ACTA ARITHMETICA
XXVII (1975)

A sharpening of the bounds for linear forms in logarithms III

by

A. BAKER (Cambridge)

In memory of Professors
Yu. V. Linnik and L. J. Mordell

1. Introduction. Let $a_1, \ldots, a_n$ be non-zero algebraic numbers with degrees at most d and suppose that the height of a_j is at most A_j $(\geqslant 4)$. Further let $b_1, \ldots, b_n$ be rational integers with absolute values at most B $(\geqslant 4)$, and let

$$\Lambda = b_1 \log a_1 + \ldots + b_n \log a_n,$$

where the logarithms are assumed to have their principal values. We prove:

THEOREM. *If* $\Lambda \neq 0$ *then* $|\Lambda| > B^{-C\Omega \log \Omega}$, *where*

$$\Omega = \log A_1 \ldots \log A_n,$$

and C *is an effectively computable number depending only on* n *and* d.

The theorem improves upon the recent work of Stark [7] which itself refined several earlier results in this field. It does not, however, include the theorems of the first two memoirs of this series [3], [4], nor indeed those of [5] or [7] wherein, in particular, the linear form Λ possesses algebraic and not merely rational integer coefficients; and it would be of much interest to eliminate $\log \Omega$ and to generalize Λ so as to incorporate these results.

The estimate of [7] was recently utilized by Stark [8] to strengthen the bound for the size of the solutions of the Diophantine equation $y^2 = x^3 + k$ obtained in [2], and moreover a special version was employed by Shorey [6] to sharpen certain theorems concerning the distribution of the primes; it seems likely that these results will admit still further improvement in the light of the work here(1).

(1) Added in proof. The work of this series has recently been applied by R. Tijdeman to show that the famous conjecture of Catalan is, in principle, decidable.

2. Main theory. We signify by $\alpha_1, \ldots, \alpha_n$, where $n \geqslant 2$, algebraic numbers as in § 1, and we denote by K the field which they generate over the rationals; further we denote by $c_1, c_2, \ldots$ numbers greater than 1 that can be specified in terms of n and d only. We suppose that there exist rational integers $b_1, \ldots, b_n$, with $b_n \neq 0$, having absolute values at most B, such that $|\Lambda| < B^{-C\Omega\log\Omega}$, where $C = C(n, d)$ is assumed sufficiently large. We proceed to prove that then, for any c_1, there exists c_2 and a prime p with $c_1 < p < c_2$ such that $K(\alpha_1^{1/p}, \ldots, \alpha_n^{1/p})$ is not an extension of K of degree p^n; we shall show in § 4 that this suffices to establish the theorem.

The notation of [3] will be adopted without change, except that we now define $L_j = [k^{1-1/(4n)}\Omega\log\Omega/\log A_j]$ $(0 \leqslant j \leqslant n)$, where $A_0 = \Omega$. It is then readily verified that Lemmas 5, 6 and 7 of [3] are valid with A replaced by Ω^Ω and $L = L_0\log\Omega$; also one easily checks that Lemma 8 of [3] holds with the range of $m_0, \ldots, m_{n-1}$ extended to cover all non-negative integers with

$$m_0 + \ldots + m_{n-1} \leqslant c_3^{-1} k\Omega\log\Omega \tag{1}$$

for some c_3 as above. We now take q to be a prime p between $k^{1/2}$ and $2k^{1/2}$ exclusive and we assume that $K(\alpha_1^{1/p}, \ldots, \alpha_n^{1/p})$ is an extension of K of degree p^n. Then, for any integers $\lambda_1', \ldots, \lambda_n'$ between 0 and $p-1$ inclusive, (2) of [3] holds with l replaced by l/p and with the $p(\lambda_{-1}, \ldots, \lambda_n)$ other than those such that $\lambda_j \equiv \lambda_j' \pmod p$ for all j, equated to 0. This gives

$$\sum_{\lambda_{-1}=0}^{L'_{-1}} \cdots \sum_{\lambda_n=0}^{L'_n} p(\lambda_{-1}, \lambda_0, \mu_1, \ldots, \mu_n)\Lambda'(l/p)\alpha_1^{\lambda_1 l} \ldots \alpha_n^{\lambda_n l} = 0 \tag{2}$$

