$a_1+a_2+a_3+a_4 = 0$, contradicting hypotheses concerning S. Thus, S represents at least 8 elements of G. The theorem follows. ∎

Attainment of the bound for $f(k)$ in Theorem 5, with $k = 4$, is shown by 1, 3, 4, 7 (mod 9). In general, precise evaluation of $f(k)$ is increasingly laborious, even though entirely elementary. We have shown $f(5) = 13$. The proof is available as an appendix in [1]. Furthermore $f(6) \leqslant 19$, and equality seems likely. (Computations in this direction are in progress.)

Szemerédi [5] can show $f(k) \geqslant ck^2$, where c is some positive constant. On the other hand, $f(k) \leqslant [\frac{1}{2}k^2]+1$, as shown by the following two examples (where s is any positive integer);

(1) $a_i = i$ for $1 \leqslant i \leqslant s$, $a_i = s^2+i$ for $s+1 \leqslant i \leqslant 2s+1$ (mod $2s^2+2s+2$), where $k = 2s+1$, and the number of elements represented is $\frac{1}{2}k^2+\frac{1}{2}$;

(2) $a_i = i$ for $1 \leqslant i \leqslant s$, $a_i = s^2-s+i$ for $s+1 \leqslant i \leqslant 2s$ (mod $2s^2+2$), where $k = 2s$, and the number of elements represented is $\frac{1}{2}k^2+1$.

It is interesting to note that in all resolved cases, $f(k)$ can be achieved within the class of cyclic groups. We conjecture this to be the case for all k.

Finally we remark that our theorems perhaps carry over to non-abelian groups, but we have no results in this direction.

References

[1] R. B. Eggleton and P. Erdös, *Two combinatorial problems in group theory*, Scientific Paper No. 117, (1971), Dept. of Math., Stat. and Comp. Sci., U. of Calgary.

[2] P. Erdös and H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith. 9 (1964), pp. 149–159. M. R. 29 (1965), # 3463.

[3] L. Moser and P. Scherk, *Distinct elements in a set of sums*, Amer. Math. Monthly 62 (1955), pp. 46–47.

[4] J. E. Olson, *A combinatorial problem on finite abelian groups, II*, J. Number Theory 1 (1969), pp. 195–199.

[5] E. Szemerédi, *On a conjecture of Erdös and Heilbronn*, Acta Arith. 17 (1970), pp. 227–229.

THE UNIVERSITY OF CALGARY
Calgary, Alberta, Canada

Received on 6. 4. 1971 (164)

ACTA ARITHMETICA
XXI (1972)

A sharpening of the bounds for linear forms in logarithms

by

A. Baker (Cambridge)

In memory of Professors
H. Davenport and W. Sierpiński

1. Introduction. The purpose of the present paper is to establish a new theorem on linear forms in the logarithms of algebraic numbers which incorporates many of the more recent developments in this field and, in certain respects, goes farther.

Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, \ldots, \alpha_{n-1}$ and α_n be at most A' and A ($\geqslant 2$) respectively. We prove:

Theorem. *For some effectively computable number $C > 0$ depending only on n, d and A', the inequalities*

$$0 < |b_1 \log\alpha_1 + \ldots + b_n \log\alpha_n| < C^{-\log A \log B} \tag{1}$$

have no solution in rational integers $b_1, \ldots, b_n$ with absolute values at most B ($\geqslant 2$).

It has been assumed that the logarithms have their principal values but the result would hold for any choice of logarithms if C were allowed to depend on their determinations. Under slightly more stringent hypotheses the theorem would be valid for any algebraic numbers $b_1, \ldots, b_n$, not merely rational integers; indeed our arguments can easily be modified to show that, for any $\varepsilon > 0$, there exists an effectively computable number C, depending only on n, d, A' and ε, such that (1) has no solution in algebraic numbers $b_1, \ldots, b_n$ with degrees at most d and heights at most B ($\geqslant 2$) if $\log A$ is replaced by $(\log A)^{1+\varepsilon}$. This strengthens a recent result of Stark and the author [3] wherein $\log A \log B$ is replaced by the maximum of $(\log A)^{1+\varepsilon}$ and $(\log B)^{cn^2/\varepsilon}$ for a sufficiently large absolute constant c. The theorem also extends the work of Feldman [4], which itself furnished refinements of the inequalities given in the third memoir of the series [1], by substituting $\log A$ for a high power of the logarithm. Furthermore, the theorem can be viewed as a variant of the result obtained in the fourth memoir of [1], implying an upper bound for H of the form $C\log A\log\log A$, where C is an effectively computable number as above.

The last remark is of particular significance in connexion with applications. Weaker forms of the assertion have been employed in, amongst other things, the study of diophantine equations and most of the results obtained in this respect can now be sharpened. More especially, the theorem yields a further effective improvement upon Liouville's inequality of 1844 relating to the approximation of algebraic numbers by rationals. It is in fact easily deduced from the work of [2] that for any algebraic number α with degree $n\geqslant 3$ there exist positive effectively computable numbers $c, \varkappa$, depending only on α, such that $|\alpha-p/q|>cq^{-n+\varkappa/\log\log q}$ for all rationals p/q $(q>0)$; this is the best estimate of its kind established to date [1].

