparent from the proof of Lemma 6, in (8) σ may be chosen in the form $\eta \pi_1^{a_1} \cdots \pi_s^{a_s}$ where $\eta \in U_K$ and $a_1, \ldots, a_s$ are non-negative rational integers.

Proof of Lemma 6. Since in the case $s = 0$ we obtained in [9] a better estimate than that occurring in (9), in what follows we suppose $s > 0$. By hypothesis we have

$$x_k = \delta_k \sigma_k, \qquad k = 1, 2, 3, \tag{10}$$

where

$$|N_{K/Q}(\delta_k)| \le N \tag{11}$$

and

$$(\sigma_k) = \mathfrak{p}_1^{u_{1k}} \cdots \mathfrak{p}_s^{u_{sk}}. \tag{12}$$

Write $u_{ik} = h_K v_{ik} + r_{ik}$ with $0 \le r_{ik} < h_K$ and $\mathfrak{p}_i^{h_K} = (\pi_i)$ with $\pi_i \in \mathbf{Z}_K$ for $i = 1, \ldots, s$. By Lemma 2 we may suppose that

$$\max_i \overline{|\pi_i|} \le \exp\left\{\frac{c_1 r}{2} R_K + h_K \log P\right\}. \tag{13}$$

Further, by (10) $(\delta_k)\mathfrak{p}_1^{r_{1k}} \cdots \mathfrak{p}_s^{r_{sk}}$ is a principal ideal with norm at most NP^{snh_K}. Applying again Lemma 2 we may write

$$x_k = \varepsilon_k \gamma_k \pi^{v_{1k}} \cdots \pi_s^{v_{sk}}, \qquad k = 1, 2, 3, \tag{14}$$

where ε_k is a unit in $\mathbf{K}$ and γ_k is an algebraic integer satisfying

$$\overline{|\gamma_k|} \le N^{1/n} P^{sh_K} \exp\left\{\frac{c_1 r}{2} R_K\right\}, \qquad k = 1, 2, 3. \tag{15}$$

Put $a_i = \min_k v_{ik}$ and $v'_{ik} = v_{ik} - a_i$ for $k = 1, 2, 3$ and $i = 1, \ldots, s$. Suppose, for convenience, that $V = \max_{1 \le i \le s} v'_{ik} = v'_{11}$ and $v'_{13} = 0$. If $r \ge 1$, let $\eta_1, \ldots, \eta_r$ be units with the properties specified in Lemma 1. By Lemma 2 we may write

$$\varepsilon_1/\varepsilon_3 = \varepsilon'_1 \eta_1^{w_{11}} \cdots \eta_r^{w_{r1}}, \qquad \varepsilon_2/\varepsilon_3 = \varepsilon'_2 \eta_1^{w_{12}} \cdots \eta_r^{w_{r2}} \tag{16}$$

where $w_{11}, \ldots, w_{r1}, w_{12}, \ldots, w_{r2}$ are rational integers and ε'_1, ε'_2 are units in $\mathbf{K}$ such that

$$\max(\overline{|\varepsilon'_1|}, \overline{|\varepsilon'_2|}) \le \exp\left\{\frac{c_1 r}{2} R_K\right\}. \tag{17}$$

(16) and (17) are valid both for $r \ge 1$ and for $r = 0$ (when the η_j do not occur in (16)). Put $\varepsilon'_3 = 1$ and $\gamma'_k = \varepsilon'_k \gamma_k$, $k = 1, 2, 3$. Then we have by (15) and (17)

$$\max_k \overline{|\gamma'_k|} \le N^{1/n} P^{sh_K} \exp\{c_1 r R_K\}. \tag{18}$$

Consequently

$$x_k = \sigma\rho_k$$

where $\sigma = \varepsilon_3\pi_1^{a_1}\cdots\pi_s^{a_s}$, $\rho_k = \gamma_k'\eta_1^{w_{1k}}\cdots\eta_r^{w_{rk}}\pi_1^{v_{1k}'}\cdots\pi_s^{v_{sk}'}$ and $w_{13} = \cdots = w_{r3} = 0$. We shall prove that σ and ρ_k, $k = 1, 2, 3$, have the required properties.