for all l with $1 \leqslant l \leqslant hp$, $(l, p) = 1$, where

$$L'_{-1} = L_{-1}, \quad L'_0 = L_0, \quad L'_j = [(L_j - \lambda_j')/p] \quad (1 \leqslant j \leqslant n), \quad \mu_j = \lambda_j' + p\lambda_j,$$

and Λ' is defined like Λ but with λ_j replaced by μ_j. In fact (2) holds with Λ' replaced by Λ; for clearly $\Delta(b_n\mu_r - b_r\mu_n; m_r)$ is a polynomial in $\gamma_r = \lambda_r - b_r\lambda_n/b_n$ with coefficients independent of the λ's and with degree m_r, whence arguing by induction with respect to $m_1 + \ldots + m_{n-1}$ as in the proof of Lemma 7, we infer that (2) remains valid if the product over r in Λ' is replaced by $\gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}}$, and the required result then follows on taking linear combinations. Thus we have shown that from the validity of (2) of [3] for $1 \leqslant l \leqslant h$ and $m_0 + \ldots + m_{n-1} \leqslant k\Omega\log\Omega$ we obtain

$$\sum_{\lambda_{-1}=0}^{L'_{-1}} \cdots \sum_{\lambda_n=0}^{L'_n} p'(\lambda_{-1}, \ldots, \lambda_n)\Lambda(l/p)\alpha_1^{\lambda_1 l} \ldots \alpha_n^{\lambda_n l} = 0$$

for all l with $1 \leqslant l \leqslant hp$, $(l, p) = 1$, and all $m_0, \ldots, m_{n-1}$ satisfying (1), where the $p'(\lambda_{-1}, \ldots, \lambda_n)$ are integers given by some subset of the $p(\lambda_{-1}, \ldots, \lambda_n)$, which, for a suitable choice of $\lambda'_{-1}, \ldots, \lambda'_n$, are not all 0.

We shall demonstrate in the next section that the argument can be repeated and one obtains, for each positive integer J, an equation as above with $L_j' \leqslant L_j/p^J$ $(1 \leqslant j \leqslant n)$ and with l/p replaced by l/p^J, valid for all l with $1 \leqslant l \leqslant hp^J$, $(l, p) = 1$, and all $m_0, \ldots, m_{n-1}$ satisfying (1) with c_3 replaced by p^{-J}. The process is continued until $L_j' = 0$ $(1 \leqslant j \leqslant n)$, which occurs for some J such that $p^J \leqslant k\Omega\log\Omega$. There remains then only the sum over λ_{-1} and λ_0, and the required contradiction follows from Lemma 2 of [3] as in § 4 of that paper; this establishes the assertion at the beginning.

3. Inductive argument. We require the proposition that for each integer $J = 0, 1, \ldots$, with $p^J \leqslant k\Omega\log\Omega$, there exist integers $p^{(J)}(\lambda_{-1}, \ldots, \lambda_n)$, not all 0, with absolute values at most $\Omega^{c_4\Omega hk}$, such that

$$\sum_{\lambda_{-1}=0}^{L_{-1}^{(J)}} \cdots \sum_{\lambda_n=0}^{L_n^{(J)}} p^{(J)}(\lambda_{-1}, \ldots, \lambda_n)\Lambda(l/p^J)\alpha_1^{\lambda_1 l} \ldots \alpha_n^{\lambda_n l} = 0 \tag{3}$$

for all integers l with $1 \leqslant l \leqslant hp^J$, $(l, p) = 1$, and all non-negative integers $m_0, \ldots, m_{n-1}$ with

$$m_0 + \ldots + m_{n-1} \leqslant p^{-J} k\Omega\log\Omega, \tag{4}$$

where $L_{-1}^{(J)} = L_{-1}$, $L_0^{(J)} = L_0$ and $L_j^{(J)} \leqslant L_j/p^J$ $(1 \leqslant j \leqslant n)$ for all J.