2. Preliminary lemmas. For any integers $k\geqslant 1$, $l\geqslant 0$ we signify by $\nu(l,k)$ the least common multiple of $l+1, l+2, \ldots, l+k$. We define

$$\Delta(x;k) = (x+1)\ldots(x+k)/k!$$

and we write $\Delta(x;0)=1$. Further, for any integer $m\geqslant 0$, we denote by $\Delta(x;k,l,m)$ the mth derivative of $\big(\Delta(x;k)\big)^l/m!$. The notation will be retained throughout the paper.

The following lemmas are recorded for later reference.

LEMMA 1. *$\big(\nu(x,k)\big)^m\Delta(x;k,l,m)$ is a positive integer when x is a positive integer and we have*

$$\Delta(x;k,l,m)\leqslant 4^{l(x+k)}, \qquad \nu(x,k)\leqslant\{c(x+k)/k\}^{2k}$$

for some absolute constant c [2].

Proof. We have

$$\Delta(x;k,l,m) = \big(\Delta(x;k)\big)^l\sum_{j_1,\ldots,j_m}\big((x+j_1)\ldots(x+j_m)\big)^{-1},$$

where $j_1,\ldots,j_m$ run through all selections of m integers from the set $1,\ldots,k$ repeated l times, and the right hand side is read as 0 if $m>kl$. For each r, $x+j_r$ divides $\nu(x,k)$, and since certainly $\Delta(x;k)$ is a rational integer, the first part of the lemma follows. Further it is clear that

$$\Delta(x;k,l,m)\leqslant\binom{x+k}{k}^l\binom{kl}{m}\leqslant 2^{l(x+k)+kl}\leqslant 4^{l(x+k)}.$$

[1] Added in proof. Feldman (Izv. Akad. Nauk SSSR ser. mat. 35 (1971), pp. 973–990) has recently improved the number on the right to $cq^{-\varkappa}$, where $\varkappa=\varkappa(\alpha)<n$. The result can also be obtained by a slight generalization of the present work, as will be shown in a sequel.

[2] The exponent 2 in the estimate for $\nu(x,k)$ can be reduced to 1, which is best possible; see a note by R. Tijdeman to appear in the problem section of Nieuw Arch. Wisk. (cf. 19 (1971), p. 165).

To obtain the final estimate we write $\nu(x,k)=\nu'\nu''$, where all prime factors of ν', ν'' are $\leqslant k$ and $>k$ respectively. Since the exponent to which any prime p divides ν' is at most $\log(x+k)/\log p$, we have

$$\log\nu'\leqslant\sum_{p\leqslant k}\log(x+k)\leqslant c'k\log(x+k)/\log k$$

and thus $\nu'\leqslant\{c''(x+k)/k\}^k$ for some absolute constants c', c''. The estimate follows on noting that ν'' divides $\Delta(x;k)\leqslant(x+k)^k/k!$.

LEMMA 2. *If $P(x)$ is a polynomial with degree $n>0$ and with coefficients in a field K then, for any integer m with $0\leqslant m\leqslant n$, the polynomials $P(x), P(x+1), \ldots, P(x+m)$ and $1, x, \ldots, x^{n-m-1}$ are linearly independent over K.*

Proof. The assertion is readily verified for $n=1$. We assume the result for $n=n'$ and we proceed to prove the validity for $n=n'+1$. Suppose therefore that $0\leqslant m\leqslant n'+1$, that $P(x)$ is a polynomial with degree $n'+1$ and that

$$R(x) = \lambda_0P(x)+\lambda_1P(x+1)+\ldots+\lambda_mP(x+m)$$

has degree at most $n'-m$ for some elements λ_j of K. We have

$$R(x) = (\lambda_0+\ldots+\lambda_m)P(x+m+1)+\sum_{j=0}^{m}(\lambda_0+\lambda_1+\ldots+\lambda_j)Q(x+j),$$

where $Q(x)=P(x)-P(x+1)$. But $Q(x)$ has degree n' and since $P(x+m+1)$ has degree $n'+1$ we see that $\lambda_0+\ldots+\lambda_m=0$. Further, the inductive hypothesis shows that

$$\lambda_0+\lambda_1+\ldots+\lambda_j = 0 \qquad (0\leqslant j\leqslant m)$$

and so $\lambda_0=\ldots=\lambda_m=0$, as required.

LEMMA 3. *Let $\alpha_1,\ldots,\alpha_n$ be non-zero elements of an algebraic number field K and let $\alpha_1^{1/p},\ldots,\alpha_n^{1/p}$ denote fixed p-th roots for some prime p. Further let $K'=K(\alpha_1^{1/p},\ldots,\alpha_{n-1}^{1/p})$. Then either $K'(\alpha_n^{1/p})$ is an extension of K' of degree p or we have*

$$\alpha_n = \alpha_1^{j_1}\ldots\alpha_{n-1}^{j_{n-1}}\gamma^p$$

for some γ in K and some integers $j_1,\ldots,j_{n-1}$ with $0\leqslant j_r<p$.