From (7) we get

$$\alpha_1\rho_1 + \alpha_2\rho_2 + \alpha_3\rho_3 = 0, \tag{19}$$

whence

$$\Gamma = -\frac{\alpha_2\rho_2}{\alpha_3\rho_3} - 1 = \frac{\alpha_1\rho_1}{\alpha_3\rho_3} \neq 0. \tag{20}$$

We are now going to derive an upper bound for $H = \max(V, W)$ where $W = \max_{j,k} |w_{jk}|$. We assume that

$$H > 16(r+1)^2 n^3 c_1 c_2 s R_K (R_K + h_K \log P)^s [R_K + s h_K \log P + \log(AN)]. \tag{21}$$

First suppose $V \geq \tau H$ where $\tau = [16rnc_2 s(rc_1 R_K + h_K \log P) + 1]^{-1}$. Since

$$\operatorname{ord}_{\mathfrak{p}_1} \alpha_3 \leq \frac{n \log A}{\log 2},$$

it follows from (20) that

$$\infty > \operatorname{ord}_{\mathfrak{p}_1} \Gamma > V - \frac{n \log A}{\log 2},$$

so, by (21),

$$\infty > \operatorname{ord}_{\mathfrak{p}_1}\left(-\frac{\alpha_2\gamma_2'}{\alpha_3\gamma_3'}\eta_1^{w_{12}}\cdots\eta_r^{w_{r2}}\pi_1^{v_{12}'-v_{13}'}\cdots\pi_s^{v_{s2}'-v_{s3}'} - 1\right) > \frac{\tau}{2} H. \tag{22}$$

Let us apply now Lemma 5 with $\mathfrak{p}_1$ and $\delta^* = \tau/2$. Write $A_j = \max(H(\eta_j), e^e)$ for $j = 1, \ldots, r$ if $r \geq 1$ and $A_j = \max(H(\pi_{j-r}), e^e)$ for $j = r+1, \ldots, r+s$. Since

$$H(\eta_j) \leq (2\overline{|\eta_j|})^n \quad \text{and} \quad H(\pi_i) \leq (2\overline{|\pi_i|})^n,$$

so by Lemma 1

$$\log A_j \le 2n \max(\log \overline{|\eta_j|}, 1) < 2nc_1R_K, \qquad j=1,\dots,r \tag{23}$$

and by (13)

$$\log A_j < 2n(c_1rR_K + h_K \log P), \qquad j=r+1,\dots,r+s. \tag{24}$$

Thus, by Lemma 1 we have

$$\Omega' = \log A_1 \cdots \log A_{r+s} < c_1(2n)^{r+s}R_K(c_1rR_K + h_K \log P)^s. \tag{25}$$

Further, we have by (18)

$$H\left(-\frac{\alpha_2\gamma_2'}{\alpha_3\gamma_3'}\right) \le (\overline{|\alpha_2\gamma_2'|} + \overline{|\alpha_3\gamma_3'|})^n \le (2A)^n NP^{snh_K} \exp\{2c_1nrR_K\} = A' \tag{26}$$

where $A' \ge A_j$ for each j. Define $T^* = c_7G_S\Omega' \log \Omega'$ with $c_7 = (16(r+s+2)n)^{12(r+s+2)}$. By Lemma 5 we get from (22)

$$H < \frac{2}{\tau} T^* \log\left\{\frac{2}{\tau} T^*\right\} \log A' < \frac{4}{\tau} c_7G_S \log\left\{\frac{2}{\tau} c_7G_S\right\}\Omega'(\log \Omega')^2 \log A'. \tag{27}$$

Suppose now that $V < \tau H$ when $V < W = H$ and $r \ge 1$. Assume, for convenience, that $W = |w_{11}|$. Then we obtain

$$w_{11} \log|\eta_1^{(j)}| + \cdots + w_{r1} \log|\eta_r^{(j)}| = \log|\rho_1^{(j)}| - \log|\gamma_1'^{(j)}| - \sum_i v_{i1}' \log|\pi_i^{(j)}|$$

for each conjugate with $j=1,\dots,r$. Suppose that the right sides attain their maximum in absolute value for $j=J$, $1 \le J \le r$. By Lemma 1 we get

$$W \le 2rc_2\left\{|\log|\rho_1^{(J)}|| + |\log|\gamma_1'^{(J)}|| + \sum_i v_{i1}' |\log|\pi_i^{(J)}||\right\}.$$