The assertion holds for $J = 0$ by Lemma 1 of [3]. We assume the result for $J = K$ and proceed to prove the validity for $J = K+1$. For any non-negative integers $m_0, \ldots, m_{n-1}$ satisfying (4) with $J = K$ we write

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

It is then readily verified that

$$|f(z)| \leqslant \Omega^{c_5\Omega hk} c_6^{L|z|/p^K},$$

and furthermore that for any integer l with $h < l/p^K \leqslant hk^{2n}$, either (3) holds with $J = K$ or

$$|f(l)| \geqslant p^{-4hKL_0}\Omega^{-c_7\Omega hk\{1+\log(l/(hp^K))\}} c_8^{-Ll/p^K};$$

these estimates follow in fact as in the proof of Lemma 6 of [3], on noting that the left-hand side of (3), multiplied by

$$p^{4hKL_0}\alpha_1^{L_1^{(K)}l} \ldots \alpha_n^{L_n^{(K)}l}\big(\nu(l; 2hp^K)\big)^{m_0},$$

is an algebraic integer, and we have $m_0 p^K \leqslant k\Omega\log\Omega$. One deduces next, as in Lemma 7 of [3], that for some ε $(0 < \varepsilon < 1)$ depending only on n and d, and for any integer J' with $0 \leqslant J' < 2n/\varepsilon$, (3) holds with $J = K$

for all integers l with $1 \leqslant l \leqslant hp^K k^{\varepsilon J'}$ and all non-negative integers $m_0, \ldots, m_{n-1}$ satisfying (4) with k replaced by $k/2^{J'}$; the argument follows closely its earlier counterpart, h and $\log A$ being replaced by hp^K and $p^{-K}\Omega\log\Omega$ respectively and, since $KL_0\log p$ does not exceed $k\Omega\log\Omega$, one obtains the same estimates as in [3] for the numbers on the right of (12) and (13) with, say, K' in place of K. Similarly one sees that the analogue of Lemma 8 of [3] holds, that is, (3) is valid with l replaced by l/p for all l with $1 \leqslant l \leqslant hkp^K$, $(l, p) = 1$, and all $m_0, \ldots, m_{n-1}$ satisfying (4) with $J = K+1$ (2). Finally one argues as in § 2 above, and this yields the required result.

4. Proof of the theorem. We adopt the notation of § 2 and record first two preliminary lemmas; here A denotes the maximum of $A_1, \ldots, A_n$ and $D = d^n$.

LEMMA 1. *If* $\Lambda \neq 0$ *then*

$$\log|\Lambda| > -4nDB\log(dA).$$

LEMMA 2. *If* $\Lambda = 0$ *but* $b_1, \ldots, b_n$ *are not all* 0 *then in fact* $\Lambda = 0$ *for some* $b_1, \ldots, b_n$, *not all* 0, *with absolute values at most*

$$(4^{n^2} D^2 \log A)^{(2n+1)^2}.$$

The first result is Lemma 6 of [1] and the second is a consequence of the main deduction of that paper; indeed it is clear that the conclusion of the last paragraph of § 2 of [1] holds when $\Lambda = 0$, and the required result follows on applying this with $n' = n$, $\delta = 1$ and $H = B-1$ $(\geqslant B^{1/n})$, where B, the maximum of the absolute values of $b_1, \ldots, b_n$, is chosen minimally.

We shall suppose, as we may without loss of generality, that $A_1 \leqslant A_2 \leqslant \ldots \leqslant A_n = A$ and that $a_1 = -1$. We can clearly suppose further that $A > C'$, $B > C'$ for some sufficiently large $C' = C'(n, d)$, for otherwise the theorem follows at once either from the result of [3] or from Lemma 1. We note also that if $\Lambda \neq 0$, then, by Lemma 1,

$$\log|\Lambda| > -cB\log A,$$

where $c = 8nD$, and thus, if $|\Lambda| < B^{-C\Omega\log\Omega}$, we have $B\log A > (C/c)\,\Omega$, whence

$$\log A_j < B^{c/C} \quad (1 \leqslant j \leqslant n-1). \tag{5}$$

We now apply the result of § 2 with $c_1 = (4d)^n$; if p is the prime indicated there, then, for some m with $0 \leqslant m < n$, $a_{m+1}^{1/p}$ does not generate an extension of $K(a_1^{1/p}, \ldots, a_m^{1/p})$ of degree p. Hence, by Lemma 3 of [3]