Proof. This is Lemma 3 of [3].

LEMMA 4. *Suppose that α, β are elements of an algebraic number field with degree D and that for some positive integer p we have $\alpha=\beta^p$. If $a\alpha$ is an algebraic integer for some positive rational integer a and if b is the leading coefficient in the minimal defining polynomial of β then $b\leqslant a^{D/p}$.*

Proof. This is Lemma 4 of [3].

3. Main lemmas. We denote by $\alpha_1, \ldots, \alpha_n$, where $n \geqslant 2$, non-zero algebraic numbers with degrees at most d and we suppose that the heights of $\alpha_1, \ldots, \alpha_{n-1}$ and α_n do not exceed A' and A respectively. By $c, c_1, c_2, \ldots$ we signify numbers greater than 1 that can be specified explicitly in terms of n, d and A' only. We suppose that there exist rational integers $b_1, \ldots, b_n$, with $b_n \neq 0$, having absolute values at most B ($\geqslant 4$) such that (1) holds, where it is assumed that the logarithms have their principal values and that $C = C(n, d, A')$ is sufficiently large for the validity of the subsequent arguments. We shall proceed to show that there exist then further rational integers $b_1', \ldots, b_n'$ with absolute values at most $c_1 B$ and an algebraic number α_n' in the field generated by the α's over the rationals with height at most $c_2 A^{1/2}$, such that (1) holds with b_r $(1 \leqslant r \leqslant n)$ and α_n replaced by b_r' and α_n' respectively; an inductive argument will then complete the proof of the theorem.

We signify by k an integer exceeding a sufficiently large number c as above and we write

$$h = L_{-1} + 1 = [\log B],$$

$$L = L_0 = \ldots = L_{n-1} = [k^{1-1/(4n)} \log A], \quad L_n = [k^{1/2}],$$

where, as usual, $[x]$ denotes the integral part of x. Further we write $f_m(z)$ for the mth derivative of $f(z)$.

LEMMA 5. *There are integers $p(\lambda_{-1}, \lambda_0, \ldots, \lambda_n)$, not all 0, with absolute values at most $A^{c_3 hk}$, such that for all integers l with $1 \leqslant l \leqslant h$ and all non-negative integers $m_0, \ldots, m_{n-1}$ with $m_0 + \ldots + m_{n-1} \leqslant k \log A$ we have*

$$\sum_{\lambda_{-1}=0}^{L_{-1}} \cdots \sum_{\lambda_n=0}^{L_n} p(\lambda_{-1}, \ldots, \lambda_n) \Delta(l) \alpha_1^{\lambda_1 l} \ldots \alpha_n^{\lambda_n l} = 0, \tag{2}$$

where

$$\Delta(z) = \Delta(z + \lambda_{-1}; h, \lambda_0 + 1, m_0) \prod_{r=1}^{n-1} \Delta(b_n \lambda_r - b_r \lambda_n; m_r).$$

Proof. Let $a_1, \ldots, a_n$ denote the leading coefficients (supposed positive) in the minimal defining polynomials of $\alpha_1, \ldots, \alpha_n$ respectively. For any non-negative integer j we have

$$(a_r \alpha_r)^j = \sum_{s=0}^{d-1} a_{rs}^{(j)} \alpha_r^s,$$

where the $a_{rs}^{(j)}$ denote rational integers with absolute values at most c_4^j or $(2A)^j$ according as $r < n$ or $r = n$. Thus on multiplying (2) by $a_1^{L_1 l} \ldots a_n^{L_n l}$ we obtain

$$\sum_{s_1=0}^{d-1} \cdots \sum_{s_n=0}^{d-1} V(s) \alpha_1^{s_1} \ldots \alpha_n^{s_n} = 0,$$

where

$$V(s) = \sum_{\lambda_{-1}=0}^{L_{-1}} \cdots \sum_{\lambda_n=0}^{L_n} p(\lambda_{-1}, \ldots, \lambda_n) \Delta(l) \prod_{r=1}^{n} \{a_r^{(L_r - \lambda_r) l} a_{r, s_r}^{(\lambda_r l)}\}.$$

Hence the lemma will be satisfied if the d^n equations $V(s) = 0$ hold. Now these represent $M \leqslant d^n h (k \log A + 1)^n$ linear equations in the $N = (L_{-1}+1) \ldots (L_n + 1)$ unknowns $p(\lambda_{-1}, \ldots, \lambda_n)$. Further, Lemma 1 shows that, after multiplying by $(\nu(0, 3h))^{m_0}$, the coefficients in these equations will be rational integers. Furthermore we have

$$(\nu(0, 3h))^{m_0} \Delta(l + \lambda_{-1}; h, \lambda_0 + 1, m_0) \leqslant c_5^{h(m_0 + L)}$$

and clearly

$$|\Delta(b_n \lambda_r - b_r \lambda_n; m_r)| \leqslant B^{m_r} \Delta(\lambda_r + \lambda_n; m_r) \leqslant 4^L (2B)^{m_r}. \tag{3}$$

Since also the absolute value of the product over r in the definition of $V(s)$ is at most $c_6^{Lh} A^{L_n h}$, we see that the absolute values of the coefficients referred to above are at most $U = A^{c_7 hk}$. Now

$$N > h k^{n + \frac{1}{4}} (\log A)^n > 2M$$

and hence (cf. Lemma 1 of [1, I]) the system of equations $V(s) = 0$ can be solved non-trivially and indeed the integers can be chosen to have absolute values at most $NU \leqslant A^{c_3 hk}$, as required.

