Let us remark finally that in Theorem 4 the assumption $\delta(A) > 0$ cannot be replaced by the following weaker assumption:

$$\delta_1(A) = \liminf_{n\to\infty} \frac{A(n)}{n} > 0.$$

This can be seen from the following example:

Let $A = \bigcup_{k=0}^{\infty} A_k$, where

$$A_k = \{2^{k+1}+1, 2^{k+1}+2, \ldots, 2^{k+1}+2^k\} \quad (k = 0, 1, \ldots).$$

It is easy to see that $\delta_1(A) = \frac{1}{2}$, $\delta_2(A) = \frac{3}{4}$ and it can easily be proved that $(\frac{3}{5}, \frac{4}{3}) \cap R(A) = \emptyset$.

References

[1] G. H. Hardy–E. M. Wright, *An introduction to the theory of numbers*, Oxford 1954.

[2] S. S. Pillai, *On some functions connected with* $\varphi(n)$, Bull. Amer. Math. Soc. 35 (1929), pp. 832-836.

[3] W. Sierpiński, *Sur une propriété des nombres naturels*, Elem. Math. 19 (1964), pp. 27-29.

[4] — *Elementary theory of numbers*, Warszawa 1964.

Reçu par la Rédaction le 6. 6. 1968

ACTA ARITHMETICA
XV (1969)

An effective p-adic analogue of a theorem of Thue

by

J. Coates (Cambridge)

I. Introduction. A famous theorem of Thue [11] states that the diophantine equation

$$f(x, y) = m, \tag{1}$$

where f denotes an irreducible binary form with integer coefficients and degree at least 3, and m is any integer, possesses only a finite number of solutions in integers x, y. Thue's theorem was extended by Siegel [10], both with regard to the basic result obtained by Thue on rational approximations to algebraic numbers, from which the theorem referred to above followed as a corollary, and in connexion with generalizations to integer solutions of equations in algebraic number fields. This work gave rise to many further developments; in particular Mahler [5], [6], [7], using Siegel's methods, established far-reaching p-adic analogues of the original theorems, and, in 1955, Roth [9] succeeded in establishing a profound improvement on the work of Thue-Siegel, giving a best possible approximation inequality.

All the work described above, however, is non-effective, in that although it establishes the finiteness of the number of solutions of diophantine equations of the type (1), it does not yield an effective algorithm for their explicit determination. In a recent paper [3], Baker gave the first effective proof of Thue's original theorem, obtaining thereby an explicit upper bound for the size of all integer solutions x, y of (1). The object of the present paper is to prove, by means of Baker's method, certain effective p-adic analogues of Thue's theorem, similar to those first obtained by Mahler in a non-effective form. As above, $f(x, y)$ will signify a binary form with integer coefficients and degree $n \geqslant 3$, irreducible over the rationals, and m will signify a non-zero integer. By $p_1, \ldots, p_s$ we shall denote a fixed set of s prime numbers, and we shall use $\mathfrak{m}$ to denote the largest integer, comprised solely of powers of $p_1, \ldots, p_s$, which divides m. Further, we shall suppose that $\varkappa$ is any number satisfying

$$\varkappa > n(s+1)+1. \tag{2}$$

Our main result is then as follows:

THEOREM 1. *All solutions of* (1) *in integers* x, y, *with* [1] $(x, y, p_1 \dots p_s) = 1$, *satisfy*

$$\max(|x|, |y|) < Ce^{(\log(|m|/|\mathfrak{m}|))^{\varkappa}},$$

where C *is an effectively computable number depending on* $n, \varkappa, p_1, \dots, p_s$ *and the coefficients of* f, *but not on* m.

It will be observed that when $s = 0$, that is when no primes $p_1, \dots, p_s$ are specified, Theorem 1 reduces to the theorem of Baker mentioned earlier. Further it will be seen that if m is comprised only of powers of $p_1, \dots, p_s$, then $|m|/|\mathfrak{m}| = 1$, and so all solutions of (1) in integers x, y with $(x, y, p_1 \dots p_s) = 1$ are bounded by an effectively computable number not depending on m. Furthermore it is clear from the theorem that, for any given m, one can effectively compute the set of all rational numbers x, y satisfying (1), the denominators of which are divisible solely by powers of $p_1, \dots, p_s$.

Theorem 1 can be interpreted in terms of rational approximations to algebraic numbers. Let $f(x)$ be an irreducible polynomial with integer coefficients and degree $n \geqslant 3$. Again let $p_1, \dots, p_s$ denote a fixed set of primes, and suppose that $\varkappa$ satisfies (2). We signify by $|\ |_{p_1}, \dots, |\ |_{p_s}$ the usual valuations of the rational field defined by $p_1, \dots, p_s$, normalized so that $|p_j|_{p_j} = 1/p_j$ [2]. It is then apparent from Theorem 1 that the following result holds.

THEOREM 2. *For any pair of relatively prime integers* q, r, *we have*

$$|q^n f(r/q)| \prod_{j=1}^{s} |q^n f(r/q)|_{p_j} > ce^{(\log Q)^{1/\varkappa}},$$

where $Q = \max(|q|, |r|)$, *and* $c > 0$ *is an effectively computable number depending on* $n, \varkappa, p_1, \dots, p_s$ *and the coefficients of* f, *but not on* q *or* r.

The inequality asserted by Theorem 2 gives an effective limit to the degree of precision by which the complex or p-adic zeros of f can be approximated by rationals r/q. When $s = 0$, Theorem 2 becomes essentially Theorem 2 of [3], which relates to the approximation of a real zero of f.

As regards the proof of these results, our work involves extensions of the various analytic techniques of [3] to functions defined on the completion of the algebraic closure of the field of p-adic numbers. We shall assume an acquaintance with the elements of algebraic number theory as expounded, for example, in Artin [2], Hecke [4], or O'Meara [8].

(1) By $(a, b, \dots)$ we mean the greatest common divisor of $a, b, \dots$

(2) See, e.g. Artin [2].

In addition, we make use of certain simple properties of the Schnirelman line integral as described, for example, in the appendix to [1].

In conclusion, I wish to express my sincere thanks to Dr. A. Baker, both for allowing me to see a manuscript of [3] prior to its publication, and for his valuable advice.

II. Notation. In the sequel, Q will denote the field of rational numbers, K will denote an algebraic extension of Q of finite degree d, $\mathfrak{p}$ will denote a prime ideal in K, and p will denote the unique rational prime divisible by $\mathfrak{p}$. We signify, as usual, the exponent to which $\mathfrak{p}$ divides an arbitrary element a of K by $\mathrm{ord}_{\mathfrak{p}} a$, and define the valuation $|\ |_{\mathfrak{p}}$ on K by $|a|_{\mathfrak{p}} = p^{-j}$, where $j = (\mathrm{ord}_{\mathfrak{p}} a)/(\mathrm{ord}_{\mathfrak{p}} p)$. We retain $|\ |$ for the ordinary absolute value.

Let now Q_p denote the completion of Q with respect to the p-adic valuation $|\ |_p$. The valuation of Q_p extends uniquely to the algebraic closure of Q_p [3]. We denote by Ω_p the completion of the algebraic closure of Q_p equiped with the valuation $|\ |_p$ extending that of Q_p. Certain results from the theory of analytic functions on Ω_p will play a fundamental role in our work, and we now mention these briefly. An *analytic function* on a disc $|z|_p < R$ in Ω_p is defined to be a power series $f(z) = \sum_{m=0}^{\infty} a_m z^m$ which converges in the disc, that is, $\lim_{m\to\infty} |a_m z^m|_p = 0$ when $|z|_p < R$. By a *meromorphic function*, we mean the quotient of two analytic functions. We shall, in particular, make use of the analytic functions

$$\exp z = \sum_{m=0}^{\infty} \frac{z^m}{m!}, \qquad \log(1+z) = \sum_{m=1}^{\infty} (-1)^{m+1} \frac{z^m}{m},$$

which are defined for $|z|_p < p^{-1/(p-1)}$ and $|z|_p < 1$, respectively. These functions satisfy the usual functional equations in their regions of convergence. Further we have

$$|\exp z - 1|_p = |z|_p, \qquad |\log(1+z)|_p = |z|_p, \tag{3}$$

for all z satisfying $|z|_p < p^{-1/(p-1)}$.

Let $f(z)$ be a meromorphic function on the disc $|z|_p < R$, and let Γ, a be elements of Ω_p satisfying $|\Gamma|_p < R$, $|a|_p < R$. We define the *Schnirelman line integral* of $f(z)$ on Γ with centre $z = a$ to be the limit

$$\int_{\Gamma, a} f(z)\,dz = \lim_{\substack{m\to\infty \\ (m,p)=1}} \frac{1}{m} \sum_{k=1}^{m} f(a + \Gamma_{\eta_k^{(m)}}),$$

(3) To extend the valuation of Q_p to its algebraic closure, we define $|a|_p$, for an arbitrary element a in the closure, to be $|Na|_p^{1/n}$, where Na and n denote respectively the norm and degree of a over Q_p; see Artin [2].

when it exists, where $\eta_1^{(m)}, \ldots, \eta_m^{(m)}$ denote the mth roots of unity in Ω_p. The properties of this integral, which are analogous to those of the classical complex line integral, are given in the appendix to [1], and shall be used without comment. The most important of these properties for us is the analogue of Cauchy's integral formula, namely, if $f(z)$ is analytic in the disc $|z|_p < R$ and x is such that $|x-a|_p < |\Gamma|_p$, then

$$f_n(x) = n! \int_{\Gamma,a} \frac{f(z)(z-a)}{(z-x)^{n+1}}\, dz,$$

where $f_n(x)$ denotes the nth derivative of $f(z)$ evaluated at $z = x$. Also we shall make frequent reference to the fact that

$$\left| \int_{\Gamma,a} f(z)\, dz \right|_p \leqslant \max |f(z)|_p,$$

where the maximum is over all z with $|z-a|_p = |\Gamma|_p$; this is clear from the definition.

Finally, we record the product formula for K, to which repeated reference will be made. Namely, if β is any non-zero element of K, we have

$$\prod_{\mathfrak{p}} |\beta|_{\mathfrak{p}}^{n_{\mathfrak{p}}} = 1,$$

where the product ranges over all valuations of K, both archimedean and non-archimedean, and $n_{\mathfrak{p}}$ [4] is the degree of the completion of K at $\mathfrak{p}$ over the completion of Q at p; the formula follows immediately from the familiar equations

$$\prod_{p} |N\beta|_p = 1, \qquad |N\beta|_p = \prod_{\mathfrak{p}|p} |\beta|_{\mathfrak{p}}^{n_{\mathfrak{p}}},$$

where, as usual, $N\beta$ denotes the field norm of β. We deduce at once that, if β is a non-zero integer in K, we have

$$|\beta|_{\mathfrak{p}} |\beta^{(1)}| \ldots |\beta^{(d)}| \geqslant 1, \tag{4}$$

where $\beta^{(1)}, \ldots, \beta^{(d)}$ denote the complex field conjugates of β.

III. The p-adic logarithms of algebraic numbers. Let K be an algebraic number field of degree d, generated by an element θ with height [5] Θ. Let $\alpha_1, \ldots, \alpha_n$ be $n \geqslant 2$ non-zero elements of K, with heights

[4] Alternatively when $\mathfrak{p}$ is non-archimedean $n_{\mathfrak{p}} = e_{\mathfrak{p}} f_{\mathfrak{p}}$, where $e_{\mathfrak{p}}$ is the exponent to which $\mathfrak{p}$ divides p and $f_{\mathfrak{p}}$ is defined by the property that the number of elements in the residue field of $\mathfrak{p}$ is $p^{f_{\mathfrak{p}}}$.

[5] As usual, the height of an algebraic number is defined to be the maximum of the ordinary absolute values of the relatively prime integer coefficients in its minimal polynomial.

$A_1, \ldots, A_n$, respectively, and write $A = A_n$. Let $\mathfrak{p}$ be any prime ideal of K, and let p be the unique rational prime divisible by $\mathfrak{p}$. Suppose further that, for some number $\Xi > 0$, we have

$$\max\{|\alpha_i|_{\mathfrak{p}}, |\alpha_i|_{\mathfrak{p}}^{-1}\} \leqslant \Xi \qquad (1 \leqslant i \leqslant n), \tag{5}$$

and let $\delta, \varkappa$ be real numbers with

$$\delta > 0, \qquad \varkappa > n+1.$$

We shall prove in § V that Theorem 1 can be reduced to a verification of the following result.

THEOREM 3. *If $b_1, \ldots, b_{n-1}$ are rational integers, with absolute values at most H, satisfying*

$$0 < |\alpha_1^{b_1} \ldots \alpha_{n-1}^{b_{n-1}} - \alpha_n|_{\mathfrak{p}} < e^{-\delta H}, \tag{6}$$

then

$$H < \max\{C, (\log A)^{\varkappa}\},$$

where C is an effectively computable number depending on n, d, Θ, Ξ, $A_1, \ldots, A_{n-1}$, p, δ, $\varkappa$, but not on A.

The purpose of this section is to show that it suffices to establish a modified form of Theorem 3, involving an inequality for a linear form in the p-adic logarithms of algebraic numbers, in place of (6). First we make a preliminary observation concerning the condition (5). It will in fact suffice to prove Theorem 3 with (5) replaced by

$$|\alpha_i - 1|_{\mathfrak{p}} < p^{-\nu} \qquad (1 \leqslant i \leqslant n), \tag{7}$$

where $\nu = 20\,d$. This new condition is required for the convergence of the p-adic logarithms at the points α_i. The number ν is chosen for later convenience, and our work could be modified so that a less stringent inequality could be taken here. As regards the proof that (5) can be replaced by (7), we assume that the hypotheses of Theorem 3 hold with the original condition (5), and we suppose that the theorem has been proven under the new condition (7). We note first that (5) and (6) imply that $|x|_{\mathfrak{p}} = |y|_{\mathfrak{p}}$, where, for brevity, we have written x for $\alpha_1^{b_1} \ldots \alpha_{n-1}^{b_{n-1}}$ and y for α_n. For otherwise we would have either $|x|_{\mathfrak{p}} < |y|_{\mathfrak{p}}$ or $|x|_{\mathfrak{p}} > |y|_{\mathfrak{p}}$; the first alternative is impossible for sufficiently large H since it would give

$$\Xi^{-1} \leqslant |y|_{\mathfrak{p}} \leqslant \max(|x-y|_{\mathfrak{p}}, |x|_{\mathfrak{p}}) = |x-y|_{\mathfrak{p}} < e^{-\delta H},$$

and the second alternative is also impossible since it would give

$$\Xi^{-1} \leqslant |y|_{\mathfrak{p}} < |x|_{\mathfrak{p}} \leqslant \max(|x-y|_{\mathfrak{p}}, |y|_{\mathfrak{p}}) = |x-y|_{\mathfrak{p}} < e^{-\delta H}.$$

Now choose an element π in K such that $\mathrm{ord}_{\mathfrak{p}}\pi = 1$; such an element is given, for example, by one of the numbers in an integral basis for $\mathfrak{p}$, and so can be chosen to have height bounded above by a number depending only on d, Θ and p. Since $|x|_{\mathfrak{p}} = |y|_{\mathfrak{p}}$, we have $\sum_{i=1}^{n-1} b_i\sigma_i = \sigma_n$, where σ_i denotes $\mathrm{ord}_{\mathfrak{p}}a_i$ $(1 \leqslant i \leqslant n)$. Thus, on writing $a_i' = a_i\pi^{-\sigma_i}$ and $x' = a_1'^{b_1}\dots a_{n-1}'^{b_{n-1}}$, $y' = a_n'$, we deduce from (6) that

$$0 < |x'-y'|_{\mathfrak{p}} < e^{-\delta H}|\pi^{-\sigma_n}|_{\mathfrak{p}} \overset{!}{<} e^{-\frac{\delta}{2}H},$$

if H is sufficiently large. Further, it is clear that for each suffix i with $1 \leqslant i \leqslant n$, we have $\mathrm{ord}_{\mathfrak{p}}a_i' = 0$ and, from (5), $\log A_i'/\log A_i$, where A_i' denotes the height of a_i', is bounded above by a number depending only on d, Θ, Ξ, and p (cf. [3], § 6). Since $\mathrm{ord}_{\mathfrak{p}}(a_i') = 0$, it follows from the generalization of Euler's theorem to algebraic number fields ([6]) that there is an integer q, bounded above by a number depending only on d, Θ and p, such that

$$|a_i'^q - 1|_{\mathfrak{p}} < p^{-\nu} \quad (1 \leqslant i \leqslant n).$$

Also we observe that

$$|x'^q - y'^q|_{\mathfrak{p}} = |x'-y'|_{\mathfrak{p}}|x'^{q-1} + x'^{q-2}y' + \dots + y'^{q-1}|_{\mathfrak{p}} \leqslant |x'-y'|_{\mathfrak{p}} < e^{-\frac{\delta}{2}H},$$

and we cannot have $x'^q = y'^q$, since this would imply that $x' = \omega y'$, where ω is a qth root of unity in K, whence

$$0 < |\omega - 1|_{\mathfrak{p}} = |y'|_{\mathfrak{p}}|\omega - 1|_{\mathfrak{p}} = |x'-y'|_{\mathfrak{p}} < e^{-\frac{\delta}{2}H},$$

which is impossible for sufficiently large H by virtue of the fact that, by (4), $|\omega - 1|_{\mathfrak{p}} \geqslant 2^{-d}$. Further, we note that $\log A_i''/\log A_i$, where A_i'' denotes the height of $a_i'^q$, is bounded above by a number depending only on d, Θ, Ξ, and p. Hence we see that all the hypotheses of Theorem 3 are satisfied with $a_1, \dots, a_n$ replaced by $a_1'^q, \dots, a_n'^q$, δ replaced by $\delta/2$, $\varkappa$ replaced by $\frac{1}{2}(\varkappa+n+1)$, and with the new condition (7) in place of (5), provided that we assume, as we may, that H is sufficiently large. The conclusion of Theorem 3 with these new quantities implies the corresponding conclusion with the original quantities, since, as remarked earlier, $\log A_i''/\log A_i$ is bounded above by a number depending only on d, Θ, Ξ, and p.

(6) The form of Euler's theorem given, for example, in Hecke [4], p. 102, must be modified slightly to give the result asserted above. In [4], the hypotheses require that a be an integer in K; in fact the assertion remains valid if a is any element of K with $\mathrm{ord}_{\mathfrak{p}}a = 0$. For choose an integer β in K such that $\mathrm{ord}_{\mathfrak{p}}\beta = 0$ and βa is an integer in K. Then, by the result in [4], $\mathrm{ord}_{\mathfrak{p}}(\beta^q - 1) > \nu\mathrm{ord}_{\mathfrak{p}}\ p$, $\mathrm{ord}_{\mathfrak{p}}((\beta a)^q - 1) > \nu\mathrm{ord}_{\mathfrak{p}}p$, and so $\mathrm{ord}_{\mathfrak{p}}(a^q - 1) > \nu\mathrm{ord}_{\mathfrak{p}}p$.

We can now state the version of Theorem 3 which we shall ultimately establish. We adopt the same notation as before; $a_1, \dots, a_n$ denote elements of K satisfying (7), δ is any positive number, and $\varkappa > n+1$. However, in order to define $\log a_i$, we regard K as embedded in Ω_p in such a way that the valuations $|\ |_{\mathfrak{p}}$ of K and $|\ |_p$ of Ω_p coincide, and we treat this embedding as an identification.

THEOREM 4. *Suppose that $b_1, \dots, b_n$ are integers with absolute values at most H^g, where H, g are positive integers, satisfying*

$$0 < |b_1\log a_1 + \dots + b_n\log a_n|_p < e^{-\delta H}. \tag{8}$$

Suppose further that there are no integers $b_1', \dots, b_n'$, with absolute values at most H, satisfying $b_1'\log a_1 + \dots + b_n'\log a_n = 0$ other than $b_1' = \dots = b_n' = 0$. Then

$$H < \max\{C, (\log A)^{\varkappa}\},$$

where C is an effectively computable number depending on $n, d, A_1, \dots, A_{n-1}, p, g, \delta, \varkappa$, but not on A.

We now show that Theorem 4 implies Theorem 3. Suppose therefore that the hypotheses of Theorem 3 hold with (5) replaced by (7). Then, from (3),

$$|\log a_i|_p = |a_i - 1|_p < p^{-\nu} \quad (1 \leqslant i \leqslant n), \tag{9}$$

whence $|z|_p < p^{-\nu}$, where $z = b_1\log a_1 + \dots + b_{n-1}\log a_{n-1} - \log a_n$. Thus by (3) again and condition (6) of Theorem 3, we obtain

$$0 < |z|_p = |\exp z - 1|_p = |a_1^{b_1}\dots a_{n-1}^{b_{n-1}}a_n^{-1} - 1|_p < e^{-\delta H};$$

for clearly (7) implies that $|a_n|_p = 1$. It suffices now to deduce the existence of an integer k, with $1 \leqslant k \leqslant n$, possessing the following properties: (i) There are integers $b_1, \dots, b_n$, with absolute values at most $(2H)^{n-k+1}$, such that (8) holds; (ii) At least $n-k$ of the integers $b_1, \dots, b_n$ are zero; (iii) The only integers $b_1', \dots, b_n'$, with absolute values at most H, such that $b_1'\log a_1 + \dots + b_n'\log a_n = 0$, and such that $b_j' = 0$ whenever $b_j = 0$, are given by $b_1' = \dots = b_n' = 0$. For having established the existence of such a k, the conclusion of Theorem 3 follows from that of Theorem 4, the latter being applied with n now given by the number of non-zero b_j, and g defined as twice the original n. Note here that Theorem 4 is applied to an arbitrary subset of the original $a_1, \dots, a_n$ and the necessity to distinguish between $A = A_n$ and $A_1, \dots, A_{n-1}$ does not always arise. To prove the assertion, we note first that (i) and (ii) hold for $k = n$ (since $0 < |z|_p < e^{-\delta H}$, with z defined as above), and so we may assume that (iii) does not hold for $k = n$. It follows that there is a least positive integer k for which (i) and (ii) hold but (iii) does not,

and by (ii) we may assume that $k > 1$. Let $b_1', \ldots, b_n'$ be a set of integers with the properties specified by (iii) other than $b_1' = \ldots = b_n' = 0$, say $b_l' \neq 0$, and put

$$b_j'' = b_j b_l' - b_j' b_l \quad (1 \leqslant j \leqslant n),$$

where $b_1, \ldots, b_n$ are integers satisfying (i) and (ii). Then

$$0 < |b_1'' \log a_1 + \ldots + b_n'' \log a_n|_p = |b_l'|_p |b_1 \log a_1 + \ldots + b_n \log a_n|_p < e^{-\delta H}.$$

Further, $b_j'' = 0$ whenever $b_j = 0$, and since also $b_l'' = 0$, $b_l' \neq 0$, it follows that at least $n-k+1$ of the integers $b_1'', \ldots, b_n''$ are zero. Moreover, the b_j'' have absolute values at most $(2H)^{n-k+2}$. Thus (i) and (ii) hold with k replaced by $k-1$. But, by the minimal choice of k, (iii) must hold with k replaced by $k-1$, and so $k-1$ has all the required properties. This completes the proof that Theorem 4 implies Theorem 3.

IV. Proof of Theorem 4. The notation introduced in § III will be assumed without change. $C, c_1, c_2, \ldots$ will denote positive numbers which can be specified explicitly in terms of $n, d, A_1, \ldots, A_{n-1}, p, g, \delta$, and $\varkappa$ only. The number C, which will finally represent the constant occurring in the enunciation of Theorem 4, will be supposed sufficiently large throughout. We assume now that the hypotheses of Theorem 4 hold but that the conclusion is not valid, and we shall ultimately deduce a contradiction. Thus we assume that there exist rational integers $b_1, \ldots, b_n$ with absolute values at most H^g such that (8) holds, that the only integers $b_1', \ldots, b_n'$ with absolute values at most H such that $b_1' \log a_1 + \ldots + b_n' \log a_n = 0$ are given by $b_1' = \ldots = b_n' = 0$, and that

$$H \geqslant \max\{C, (\log A)^{\varkappa}\}. \tag{10}$$

Further, we assume that $b_n \neq 0$; this involves no loss of generality for, by (8), one at least of $b_1, \ldots, b_n$ is not 0, and clearly, if $b_n = 0$ then the conclusion of Theorem 4 would follow from the analogous theorem for a subset of $a_1, \ldots, a_n$. For brevity, we write

$$\beta_j = -b_j/b_n, \quad \xi = \beta_1 \log a_1 + \ldots + \beta_{n-1} \log a_{n-1} - \log a_n \quad (1 \leqslant j < n).$$

The inequality (8) can be written in the form $0 < |\xi|_p < e^{-\delta H} |b_n|_p^{-1}$, and thus, since $|b_n|_p^{-1} \leqslant H^g$, this implies that $0 < |\xi|_p < e^{-\frac{\delta}{2} H}$ when H is sufficiently large. In particular, $|\xi|_p < p^{-\nu}$ when H is sufficiently large, and from this last inequality and (9) it is clear that

$$|\beta_1 \log a_1 + \ldots + \beta_{n-1} \log a_{n-1}|_p \leqslant \max\{|\xi|_p, |\log a_n|_p\} < p^{-\nu}. \tag{11}$$

Now (3), (9) and (11) together with the inequality $0 < |\xi|_p < e^{-\frac{\delta}{2} H}$ show that

$$0 < |\mu a_n^{-1} - 1|_p < e^{-\frac{\delta}{2} H},$$

where μ denotes $\exp(\beta_1 \log a_1 + \ldots + \beta_{n-1} \log a_{n-1})$. Since $|a_n|_p = 1$, we conclude finally that

$$0 < |\mu - a_n|_p < e^{-\frac{\delta}{2} H}. \tag{12}$$

In the following, we shall write a_j^z, μ^z briefly for the analytic functions $\exp(z \log a_j)$, $\exp(z \log \mu)$, respectively. Since $|\log a_j|_p < p^{-\nu}$ and $|\log \mu|_p < p^{-\nu}$, the power series defining these functions certainly converge for all z satisfying $|z|_p < p^{\nu-1}$.

We now define

$$\varrho = 2/(\varkappa + n + 1), \quad \varepsilon = \{1 - 1/(\varrho\varkappa)\}/(2n),$$

and we observe that, since $\varkappa > n+1$, we have

$$1/\varkappa < \varrho < 1/(n+1), \quad 0 < \varepsilon < 1/(2n).$$

We write [7]

$$k = [H^{\varrho}], \quad h = [k^{\varepsilon/A}],$$
$$L = L_1 = \ldots = L_{n-1} = [k^{1-\varepsilon}], \quad L_n = [k^{n\varepsilon}].$$

We shall now give a series of seven lemmas from which we shall ultimately derive a contradiction.

LEMMA 1. *Let M, N be integers with $N > M > 0$, and let u_{ij} $(1 \leqslant i \leqslant M, 1 \leqslant j \leqslant M)$ be integers with absolute values at most U. Then there exist integers $x_1, \ldots, x_N$, not all 0, with absolute values at most $(NU)^{M/(N-M)}$, such that*

$$\sum_{j=1}^{N} u_{ij} x_j = 0 \quad (1 \leqslant i \leqslant M).$$

Proof. See § 4 of [3].

LEMMA 2. *There exist integers $p(\lambda_1, \ldots, \lambda_n)$, not all 0, with absolute values at most e^{hk}, such that for all non-negative integers $m_1, \ldots, m_{n-1}$ satisfying $m_1 + \ldots + m_{n-1} \leqslant k$, the function*

$$\Phi_{m_1,\ldots,m_{n-1}}(z) = P \sum_{\lambda_1=0}^{L_1} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \ldots, \lambda_n) a_1^{\lambda_1 z} \ldots a_{n-1}^{\lambda_{n-1} z} \mu^{\lambda_n z} \gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}},$$

where $P = (\log a_1)^{m_1} \ldots (\log a_{n-1})^{m_{n-1}}$ and $\gamma_r = \lambda_r + \lambda_n \beta_r$ $(1 \leqslant r < n)$, satisfies

$$|\Phi_{m_1,\ldots,m_{n-1}}(l)|_p < e^{-\frac{\delta}{4} H} \tag{13}$$

for all integers l with $1 \leqslant l \leqslant h$.

[7] If a is a real number, $[a]$ denotes the integral part of a.

Proof. We shall choose the $p(\lambda_1, \ldots, \lambda_n)$ such that

$$\sum_{\lambda_1=0}^{L_1} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \ldots, \lambda_n) a_1^{\lambda_1 l} \ldots a_n^{\lambda_n l} \gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}} = 0 \tag{14}$$

for the above ranges of l and $m_1, \ldots, m_{n-1}$, and we shall subsequently verify that this implies (13). Let $a_1, \ldots, a_n$ denote the leading coefficients, supposed positive, in the minimal polynomials of $\alpha_1, \ldots, \alpha_n$, respectively. Then, for any non-negative integer j,

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

where the $a_{rs}^{(j)}$ are integers with absolute values at most c_1^j or $(2A)^j$, according as $r < n$ or $r = n$ (see [3], § 3). Thus, multiplying (14) by $a_1^{L_1 l} \ldots a_n^{L_n l} b_n^{m_1+\ldots+m_{n-1}}$, and substituting for the powers of $a_r \alpha_r$, we obtain the equation

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

where

$$V(s) = \sum_{\lambda_1=0}^{L_1} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \ldots, \lambda_n) v(\lambda, s),$$

and

$$v(\lambda, s) = a_n^{(L_n-\lambda_n)l} a_{n,s_n}^{(\lambda_n l)} \prod_{r=1}^{n-1} \{a_r^{(L-\lambda_r)l} a_{r,s_r}^{(\lambda_r l)} (b_n \lambda_r - b_r \lambda_n)^{m_r}\}.$$

Hence (14) will hold if the d^n equations $V(s) = 0$ are satisfied. These are linear equations in the $p(\lambda_1, \ldots, \lambda_n)$ with integer coefficients. Since $l \leqslant h$, $m_1+\ldots+m_{n-1} \leqslant k$, $L_n < L$, and, by hypothesis, the integers b_r have absolute values at most H^g, the coefficient $v(\lambda, s)$ of $p(\lambda_1, \ldots, \lambda_n)$ in the linear form $V(s)$ has absolute value at most

$$U = (2A)^{L_n h} c_2^{Lh} (2LH^g)^k.$$

There are at most $(k+1)^{n-1}h$ distinct sets of integers $l, m_1, \ldots, m_{n-1}$, and hence there are

$$M \leqslant d^n (k+1)^{n-1} h \leqslant d^n 2^{n-1} k^{n-1+\varepsilon/4}$$

equations corresponding to them. On the other hand, there are $N = (L_1+1) \ldots (L_n+1)$ unknowns $p(\lambda_1, \ldots, \lambda_n)$, and

$$N > k^{(n-1)(1-\varepsilon)+n\varepsilon} = k^{n-1+\varepsilon} > 2M,$$

since $k^{\frac{3}{4}\varepsilon}$ clearly exceeds $2^n d^n$ when k is sufficiently large. It follows from Lemma 1 that the system of equations $V(s) = 0$ has a non-trivial solution such that the integers $p(\lambda_1, \ldots, \lambda_n)$ have absolute values at most NU. Now by (10)

$$L_n \log A \leqslant k^{n\varepsilon} H^{1/\varkappa} \leqslant k^{n\varepsilon} (2k)^{1/\varrho\varkappa} \leqslant 2k^{1-n\varepsilon}, \tag{15}$$

and since also

$$2LH^g \leqslant kH^g \leqslant e^{h/2}$$

when H is sufficiently large, it follows easily that

$$NU \leqslant k^n (2c_2)^{Lh} e^{hL_n \log A} e^{hk/2} \leqslant e^{hk},$$

is required.

It remains only to verify that (14) implies (13). By virtue of (14), we have

$$\Phi_{m_1,\ldots,m_{n-1}}(l) = P \sum_{\lambda_1=0}^{L_1} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \ldots, \lambda_n) a_1^{\lambda_1 l} \ldots \alpha_{n-1}^{\lambda_{n-1} l} (\mu^{\lambda_n l} - \alpha_n^{\lambda_n l}) \gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}}. \tag{16}$$

Now, noting that $|\alpha_n|_p = 1$, $|\mu|_p = 1$ and applying (12), it is clear that

$$|\mu^{\lambda_n l} - \alpha_n^{\lambda_n l}|_p = |\mu - \alpha_n|_p |\mu^{\lambda_n l - 1} + \ldots + \alpha_n^{\lambda_n l - 1}|_p \leqslant |\mu - \alpha_n|_p < e^{-\frac{\delta}{2}H}.$$

Thus, since

$$|\gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}}|_p \leqslant (H^g)^k \leqslant e^{hk/2}, \quad |a_i|_p = 1, \quad |\log a_i|_p < 1 \quad (1 \leqslant i < n),$$

it follows from (16) that

$$|\Phi_{m_1,\ldots,m_{n-1}}(l)|_p < e^{\frac{hk}{2}} e^{-\frac{\delta}{2}H} \leqslant e^{-\frac{\delta}{4}H};$$

the last inequality is valid since $e^{\frac{hk}{2}} e^{-\frac{\delta}{4}H} \leqslant 1$ when H is sufficiently large. This completes the proof of the lemma.

Lemma 3. *For any non-negative integers $m_1, \ldots, m_{n-1}$ with $m_1+\ldots+m_{n-1} \leqslant k$, and any integer l satisfying $1 \leqslant l \leqslant hk^{(1/\varrho)+\varepsilon/2-1}$, either* (13) *holds or*

$$|\Phi_{m_1,\ldots,m_{n-1}}(l)|_p > (c_6^{Ll} e^{2hk})^{-d}. \tag{17}$$

Proof. Define

$$Q' = P' \sum_{\lambda_1=0}^{L_1} \ldots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \ldots, \lambda_n) a_1^{\lambda_1 l} \ldots a_n^{\lambda_n l} \gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}},$$

where $P' = a_1^{L_1 l} \ldots a_n^{L_n l} b_n^{m_1+\ldots+m_{n-1}}$, and, as in the proof of Lemma 2, $a_1, \ldots, a_n$ are the leading coefficients of the minimal polynomials of $\alpha_1, \ldots, \alpha_n$. It is clear that Q' is an integer in K. Noting that

$$|b_n^{m_1+\ldots+m_{n-1}} \gamma_1^{m_1} \ldots \gamma_{n-1}^{m_{n-1}}| \leqslant (2LH^g)^k \leqslant e^{hk/2},$$

we see that any complex conjugate of Q', obtained by substituting arbitrary complex conjugates for the α_r, has absolute value at most

$$(L_1+1)\dots(L_n+1)c_3^{Ll}(dA)^{2L_nl}e^{\frac{3}{2}hk}$$

(cf. [3], § 3). Since, by (15), $lL_n\log A \leqslant 2lk^{1-ne}$, this last expression is at most $c_4^{Ll}e^{\frac{7}{4}hk}$. Thus, either $Q'=0$, or by (4)

$$|Q'|_p \geqslant (c_4^{Ll}e^{\frac{7}{4}hk})^{-d}. \tag{18}$$

Now it is evident that

$$|\Phi_{m_1,\dots,m_{n-1}}(l)|_p \geqslant |P|_p\{|Q'P'^{-1}|_p - |Q'P'^{-1}-\Phi_{m_1,\dots,m_{n-1}}(l)P^{-1}|_p\}. \tag{19}$$

By a similar argument to that given at the end of the proof of Lemma 2, we deduce that

$$|Q'P'^{-1}-\Phi_{m_1,\dots,m_{n-1}}(l)P^{-1}|_p < e^{-\frac{\delta}{4}H}. \tag{20}$$

In particular, this shows that (13) certainly is valid if $Q'=0$. If, however, $Q'\neq 0$, then applying the estimates

$$|P'|_p \leqslant 1, \quad L \leqslant k^{1-\varepsilon}, \quad l \leqslant hk^{(1/\varrho)+\varepsilon/2-1}, \quad h \leqslant k^{\varepsilon/4},$$

it follows from (18) that

$$|Q'P'^{-1}|_p \geqslant 2e^{-\frac{\delta}{4}H}. \tag{21}$$

The inequalities (20) and (21) plainly imply that

$$|Q'P'^{-1}-\Phi_{m_1,\dots,m_{n-1}}(l)P^{-1}|_p < \tfrac{1}{2}|Q'P'^{-1}|_p,$$

and thus we deduce from (19) that

$$|\Phi_{m_1,\dots,m_{n-1}}(l)|_p > \tfrac{1}{2}|P|_p|Q'P'^{-1}|_p.$$

But by (18), (3) and (4) (cf. [3], § 3), we have the estimates

$$|Q'P'^{-1}|_p \geqslant |Q'|_p \geqslant (c_4^{Ll}e^{\frac{7}{4}hk})^{-d},$$

$$|P|_p = |\alpha_1-1|_p^{m_1}\dots|\alpha_{n-1}-1|_p^{m_{n-1}} \geqslant c_5^{-k},$$

and so

$$|\Phi_{m_1,\dots,m_{n-1}}(l)|_p > (c_6^{Ll}e^{2hk})^{-d}.$$

This completes the proof of Lemma 3.

LEMMA 4. *Let J be any integer satisfying $0 \leqslant J < \tau$, where*

$$\tau = \varepsilon^{-1}(n-1+\varrho^{-1})+1.$$

Then (13) *holds for all integers l with $1 \leqslant l \leqslant hk^{eJ/2}$, and each set of non-negative integers $m_1, \dots, m_{n-1}$ with $m_1+\dots+m_{n-1} \leqslant k/2^J$.*

Proof. The lemma is true for $J=0$ by Lemma 2. We let I be an integer satisfying $0 \leqslant I < \tau-1$, and we assume that the lemma is true for $J = 0, 1, \dots, I$. We prove the validity of the lemma for $J = I+1$.

We begin by defining

$$R_J = [hk^{eJ/2}], \quad S_J = [k/2^J] \quad (J = 0, 1, \dots).$$

Then it suffices to prove that for any integer l with $R_I < l \leqslant R_{I+1}$, and any set of non-negative integers $m_1, \dots, m_{n-1}$ with $m_1+\dots+m_{n-1} \leqslant S_{I+1}$, we have

$$|f(l)|_p < e^{-\frac{\delta}{4}H}, \tag{22}$$

where $f(z)$ denotes $\Phi_{m_1,\dots,m_{n-1}}(z)$. Let $f_m(z)$ denote the mth derivative of $f(z)$. By our inductive hypothesis, we see that for each integer r with $1 \leqslant r \leqslant R_I$, and each integer m with $0 \leqslant m \leqslant S_{I+1}$, we have

$$|f_m(r)|_p < e^{-\frac{\delta}{4}H}; \tag{23}$$

for $f_m(r)$ is given by

$$f_m(r) = P\sum_{\lambda_1=0}^{L_1}\dots\sum_{\lambda_n=0}^{L_n} p(\lambda_1,\dots,\lambda_n)\alpha_1^{\lambda_1 r}\dots\alpha_{n-1}^{\lambda_{n-1}r}\mu^{\lambda_n r}\gamma_1^{m_1}\dots\gamma_{n-1}^{m_{n-1}}\times$$
$$\times(\gamma_1\log\alpha_1+\dots+\gamma_{n-1}\log\alpha_{n-1})^m,$$

and on expanding the mth power of the linear form on the right we obtain

$$f_m(r) = \sum_{\substack{j_1=0\\ j_1+\dots+j_{n-1}=m}}^{m}\dots\sum_{j_{n-1}=0}^{m}\frac{m!}{j_1!\dots j_{n-1}!}\Phi_{m_1+j_1,\dots,m_{n-1}+j_{n-1}}(r);$$

the valuation of each term in the last multiple sum is at most $e^{-\frac{\delta}{4}H}$, since

$$m_1+\dots+m_{n-1}+j_1+\dots+j_{n-1} \leqslant k/2^I,$$

and $m!/(j_1!\dots j_{n-1}!)$, with $j_1+\dots+j_{n-1}=m$, is an integer.

We write, for brevity,

$$F(z) = \{(z-1)\dots(z-R_I)\}^{S_{I+1}+1},$$

and we denote by Γ, Γ^* elements of Ω_p satisfying

$$|\Gamma|_p = p^{\nu-2}, \quad |\Gamma^*|_p \leqslant 1/2R_{I+1},$$

respectively. Then

$$\int_{\Gamma,0} \frac{zf(z)}{(z-l)F(z)}\,dz = \frac{f(l)}{F(l)} + \sum_{r=1}^{R_I}\sum_{m=0}^{S_{I+1}} \frac{f_m(r)}{m!}\int_{\Gamma^*,r} \frac{(z-r)^{m+1}}{(z-l)F(z)}\,dz. \tag{24}$$

Here, of course, the integrals are Schnirelman line integrals as defined in § II. To verify this, we observe that the integral on the left is the sum of the residues of $f(z)/\{(z-l)F(z)\}$ (cf. [1], Theorem 13 of Appendix), and the residue at $z=r$ is given by

$$\frac{1}{S_{I+1}!}\frac{d^{S_{I+1}}}{dz^{S_{I+1}}}\left(\frac{(z-r)^{S_{I+1}+1}f(z)}{(z-l)F(z)}\right)$$

evaluated at $z=r$. On the other hand, the integral on Γ^* with centre $z=r$ on the right is given by

$$\frac{1}{(S_{I+1}-m)!}\frac{d^{S_{I+1}-m}}{dz^{S_{I+1}-m}}\left(\frac{(z-r)^{S_{I+1}+1}}{(z-l)F(z)}\right)$$

again evaluated at $z=r$, and (24) now follows by Leibnitz's theorem.

We now obtain an upper bound for the valuation of the double sum on the right of (24). For those z satisfying $|z-r|_p = |\Gamma^*|_p$, we have, by (4) and the definition of Γ^*,

$$1/R_{I+1} \leqslant |r-s|_p \leqslant \max\{|z-s|_p, |z-r|_p\} = |z-s|_p \qquad (s=1,\ldots,R_{I+1};\ s\neq r),$$

whence

$$\left|\int_{\Gamma^*,r}\frac{(z-r)^{m+1}}{(z-l)F(z)}\,dz\right|_p \leqslant \max_{|z-r|_p=|\Gamma^*|_p}\left|\frac{(z-r)^{m+1}}{(z-l)F(z)}\right|_p \leqslant R_{I+1}^{(R_{I+1})(S_{I+1}+1)}.$$

Since

$$R_{I+1}\leqslant hk^{\varepsilon\tau/2},\quad S_{I+1}+1\leqslant k,\quad R_I+1\leqslant 2hk^{\varepsilon(\tau-1)/2},\quad h\leqslant k^{\varepsilon/4},\quad k\leqslant H^{\varrho},$$

it follows that

$$\left|\int_{\Gamma^*,r}\frac{(z-r)^{m+1}}{(z-l)F(z)}\,dz\right|_p \leqslant e^{2H^{\nu'}\log H^{\theta'}},$$

where, for brevity, we have written

$$\nu' = \tfrac{1}{2}\{1+(n+1)\varrho\}+\tfrac{1}{4}\varepsilon\varrho,\qquad \theta' = \tfrac{1}{2}\varepsilon\tau\varrho+\tfrac{1}{4}\varepsilon\varrho.$$

Noting that $|1/m!|_p \leqslant m! \leqslant k^k$ and applying (23), we conclude that the double sum on the right of (24) has valuation at most

$$e^{-\frac{\delta}{4}H+2H^{\nu'}\log H^{\theta'}+H^{\varrho}\log H^{\varrho}} < e^{-\frac{\delta}{8}H};$$

the last inequality is valid for sufficiently large H since clearly

$$\nu' = \frac{1}{2}+\frac{1}{\varkappa+n+1}\left\{n+1+\frac{\varkappa-n-1}{8n}\right\} < \frac{1}{2}+\frac{1}{\varkappa+n+1}\left\{n+1+\frac{\varkappa-n-1}{2}\right\} = 1.$$

We next observe that, since $R_{I+1}\leqslant hk^{\varepsilon\tau/2}$ and

$$\tfrac{1}{2}\varepsilon\tau = \tfrac{1}{2}(n+1+1/\varrho)+\tfrac{1}{2}\varepsilon-1 < 1/\varrho+\tfrac{1}{2}\varepsilon-1,$$

l satisfies the condition of Lemma 3. Consequently either (13) holds, in which case there is nothing more to prove, or

$$|f(l)|_p > (c_6^{Ll}e^{2hk})^{-d}. \tag{25}$$

We show that this last inequality leads to a contradiction. For if this inequality is valid, then since $LR_{I+1}\leqslant k^{(1/\varrho)-\varepsilon/4}$ and $hk\leqslant k^{1+\varepsilon/4}$, we immediately obtain

$$|f(l)|_p > 2e^{-\frac{\delta}{8}H}. \tag{26}$$

But it was shown in the last paragraph that the double sum on the right of (24) has valuation at most $e^{-\frac{\delta}{8}H}$. Hence, applying (26) and the estimate $|F(l)|_p\leqslant 1$, it follows from (24) that

$$\frac{1}{2}\left|\frac{f(l)}{F(l)}\right|_p < \left|\int_{\Gamma,0}\frac{zf(z)}{(z-l)F(z)}\,dz\right|_p. \tag{27}$$

We now obtain an upper bound for the right side of this inequality. For those z satisfying $|z|_p = |\Gamma|_p = p^{\nu-2}$, we have

$$p^{\nu-2} = |z|_p \leqslant \max\{|z-s|_p, |s|_p\} = |z-s|_p \qquad (s=1,\ldots,R_{I+1}),$$

and so for such z

$$|F(z)|_p \geqslant p^{(\nu-2)R_I(S_{I+1}+1)},\qquad |z-l|_p \geqslant p^{\nu-2}.$$

Further, by virtue of the estimates

$$|\alpha_i^{\lambda_i z}|_p\leqslant 1,\quad |\mu^{\lambda_n z}|_p\leqslant 1,\quad |P|_p<1,\quad |\gamma_1^{m_1}\ldots\gamma_{n-1}^{m_{n-1}}|_p\leqslant e^{hk/2},$$

we see that $|f(z)|_p\leqslant e^{hk/2}$ for those z satisfying $|z|_p=p^{\nu-2}$. Hence

$$\left|\int_{\Gamma,0}\frac{zf(z)}{(z-l)F(z)}\,dz\right|_p \leqslant \max_{|z|_p=|\Gamma|_p}\left|\frac{zf(z)}{(z-l)F(z)}\right|_p \leqslant e^{hk/2}p^{-(\nu-2)R_I(S_{I+1}+1)}.$$

On the other hand, (25) and the trivial estimate $|F(l)|_p\leqslant 1$ give a lower bound for the left of (27). Substituting these bounds into (27), we conclude that

$$\tfrac{1}{2}(c_6^{Ll}e^{2hk})^{-d} < e^{hk/2}p^{-(\nu-2)R_I(S_{I+1}+1)},$$

whence

$$c_7^{-Ll}e^{-3d\delta hk} < p^{-(\nu-2)R_I(S_{I+1}+1)}. \tag{28}$$

But this is impossible for sufficiently large H. For if $I = 0$, the left side of (28) is greater than $e^{-4d\delta hk}$, and the right side is at most $e^{-\frac{1}{2}hk(\nu-2)\log p}$, and these estimates are contradictory, since, by virtue of the definition $\nu = 20d$, we have

$$\tfrac{1}{2}(\nu-2)\log p \geqslant \tfrac{18}{4}d > 4d.$$

If $I > 0$, the left side of (28) is greater than $\exp(-c_8 hk^{eI/2+1-\varepsilon/2})$, and the right side is at most $\exp(-c_9 hk^{eI/2+1})$, and these estimates are also clearly inconsistent. We have therefore derived a contradiction from (25), and so the proof of Lemma 4 is complete.

LEMMA 5. *Let $\Phi(z) = \Phi_{0,\ldots,0}(z)$. Then, for each non-negative integer j, we have*

$$\log|\Phi_j(0)|_p < -c_{10}hk^{e(\tau-1)/2+1}, \tag{29}$$

where $\Phi_j(z)$ denotes the j-th derivative of $\Phi(z)$.

Proof. Put

$$X = [hk^{e(\tau-1)/2}], \qquad Y = [k/2^\tau].$$

Then, by Lemma 4, (13) holds for each integer l with $1 \leqslant l \leqslant X$, and each set of non-negative integers $m_1, \ldots, m_{n-1}$ with $m_1+\ldots+m_{n-1} \leqslant Y$. Since this is so, a similar argument to that given at the beginning of the proof of Lemma 4 shows that, for each integer r with $1 \leqslant r \leqslant X$ and each integer m with $0 \leqslant m \leqslant Y$, we have

$$|\Phi_m(r)|_p < e^{-\frac{\delta}{4}H}. \tag{30}$$

Now let w denote any element of Ω_p satisfying $|w|_p = p$. We proceed to give an upper bound for $|\Phi(w)|_p$. Let Γ, Γ^* be elements of Ω_p satisfying $|\Gamma|_p = p^{\nu-2}$, $|\Gamma^*|_p \leqslant 1/2X$, respectively, and let

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

Then, as in the proof of Lemma 4, we have

$$\int_{\Gamma,0} \frac{z\Phi(z)}{(z-w)E(z)}\,dz = \frac{\Phi(w)}{E(w)} + \sum_{r=1}^{X}\sum_{m=0}^{Y} \frac{\Phi_m(r)}{m!}\int_{\Gamma^*,r} \frac{(z-r)^{m+1}}{(z-w)E(z)}\,dz. \tag{31}$$

For those z satisfying $|z-r|_p = |\Gamma^*|_p$, it is clear that

$$1/X \leqslant |r-s|_p \leqslant \max\{|z-s|_p, |z-r|_p\} = |z-s|_p \quad (s = 1, \ldots, X, s \neq r),$$

$$p = |w|_p \leqslant \max\{|z-r|_p, |z-w|_p, |r|_p\} = |z-w|_p,$$

whence

$$\left|\int_{\Gamma^*,r} \frac{(z-r)^{m+1}}{(z-w)E(z)}\,dz\right|_p \leqslant X^{X(Y+1)}.$$

Since $X \leqslant hk^{e(\tau-1)/2}$, $Y+1 \leqslant k$, it follows from (30) (cf. the proof of Lemma 4) that the valuation of the double sum on the right of (31) is at most $e^{-\frac{\delta}{8}H}$. Hence

$$\left|\frac{\Phi(w)}{E(w)}\right|_p \leqslant \left|\int_{\Gamma,0} \frac{z\Phi(z)}{(z-w)E(z)}\,dz\right|_p + e^{-\frac{\delta}{8}H}.$$

By similar estimates to those given in the proof of Lemma 4, it is easily verified that for those z satisfying $|z|_p = |\Gamma|_p$ we have

$$|E(z)|_p \geqslant p^{(\nu-2)X(Y+1)}, \qquad |z-w|_p \geqslant p^{\nu-2}, \qquad |\Phi(z)|_p \leqslant 1,$$

and thus estimating the integral we see that

$$\left|\frac{\Phi(w)}{E(w)}\right|_p \leqslant p^{-(\nu-2)X(Y+1)} + e^{-\frac{\delta}{8}H}.$$

Now $X \leqslant hk^{e(\tau-1)/2}$, $Y+1 \leqslant k$, whence it is clear (cf. again the proof of Lemma 4) that $e^{-\frac{\delta}{8}H} < p^{-(\nu-2)X(Y+1)}$, and so

$$\left|\frac{\Phi(w)}{E(w)}\right|_p < 2p^{-(\nu-2)X(Y+1)}.$$

But, using the estimates

$$X \geqslant \tfrac{1}{2}hk^{e(\tau-1)/2}, \qquad Y+1 \geqslant k/2^\tau, \qquad |E(w)|_p \leqslant p^{X(Y+1)},$$

we conclude that

$$|\Phi(w)|_p < e^{-c_{10}hk^{\frac{1}{2}e(\tau-1)+1}}. \tag{32}$$

The inequality (29) now follows easily from the integral formula (cf. [1], Theorem 8 of Appendix)

$$\Phi_j(0) = j!\int_{\Lambda,0} \frac{w\Phi(w)}{w^{j+1}}\,dw \qquad (j = 0, 1, \ldots),$$

where Λ denotes an element of Ω_p satisfying $|\Lambda|_p = p$.

LEMMA 6. *Let $t_1, \ldots, t_n$ be integers with absolute values at most T, and let*

$$W = t_1\log a_1 + \ldots + t_n\log a_n.$$

Then either $W = 0$ or

$$|W|_p \geqslant (c_{11}^T A^{2|t_n|})^{-d}.$$

Proof. Let a_j' $(1 \leqslant j \leqslant n)$ be the leading coefficient (supposed positive) of the minimal polynomial of α_j or α_j^{-1} according as $t_j > 0$ or $t_j \leqslant 0$. Then

$$w = a_1'^{|t_1|} \dots a_n'^{|t_n|}(\alpha_1^{t_1} \dots \alpha_n^{t_n} - 1)$$

is an algebraic integer in K. Further, any of its complex conjugates, obtained by substituting arbitrary complex conjugates for $\alpha_1, \dots, \alpha_n$, has absolute value at most $c_{11}^T A^{2|t_n|}$ (cf. [3], § 3). If $W \neq 0$, then $w \neq 0$, and thus (4) implies that

$$|w|_p \geqslant (c_{11}^T A^{2|t_n|})^{-d}.$$

Hence, on using (3), we obtain

$$|W|_p \geqslant |a_1'^{|t_1|} \dots a_n'^{|t_n|}|_p |W|_p = |w|_p \geqslant (c_{11}^T A^{2|t_n|})^{-d},$$

and this completes the proof of Lemma 6.

Lemma 7. *Let $d_1, \dots, d_m$ be any $m \geqslant 2$ numbers in Ω_p, and let $\omega_1, \dots, \omega_m$ be m distinct numbers in Ω_p with $|\omega_i|_p \leqslant 1$ $(1 \leqslant i \leqslant m)$. Let $g(z)$ denote the function $\sum_{i=1}^{m} d_i \exp(\omega_i z)$. Then*

$$\max_{0 \leqslant j \leqslant m-1} |g_j(0)|_p \geqslant \max_{1 \leqslant i \leqslant m} |d_i|_p \Big| \prod_{\substack{l=1 \\ l \neq i}}^{m} (\omega_i - \omega_l) \Big|_p,$$

where $g_j(z)$ denotes the j-th derivative of $g(z)$.

Proof. For each suffix i with $1 \leqslant i \leqslant m$, let the numbers σ_{ji} be defined by the equation

$$\prod_{\substack{l=1 \\ l \neq i}}^{m} (z - \omega_l) \Big/ \prod_{\substack{l=1 \\ l \neq i}}^{m} (\omega_i - \omega_l) = \sum_{j=0}^{m-1} \sigma_{ji} z^j. \tag{33}$$

It is clear from this definition that

$$\sum_{j=0}^{m-1} \sigma_{ji} \omega_f^j = \begin{cases} 0 & \text{if} \quad i \neq f, \\ 1 & \text{if} \quad i = f, \end{cases}$$

whence

$$\sum_{j=0}^{m-1} \sigma_{ji} g_j(0) = \sum_{j=0}^{m-1} \sigma_{ji} \sum_{f=1}^{m} d_f \omega_f^j = d_i.$$

Thus we have

$$\max_{0 \leqslant j \leqslant m-1} |g_j(0)|_p \geqslant |d_i|_p / \max_{0 \leqslant j \leqslant m-1} |\sigma_{ji}|_p.$$

But since $|\omega_i|_p \leqslant 1$, it is evident from (33) that

$$\max_{0 \leqslant j \leqslant m-1} |\sigma_{ji}|_p \leqslant 1 \Big/ \Big| \prod_{\substack{l=1 \\ l \neq i}}^{m} (\omega_i - \omega_l) \Big|_p \qquad (1 \leqslant i \leqslant m).$$

On combining these last two estimates, we obtain Lemma 7.

We can now derive a contradiction and thereby complete the proof of Theorem 4. Define

$$\Psi(z) = \sum_{\lambda_1=0}^{L_1} \dots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \dots, \lambda_n) \alpha_1^{\lambda_1 z} \dots \alpha_n^{\lambda_n z},$$

and recall that $\Phi(z) = \Phi_{0,\dots,0}(z)$. Then

$$\Psi_j(0) - \Phi_j(0) = \sum_{\lambda_1=0}^{L_1} \dots \sum_{\lambda_n=0}^{L_n} p(\lambda_1, \dots, \lambda_n)\big(u(\lambda)^j - v(\lambda)^j\big) \qquad (j = 0, 1, \dots),$$

where, for brevity, we have written

$$u(\lambda) = \lambda_1 \log \alpha_1 + \dots + \lambda_n \log \alpha_n, \qquad v(\lambda) = \gamma_1 \log \alpha_1 + \dots + \gamma_{n-1} \log \alpha_{n-1}.$$

Now

$$|u(\lambda)^j - v(\lambda)^j|_p = |\lambda_n|_p |\xi|_p |u(\lambda)^{j-1} + \dots + v(\lambda)^{j-1}|_p < e^{-\frac{\delta}{2}H} \qquad (j = 1, 2, \dots),$$

the last inequality being valid by virtue of the estimate $|\xi|_p < e^{-\frac{\delta}{2}H}$ derived earlier from (8) and the fact that $|u(\lambda)|_p \leqslant 1$, $|v(\lambda)|_p \leqslant 1$, and $|\lambda_n|_p \leqslant 1$. It follows that

$$|\Psi_j(0) - \Phi_j(0)|_p < e^{-\frac{\delta}{2}H} \qquad (j = 0, 1, \dots),$$

and Lemma 5 implies that, for $j = 0, 1, \dots$,

$$|\Psi_j(0)|_p < \max\{e^{-c_{10} h k^{\frac{1}{2}s(\tau-1)+1}}, e^{-\frac{\delta}{2}H}\} = e^{-c_{10} h k^{\frac{1}{2}s(\tau-1)+1}} \tag{34}$$

(cf. the proof of Lemma 4).

On the other hand, Lemma 7 can be applied to the function $\Psi(z)$ to give a lower bound for one of the $|\Psi_j(0)|_p$. The ω_i of Lemma 7 are then just the $\lambda_1 \log \alpha_1 + \dots + \lambda_n \log \alpha_n$. Hence the factor $\omega_i - \omega_l$ appearing in Lemma 7 is a linear form in $\log \alpha_1, \dots, \log \alpha_n$ with integer coefficients, which are not all zero, and which have absolute values at most $L \leqslant k^{1-s} \leqslant H$. Thus by the hypotheses of Theorem 4, $\omega_i - \omega_l \neq 0$ whenever $i \neq l$, and so Lemma 6 implies that

$$|\omega_i - \omega_l|_p \geqslant (c_{11}^L A^{2L_n})^{-d}.$$

This inequality, together with the estimates

$$L \leqslant k^{1-s}, \qquad L_n \log A \leqslant 2k^{1-ns}, \qquad (L_1+1) \dots (L_n+1) \leqslant 2^n k^{n-1+s},$$

$$|p(\lambda_1, \dots, \lambda_n)|_p \geqslant e^{-hk},$$

allows us to deduce from Lemma 7 that

$$\max_{0 \leqslant j \leqslant (L_1+1)\dots(L_n+1)-1} |\Psi_j(0)|_p \geqslant e^{-c_{12} k^n}. \tag{35}$$

But $n < \frac{1}{2}\varepsilon(\tau-1)+1+\frac{1}{4}\varepsilon$, and so (34) and (35) are contradictory for sufficiently large H. Thus (10) cannot be valid, and this completes the proof of Theorem 4.

V. Proof of Theorem 1. The purpose of this section is to show that Theorem 1 is a consequence of Theorem 3 of the present paper and Theorem 3 of [3].

We first show that it suffices to establish a modified form of Theorem 1. I assert that we can assume that the coefficient of x^n in the binary form $f(x, y)$ of Theorem 1 is equal to 1. For, denoting this coefficient by a, we see that $a \neq 0$ since $f(x, y)$ is irreducible. Therefore if we put $X = ax$, $Y = y$, we have $a^{n-1}f(x, y) = F(X, Y)$, where $F(X, Y)$ is an irreducible binary form of degree n in which the coefficient of X^n is equal to 1. If now x, y are integers, with $(x, y, p_1 \dots p_s) = 1$, satisfying the equation (1), then plainly

$$F(X/b,\ Y/b) = a^{n-1}m/b^n,$$

where b denotes the largest integer, comprised solely of powers of $p_1, \dots, p_s$, which divides both X and Y. Since $(X/b, Y/b, p_1 \dots p_s) = 1$ and b, being a divisor of a, is bounded above by $|a|$, then we can clearly deduce Theorem 1 for the binary form $f(x, y)$ from the corresponding result for $F(X, Y)$.

We also make a modification in the equation (1). Recall that m is the largest integer, comprised solely of powers of $p_1, \dots, p_s$, which divides m. Suppose that $m = p_1^{e_1} \dots p_s^{e_s}$, where $e_1, \dots, e_s$ are non-negative integers. Dividing each of these exponents by n, we have $m = p_1^{d_1} \dots p_s^{d_s} p_1^{ne'_1} \dots p_s^{ne'_1}$, where $d_1, \dots, d_s, e'_1, \dots, e'_s$ are integers such that $0 \leqslant d_i < n$ for $1 \leqslant i \leqslant s$. Thus, if we define

$$x' = x/p_1^{e'_1} \dots p_s^{e'_s}, \quad y' = y/p_1^{e'_1} \dots p_s^{e'_s}, \quad m' = m/p_1^{ne'_1} \dots p_s^{ne'_s},$$

it is clear that (1) can be written in the form

$$f(x', y') = m'. \tag{36}$$

Here the integer m' has the important property that

$$|m'|_{p_i} \geqslant p_i^{-(n-1)} \quad (1 \leqslant i \leqslant s),$$

and, as this property is needed for our later arguments, we shall henceforth consider the equation (36) rather than the original equation. Of course, x' and y' are now rational numbers, but their denominators are composed solely of powers of $p_1, \dots, p_s$.

Before proceeding to our principal argument, we introduce more notation and recall several facts from algebraic number theory. Put $\sigma = s+1$, and let $|\ |_{r_1}, |\ |_{r_2}, \dots, |\ |_{r_\sigma}$ denote respectively the valuations

$|\ |, |\ |_{p_1}, \dots, |\ |_{p_s}$ of Q, the field of rational numbers. In a similar notation to that used before, let Ω_{r_i} denote the completion of the algebraic closure of the completion of Q with respect to $|\ |_{r_i}$. Thus, in particular, Ω_{r_1} is the field of complex numbers. Plainly, $f(x', y')$ will factorize in each Ω_{r_i} into a product of linear factors of the form

$$f(x', y') = (x' - a_i^{(1)}y') \dots (x' - a_i^{(n)}y') \quad (1 \leqslant i \leqslant \sigma), \tag{37}$$

where $a_i^{(1)}, \dots, a_i^{(n)}$ are distinct elements of Ω_{r_i}. Let $\mathfrak{K}$ be the number field which is obtained by adjoining $a = a_1^{(1)}$ to Q. Clearly the n subfields of Ω_{r_i}, which are isomorphic to $\mathfrak{K}$, are the fields which are obtained by adjoining the n numbers $a_i^{(j)}$ $(1 \leqslant j \leqslant n)$ to Q. If ξ is any element of $\mathfrak{K}$, we shall denote by $\xi_i^{(j)}$ the image of ξ under that embedding of $\mathfrak{K}$ in Ω_{r_i} which is defined by mapping a to $a_i^{(j)}$.

Since $f(x', y')$ is irreducible over Q, $\mathfrak{K}$ will have degree n over Q. Thus there are at most n valuations of $\mathfrak{K}$ extending any given valuation of Q, and hence there will be at most $n\sigma$ elements in the set $S = \{|\ |_{\mathfrak{K}_1}, \dots, |\ |_{\mathfrak{K}_e}\}$ of valuations of $\mathfrak{K}$ extending the set $s = \{|\ |_{r_1}, \dots, |\ |_{r_\sigma}\}$ of valuations of Q. It will be assumed that the reader is familiar with the fact (cf. [8], p. 30) that every valuation $|\ |_{\mathfrak{K}}$ of $\mathfrak{K}$ extending the valuation $|\ |_{r_i}$ of Q is given by

$$|\xi|_{\mathfrak{K}} = |\xi_i^{(j)}|_{r_i} \quad (\xi \in \mathfrak{K})$$

for some fixed, but not in general unique, superscript j. In particular, frequent use will be made of the well known equations

$$\sum_{\mathfrak{K}|r_i} n_{\mathfrak{K}} = n, \quad \prod_{\mathfrak{K}|r_i} |\xi|_{\mathfrak{K}}^{n_{\mathfrak{K}}} = |\xi_i^{(1)} \dots \xi_i^{(n)}|_{r_i}, \tag{38}$$

where $n_{\mathfrak{K}}$ denotes the degree of the completion of $\mathfrak{K}$ at $|\ |_{\mathfrak{K}}$ over the completion of Q at $|\ |_{r_i}$, and both the sum and the product are taken over all valuations of $\mathfrak{K}$ extending $|\ |_{r_i}$ (cf. § II).

The S-units in $\mathfrak{K}$ will play a fundamental role in our proof, and we now state their main properties. By definition, an S-unit η is an element of $\mathfrak{K}$ whose valuation is equal to 1 for every valuation of $\mathfrak{K}$ not in S. Thus, by the product formula, we have

$$\prod_{\mathfrak{K} \in S} |\eta|_{\mathfrak{K}}^{n_{\mathfrak{K}}} = 1.$$

It is well known (cf. [8], p. 77) that the following generalization of Dirichlet's unit theorem is valid for S-units. There are $\varrho - 1$ S-units, which we shall denote by $\eta_1, \dots, \eta_{\varrho-1}$, with the property that the determinant

$$\Delta = \begin{vmatrix} \log|\eta_1|_{\mathfrak{K}_1} & \dots & \log|\eta_{\varrho-1}|_{\mathfrak{K}_1} \\ \dots\dots\dots\dots\dots & & \\ \log|\eta_1|_{\mathfrak{K}_{\varrho-1}} & \dots & \log|\eta_{\varrho-1}|_{\mathfrak{K}_{\varrho-1}} \end{vmatrix}$$

is not zero. Further, $\eta_1, \dots, \eta_{\varrho-1}$ can be chosen so that not only is $\Delta \neq 0$, but also

$$(39) \quad |\Delta| \geqslant C_1, \quad \left|\log|\eta_i|_{\mathfrak{R}_j}\right| \leqslant C_2 \quad (1 \leqslant i \leqslant \varrho-1, 1 \leqslant j \leqslant \varrho-1),$$

where C_1, C_2 denote positive numbers, which can be specified explicitly in terms of n, the coefficients of $f(x', y')$, and $p_1, \dots, p_s$. It should be noted that, although explicit values for C_1, C_2 are not given in [8], the proof can easily be modified to obtain the more precise result.

We now come to the main argument. Throughout the following, $C_3, C_4, \dots$ will denote positive numbers which can be specified explicitly in terms of n, the coefficients of f, and $p_1, \dots, p_s$. As remarked earlier, we shall use the equation (36), rather than the original equation (1). Thus x', y' will denote rational numbers satisfying (36), whose denominators are composed solely of powers of $p_1, \dots, p_s$. We put

$$\beta = x' - \alpha y'.$$

By the factorization (37), and the fact that $f(x', y') = m'$, we have

$$(40) \quad |\beta_i^{(1)} \dots \beta_i^{(n)}|_{r_i} = |m'|_{r_i} \quad (1 \leqslant i \leqslant \sigma).$$

Multiplying these σ equations together and using (38), we obtain

$$(41) \quad \prod_{\mathfrak{R} \in S} |\beta|_{\mathfrak{R}}^{n_{\mathfrak{R}}} = \prod_{i=1}^{\sigma} |m'|_{r_i},$$

and, taking logarithms and again using (38), it follows that

$$(42) \quad \sum_{\mathfrak{R} \in S} n_{\mathfrak{R}} \log(\varphi^{-1}|\beta|_{\mathfrak{R}}) = 0,$$

where, for brevity, we have written φ for $\{\prod_{i=1}^{\sigma} |m'|_{r_i}\}^{1/n\sigma}$. Note that the number on the right of (41) is precisely $|m|/\mathfrak{m}$; in the subsequent discussion the equation (41) will play a similar role to the equation (40) of [3], and it is this change from $|m|$ to $|m|/\mathfrak{m}$ which leads to the more general form of Theorem 1.

Now I assert that we can find integers $b_1, \dots, b_{\varrho-1}$ such that

$$\gamma = \beta \eta_1^{b_1} \dots \eta_{\varrho-1}^{b_{\varrho-1}}$$

satisfies

$$(43) \quad |\log(\varphi^{-1}|\gamma|_{\mathfrak{R}_i})| \leqslant C_3 \quad (1 \leqslant i \leqslant \varrho).$$

To prove this, we observe that, since $\Delta \neq 0$, there exist real numbers $b_1', \dots, b_{\varrho-1}'$ such that

$$\sum_{j=1}^{\varrho-1} b_j' \log|\eta_j|_{\mathfrak{R}_i} + \log(\varphi^{-1}|\beta|_{\mathfrak{R}_i}) = 0 \quad (1 \leqslant i \leqslant \varrho-1),$$

whence, choosing integers $b_1, \dots, b_{\varrho-1}$ so that $|b_i - b_i'| \leqslant 1/2$ for $1 \leqslant i \leqslant \varrho-1$, it is clear that the element γ of $\mathfrak{K}$ defined above satisfies

$$(44) \quad \left|\log(\varphi^{-1}|\gamma|_{\mathfrak{R}_i})\right| \leqslant (\varrho-1)C_2/2 \quad (1 \leqslant i \leqslant \varrho-1).$$

But, since $\eta_1, \dots, \eta_{\varrho-1}$ are S-units, we have

$$\prod_{\mathfrak{R} \in S} |\gamma|_{\mathfrak{R}}^{n_{\mathfrak{R}}} = \prod_{\mathfrak{R} \in S} |\beta|_{\mathfrak{R}}^{n_{\mathfrak{R}}},$$

and so it follows from (41) that

$$(45) \quad \sum_{\mathfrak{R} \in S} n_{\mathfrak{R}} \log(\varphi^{-1}|\gamma|_{\mathfrak{R}}) = 0.$$

Now (44) and (45) together plainly imply (43).

We next obtain an upper estimate for the height of γ. Let

$$g(x) = d(x - \gamma_1^{(1)}) \dots (x - \gamma_1^{(n)}),$$

where d is an integer chosen so that this polynomial has relatively prime integer coefficients. Since the denominators of x', y' are composed solely of powers of $p_1, \dots, p_s$, the valuations of β, and so also of γ, are at most equal to 1 for every valuation of $\mathfrak{K}$ which does not belong to S. Thus there exists an integer d', composed solely of powers of $p_1, \dots, p_s$, with the property that $d'\gamma$ is an algebraic integer in $\mathfrak{K}$. But d must divide d'^n, and therefore d is composed solely of powers of $p_1, \dots, p_s$, whence

$$(46) \quad |d| = 1 \Big/ \prod_{i=2}^{\sigma} |d|_{r_i}.$$

We now obtain a lower bound for the $|d|_{r_i}$. If $h(x)$ denotes a polynomial with coefficients in Ω_{r_i}, we define $|h|_{r_i}$ to be the maximum of the valuations of the coefficients of $h(x)$. Since $|\ |_{r_i}$ is a non-archimedean valuation for $2 \leqslant i \leqslant \sigma$, the same argument as that used to prove the lemma of Gauss (cf. [8], p. 25) shows that $|h_1 h_2|_{r_i} = |h_1|_{r_i} |h_2|_{r_i}$ for any two polynomials $h_1(x), h_2(x)$. Hence, applying this result to the polynomial

$$g(x) = d(x - \gamma_i^{(1)}) \dots (x - \gamma_i^{(n)}) \quad (2 \leqslant i \leqslant \sigma),$$

we obtain that

$$|g|_{r_i} = |d|_{r_i} \prod_{j=1}^{n} \max(1, |\gamma_i^{(j)}|_{r_i}) \quad (2 \leqslant i \leqslant \sigma).$$

But $|g|_{r_i} = 1$ for $2 \leqslant i \leqslant \sigma$, since the coefficients of $g(x)$ are, by hypothesis, relatively prime integers. Thus, by virtue of (43),

$$|d|_{r_i} \geqslant e^{-nC_3} \varphi^{-n} \quad (2 \leqslant i \leqslant \sigma),$$

and so it follows from (46) that

$$|d| \leqslant e^{n(\sigma-1)C_3}\varphi^{n(\sigma-1)}. \tag{47}$$

Now the minimal polynomial of γ divides $g(x)$. The roots of this minimal polynomial are therefore a subset of $\gamma_1^{(1)}, \ldots, \gamma_1^{(n)}$, and its highest coefficient divides d. Hence (43) and (47) clearly imply that the height of γ is at most $C_4\varphi^{n\sigma}$. But by definition

$$\varphi^{n\sigma} = \prod_{i=1}^{\sigma} |m'|_{r_i} = |m|/\mathfrak{m},$$

and thus the height of γ is at most $C_4|m|/\mathfrak{m}$.

From the definition of γ it is clear that

$$\log|\beta/\gamma|_{\mathfrak{R}_j} = -b_1\log|\eta_1|_{\mathfrak{R}_j} - \ldots - b_{\varrho-1}\log|\eta_{\varrho-1}|_{\mathfrak{R}_j} \quad (1 \leqslant j \leqslant \varrho-1),$$

whence, solving these equations, we obtain

$$-b_k = \sum_{j=1}^{\varrho-1} \frac{\Delta_{jk}}{\Delta}\log|\beta/\gamma|_{\mathfrak{R}_j} \quad (1 \leqslant k \leqslant \varrho-1),$$

where Δ_{jk} denotes the cofactor of the element in the jth row and kth column of the determinant Δ. Thus, if H denotes the maximum of the absolute values of $b_1, \ldots, b_{\varrho-1}$, at least one of the numbers

$$\left|\log|\beta/\gamma|_{\mathfrak{R}_j}\right| \quad (1 \leqslant j \leqslant \varrho-1)$$

must exceed C_5H. Let this maximum be given by $j = J$. Then, by (43),

$$\left|\log(\varphi^{-1}|\beta|_{\mathfrak{R}_J})\right| \geqslant \left|\log|\beta/\gamma|_{\mathfrak{R}_J}\right| - \left|\log(\varphi^{-1}|\gamma|_{\mathfrak{R}_J})\right| \geqslant C_5H - C_3,$$

and this inequality together with (42) plainly implies that there is a suffix I, with $1 \leqslant I \leqslant \varrho$, such that

$$\log(\varphi^{-1}|\beta|_{\mathfrak{R}_I}) \leqslant -(C_5H-C_3)/(n\sigma-1).$$

But, as was remarked earlier, $|\beta|_{\mathfrak{R}_I} = |\beta_i^{(j)}|_{r_i}$ for some pair of indices i, j with $1 \leqslant i \leqslant \sigma$ and $1 \leqslant j \leqslant n$, and thus we have shown that

$$\log(\varphi^{-1}|\beta_i^{(j)}|_{r_i}) \leqslant -(C_5H-C_3)/(n\sigma-1). \tag{48}$$

In particular, this implies that $|\beta_i^{(j)}|_{r_i} \leqslant e^{C_3/(n\sigma-1)}\varphi$, and so it follows from (40) and the inequality $|m'|_{r_i} \geqslant p_{i-1}^{-n}$ that

$$|\beta_i^{(k)}|_{r_i} \geqslant C_6\varphi^{-1/(n-1)} \tag{49}$$

for some superscript $k \neq j$. Let h denote any superscript other than k or j. Since $n \geqslant 3$, such a superscript certainly exists.

As an immediate consequence of the identity

$$(a_i^{(k)}-a_i^{(j)})\beta_i^{(h)} - (a_i^{(h)}-a_i^{(j)})\beta_i^{(k)} = (a_i^{(k)}-a_i^{(h)})\beta_i^{(j)},$$

we obtain the equation

$$a_1^{b_1}\ldots a_{\varrho-1}^{b_{\varrho-1}} - a_\varrho = \omega,$$

where

$$\omega = \frac{(a_i^{(k)}-a_i^{(h)})\beta_i^{(j)}\gamma_i^{(k)}}{(a_i^{(k)}-a_i^{(j)})\beta_i^{(k)}\gamma_i^{(h)}},$$

$$a_\varrho = \frac{(a_i^{(h)}-a_i^{(j)})\gamma_i^{(k)}}{(a_i^{(k)}-a_i^{(j)})\gamma_i^{(h)}}, \qquad a_g = \frac{\eta_{jl}^{(k)}}{\eta_{jl}^{(h)}} \quad (1 \leqslant g \leqslant \varrho-1).$$

Now by virtue of the inequalities (43), (48) and (49) and the definition of ω, it is clear that

$$0 < |\omega|_{r_i} < C_7\varphi^{n/(n-1)}e^{-C_8H}. \tag{50}$$

Further, as it was shown earlier that the height of γ is at most $C_4|m|/\mathfrak{m}$, it is easily verified (cf. [3], § 6) that

$$\log A \leqslant C_9\big(1+\log(|m|/\mathfrak{m})\big), \tag{51}$$

where A denotes the height of a_ϱ. Also we have by (43)

$$C_{10}^{-1} < |a_\varrho|_{r_i} < C_{11}. \tag{52}$$

We are now in a position where we can apply either Theorem 3 of the present paper or Theorem 3 of [3], according as Ω_{r_i} is a p-adic field or the complex field. In either case we shall deduce that

$$H < \max\big\{C_{12}, C_{13}\big(\log(|m|/\mathfrak{m})\big)^{\varkappa'}\big\}. \tag{53}$$

Here $\varkappa' = \frac{1}{2}\big(\varkappa + n(s+1)+1\big)$, and $\varkappa$ is the number specified in Theorem 1, which we recall is assumed to be greater than $n(s+1)+1$. Before proving this assertion, we observe that we can make the following simplification. The inequality (50) can be replaced by

$$0 < |\omega|_{r_i} < e^{-\frac{C_8}{2}H}, \tag{54}$$

for (53) is certainly true if $C_7\varphi^{n/(n-1)}e^{-\frac{C_8}{2}H} > 1$.

We now proceed to verify (53). We assume first that Ω_{r_i} is a p-adic field. Let K be the number field which is obtained by adjoining $\alpha_i^{(1)}, \ldots, \alpha_i^{(n)}$ to Q. Then K has degree at most n^n, and is generated over Q by an element θ with height at most C_{14} (cf. [12], p. 126). By making use of (39), a similar argument to that given for estimating the height of γ shows that

each of $\alpha_1, \ldots, \alpha_{\varrho-1}$ has height at most C_{15}. Let $\mathfrak{p}$ be the set of all algebraic integers ξ in K satisfying $|\xi|_{r_i} < 1$. Then $\mathfrak{p}$ is clearly a prime ideal, and the valuation of K determined by $\mathfrak{p}$ is none other than $|\ |_{r_i}$. Let $\Xi = \max\{C_{10}, C_{11}, e^{2C_2}\}$. Then, by virtue of (39), (52), (54) and the fact that $\varkappa' > n(s+1)+1$, all the hypotheses of Theorem 3 are satisfied with $\alpha_1, \ldots, \alpha_n$ replaced by $\alpha_1, \ldots, \alpha_\varrho$, δ replaced by $C_8/2$, and $\varkappa$ replaced by $\varkappa'$. Note that the inequality $\varkappa' > \varrho+1$ is valid since plainly $\varrho \leqslant n(s+1)$. The assertion (53) then follows from the conclusion of Theorem 3 and (51).

We suppose next that Ω_{r_i} is the complex field. Then, as above, each of $\alpha_1, \ldots, \alpha_\varrho$ has height at most C_{15}. Let $A' = \max\{C_{11}, C_{10}\}$. Thus, by (52), (54) and the inequality $\varkappa' > n(s+1)+1$, it is clear that all the hypotheses of Theorem 3 of [3] are satisfied with $\alpha_1, \ldots, \alpha_n$ replaced by $\alpha_1, \ldots, \alpha_\varrho$, δ replaced by $C_8/2$, and $\varkappa$ replaced by $\varkappa'$. Note that $\varkappa' > \varrho+1$ or $\varkappa' > \varrho+2$ according as $\alpha_1, \ldots, \alpha_\varrho$ are or are not all real, since for these two cases we have the respective inequalities $\varrho \leqslant n(s+1)$, $\varrho \leqslant n(s+1)-1$. The assertion (53) then follows from the conclusion of Theorem 3 of [3] and (51).

We can now finish the proof of Theorem 1. By (39), (43), (53), we have

$$|\beta_i^{(j)}|_{r_i} = |\gamma_i^{(j)}|_{r_i} |\eta_{1i}^{(j)-b_1} \ldots \eta_{\varrho-1,i}^{(j)-b_{\varrho-1}}|_{r_i} < C_{16} e^{C_{17}(\log(|m|/\mathfrak{m}))^{\varkappa'}} \quad (1 \leqslant i \leqslant \sigma, 1 \leqslant j \leqslant n).$$

Hence the identities

$$x' = \frac{\alpha_i^{(h)}\beta_i^{(j)} - \alpha_i^{(j)}\beta_i^{(h)}}{\alpha_i^{(h)} - \alpha_i^{(j)}}, \qquad y' = \frac{\beta_i^{(j)} - \beta_i^{(h)}}{\alpha_i^{(h)} - \alpha_i^{(j)}} \qquad (1 \leqslant i \leqslant \sigma;\ h \neq j)$$

imply that

$$(55) \qquad |x'|_{r_i} < C_{18} e^{C_{19}(\log(|m|/\mathfrak{m}))^{\varkappa'}}, \quad |y'|_{r_i} < C_{18} e^{C_{19}(\log(|m|/\mathfrak{m}))^{\varkappa'}} \quad (1 \leqslant i \leqslant \sigma).$$

But

$$x' = x/(p_1^{e_1'} \ldots p_s^{e_s'}), \qquad y' = y/(p_1^{e_1'} \ldots p_s^{e_s'}),$$

and thus, since $(x, y, p_1 \ldots p_s) = 1$ by hypothesis, it follows from (55) that

$$|p_i^{e_i'}| < C_{18} e^{C_{19}(\log(|m|/\mathfrak{m}))^{\varkappa'}} \qquad (1 \leqslant i \leqslant s).$$

Applying (55) again, we obtain

$$|x| = |x'|\,|p_1^{e_1'} \ldots p_s^{e_s'}| < C_{18}^{s+1} e^{(s+1)C_{19}(\log(|m|/\mathfrak{m}))^{\varkappa'}},$$

$$|y| = |y'|\,|p_1^{e_1'} \ldots p_s^{e_s'}| < C_{18}^{s+1} e^{(s+1)C_{19}(\log(|m|/\mathfrak{m}))^{\varkappa'}}.$$

If $(\log(|m|/\mathfrak{m}))^{\varkappa-\varkappa'} \leqslant (s+1)C_{19}$, these inequalities clearly imply that $\max(|x|, |y|) < C_{20}$, and so the conclusion of Theorem 1 is certainly valid; and it is again obvious if $(\log(|m|/\mathfrak{m}))^{\varkappa-\varkappa'} > (s+1)C_{19}$. The proof of Theorem 1 is therefore complete.

References

[1] W. Adams, *Transcendental numbers in the P-adic domain*, Amer. Journ. Math. 87 (1966), pp. 279-308.

[2] E. Artin, *Theory of algebraic numbers*, Göttingen 1956.

[3] A. Baker, *Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms*, Phil. Trans. Roy. Soc., London, A 263 (1968), pp. 173-191; *II. The Diophantine equation* $y^2 = x^3 + k$, ibidem, A 263 (1968), pp. 193-208.

[4] E. Hecke, *Theorie der algebraischen Zahlen*, Leipzig 1923.

[5] K. Mahler, *Zur Approximation algebraischer Zahlen I*, Math. Ann. 107 (1933), pp. 691-730.

[6] — *Zur Approximation algebraischer Zahlen II*, ibidem, 108 (1933), pp. 37-55.

[7] — *Zur Approximation algebraischer Zahlen III*, Acta Math. 62 (1934), pp. 91-166.

[8] O. O'Meara, *Introduction to Quadratic Forms*, Berlin 1963.

[9] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), pp. 1-20.

[10] C. Siegel, *Approximation algebraischer Zahlen*, Math. Zeitschr. 10 (1921), pp. 173-213; = Ges. Abhandlungen I, pp. 6-46.

[11] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, Journ. Reine Angew. Math. 135 (1909), pp. 284-305.

[12] B. van der Waerden, *Modern Algebra*, New York 1953, Revised english edition.

Added in proof. A note by A. I. Vinogradov and V. G. Sprindžuk (Mat. Zametki 3 (1968), pp. 369-376) has recently been published concerning the equation $f(x, y) = mp_1^{j_1} \ldots p_s^{j_s}$. The method of treatment outlined therein is different from that employed here and would seem to apply only under certain restrictive conditions.

TRINITY COLLEGE
Cambridge, England

Reçu par la Rédaction le 20. 6. 1968