(2) In the proofs of the analogues of Lemmas 7 and 8, the factors $(z-l)$ in $F(z)$ and $E(z)$ with $(l, p) > 1$ must be deleted; the arguments are not substantially affected.

we have

$$a_{m+1} = a_1^{r_1} \ldots a_m^{r_m} \gamma^p \tag{6}$$

for some γ in K and some integers $r_1, \ldots, r_m$ with $0 \leqslant r_j < p$. We shall suppose that the height $A' = A_{m+1}$ of a_{m+1} satisfies

$$\log A' < cB^{c/C}, \tag{7}$$

and we verify first that this involves no loss of generality. In fact, if $m \leqslant n-2$, (7) is a weaker version of (5); thus we assume that $m = n-1$, whence $A' = A$. Clearly each conjugate of

$$\gamma = a_n^{1/p} a_1^{-r_1/p} \ldots a_m^{-r_m/p}$$

has absolute value at most $(dA)^{1/p}(dA_m)^m$, and thus, by Lemma 4 of [3], the height of γ is at most $(2dA_m)^{2mD} A^{2D/p}$. This would be less than $A^{1/2}$ if (7) did not hold, for then (5) would give $A_m^c < A$. But from (6) we see that

$$\log a_n = r_1 \log a_1 + \ldots + r_m \log a_m + p\log\gamma$$

for some value of $\log\gamma$, and thus

$$\Lambda = b_1' \log a_1 + \ldots + b_m' \log a_m + b_n' \log\gamma$$

where

$$b_j' = b_j + b_n r_j \quad (1 \leqslant j \leqslant m), \qquad b_n' = b_n p.$$

The integers b_j' plainly have absolute values at most $2pB$ and hence, on modifying b_1' if necessary so as to make $\log\gamma$ principal-valued, we see that the theorem would follow by induction on A. It suffices therefore to assume that (7) is valid.

We now construct, as far as possible, a sequence $\gamma_1 = \gamma, \gamma_2, \gamma_3, \ldots$ of elements of K such that $\gamma_l = a_1^{r_{l1}} \ldots a_m^{r_{lm}} \gamma_{l+1}^p$ $(l = 1, 2, \ldots)$, where the r_{lj} are integers with $0 \leqslant r_{lj} < p$. Clearly we have

$$a_{m+1} = a_1^{s_{l1}} \ldots a_m^{s_{lm}} \gamma_l^{p^l}, \tag{8}$$

where the s_{lj} are integers with $0 \leqslant s_{lj} < p^l$, and from this we deduce as above that the height of γ_l is at most $(2DA')^{2nD}$. Let H be the bound specified in Lemma 2 with the latter number in place of A and with $n+1$ in place of n. We distinguish two cases according as the sequence terminates for some l with $p^l \leqslant H$ or it does not. In the latter case, let l be the least integer with $p^l > H$. From (8), taking logarithms, and Lemma 2, we see that there exist integers $b', b_1', \ldots, b_{m+1}'$, not all 0, with absolute values at most H, such that

$$b_1' \log a_1 + \ldots + b_{m+1}' \log a_{m+1} + b' \log\gamma_l = 0,$$

and, on utilizing (8) again and eliminating γ_l, we obtain

$$b_1'' \log a_1 + \ldots + b_{m+1}'' \log a_{m+1} = 0 \tag{9}$$

for some integer b_1'', where

$$b_j'' = p^l b_j - b' s_{lj} \quad (1 < j \leqslant m), \quad b_{m+1}'' = p^l b_{m+1}' + b'.$$

Now the b_j'' $(j > 1)$ are integers with absolute values at most $2pH^2$; thus all b_j'' have absolute values at most $2npH^2$ and, by (7), this is less than B if C is sufficiently large. Further, from (9), we can plainly express $b_{m+1}''\Lambda$ as a linear form in the $\log \alpha_j$ with $j \neq m+1$ and with integer coefficients having absolute values at most $2B^2$. Hence, if $b_{m+1}'' \neq 0$, the theorem follows by induction on n. If $b_{m+1}'' = 0$ then, since $p^l > H$, we have $b' = 0$ and so $b_j'' \neq 0$ for some $j \leqslant m$; in this case the elimination of $\log \alpha_j$ furnishes the desired conclusion.