LEMMA 6. *For any non-negative integers $m_0, \ldots, m_{n-1}$ with $m_0 + \ldots + m_{n-1} \leqslant k \log A$, let*

$$f(z) = \sum_{\lambda_{-1}=0}^{L_{-1}} \cdots \sum_{\lambda_n=0}^{L_n} p(\lambda_{-1}, \ldots, \lambda_n) \Delta(z) \alpha_1^{\gamma_1 z} \ldots \alpha_{n-1}^{\gamma_{n-1} z}$$

where $\gamma_r = \lambda_r - b_r \lambda_n / b_n$ $(1 \leqslant r < n)$. We have

$$|f(z)| \leqslant A^{c_8 hk} c_9^{L|z|}. \tag{4}$$

Further, for any integer l with $h < l \leqslant hk^{2n}$, either (2) *holds or*

$$|f(l)| \geqslant A^{-c_{10} hk \{1 + \log(l/h)\}} c_{11}^{-Ll}. \tag{5}$$

Proof. We begin with the preliminary observation that, by virtue of (1), we have

$$|\alpha_n - \alpha_n'| < C^{-\frac{1}{4} \log A \log B}, \tag{6}$$

where

$$\alpha_n' = \alpha_1^{-b_1/b_n} \ldots \alpha_{n-1}^{-b_{n-1}/b_n}; \tag{7}$$

for clearly

$$|\log \alpha_n - \log \alpha_n'| < C^{-\log A \log B},$$

where the second logarithm is not necessarily principal-valued, and (6) follows on noting that

$$|e^{z}-1| \leqslant |z|\, e^{|z|}$$

for any z and that (see [1, IV])

$$(8) \qquad |\log a_n| \leqslant 4\log(dA).$$

Now (6) implies, in particular, that

$$|a_n'^{z}| \leqslant e^{(|\log a_n|+1)|z|}$$

and from (8) we have

$$L_n |\log a_n| \leqslant L.$$

Further it is clear that

$$|a_1^{\lambda_1 z} \ldots a_{n-1}^{\lambda_{n-1} z}| \leqslant c_{12}^{L|z|},$$

and since

$$|z+\lambda_{-1}| \leqslant [|z|]+h$$

we deduce from Lemma 1 that

$$|\Delta(z+\lambda_{-1};\, h,\, \lambda_0+1,\, m_0)| \leqslant c_{13}^{L(|z|+h)}.$$

On combining this with (3) we obtain

$$|\Lambda(z)| \leqslant A^{c_{14}hk} c_{13}^{L|z|}$$

and the required estimate (4) follows easily.

To prove the second assertion we begin by noting that the left-hand side of (2), say Q, is an algebraic number with degree at most d^n. Further, by estimates similar to those given above, it is readily verified that each conjugate of Q, obtained by substituting arbitrary conjugates for $a_1, \ldots, a_n$, has absolute value at most $A^{c_{15}hk} c_{16}^{Ll}$. Furthermore, from Lemma 1 we see that, on multiplying Q by

$$P = a_1^{L_1 l} \ldots a_n^{L_n l} (\nu(l, 2h))^{m_0},$$

where $a_1, \ldots, a_n$ are defined as in Lemma 5, we obtain an algebraic integer and

$$P \leqslant c_{17}^{Ll} (c_{18} l/h)^{4hm_0}.$$

Hence we conclude that either $Q = 0$ or

$$|Q| \geqslant A^{-c_{19}hk} c_{20}^{-Ll} (l/h)^{-c_{21}hm_0};$$

and since $m_0 \leqslant k \log A$, the number on the right exceeds the right-hand side of (5) for some c_{10} and c_{11}. But, as above, we deduce easily from (6) that

$$|Q - f(l)| \leqslant A^{c_{22}lk} C^{-\frac{1}{2}\log A \log B}$$

and, if $l \leqslant hk^{2n}$ and C is larger than some function of k, the number on the right is at most

$$C^{-\frac{1}{4}\log A \log B} \leqslant \tfrac{1}{2}|Q|.$$

Hence, if $Q \neq 0$, we obtain $|f(l)| > \frac{1}{2}|Q|$ and this proves (5).

LEMMA 7. *For some ε $(0 < \varepsilon < 1)$ depending only on n, d and A', and any integer J with $0 \leqslant J \leqslant 2n/\varepsilon$, (2) is satisfied for all integers l with $1 \leqslant l \leqslant hk^{\varepsilon J}$ and all non-negative integers $m_0, \ldots, m_{n-1}$ with $m_0 + \ldots + m_{n-1} \leqslant (k/2^J)\log A$.*

Proof. We shall show that in fact a suitable value for ε is $(2^8 n c_{10})^{-1}$, where c_{10} is the number indicated in (5). The lemma is valid for $J = 0$ by Lemma 5. We suppose that K is an integer satisfying $0 \leqslant K \leqslant (2n/\varepsilon)-1$ and we assume that the lemma has been verified for $J = 0, 1, \ldots, K$. We proceed to prove the lemma for $J = K+1$.

We begin by defining

$$R_J = [hk^{\varepsilon J}], \qquad S_J = [(k/2^J)\log A] \qquad (J = 0, 1, \ldots).$$

It suffices then to prove that (5) is untenable, whence, in view of Lemma 6, (2) holds, for any integer l with $R_K < l \leqslant R_{K+1}$ and any set of non-negative integers $m_0, \ldots, m_{n-1}$ with $m_0 + \ldots + m_{n-1} \leqslant S_{K+1}$. First we make the preliminary observation that, by virtue of our inductive hypothesis, we have

$$(9) \qquad |f_m(r)/m!| < C^{-\frac{1}{4}\log A \log B}$$

for each integer r with $1 \leqslant r \leqslant R_K$ and each integer m satisfying $0 \leqslant m \leqslant S_{K+1}$. For clearly $f_m(r)$ is given by

$$(\partial/\partial z_0 + \ldots + \partial/\partial z_{n-1})^m \Phi(z_0, \ldots, z_{n-1})$$

evaluated at $z_0 = \ldots = z_{n-1} = r$, where

$$\Phi(z_0, \ldots, z_{n-1}) = \sum_{\lambda_{-1}=0}^{L_{-1}} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_{-1}, \ldots, \lambda_n)\, \Lambda(z_0)\, a_1^{\gamma_1 z_1} \ldots a_{n-1}^{\gamma_{n-1} z_{n-1}}.$$

Arguing by induction with respect to $\mu_1 + \ldots + \mu_{n-1}$ and noting that $\Delta(b_n\lambda_j - b_j\lambda_n;\, m_j)$ is a polynomial in γ_j with coefficients independent of the λ's and with degree m_j, we obtain from (2)

$$(m_0+\mu_0)! \sum_{\lambda_{-1}=0}^{L_{-1}} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_{-1}, \ldots, \lambda_n)\, \Lambda' \gamma_1^{\mu_1} \ldots \gamma_{n-1}^{\mu_{n-1}} a_1^{\lambda_1 r} \ldots a_n^{\lambda_n r} = 0$$

for all non-negative integers $\mu_0, \ldots, \mu_{n-1}$ with $\mu_0 + \ldots + \mu_{n-1} = m$, where Λ' is given by $\Lambda(r)$ with $m_0 + \mu_0$ in place of m_0. But the sum on the left differs from

$$m_0!\, (\log a_1)^{-\mu_1} \ldots (\log a_{n-1})^{-\mu_{n-1}} (\partial/\partial z_0)^{\mu_0} \ldots (\partial/\partial z_{n-1})^{\mu_{n-1}} \Phi(z_0, \ldots, z_{n-1})$$

evaluated at $z_0 = \ldots = z_{n-1} = r$, only in the substitution of α_n for α_n', where α_n' is defined by (7), and the required inequality (9) now follows easily from (6) by estimates similar to those employed in the proof of Lemma 6 [3].

We write, for brevity,

$$F(z) = \{(z-1)\ldots(z-R_K)\}^{S_{K+1}+1}$$

and we denote by Γ the circle in the complex plane, described in the positive sense, with centre the origin and radius $R_{K+1}k^{1/(8n)}$. By Cauchy's residue theorem we have

$$(10)\qquad \frac{1}{2\pi i}\int_{\Gamma}\frac{f(z)}{(z-l)F(z)}\,dz = \frac{f(l)}{F(l)} + \frac{1}{2\pi i}\sum_{r=1}^{R_K}\sum_{m=0}^{S_{K+1}}\frac{f_m(r)}{m!}\int_{\Gamma_r}\frac{(z-r)^m}{(z-l)F(z)}\,dz,$$

where Γ_r denotes the circle in the complex plane, described in the positive sense, with centre r and radius $\frac{1}{2}$. Since, for z on Γ_r,

$$|(z-r)^m/F(z)| \leqslant \{\tfrac{1}{8}(R_K-r-1)!\,(r-2)!\}^{-S_{K+1}-1} \leqslant 8^{R_K S_{K+1}}(R_K!)^{-S_{K+1}-1},$$

we deduce from (9) that $1/2\pi$ times the absolute value of the double sum on the right of (10) is at most

$$R_K(S_{K+1}+1)\,8^{R_K S_{K+1}+1}(R_K!)^{-S_{K+1}-1}C^{-\frac{1}{4}\log A\log B}.$$

Further, for $l \leqslant R_{K+1}$, we have

$$|F(l)| \leqslant \{(l-1)!/(l-R_K-1)!\}^{S_{K+1}+1} \leqslant (2^{R_{K+1}}R_K!)^{S_{K+1}+1}$$

and, if (5) holds, then $|f(l)| > C^{-\frac{1}{2}\log A\log B}$. Thus we see that the absolute value of the number on the right of (10) exceeds $\frac{1}{2}|f(l)/F(l)|$.

Now let θ and Θ denote respectively the upper bound of $|f(z)|$ and the lower bound of $|F(z)|$ with z on Γ. Since $2|z-l|$ with z on Γ exceeds the radius of Γ, we obtain from (10)

$$(11)\qquad 4\theta|F(l)| > \Theta|f(l)|.$$

Clearly we have

$$\Theta \geqslant (\tfrac{1}{2}R_{K+1}k^{1/(8n)})^{R_K(S_{K+1}+1)}$$

and, from (4),

$$\theta \leqslant A^{c_8hk}c_9^{LR_{K+1}k^{1/(8n)}}.$$

(3) Note that $|\gamma_j|^{\mu_j}/\mu_j! \leqslant B^{\mu_j}e^{2L}$ and $m! \geqslant \mu_0!\ldots\mu_{n-1}!$.

Thus we see that

$$(12)\qquad \log\left(\Theta|F(l)|^{-1}\right) \geqslant R_K(S_{K+1}+1)\log\left(\tfrac{1}{2}k^{1/(8n)}\right)$$

and, by virtue of (5),

$$(13)\qquad \log\left(\theta|f(l)|^{-1}\right) \leqslant \{c_8+2c_{10}\log(R_{K+1}/h)\}hk\log A + c_{23}LR_{K+1}k^{1/(8n)}.$$

But the number on the right of (12) is at least

$$2^{-K-6}n^{-1}hk^{\varepsilon K+1}\log k\log A$$

and that on the right of (13) is at most

$$\{c_8+2c_{10}\,\varepsilon(K+1)\log k + c_{23}k^{\varepsilon(K+1)-1/(8n)}\}hk\log A.$$

Further, with the value of ε given at the beginning, we have $2c_{10}\varepsilon = 2^{-7}n^{-1}$ and $\varepsilon < (8n)^{-1}$. Thus (11) is untenable if k is sufficiently large; the contradiction implies the validity of (2) and the lemma follows by induction.

LEMMA 8. *For all integers $l, m_0, \ldots, m_{n-1}, q$ with*

$$1 \leqslant l \leqslant hk,\quad 0 \leqslant m_r \leqslant L\ (0 \leqslant r < n),\quad 2 < q \leqslant 2L_n,\quad (l, q) = 1,$$

(2) is satisfied with l replaced by l/q.

Proof. Let $f(z)$ be defined as in Lemma 6 with $m_0, \ldots, m_{n-1}$ any integers as above. From Lemma 7 we see that (2) holds for all integers l with $1 \leqslant l \leqslant X$ and all non-negative integers $m_0, \ldots, m_{n-1}$ with $m_0+\ldots+m_{n-1} \leqslant Y$, where

$$X = [hk^{n+1}],\qquad Y = [c_{24}k\log A]$$

and $c_{24} = 2^{-(2n/\varepsilon)-1}$. Further, as in the proof of Lemma 7, we see that this implies the validity of (9) for all integers r, m with $1 \leqslant r \leqslant X$, $0 \leqslant m \leqslant Y$. On writing, for brevity,

$$E(z) = \{(z-1)\ldots(z-X)\}^{Y+1}$$

and denoting by Γ the circle in the complex plane, described in the positive sense, with centre the origin and radius $Xk^{1/(8n)}$, we deduce from Cauchy's residue theorem that

$$\frac{1}{2\pi i}\int_{\Gamma}\frac{f(z)}{(z-l/q)E(z)}\,dz = \frac{f(l/q)}{E(l/q)} + \frac{1}{2\pi i}\sum_{r=1}^{X}\sum_{m=0}^{Y}\frac{f_m(r)}{m!}\int_{\Gamma_r}\frac{(z-r)^m}{(z-l/q)E(z)}\,dz,$$

where l, q are any integers satisfying the hypotheses of the lemma and Γ_r denotes the circle in the complex plane described in the positive sense with centre r and radius $1/(2q)$. Since, for z on Γ_r,

$$|(z-r)^m/E(z)| \leqslant \{(8q)^{-1}(X-r-1)!\,(r-2)!\}^{-Y-1} \leqslant 8^{XY}(8q)^{Y+1}(X!)^{-Y-1},$$

it follows from (9) that the absolute value of the double sum on the right of the above equation is at most

$$X(Y+1)8^{XY}(8q)^{Y+2}(X!)^{-Y-1}C^{-\frac{1}{4}\log A\log B} \leqslant (X!)^{-Y-1}C^{-\frac{1}{8}\log A\log B}.$$

Further, by virtue of Lemma 6, we have, for any z on Γ,

$$|f(z)| < A^{c_8hk}c_9^{LXk^{1/(8n)}},$$

and it is clear that

$$|E(z)| \geqslant (\tfrac{1}{2}Xk^{1/(8n)})^{X(Y+1)}$$

and

$$|E(l/q)| \leqslant (2X)^{X(Y+1)} \leqslant 8^{X(Y+1)}(X!)^{Y+1}.$$

Thus we obtain

$$|f(l/q)| < A^{c_8hk}c_9^{LXk^{1/(8n)}}(\tfrac{1}{4}k^{1/(8n)})^{-X(Y+1)} + C^{-\frac{1}{16}\log A\log B},$$

and, since

$$Lk^{1/(8n)} < k \quad \text{and} \quad c_{25}hk^{n+2}\log A < X(Y+1) < \tfrac{1}{32}\log A\log B\log C,$$

the number on the right is at most e^{-XY}.

We now utilize the latter estimate to confirm the validity of (2) with l replaced by l/q. Let the left-hand side of (2) thus modified be denoted by Q. Clearly Q is an algebraic number with degree at most $(dq)^n$ and each conjugate has absolute value at most $A^{c_{26}hk^2}$. Further it is easily verified, on recalling the expression for $\Delta(x; k, l, m)$ given in the proof of Lemma 1, that on multiplying Q by

$$q^{L_0h}a_1^{L_1h}\ldots a_n^{L_nh}(\nu(0, 2hk))^{m_0} \leqslant A^{c_{27}hk^2},$$

one obtains an algebraic integer. Thus, if $Q \neq 0$, we have

$$|Q| \geqslant A^{-c_{28}hk^2q^n}.$$

But it is easily seen from (6) that

$$|Q-f(l/q)| < C^{-\frac{1}{8}\log A\log B}$$

whence $|f(l/q)| \geqslant \frac{1}{2}|Q|$. Since $q \leqslant 2k^{1/2}$ it is clear that the estimate for $|Q|$ given above is inconsistent with the upper bound e^{-XY} for $|f(l/q)|$ obtained earlier. Hence we conclude that $Q = 0$, as required.

4. Proof of the theorem. It is well-known that there exists at least one prime p between L_n and $2L_n$ exclusive and we take $q = p$ in Lemma 8. On writing (2) with l replaced by l/p in the form

$$\sum_{\lambda_n=0}^{L_n}\Big(\sum_{\lambda_{-1}=0}^{L_{-1}}\cdots\sum_{\lambda_{n-1}=0}^{L_{n-1}} p(\lambda_{-1}, \ldots, \lambda_n)\Delta(l/p)\alpha_1^{\lambda_1 l/p}\ldots\alpha_{n-1}^{\lambda_{n-1}l/p}\Big)\alpha_n^{\lambda_n l/p} = 0$$

we see that Lemma 3 implies that either each of the expressions in parenthesis is 0 for all $m_0, \ldots, m_{n-1}$ with $0 \leqslant m_r \leqslant L$ or

$$\alpha_n^l = \alpha_1^{lj_1}\ldots\alpha_{n-1}^{lj_{n-1}}\alpha'^p \tag{14}$$

for some integers $j_1, \ldots, j_{n-1}$ with $0 \leqslant j_r < p$ and some element α' in the field K generated by the α's over the rationals. We first show that the above expressions cannot all vanish for every l with $1 \leqslant l \leqslant hk$ and $(l, p) = 1$.

In fact this would imply that

$$\sum_{\lambda_{n-1}=0}^{L_{n-1}}\Big(\sum_{\lambda_{-1}=0}^{L_{-1}}\cdots\sum_{\lambda_{n-2}=0}^{L_{n-2}} p(\lambda_{-1}, \ldots, \lambda_n)\Delta'(l/p)\alpha_1^{\lambda_1 l/p}\ldots\alpha_{n-1}^{\lambda_{n-1}l/p}\Big)\Delta' = 0$$
$$(0 \leqslant m_{n-1} \leqslant L),$$

where

$$\Delta' = \Delta(b_n\lambda_{n-1}-b_{n-1}\lambda_n; m_{n-1}), \quad \Delta'(l/p) = \Delta(l/p)/\Delta',$$

and since the polynomials $\Delta(x; m_{n-1})$ $(0 \leqslant m_{n-1} \leqslant L)$ are linearly independent we see that the determinant of order $L+1$ with Δ' in the $(\lambda_{n-1}+1)$th row and $(m_{n-1}+1)$th column is not 0. Hence the new sums in parenthesis above would all vanish, and by repeated application of the argument we would obtain

$$\sum_{\lambda_{-1}=0}^{L_{-1}}\sum_{\lambda_0=0}^{L_0} p(\lambda_{-1}, \ldots, \lambda_n)\Delta(\lambda_{-1}+l/p; h, \lambda_0+1, m_0) = 0$$
$$(0 \leqslant \lambda_1 \leqslant L, \ldots, 0 \leqslant \lambda_n \leqslant L).$$

Now if this equation were to hold for all integers l, not divisible by p, with $1 \leqslant l \leqslant hk$ and all m_0 with $0 \leqslant m_0 \leqslant L$ then the polynomial

$$P(x) = \sum_{\lambda_{-1}=0}^{L_{-1}}\sum_{\lambda_0=0}^{L_0} p(\lambda_{-1}, \ldots, \lambda_n)\big(\Delta(\lambda_{-1}+x; h)\big)^{\lambda_0+1}$$

would have at least

$$(hk-[hk/p])(L+1) > h(L_0+1)$$

zeros counted with multiplicities. But since $\Delta(\lambda_{-1}+x; h)$ has degree $h = L_{-1}+1$, it would follow that $P(x)$ vanishes identically; from Lemma 2 we see that the polynomials

$$\big(\Delta(\lambda_{-1}+x; h)\big)^{\lambda_0+1} \quad (0 \leqslant \lambda_{-1} \leqslant L_{-1},\ 0 \leqslant \lambda_0 \leqslant L)$$

are linearly independent and thus $p(\lambda_{-1}, \ldots, \lambda_n)$ would be 0 for all $\lambda_{-1}, \ldots, \lambda_n$. The contradiction proves the assertion.

Hence we conclude that (14) holds for some integer l, not divisible by p, with $1 \leqslant l \leqslant hk$, and some numbers $j_1, \ldots, j_{n-1}$ and α' as indicated above. This gives

$$a_n = a_1^{j_1} \ldots a_{n-1}^{j_{n-1}} a_n'^p$$

where $a_n' = \alpha'^{1/l}$ for some lth root. In particular we see that $a_n'^p$ is an element of K whence, since $(l, p) = 1$, it follows that a_n' must itself be an element of K. We assume now, as we may without loss of generality, that $a_1 = -1$; then

$$\log a_n = (j_1+j)\log a_1 + \ldots + j_{n-1}\log a_{n-1} + p\log a_n',$$

where all the logarithms have their principal values and j is a rational integer with absolute value at most np. On substituting for $\log a_n$ in (1) we obtain

$$0 < |b_1'\log a_1 + \ldots + b_{n-1}'\log a_{n-1} + b_n'\log a_n'| < C^{-\log A \log B},$$

where

$$b_1' = b_1 + b_n(j_1+j), \quad b_n' = pb_n, \quad b_r' = b_r + b_n j_r \quad (1 < r < n).$$

Clearly $b_1', \ldots, b_n'$ are rational integers with absolute values at most $6nk^{1/2}B$. Further we observe that each conjugate of

$$a_n'^p = a_n a_1^{-j_1} \ldots a_{n-1}^{-j_{n-1}}$$

has absolute value at most $(dA')^{np} dA$, and the same estimate holds for some integer a such that $a a_n'^p$ is an algebraic integer. Thus, from Lemma 4, we deduce that the height of a_n' is at most $(2dA')^{4nD}A^{2D/p}$, where D $(\leqslant d^n)$ denotes the degree of K. Since $p > k^{1/2}$ we have $2D/p < \frac{1}{2}$ and this confirms the assertions made at the beginning of § 3.

The proof of the theorem is now completed by induction. We can suppose that $B \geqslant c_1^4$ for otherwise the result holds trivially (cf. [1, IV], Lemma 6). If also $A \geqslant c_2^4$ then (1) clearly remains valid with $c_1 B$ and $c_2 A^{1/2}$ substituted for B and A respectively. Thus we can repeat the above argument and obtain for each $s = 1, 2, \ldots$ a set of integers $b_1^{(s)}, \ldots, b_n^{(s)}$ with absolute values at most $c_1^s B$ and an element $a_n^{(s)}$ of K with height at most

$$c_2^{1+\frac{1}{2}+\ldots+(\frac{1}{2})^{s-1}} A^{(\frac{1}{2})^s}$$

such that (1) holds with $b_1^{(s)}, \ldots, b_n^{(s)}$ and $a_n^{(s)}$ in place of $b_1, \ldots, b_n$ and a_n respectively. The algorithm terminates for some $s \leqslant 2\log\log A$ when the height of $a_n^{(s)}$ is at most c_2^4, and the insolubility of (1) with C sufficiently large is then apparent from the work of [4]. Alternatively we can argue that since there are only finitely many algebraic numbers with bounded degree and height, the process can be continued to yield a number c, independent of A, such that $a_n^{(j)} = a_n^{(j')}$ for distinct $j, j' \leqslant c + 2\log\log A$.

This gives

$$a_n^{(j)q} = a_1^{p_1} \ldots a_{n-1}^{p_{n-1}}$$

where $p_1, \ldots, p_{n-1}, q$ denote rational integers with absolute values at most $p^{c+2\log\log A}$; on substituting for $\log a_n^{(j)}$ in the inequality derived from (1) after j steps we obtain a linear form in which $b_n = 0$ and $b_1, \ldots, b_{n-1}$ are rational integers having absolute values at most $(\log A)^{c_{29}} B$. After repeating the argument n times we derive an inequality involving only one logarithm and recalling that, by hypothesis, the original linear form does not vanish, this is plainly untenable. The contradiction proves the theorem.

References

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

[2] — *Contributions to the theory of Diophantine equations; I: On the representation of integers by binary forms*, Philos. Trans. Royal Soc. London A263 (1968), pp. 173–191.

[3] — and H. M. Stark, *On a fundamental inequality in number theory*, Annals of Math. 94 (1971), pp. 190–199.

[4] N. I. Feldman, *Improvements on the bounds for linear forms in the logarithms of algebraic numbers* (in Russian), Mat. Sbornik 77 (119) (1968), pp. 423–436.

Received on 17. 4. 1971 (159)