Thus, by (13), (18) and (21) we obtain

$$\begin{aligned}|\log|\rho_1^{(J)}|| &\ge \frac{1}{2rc_2} W - (\log N + snh_K \log P + c_1rnR_K) - \tau Wsn(c_1rR_K + h_K \log P)\\ &\ge \frac{3}{8rc_2} H.\end{aligned}$$

But we have

$$\log|N_{K/Q}(\rho_1)|=\log|N_{K/Q}(\gamma_1')|+\sum_i v_{i1}'\log|N_{K/Q}(\pi_i)|$$
$$\leq \log N+snh_K\log P+c_1rnR_K+\tau Hsnh_K\log P\leq \frac{1}{8rc_2}H.$$

Hence

$$\log|\rho_1^{(g)}|\leq -\frac{1}{4r(n-1)c_2}H$$

for some $1\leq g\leq n$. Further it is easy to see that

$$\log\left|\frac{\alpha_1^{(g)}}{\alpha_3^{(g)}\rho_3^{(g)}}\right|\leq \log(2A)+(n-1)\log\overline{|\alpha_3\rho_3|}\leq \frac{1}{8r(n-1)c_2}H.$$

Thus we have

$$0<|\Gamma^{(g)}|=\left|\frac{\alpha_1^{(g)}\rho_1^{(g)}}{\alpha_3^{(g)}\rho_3^{(g)}}\right|<e^{-\delta H} \tag{28}$$

where $\delta=(8n^2c_2)^{-1}$. We can now apply Lemma 4 in a similar way as we applied Lemma 5 before. Write $c_8=(25(r+s+3)n)^{10(r+s+3)}$ and $T'=c_8\Omega'\log\Omega'$. Since $\delta\leq 2(r+s+1)c_8^{-1/2}T'$, by Lemma 4 we have

$$H<32en^2c_2T'\log(32e(r+s+1)n^2c_2T')\log A'$$

and, by (25) and (26), we get

$$H<32en^2c_2c_8\log(32(r+s+1)n^2c_2c_8)\Omega'(\log\Omega')^2\log A'. \tag{29}$$

It is easily seen that the right hand sides of (27) and (29) can be estimated from above by

$$(25(r+s+3)n)^{14r+12s+31}G_S(\log P)$$
$$\times[s(R_K+h_K\log P)\log(1+sh_KR_K)+1]\cdot\Omega'(\log\Omega')^2\log A'.$$

So by (25) we have

$$H<c_9G_S(\log P)[s(R_K+h_K\log P)\log(1+sh_KR_K)+1]R_K(R_K+h_K\log P)^s$$
$$\cdot[\log R_K^*+s\log(1+R_Kh_K\log P)]^2[R_K+sh_K\log P+\log(AN)] \tag{30}$$

where $c_9=(25(r+s+3)n)^{17.5r+13s+2rs+34.5}$. Finally, by virtue of (13), (18), (23) and (30)

$$\overline{|\rho_k|}\le\overline{|\gamma_k'|}\left(\prod_{j=1}^{r}\overline{|\eta_j|}^{n-1}\right)^H\cdot\left(\prod_{i=1}^{s}\overline{|\pi_i|}\right)^H$$

$$\le\exp\{c_9n(r+1)c_1G_S(\log P)[s(R_K+h_K\log P)\log(1+sh_KR_K)+1]$$

$$\cdot R_K((s+1)R_K+sh_K\log P)(R_K+h_K\log P)^s[\log R_K^*+s\log(1+R_Kh_K\log P)]^2$$

$$\cdot[R_K+sh_K\log P+\log(AN)]\}.$$

Since $c_9n(r+1)c_1\le(25(r+s+3)n)^{19r+13s+2rs+36}$, (9) is proved.

4. Proof of the theorem

If $r+s=0$ and x_1, x_2 is a solution of (2) then x_1 and x_2 are roots of unity. Assume that x_1', x_2' is another solution of (2) and $m_1\le m^{1-\varepsilon}$. Then we have $\beta(x_2'-x_2)=\alpha_1(x_1x_2'-x_1'x_2)$ and, by taking the norm on both sides, we arrive at a contradiction.

We suppose now that $r+s>0$ and that (2) is solvable in S-units x_1, x_2. We first show that we can make certain assumptions without loss of generality. Write $(\beta)=\mathfrak{a}\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_s^{b_s}$ where $\mathfrak{a}$ is an integral ideal in $\mathbf{K}$ such that $(\mathfrak{a},\mathfrak{p}_1\cdots\mathfrak{p}_s)=1$. Putting $\mathfrak{p}_i^{h_K}=(\pi_i)$ with some fixed $\pi_i\in\mathbf{Z}_K$ and $b_i=h_Kw_i+d_i$ with $0\le d_i<h_K$, we obtain $\mathfrak{a}\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_s^{d_s}=(\vartheta)$ for some $\vartheta\in\mathbf{Z}_K$. Since

$$m\le|N_{K/Q}(\vartheta)|=mN_{K/Q}(\mathfrak{p}_1^{d_1}\cdots\mathfrak{p}_s^{d_s})\le P^{snh_K}\cdot m,$$

it follows from Lemma 2 that an associate ϑ' of ϑ can be determined such that

$$c_{10}m^{1/n}\le|\vartheta'^{(l)}|\le c_{11}m^{1/n},\qquad l=1,\dots,n,$$

with

$$c_{10}=\exp\left\{-\frac{c_1r}{2}R_K\right\},\qquad c_{11}=P^{sh_K}\exp\left\{\frac{c_1r}{2}R_K\right\}.$$

Now $\beta=\xi\pi_1^{w_1}\cdots\pi_s^{w_s}\vartheta'$ where ξ is a fixed unit in $\mathbf{K}$ and $\pi_i\nmid\vartheta'$ for $i=1,\dots,s$. Since $\xi\pi_1^{w_1}\cdots\pi_s^{w_s}$ is a fixed S-unit in $\mathbf{K}$, multiplying both sides of (2) by

$(\xi\pi_1^{w_1}\cdots\pi_s^{w_s})^{-1}$ and incorporating this S-unit in x_1, x_2 we get (2) with β replaced by ϑ'. So we may suppose without loss of generality that in (2)

$$m\leq|N_{K/Q}(\beta)|\quad\text{and}\quad c_{10}m^{1/n}\leq|\beta^{(l)}|\leq c_{11}m^{1/n},\qquad l=1,\ldots,n. \tag{31}$$

Similarly, we may assume that in (2)

$$m_k\leq|N_{K/Q}(\alpha_k)|\leq P^{snh_K}m_k,\qquad|\alpha_k^{(l)}|\leq c_{11}m_k^{1/n},\qquad l=1,\ldots,n \tag{32}$$

and $\pi_i\nmid\alpha_k$ for $k=1$, 2 and $i=1,\ldots,s$.

Let x_1, x_2 be an arbitrary but fixed solution of (2) in S-units. Then we have

$$(x_k)=\mathfrak{p}_1^{a_{k1}}\cdots\mathfrak{p}_s^{a_{ks}},\qquad k=1,2, \tag{33}$$

with some rational integers $a_{k1},\ldots,a_{ks}$. Write $a_{ki}=h_Kv_{ki}+a'_{ki}$ with $0\leq a'_{ki}<h_K$. Then $\mathfrak{p}_1^{a'_{k1}}\cdots\mathfrak{p}_s^{a'_{ks}}$ is principal, say (τ_k), and $\tau_k\in\mathbf{Z}_K$. By Lemma 2 we may suppose that

$$\overline{|\pi_i|}\leq\exp\left\{\frac{c_1r}{2}R_K+h_K\log P\right\},\qquad i=1,\ldots,s \tag{34}$$

and

$$\overline{|\tau_k|}\leq\exp\left\{\frac{c_1r}{2}R_K+sh_K\log P\right\},\qquad k=1,2.$$

Consequently, there are units κ_1, κ_2 in $\mathbf{K}$ such that $x_k=\kappa_k\tau_k\pi_1^{v_{k1}}\cdots\pi_s^{v_{ks}}$. If $r\geq1$, let $\eta_1,\ldots,\eta_r$ be units with the properties specified in Lemma 1. Then $\kappa_k=\kappa'_k\eta_1^{y_{k1}}\cdots\eta_r^{y_{kr}}$ where κ'_k is a unit satisfying

$$\overline{|\kappa'_k|}\leq\exp\left\{\frac{c_1r}{2}R_K\right\},\qquad k=1,2.$$

With the notation $\chi_k=\kappa'_k\tau_k$ we have

$$x_k=\chi_k\eta_1^{y_{k1}}\cdots\eta_r^{y_{kr}}\pi_1^{v_{k1}}\cdots\pi_s^{v_{ks}} \tag{35}$$

and

$$\overline{|\chi_k|}\leq\exp\{c_1rR_K+sh_K\log P\}. \tag{36}$$

We are now going to give an upper bound for the solutions of

$$\alpha_1\chi_1\eta_1^{y_{11}}\cdots\eta_r^{y_{1r}}\pi_1^{v_{11}}\cdots\pi_s^{v_{1s}}+\alpha_2\chi_2\eta_1^{y_{21}}\cdots\eta_r^{y_{2r}}\pi_1^{v_{21}}\cdots\pi_s^{v_{2s}}=\beta \tag{37}$$

in rational integers y_{kj}, v_{ki}. Write $Y_3=\prod_{i=1}^s \pi_i^{-\min(v_{1i},v_{2i},0)}$ and multiply both sides of (37) by Y_3. Putting $Y_k=Y_3\eta_1^{y_{k1}}\cdots\eta_r^{y_{kr}}\pi_1^{v_{k1}}\cdots\pi_s^{v_{ks}}$ for $k=1,2$, from (37) we get

$$\alpha_1\chi_1Y_1+\alpha_2\chi_2Y_2=\beta Y_3. \tag{38}$$

We could now apply Lemma 6 to (38) and we should obtain

$$Y_k=\eta\rho_k,\qquad k=1,2,3;\ \max_{1\le k\le 3}\overline{|\rho_k|}\le c_{12}m^{c_{13}} \tag{39}$$

where $\eta\in U_K$, $\rho_k\in\mathbf{Z}_K$ and c_{12}, c_{13} are explicit constants. This would imply an explicit upper bound for $|y_{kj}|$ and $|v_{ki}|$. However, we can get a slightly better estimate if we observe that the equation (38) is of the same type as (19). Thus, by (30) we have

$$\max_{k,j,i}(|y_{kj}|,|v_{ki}|)\le c_{14}\log m \tag{40}$$

where

$$c_{14}=2\cdot 3^n c_9 P^n(\log P)[s(R_K+h_K\log P)\log(1+sR_Kh_K)+1]R_K$$
$$\cdot(R_K+h_K\log P)^s[\log R_K^*+s\log(1+h_KR_K\log P)]^2$$

with the constant c_9 occurring in the proof of Lemma 6.

Let $c_{15}>0$ be a number determined later. We shall now prove that (37) (i.e. (2)) has at most $r+1$ solutions

$$x_1=\chi_1\eta_1^{y_{11}}\cdots\eta_r^{y_{1r}}\pi_1^{v_{11}}\cdots\pi_s^{v_{1s}},\qquad x_2=\chi_2\eta_1^{y_{21}}\cdots\eta_r^{y_{2r}}\pi_1^{v_{21}}\cdots\pi_s^{v_{2s}}$$

such that

$$\max_{k,i}|v_{ki}|\le c_{15}\log m. \tag{41}$$

Write $\eta_1^{y_{k1}}\cdots\eta_r^{y_{kr}}=\varepsilon_k$ in x_k. Suppose that (37) has at least $r+2$ solutions x_1, x_2 with the property (41). Assume that $m_1\le m^{1-\varepsilon}$. Let us order the conjugates of

$\alpha_1\varepsilon_1$ in the same way as in Section 3. By (32) we have

$$\prod_{i=1}^{r_1} |(\alpha_1\varepsilon)^{(i)}| \prod_{i=r_1+1}^{r_1+r_2} |(\alpha_1\varepsilon_1)^{(i)}|^2 \le P^{snh_K} m_1 \le P^{snh_K} m^{1-\varepsilon} \tag{42}$$

for each of the $r+2$ solutions. Hence there exists at least two solutions for which $|(\alpha_1\varepsilon_1)^{(l)}|$ is minimal for the same l, $1 \le l \le r_1 + r_2 = r+1$. For these two solutions we have

$$|(\alpha_1\varepsilon_1)^{(l)}| \le P^{sh_K} m^{1/n-\varepsilon/n} \tag{43}$$

and, by (34) and (41),

$$|(\pi_1^{v_{11}} \cdots \pi_s^{v_{1s}})^{(l)}| \le m^{c_{16}}$$

where

$$c_{16} = c_{15}\left[sn\left(\frac{c_1 r}{2} R_K + h_K \log P\right) + 1\right].$$

So, by taking

$$c_{16} = \varepsilon/2n \left(\text{i.e. } c_{15} = \frac{\varepsilon}{2n}\left[s(n-1)\left(\frac{c_1 r}{2} R_K + h_K \log P\right) + 1\right]^{-1}\right)$$

we get

$$|\beta^{(l)} - \alpha_2^{(l)} x_2^{(l)}| = |(\alpha_1\varepsilon_1)^{(l)}| |x_1^{(l)}| |(\pi_1^{v_{11}} \cdots \pi_s^{v_{1s}})^{(l)}| \le c_{17} m^{1/n + c_{16} - \varepsilon/n} = c_{17} m^{1/n - \varepsilon/2n} \tag{44}$$

where $c_{17} = \exp\{c_1 r R_K + 2sh_K \log P\}$. We deduce from (3), (31) and (44) that

$$|\alpha_2^{(l)} x_2^{(l)}| \ge |\beta^{(l)}| - c_{17} m^{1/n - \varepsilon/2n} \ge c_{10} m^{1/n} - c_{17} m^{1/n - \varepsilon/2n} \ge \frac{c_{10}}{2} m^{1/n}. \tag{45}$$

Let x_1, x_2 and $x_1' = \chi_1' \eta_1^{y_{11}'} \cdots \eta_r^{y_{1r}'} \pi_1^{v_{11}'} \cdots \pi_s^{v_{1s}'}$, $x_2' = \chi_2' \eta_1^{y_{21}'} \cdots \eta_r^{y_{2r}'} \pi_1^{v_{21}'} \cdots \pi_s^{v_{2s}'}$ denote the two solutions in question. From (44) we obtain

$$|\alpha_2^{(l)} x_2'^{(l)} - \alpha_2^{(l)} x_2^{(l)}| \le 2c_{17} m^{1/n - \varepsilon/2n},$$

whence, by (45) and (3),

$$\left|\frac{x_2'^{(l)}}{x_2^{(l)}}-1\right| = |\Gamma^{(l)}| < \exp\left\{-\frac{\varepsilon}{8nc_{14}}(2c_{14}\log m)\right\} \tag{46}$$

where

$$\Gamma = \frac{\chi_2'}{\chi_2}\eta_1^{y'_{21}-y_{21}}\cdots\eta_r^{y'_{2r}-y_{2r}}\pi_1^{v'_{21}-v_{21}}\cdots\pi_s^{v'_{2s}-v_{2s}}-1.$$

Here we may suppose that

$$\frac{\chi_2'}{\chi_2}\neq 1.$$

In (46)

$$\frac{x_2'^{(l)}}{x_2^{(l)}}-1\neq 0,$$

since otherwise we should have $x_2'=x_2$ and, from (2), $x_1'=x_1$. Since in view of (40) we have $|y_{2j}'-y_{2j}|$, $|v_{2i}'-v_{2i}|\leq 2c_{14}\log m$ for each i and j, we may apply Lemma 4 to (46) with $\delta=\varepsilon(8nc_{14})^{-1}$ and we get

$$2c_{14}\log m \leq \frac{4e}{\varepsilon}(8nc_{14})T'\log\left[\frac{4e(r+s+1)}{\varepsilon}(8nc_{14})T'\right]\log A'$$

where $T'=c_{18}\Omega'\log\Omega'$, $c_{18}=(25(r+s+3)n)^{10(r+s+3)}$ with the Ω' specified in (25) and

$$H\left(\frac{\chi_2'}{\chi_2}\right)\leq(\overline{|\chi_2'|}+\overline{|\chi_2|})^n\leq(2c_{17})^n=A'. \tag{47}$$

Thus we have

$$\log m\leq\varepsilon^{-1}\log\left(\frac{2}{\varepsilon}\right)(25(r+s+3)n)^{20(r+2)+13s}\cdot P^nR_K(R_K+h_K\log P)^s$$
$$\cdot(R_K+sh_K\log P)[s(R_K+h_K\log P)+1]\log(R_K^*(1+sh_KP))$$

which contradicts (3).

We shall now prove that (37) has at most $4s$ solutions x_1, x_2 for which

$$\max_{k,i} |v_{ki}| > c_{15} \log m \tag{48}$$

with

$$c_{15} = \frac{\varepsilon}{2n}\left[sn\left(\frac{c_1 r}{2} R_K + h_K \log P\right) + 1\right]^{-1}.$$

Assume that (37) has at least $4s+1$ solutions with the property (48). Then we may assume, for convenience, that there exist three solutions for which $|v_{11}| > c_{15} \log m$.

First suppose that for at least two of these solutions, say for x_1, x_2 and x_1', x_2', v_{11} and v_{11}' are positive. Since $\pi_1 \nmid \beta$, from (37) we deduce that $\mathrm{ord}_{\pi_1}(\alpha_2 x_2) \leq 0$. Further (37) implies $\mathrm{ord}_{\pi_1}(\beta - \alpha_2 x_2) \geq v_{11}$ and $\mathrm{ord}_{\pi_1}(\beta - \alpha_2 x_2') \geq v_{11}'$, whence, by (48),

$$\infty > \mathrm{ord}_{\pi_1}(\alpha_2 x_2' - \alpha_2 x_2) > c_{15} \log m$$

and hence

$$\infty > \mathrm{ord}_{\mathfrak{p}_1} \Gamma \geq \mathrm{ord}_{\pi_1}\left(\frac{x_2'}{x_2} - 1\right) > \delta^*(2c_{14} \log m)$$

with

$$\delta^* = \frac{c_{15}}{2c_{14}} < 1.$$

Consequently, by Lemma 5 we have

$$2c_{14} \log m < (\delta^*)^{-1} T^* \log((\delta^*)^{-1} T^*) \log A'$$

where $T^* = c_{19} G_S \Omega' \log \Omega'$, $c_{19} = [16(r+s+2)n]^{12(r+s+2)}$ and G_S is defined as in Lemma 6. Thus

$$\log m < \frac{c_{19}}{c_{15}} G_S \Omega' \log \Omega' \log\left[\frac{2c_{14}}{c_{15}} c_{19} G_S \Omega' \log \Omega'\right] \log A'$$

$$\leq \varepsilon^{-1} \log \left(\frac{2}{\varepsilon}\right)(25(r+s+3)n)^{20(r+2)+13s} P^n R_K (R_K + h_K \log P)^s$$

$$\cdot (R_K + sh_K \log P)[s(R_K + h_K \log P)+1] \log (R_K^*(1+sh_K P))$$

and, in view of (3), this yields a contradiction.

Finally suppose that there exist two solutions, say x_1, x_2 and x_1', x_2', for which $|v_{11}|$, $|v_{11}'| > c_{15} \log m$ and v_{11}, v_{11}' are negative. Since $\pi_1 \nmid \alpha_1$, we can reduce this case to the preceding one by multiplying both sides of (37) by x_1^{-1} and $x_1'^{-1}$ respectively. This completes the proof of our theorem.

To prove the Remark stated after our Theorem it is enough to show that there exist no solution x_1, x_2 with the properties $|v_{11}| > c_{15} \log m$ and $v_{11} < 0$. Indeed, the existence of such a solution x_1, x_2 would imply

$$\operatorname{ord}_{\pi_1}\left(-\frac{\alpha_1 x_1}{\alpha_2 x_2} - 1\right) > c_{15}' \log m$$

which would yield a contradiction in a similar way as in the above proof. If in particular $\mathbf{K} = \mathbf{Q}$, $s \geq 1$ and (2) is solvable then in our above proof (48) must hold. So, in this case the number of solutions is at most $2s$.

REFERENCES

[1] BAKER, A., *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London, Ser. A., *263* (1968), 173–208.

[2] ——, *A sharpening of the bounds for linear forms in logarithms II*, Acta Arith., *25* (1973), 33–36.

[3] ——, Transcendental number theory, Cambridge, 1975.

[4] CHOODNOVSKY, G. V., *The Gelfond–Baker method in problems of diophantine approximation*, Colloquia Math. Soc. János Bolyai, *13*. Topics in number theory, Debrecen, 1974; pp. 19–30 (1976).

[5] DOBROWOLSKI E., *On the maximal modulus of conjugates of an algebraic integer*, Bull. Acad. Polon. Sci., *26* (1978), 291–92.

[6] GYŐRY, K., *Sur l'irréductibilité d'une classe des polynômes II*, Publ. Math. Debrecen, *19* (1972), 293–326.

[7] ——, *Sur une classe des corps de nombres algébriques et ses applications*, Publ. Math. Debrecen, *22* (1975), 151–175.

[8] ——, *On polynomials with integer coefficients and given discriminant V, p-adic generalizations*, Acta Math. Acad. Sci. Hungar., *32* (1978), 175–190.

[9] ——, *On the solutions of linear diophantine equations in algrebraic integers of bounded norm*, Ann. Univ. Budapest Eötvös, Sect. Math., to appear.

[10] ——, *On the reducibility of a class of polynomials III, 26* (1978), 291–92.

[11] LANG, S., *Diophantine geometry*, New York and London, 1962.

[12] LEWIS, D. J. and MAHLER, K., *On the representation of integers by binary forms*, Acta Arith., *6* (1961), 333–363.

[13] MAHLER, K., *On algebraic relations between two units of an algebraic field*, Algèbre et Théorie des Nombres, Colloques Internationaux du Centre National de la Recherche Scientifique, No. 24, pp. 47–55. CNRS, Paris, 1950.
[14] MORDELL, L. J., *Diophantine equations*, Academic Press, London and New York, 1969.
[15] NAGELL, T., *Sur une propriété des unités d'un corps algébrique*, Arkiv för Mat., *5* (1964), 343–356.
[16] ——, *Quelques problèmes relatifs auz unités algébriques*, Arkiv för Mat., *8* (1969), 115–127.
[17] ——, *Sur un type particulier d'unités algébriques*, Arkiv för Mat., *8* (1969), 163–184.
[18] NEWMAN, M., *Units in arithmetic progression in an algebraic number field*, Proc. Amer. Math. Soc., *43* (1974), 266–268.
[19] PARRY, C. J., *The P-adic generalisation of the Thue–Siegel theorem*, Acta Math., *83* (1950), 1–100.
[20] VAN DER POORTEN, A. J., Linear forms in logarithms in the p-adic case, *Transcendence Theory: Advances and Applications*, pp. 29–57. Academic Press, London and New York, 1977.
[21] —— and LOXTON, J. H., *Multiplicative relations in number fields*, Bull. Austral. Math. Soc., *16* (1977), 83–98. Corregindum and addendum, ibid., *17* (1977), 151–156.
[22] SIEGEL, C. L., *Approximation algebraischer Zahlen*, Math. Z., *10* (1921), 173–213.
[23] ——, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. *1* (1926), 66–68.
[24] ——, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen, Math.-Phys. Kl. *II* (1969), 71–86.
[25] SKOLEM, TH., *Diophantische Gleichungen*, Springer Verlag, Berlin, 1938.
[26] SPRINDŽUK, V. G., *Algebraic number fields with large class number* (in Russian), Izv. Akad. Nauk SSSR, Ser. Mat., *38* (1974), 971–982.
[27] ——, *Hyperelliptic diophantine equation and class numbers* (in Russian), Acta Arith., *30* (1976), 95–108.

Mathematical Institute
Kossuth Lajos University
H-4010 Debrecen 10
Hungary

Received January 12, 1979