It remains to consider the possibility that the sequence terminates for some l with $p^l \leqslant H$. From (8) we see that Λ can be expressed as a linear form in the $\log \alpha_j$ with α_{m+1} replaced by γ_l and with integer coefficients having absolute values at most $2nHB$; further, from (7), this is less than B^2 if C is sufficiently large. Furthermore, since by supposition the sequence terminates, we deduce from Lemma 3 of [3] that $\gamma_l^{1/p}$ generates an extension of $K(\alpha_1^{1/p}, \ldots, \alpha_m^{1/p})$ of degree p. Recalling that γ_l has height A'', say, where $\log A''/\log A'$ is bounded in terms of n and d only, it follows that the hypotheses of § 2 hold with γ_l substituted for α_{m+1} and with a reduced value of C. After at most n such substitutions this contradicts the result of § 2 (since the choice of p there depends only on n and d) and the contradiction proves the theorem.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers IV*, Mathematika 15 (1968), pp. 204–216.

[2] — *Contributions to the theory of Diophantine equations II; The Diophantine equation* $y^2 = x^3 + k$, Phil. Trans. Royal Soc. London A263 (1968), pp. 193–208.

[3] — *A sharpening of the bounds for linear forms in logarithms*, Acta Arith. 21 (1972), pp. 117–129.

[4] — *A sharpening of the bounds for linear forms in logarithms II*, Acta Arith. 24 (1973), pp. 33–36.

[5] — *A central theorem in transcendence theory*, in *Diophantine approximation and its applications* (Academic Press, 1973), pp. 1–23.

[6] T. N. Shorey, *On gaps between numbers with a large prime factor II*, Acta Arith. 25 (1974), pp. 365–373.

[7] H. M. Stark, *Further advances in the theory of linear forms in logarithms*, in *Diophantine approximation and its applications*, Academic Press, 1973, pp. 255–293.

[8] — *Effective estimates of solutions of some diophantine equations*, Acta Arith. 24 (1973), pp. 251–259.

Received on 25. 8. 1973 (442)

ACTA ARITHMETICA
XXVII (1975)

Применения дисперсионного метода в проблеме Гольдбаха

Б. М. Бредихин, Н. А. Яковлева (Куйбышев)

1. Многие аддитивные задачи с простыми числами решаются с помощью метода оценки тригонометрических сумм, открытого И. М. Виноградовым [5], в соединении с теоремами, касающимися распределения простых чисел в арифметических прогрессиях с медленно растущей разностью. При сведении тригонометрических сумм по простым числам к двойным суммам фундаментальной является идея И. М. Виноградова по „сглаживанию" таких сумм.

В основе дисперсионного метода, разработанного Ю. В. Линником [8], также лежит идея „сглаживания" наряду с рассуждениями, имеющими свои истоки в классической работе П. Л. Чебышева *О средних величинах* (см. [12]).

Эта же идея используется в методе большого решета, созданного Ю. В. Линником [9] и позволившего получить ряд теорем, относящихся к распределению простых чисел в арифметических прогрессиях в среднем.

В самое последнее время Ю. В. Линник (совместно с одним из авторов данной статьи) рассмотрел применения дисперсионного метода и теорем о простых числах к некоторым тернарным аддитивным задачам (см. [2] – [4]).

В работе [4] дано новое доказательство теоремы Виноградова о представлении нечетных чисел суммами трех простых чисел (ради простоты берутся нечетные числа, не содержащие малых простых делителей).

Аналогично может быть изучено уравнение

$$p + p_1 - p_2 = p_3, \tag{1}$$

где p, p_1, p_2, p_3 пробегают простые числа, $p + p_1 \leqslant n$. Пусть $Q(n)$ — число решений уравнения (1). Почти буквальным повторением рассуждений работы [4] (с предварительным фиксированием p_3) может быть доказана следующая теорема: