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 \( \delta_1(A) = \frac{1}{4}, \delta_2(A) = \frac{2}{3} \) and it can easily be proved that \( \{\frac{1}{4}, \frac{2}{3}\} \cap E(A) = \emptyset \).

References


*Reçu par la Redaction 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

\[
f(x, y) = m,
\]

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 connection 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 \( n \geq 3 \), 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 \( w \) to denote the largest integer, comprised solely of powers of \( p_1, \ldots, p_s \), which divides \( m \). Further, we shall suppose that \( \kappa \) is any number satisfying

\[
\kappa > \frac{m(s+1)+1}{1}.
\]
Our main result is then as follows:

**Theorem 1.** All solutions of (1) in integers \(x, y, \) with (1) \((x, y, p_1, \ldots, p_s) = 1,\) satisfy

\[
\max(|x|, |y|) < C_0 \max(x, y, s),
\]

where \(C_0\) is an effectively computable number depending on \(n, \lambda, p_1, \ldots, p_s,\) and the coefficients of \(f,\) but not on \(m.\)

It will be observed that when \(x = 0,\) that is when no primes \(p_1, \ldots, p_s,\) 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 \(p_1, \ldots, p_s,\) then \(|m|/m = 1,\) and so all solutions of (1) in integers \(x, y,\) with \((x, y, p_1, \ldots, p_s) = 1\) are bounded by an effectively computable number not depending on \(m.\) Furthermore it is clear from the proof that, for any given \(m,\) one can effectively compute the set of all rational numbers \(a, b\) satisfying (1), the denominators of which are divisible solely by powers of \(p_1, \ldots, p_s.\)

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 \(n \geq 3.\) Again let \(p_1, \ldots, p_s\) be a fixed set of primes, and suppose that \(x\) satisfies (2). We signify by \(|l_{p_1}, \ldots, l_{p_s}|\) the usual valuations of the rational field defined by \(p_1, \ldots, p_s,\) normalized so that \(|p_1p_s| = 1/p_1(1).\) 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

\[
|q|^{-\infty} f(r/q) \prod_{i=1}^{s} |q|^{-\infty} f(r/q) \geq C_1 q^{1/\lambda} r^{1/\lambda},
\]

where \(C_1 = \max(|q|, |r|),\) and \(c > 0\) is an effectively computable number depending on \(n, \lambda, p_1, \ldots, p_s,\) 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 \(p\)-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 [5].

In addition, we make use of certain simple properties of the Schonireibman 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 \(d,\) \(p\) will denote a prime ideal in \(K,\) and \(q\) will denote the unique prime ideal belonging to \(p.\) We signify, as usual, the exponent to which \(p\) divides an arbitrary element \(a\) of \(K\) by \(ord_p a,\) and define the valuation \(|\cdot|_p\) on \(K\) by \(|a|_p = p^{-e},\) where \(e = (ord_p a)/(ord_p p).\) We retain \(|\cdot|\) for the ordinary absolute value.

Let now \(Q_p\) denote the completion of \(Q\) with respect to the \(p\)-adic valuation \(|\cdot|_p.\) The valuation of \(Q_p\) extends uniquely to the algebraic closure of \(Q_p\) (5). We denote by \(Q_p\) the completion of the algebraic closure of \(Q_p\) equipped with the valuation \(|\cdot|_p\) extending that of \(Q_p.\) Certain results from the theory of analytic functions on \(Q_p\) will play a fundamental role in our work, and we now mention these briefly. An analytic function on a disc \(|z| < R\) in \(Q_p\) is defined to be a power series \(f(z) = \sum a_n z^n\) which converges in the disc, that is, \(|a_n z^n|_p = 0\) when \(|z| < R.\)

By a meromorphic function, we mean the quotient of two analytic functions. We shall, in particular, make use of the analytic functions

\[
exp_z = \prod_{m=n}^{\infty} \frac{z^m}{m!}, \quad \log(1+z) = \sum_{m=n}^{\infty} (-1)^{m+1} \frac{z^m}{m},
\]

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

\[
|exp_{-1}|_p = |z|_p, \quad |log(1+z)|_p = |z|_p,
\]

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 \(f(z)\) be a measure on \(Q_p\) satisfying \(|f(z)|_p < R\) \(|z|_p < R.\) We define the Schnireibman line integral of \(f(z)\) on \(L\) with centre \(z = a\) to be the limit

\[
\int_{L} f(z)dz = \lim_{m \to \infty} \frac{1}{m} \sum_{k=1}^{m} f(z),
\]

(5) To extend the valuation of \(Q_p\) to its algebraic closure, we define \(|a|_p\), for an arbitrary \(a\) in the closure, to be \(|N_a|_p^m\), where \(N_a\) and \(m\) denote respectively the norm and degree of \(a\) over \(Q_p;\) see Artin [2].
when it exists, where \( \eta_1^{(n)}, \ldots, \eta_m^{(n)} \) denote the \( m \)th roots of unity in \( \Omega_p \).

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 \( |z|_p < R \), \( R > 0 \) and \( x \) is such that \( |x - a|_p < |R|_p \), then

\[
f_n(x) = i^n \int_{\gamma_a} \frac{f(z)(z - a)}{(z - a)^{n+1}} \, dz,
\]

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

\[
\left| \int_{\gamma_a} f(z) \, dz \right|_p \leq \max \left| f(z) \right|_p |
\]

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

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

\[
\prod_p \left| \beta \right|_p = 1,
\]

where the product ranges over all valuations of \( K \), both archimedean and non-archimedean, and \( \eta_1^{(n)} \) is the degree of the completion of \( K \) at \( p \) over the completion of \( Q \) at \( p \); the formula follows immediately from the familiar equations

\[
\prod_p \left| N \beta \right|_p = 1, \quad |N\beta|_p = \prod_p |\beta|_p.
\]

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

\[
|\beta|_p \mid \beta(0) \mid \beta(1) \mid \ldots \mid \beta(d) | \geq 1,
\]

where \( \beta(0), \ldots, \beta(d) \) denote the complex field conjugates of \( \beta \).

**III. The \( p \)-adic logarithms of algebraic numbers.** Let \( K \) be an algebraic number field of degree \( d \), generated by an element \( \theta \) with height \( ^{(n)} \theta \). Let \( a_1, \ldots, a_n \) be \( n \geq 2 \) elements of \( K \), with heights

\[
(4) \text{ Alternatively when } p \text{ is non-archimedean } a_p = a_{p_0}, \text{ where } a_p \text{ is the exponent to which } p \text{ divides } p \text{ and } f_p \text{ is defined by the property that the number of elements in the residue field of } p \text{ is } p^b.
\]

\[
(5) \text{ As usual, the height of an algebraic number is defined to be the maximum of the ordinary absolute values of the relatively prime integral coefficients in its minimal polynomial.}
\]

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

\[
(5) \max \{|a|_p, |a|_p^{-1} \} < E \quad (1 \leq i \leq n),
\]

and let \( \delta, \nu \) be real numbers with

\[
(6) \delta > 0, \quad \nu > n + 1.
\]

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

**Theorem 3.** If \( b_1, \ldots, b_n \) are rational integers, with absolute values at most \( H \), satisfying

\[
0 < |b_1|, \ldots, |b_n|^{-1} - a_i < e^{-H},
\]

then

\[
H < \max \{C, (\log A)^\gamma\},
\]

where \( C \) is an effectively computable number depending on \( n, d, \theta, E, A_1, \ldots, A_n, \delta, \nu \), 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

\[
(7) \left| a_i - 1 \right|_p < e^{-\nu} \quad (1 \leq i \leq n),
\]

where \( \nu = 20d \). This new condition is required for the convergence of the \( p \)-adic logarithms at the points \( a_i \). The number \( \nu \) 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 assert 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 \( |a|_p = |y|_p \), where, for brevity, we have written \( z \) for \( \eta_1^{(n)} \ldots \eta_n^{(n)} \) and \( y \) for \( a \). For otherwise we would have either \( |a|_p \geq |y|_p \) or \( |a|_p \geq |y|_p \). The first alternative is impossible for sufficiently large \( H \) since it would give

\[
(\star) \left| a_i - 1 \right|_p < e^{-\nu},
\]

and the second alternative is also impossible since it would give

\[
(\star\star) \left| a_i - 1 \right|_p \leq \max \{|x - y|_p, |x|_p\} < |x - y|_p < e^{-4H},
\]
Now choose an element \( x \) in \( K \) such that \( \text{ord}_p x = 1 \); such an element is
given, for example, by one of the numbers in an integral basis for \( p \), and
so can be chosen to have height bounded above by a number depen-
ding only on \( d, \theta, \Sigma \) and \( p \). Since \( |x|_p = |y|_p \), we have \[ \sum_{i=1}^{n} b_i c_i = c_i, \]
where \( c_i \) denotes \( \text{ord}_p a_i (1 \leq i \leq n) \). Thus, on writing \( a_i = a_i x^{-n} \) and \( y^* = a_i^{\frac{1}{n}} \ldots a_i^{-\frac{1}{n}} y = a_i \), we deduce from (6) that
\[ 0 < |y^* - y^*_i| < e^{-\frac{8}{2n}} |x|^n a_i. \]
If \( H \) is sufficiently large. Further, it is clear that for each suffix \( i \) with
\( 1 \leq i \leq n \), we have \( \text{ord}_p a_i = 0 \) and, from (3), \( \log A_i / \log A \), where \( A_i \) denotes
the height of \( a_i \), is bounded above by a number depending only on \( d, \theta, \Sigma \), and \( p \). Hence we see that all the hypotheses of Theorem 3 are satisfied with \( a_1, \ldots, a_n \) replaced by \( a_1^2, \ldots, a_n^2 \) replaced by \( a_i \delta_{2, x} \) and
by 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, \( \log A_i / \log A \) is bounded above by
a number depending only on \( d, \theta, \Sigma \), and \( p \).

(4) The form of Euler's theorem given, for example, in Hoekoe [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 \( \text{ord}_p a = 0 \). For choose an integer \( \delta \) in \( K \) such that \( \text{ord}_p \delta = 0 \) and \( \delta a \) is an integer in \( K \). Then, by the results in [4], \( \text{ord}_p (\delta^m - 1) > \text{ord}_p p \), \( \text{ord}_p (\delta^m - 1) > \text{ord}_p p \),
and so \( \text{ord}_p (\delta^m - 1) > \text{ord}_p p \).

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

**Theorem 4.** Suppose that \( b_1, \ldots, b_n \) are integers with absolute values
at most \( H^2 \), where \( H, y \) are positive integers, satisfying
\[ 8 < |b_1| \log a_1 + \ldots + b_n \log a_n < e^{-2H}. \]
Suppose further that there are no integers \( b'_1, \ldots, b'_n \), with absolute values at most \( H \), satisfying \( b_1 \log a_1 + \ldots + b_n \log a_n = 0 \) other than \( b_1 = \ldots = b_n = 0 \). Then
\[ H < \max \{ C, (\log A)^* \}, \]
where \( C \) is an effectively computable number depending on \( n, d, A_1, \ldots, A_n, \log a_1, \ldots, A_n, \log a_n \), 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),
\[ |log a_1\|_p = |a_1 - 1|_p < e^{-2H} \]
whence \( |p|_p < e^{-2H} \), where \( x = b_1 \log a_1 + \ldots + b_n \log a_n - \log a_n \). Thus
by (3) again and condition (6) of Theorem 3, we obtain
\[ 0 < |x|_p = |e^p - 1|_p = |a_1^2 \ldots a_n^2|_p a_1^2 - 1 = e^{-2H} \]
for clearly (7) implies that \( |a|_p = 1 \). It suffices now to deduce the
existence of an integer \( k \) with \( 1 \leq k \leq n \), possessing the following
properties: (i) There are integers \( b_1, \ldots, b_n \), with absolute values at most
\( (2H)^{n-1} \), such that (9) holds; (ii) At least \( n - k \) of the integers \( b_1, \ldots, b_n \) are zero; (iii) The only integers \( b'_1, \ldots, b'_n \), with absolute values at most \( H \), such that \( b_1 \log a_1 + \ldots + b'_n \log a_n = 0 \), and such that \( b'_i = 0 \) whenever \( b_i = 0 \), are given by \( b'_i = \ldots = b_i = 0 \). 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 \( b_i \) and \( p \) defined as twice the original \( n \). Note here that Theo-
rem 4 is applied to an arbitrary subset of the original \( a_1, \ldots, a_n \) and the
necessity to distinguish between \( A = A_k \) and \( A_1, \ldots, A_n \) does not
ever always arise. To prove the assertion, we note first that (i) and (ii) hold
for \( k = n \) (since \( 0 < |p|_p < e^{-2H} \), 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 (i) 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 \( b'_1 = \cdots = b'_n = 0 \), say \( b'_j \neq 0 \), and put \( b''_j = b'_j - b'_j b'_1 \) (\( 1 \leq j \leq n \)),

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

\[
0 < |b''_j \log a_1 + \cdots + b''_j \log a_n| = |b''_j| |b'_j| |\log a_1 + \cdots + b'_j \log a_n| < e^{-\epsilon H}.
\]

Further, \( b''_j = 0 \) whenever \( b'_j = 0 \), and since also \( b''_j = 0 \), \( b''_j \neq 0 \), 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 \((2H)^{n-k+1} \). 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 \( n, \delta, A_1, \ldots, A_{n-1}, p, g, \delta, \sigma \), and \( x \) 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 derive a contradiction. Thus we assume that there exist rational integers \( b_1, \ldots, b_n \) with absolute values at most \( H' \) such that (8) holds, that the only integers \( b_1, \ldots, b_n \) with absolute values at most \( H \) such that \( b_i \log a_1 + \cdots + b_i \log a_n = 0 \) are given by \( b'_1 = \cdots = b'_n = 0 \), and that

\[
H \geq 10 C (\log A)^{\eta}.
\]

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

\[
b_j = -b'_j b_n, \quad \xi_j = b_j \log a_1 + \cdots + b_j \log a_n - b_j \log a_n = 1 \leq j \leq n.
\]

The inequality (8) can be written in the form

\[
0 < |\xi_j| < e^{-\epsilon H} |b_j|^{-1},
\]

and thus, since \( |b_j|^{-1} \leq e^{\epsilon H} \) when \( H \) is sufficiently large. In particular, \(|\xi_j| < e^{-\epsilon H} \) when \( H \) is sufficiently large, and from this last inequality and (9) it is clear that

\[
|b_i \log a_1 + \cdots + b_i \log a_n - b_i \log a_n| \leq \max (|\xi_i|, |\log a_n|) < e^{-\epsilon H}, \tag{11}
\]

Now (3), (9) and (11) together with the inequality \( 0 < |\xi_j| < e^{-\epsilon H} \) show that

\[
0 < |\mu a_n^{-1} - 1| < e^{-\epsilon H},
\]

where \( \mu \) denotes \( \exp(b_1 \log a_1 + \cdots + b_n \log a_n - 1) \). Since \( |a_n| = 1 \), we conclude finally that

\[
0 < |\nu - a_n| < e^{-\epsilon H}. \tag{12}
\]

In the following, we shall write \( a \), \( p \) briefly for the analytic functions \( \exp(\log a_n), \exp(\log a) \), respectively. Since \( |\log a_n| < p^{-1} \) and \( |\log a| < p^{-1} \), the power series defining these functions certainly converge for all \( x \) satisfying \( |x| < p^{-1} \).

We now define

\[
\theta = 2/(x + n + 1), \quad \delta = (1 - 1/(2x))(1/2n),
\]

and observe that, since \( x > n + 1 \), we have

\[
1/\delta < \epsilon < 1/(n + 1), \quad 0 < \epsilon < 1/(2n).
\]

We write (12)

\[
\mu = \mu' \log a, \quad k = (K^a),
\]

\[
L = L_1 = \cdots = L_{n-1} = [k^{1-\epsilon}], \quad L_n = [k^\epsilon].
\]

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

Lemmas 1. Let \( M, N \) be integers with \( N > M > 0 \), and let \( m_0 (1 \leq i \leq l, M \leq l \leq N) \) 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 \( \left( N U \right)^{1/(N-M)} \), such that

\[
\sum_{i=0}^{N} x_i = 0 \quad (1 \leq i \leq M).
\]

Proof. See § 4 of [3].

Lemma 2. There exist integers \( p(1, \ldots, n) \), not all 0, with absolute values at most \( \delta^H \) such that for all non-negative integers \( m_1, \ldots, m_{n-1} \) satisfying \( m_1 + \cdots + m_{n-1} \leq k \), the function

\[
\Phi_{m_1, \ldots, m_{n-1}}(x) = P \sum_{l=0}^{L_n} \cdots \sum_{l=0}^{L_n} p(1, \ldots, n) a_1^{l_1} \cdots a_n^{l_n} \delta^{k \cdot l_1 + \cdots + k \cdot l_n},
\]

where \( P = (\log a_1)^{l_1} \cdots (\log a_n)^{l_n} \) and \( \eta = \lambda t + \lambda \beta t (1 \leq \tau \leq n) \), satisfies

\[
|\Phi_{m_1, \ldots, m_{n-1}}(l)| < e^{-\epsilon H} \tag{13}
\]

for all integers \( 1 \leq l \leq h \).

(\( \delta \) 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
\[
\sum_{l=1}^{\tau_x} \ldots \sum_{l=1}^{\tau_x} p(\lambda_1, \ldots, \lambda_n) a_1^{l_1} \cdots a_n^{l_n} y_1^{m_1-1} \cdots y_n^{m_n-1} = 0
\]
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 \( a_1, \ldots, a_n \), respectively. Then, for any non-negative integer \( j \),
\[
(a_i a_j) \sum_{k=1}^{d_i} a_i^l a_j^k = \sum_{k=1}^{d_j} a_j^k a_i^l,
\]
where the \( a_i^l \) are integers with absolute values at most \( 2 \) or \( 2d_i \), according as \( r < n \) or \( r = n \) (see [3], § 3). Thus, multiplying (14) by \( a_1^{l_1} \cdots a_n^{l_n} y_1^{m_1-1} \cdots y_n^{m_n-1} \), and substituting for the powers of \( a_i a_j \), we obtain the equation
\[
\sum_{i=1}^{d_i} \sum_{j=1}^{d_j} V(a_i) a_j = 0,
\]
where
\[
V(a_i) = \sum_{i=1}^{d_i} \sum_{j=1}^{d_j} p(\lambda_1, \ldots, \lambda_n) v(\lambda_i, a_j),
\]
and
\[
v(\lambda_i, a_j) = a_1^{l_1} \cdots a_n^{l_n} y_1^{m_1-1} \cdots y_n^{m_n-1} \prod_{k=1}^{\tau_y} (a_i^{l_1} \cdots a_n^{l_n} y_1^{m_1} \cdots y_n^{m_n} a_k^{l}).
\]
Hence (14) will hold if the \( d_i \) equations \( V(a_i) = 0 \) are satisfied. These are linear equations in the \( p(\lambda_1, \ldots, \lambda_n) \) with integer coefficients. Since \( l_i \leq k_i, m_i-1 \leq k \), \( L_k \leq \tau_k \), and, by hypothesis, the integers \( k_i \) have absolute values at most \( H^2 \), the coefficient \( v(\lambda_1, a_j) \) of \( p(\lambda_1, \ldots, \lambda_n) \) in the linear form \( V(a_i) = 0 \) has absolute value at most
\[
U = (2A)^{2h} c^2 (2LH)^2.
\]
There are at most \((k+1)^{m-1} b \) distinct sets of integers \( l_1, \ldots, l_n \), and hence there are
\[
M \leq d^r (k+1)^{m-1} b \leq d^r 2^{n-1} k^{m-1} = k^{m-1}.
\]
equations corresponding to them. On the other hand, there are \( N = (L_k+1) \ldots (L_k+1) \) unknowns \( p(\lambda_1, \ldots, \lambda_n) \), and
\[
N > k^{m-1} \frac{2^{n-1} b}{2} = k^{m-1} b > 2M,
\]
since \( k^2 \) clearly exceeds \( 2^n b^n \) when \( b \) is sufficiently large. It follows from Lemma 1 that the system of equations \( V(a_i) = 0 \) has a non-trivial solution such that the integers \( p(\lambda_1, \ldots, \lambda_n) \) have absolute values at most \( N \). Now by (10)
\[
L_k \log A \leq k^{m-1} b < k^{m-1} (2L_k)^{10} \leq 2k^{m-1},
\]
and since also
\[
2LH^2 \leq kH^2 \leq k^{b/2},
\]
when \( H \) is sufficiently large, it follows easily that
\[
NU < k^{m} (2L_k)^{10} e^{L_k} a_{\lambda_1} \cdots a_{\lambda_n} \leq \phi H^{m-1} \leq \phi H^m,
\]
is required.

It remains only to verify that (14) implies (13). By virtue of (14), we have
\[
\phi(\lambda_1, \ldots, \lambda_n, \lambda) = \sum_{l=1}^{\tau_x} \ldots \sum_{l=1}^{\tau_x} p(\lambda_1, \ldots, \lambda_n) a_1^{l_1} \cdots a_n^{l_n} \phi(m_1, \ldots, m_n).
\]
Now, noting that \( |a_\lambda| = 1, |\mu_{\lambda}| = 1 \) and applying (12), it is clear that
\[
|m_1^{l_1} \cdots m_n^{l_n} | = |m_1 \cdots m_n| \leq m_1 \cdots m_n < |m_1 \cdots m_n| < e^{-1/2} H,
\]
Thus, since
\[
|y_1^{m_1} \cdots y_n^{m_n-1} | \leq |H^{m-1} | \leq e^{h/2}, \quad |a_{\lambda_1}| = 1, \quad |\lambda_1| < 1 \quad (1 \leq i \leq n),
\]
it follows from (18) that
\[
|\phi(\lambda_1, \ldots, \lambda_n, \lambda_\lambda) | < \frac{\phi H^{m-1}}{\phi H^m} \leq e^{h/2} ;
\]
the last inequality is valid since \( e^{h/2} < 1 \) 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 \( m_1+\ldots+\cdots+m_{n-1} \leq k \), and any integer \( l \) satisfying \( 1 \leq l \leq k^{m_n-1} \), either (13) holds or
\[
|\phi(\lambda_1, \ldots, \lambda_n, \lambda_\lambda) | > (d_\lambda e^{kb/2})^{-4}.
\]
**Proof.** Define
\[
Q'' = e^{2h} c^2 (2LH)^2
\]
and
\[
Q = a_1^{l_1} \cdots a_n^{l_n} y_1^{m_1-1} \cdots y_n^{m_n-1} \cdots x_1 \cdots x_n,
\]
where \( P'' = c_1^{l_1} \cdots c_n^{l_n} y_1^{m_1-1} \cdots y_n^{m_n-1} \), and, as in the proof of Lemma 2, \( a_1, \ldots, a_n \) are the leading coefficients of the minimal polynomials of \( a_1, \ldots, a_n \). It is clear that \( Q'' \) is an integer in \( K \). Noting that
\[
|b_\lambda^{(k+1)^{m-1} b} y_1^{m_1-1} \cdots y_n^{m_n-1} | \leq (2LH)^2 \leq e^{kb/2},
\]
we see that any complex conjugate of $Q'$, obtained by substituting arbitrary complex conjugates for the $a_i$, has absolute value at most
\[ (L_γ + 1) \cdots (L_n + 1) \frac{1}{(dA_{P^{-1}})^{\frac{1}{p}}}, \]
(cf. [3], § 3). Since, by (15), $\sum \log A \leq 2k \log n$, this last expression is at most $a_i^2 \frac{1}{p}$. Thus, either $Q' = 0$, or by (4)
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

Now it is evident that
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

By a similar argument to that given at the end of the proof of Lemma 2, we deduce that
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

In particular, this shows that (13) certainly is valid if $Q' = 0$. If, however, $Q' \neq 0$, then applying the estimates
\[ |P'_p|_p \leq 1, \quad L \leq k^{-1}, \quad L \leq k^L \frac{1}{p}; \]

it follows from (18) that
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

The inequalities (20) and (21) plainly imply that
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2, \]

and we deduce from (19) that
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

But by (18), (3) and (4) (cf. [3], § 3), we have the estimates
\[ |P'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2, \]
\[ |P'_p|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2, \]

and so
\[ |Q'|_p \geq \left( \frac{a_i^2 \frac{1}{p}}{p} \right)^2. \]

This completes the proof of Lemma 3.

**Lemma 4.** Let $J$ be any integer satisfying $0 \leq J < \tau$, where
\[ \tau = \frac{1}{2} \left( n - 1 + \frac{1}{p} \right) + 1. \]

Then (13) holds for all integers $l$ with $1 \leq l \leq \frac{1}{2}kL_\gamma^2$, and each set of non-negative integers $m_1, \ldots, m_{n-1}$ with $m_1 + \cdots + m_{n-1} \leq \frac{1}{2}kL_\gamma^2$.

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

We begin by defining
\[ R_J = \left( \frac{kL_\gamma^2}{J} \right), \quad S_J = \left( \frac{kL_\gamma^2}{J} \right) \quad (J = 0, 1, \ldots, J). \]

Then it suffices to prove that for any integer $l$ with $R_J < l < R_{J+1}$, and any set of non-negative integers $m_1, \ldots, m_{n-1}$ with $m_1 + \cdots + m_{n-1} < S_{J+1}$, we have
\[ \left| f(\ell) \right|_p < \epsilon^{\frac{1}{2p}}. \]

where $f(x)$ denotes $\Phi_{m_1, \ldots, m_{n-1}}(x)$. Let $f_m(x)$ denote the $m$th derivative of $f(x)$. By our inductive hypothesis, we see that for each integer $r$ with $1 \leq r \leq R_J$, and each integer $m$ with $0 \leq m < S_{J+1}$, we have
\[ \left| f_m(r) \right|_p < \epsilon^{\frac{1}{2p}}; \]

for $f_m(r)$ is given by
\[ f_m(r) = \sum_{r_1=1}^{r} \cdots \sum_{r_{n-1}=1}^{r} \frac{1}{r_1 \cdots r_{n-1}} \phi_{m_1}, \cdots, m_{n-1} \left( r_1 \cdots r_{n-1} \right) \times \cdots \times \left( \frac{1}{p} \right) \left( r_1 \cdots r_{n-1} \right) \left( m_1 \cdots m_{n-1} \right). \]

and on expanding the $m$th power of the linear form on the right we obtain
\[ f_m(r) = \sum_{r_1=1}^{r} \cdots \sum_{r_{n-1}=1}^{r} \frac{1}{r_1 \cdots r_{n-1}} \phi_{m_1}, \cdots, m_{n-1} \left( r_1 \cdots r_{n-1} \right) \left( m_1 \cdots m_{n-1} \right). \]

the valuation of each term in the last multiple sum is at most $\epsilon^{\frac{1}{2p}}$, since
\[ m_1 + \cdots + m_{n-1} + j_1 + \cdots + j_{n-1} \leq kL_\gamma^2, \]

and $m_1 \cdots m_{n-1}$, with $j_1 + \cdots + j_{n-1} = m$, is an integer.

We write, for brevity,
\[ F(x) = (x-1) \cdots (x-R_J)^{R_{J+1}}, \]

and we denote by $V$, $V^*$ elements of $\mathcal{L}_p$ satisfying
\[ \left| V \right|_p = p^{\frac{1}{2}}, \quad \left| V^* \right|_p = \frac{1}{2}kL_\gamma^2. \]
respectively. Then
\[ \int_{r_\delta}^{s} \frac{sf(s)}{(z-i)F(s)} \, ds = \frac{f(1)}{F(1)} + \sum_{r > r_\delta} \sum_{m = 1}^{\mu} \frac{f_m(r)}{m!} \int_{r_\delta}^{s} \frac{(z-i)^{m+1}}{(z-i)F(s)} \, ds. \]

Here, of course, the integrals are Schurin line integrals as defined in §II. To verify this, we observe that the integral on the left is the sum of the residues of \( f(z)/[z-i)F(z)] \) (cf. [1], Theorem 13 of Appendix), and the residue at \( z = r \) is given by
\[ \frac{1}{F(z)} \frac{d^{1+r_\delta}}{dz^{1+r_\delta}} \left( \frac{(z-r)^{1+r_\delta}}{F(z)} \right) \]
evaluated at \( z = r \).

On the other hand, the integral on \( F^\nu \) with centre \( z = r \) on the right is given by
\[ \frac{1}{(S_{1+1} - m)!} \frac{d^{m+1}}{dz^{m+1}} \left( \frac{(z-r)^{m+1}}{F(z)} \right) \]
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 \( |z-r_\delta| = |F(z)| \), we have, by (4) and the definition of \( F^\nu \),
\[ 1/R_1 < |z-r_\delta| < \max \{|z-s|, |z-r_\delta| = |z-s| \} \]
whence
\[ \int_{r_\delta}^{s} \frac{(z-r)^{m+1}}{(z-i)F(z)} \, ds \leq \max \{|z-r_\delta|, |F(z)| \} \leq R_1 R_2, \]

Since
\[ R_1 \leq k^{\mu n^2}, \quad S_{1+1} + 1 < k, \quad R_2 \leq 2k^{\mu n^2}, \quad k \leq H^2, \]
it follows that
\[ \int_{r_\delta}^{s} \frac{(z-r)^{m+1}}{(z-i)F(z)} \, ds \leq e^{(m+2)\log H^2}, \]
where, for brevity, we have written
\[ r' = \frac{1}{2}(1+(n+1)) + \frac{1}{2} \delta, \quad 0' = \frac{1}{2} \delta + \frac{1}{2} \delta. \]

Noting that \( |m/n| \leq m! \leq k^2 \) and applying (23), we conclude that the double sum on the right of (24) has valuation at most
\[ e^{-2(1)^{2} \log H^2 + 2\log H^2} < e^{-2H^2} \]
the last inequality is valid for sufficiently large \( H \) since clearly
\[ v' = 1 + \frac{1}{n} \left\lfloor \frac{n-x-1}{8} \right\rfloor < 1 + \frac{1}{n} \left\lfloor \frac{n-x-1}{2} \right\rfloor = 1. \]

We next observe that, since \( R_1 \leq k^{\mu n^2} \) and
\[ \delta = \frac{1}{2}(n+1)(1/2) + \frac{1}{2} \delta = 1/2 \delta - 1, \]

(25) holds, in which case there is nothing more to prove, or
\[ |f(z)| \geq (e^{\mu n^2} - \delta). \]

We show that this last inequality leads to a contradiction. For if this inequality is valid, then since \( LR_1 \leq k^{(n+2)\mu n^2} \) and \( k \leq (n+2)n^2 \), we immediately obtain
\[ |f(z)| \geq 2e^{-2H^2}. \]

But it was shown in the last paragraph that the double sum on the right of (24) has valuation at most \( e^{-2H^2} \). Hence, applying (26) and the estimate \( |F(z)| \leq 1 \), it follows from (24) that
\[ \frac{1}{2} \frac{f(1)}{F(1)} < \int_{r_\delta}^{s} \frac{sf(s)}{(z-i)F(z)} \, ds \]

Now we obtain an upper bound for the right side of this inequality. For those \( z \) satisfying \( |z| = |F(z)| \), we have
\[ p^{-2} = |z| \leq \max \{|z-s|, |z_i| = |z-s| \} \]
whence
\[ \frac{f(z)}{F(z)} \leq p^{-2}, \]
and so for such \( z \)
\[ |F(z)| \geq p^{-(2) \log H^2}, \quad |z-s| \geq p^{-2}. \]

Further, by virtue of the estimates
\[ |z_i| \leq 1, \quad |z_i| \leq 1, \quad |z| \leq 1, \quad |z| \leq 1, \quad |z| \leq 1, \quad |z| \leq 1, \quad |z| \leq 1, \]

we see that \( |f(z)| \leq e^{\mu n^2} \) for those \( z \) satisfying \( |z| \leq p^{-2} \). Hence
\[ \int_{r_\delta}^{s} \frac{sf(s)}{(z-i)F(z)} \, ds \leq \max \{|z-s|, |z_i| = |z-s| \} \leq e^{\mu n^2} p^{-(2) \log H^2}. \]

On the other hand, (25) and the trivial estimate \( |F(z)| \leq 1 \) give a lower bound for the left of (27). Substituting these bounds into (27), we conclude that
\[ e^{(2) \log H^2} < e^{(2) \log H^2}. \]
whence

\[ c' \cdot e^{-2k} > p^{-r} = \varepsilon^{2k} \cdot e^{-2k} \]  

But this is impossible for sufficiently large \( H \). For if \( I = 0 \), the left side of (28) is greater than \( e^{-2k} \), and the right side is at most \( e^{-2k} \cdot e^{-2k} \), and these estimates are contradictory, since, by virtue of the definition \( r = 20d \), we have

\[ \frac{1}{2} (r - 2) \log p > \frac{1}{2} d > 4d. \]

If \( I > 0 \), the left side of (28) is greater than \( \exp(-c_1 \cdot H^{r-2k} \cdot e^{-2k}) \), and the right side is at most \( \exp(-c_1 \cdot H^{2k-2k}) \), 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 \( \Phi(z) = \Phi_{m,n}(z) \). Then, for each non-negative integer \( j \), we have

\[ \log \left| \Phi_j(0) \right| < -c_2 \cdot H^{m-2k} \]

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

**Proof.** Put

\[ X = [\lambda H^{m-2k} \cdot 1/2] \]

Then, by Lemma 4, (13) holds for each integer \( i \) with \( 1 \leq i \leq X \), and each set of non-negative integers \( m_1, \ldots, m_{m-1} \) with \( m_1 + \cdots + m_{m-1} \leq X \). 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 \( 1 \leq r \leq X \) and each integer \( m \) with \( 0 \leq m \leq Y \), we have

\[ |\Phi_m(r)| < e^{-\frac{r}{2H}} \]

Now let \( \omega \) denote any element of \( \Omega \), satisfying \( |\omega|_p = p \). We proceed to give an upper bound for \( |\Phi(\omega)|_p \). Let \( I, I'' \) be elements of \( \Omega \), satisfying \( |I|_p = p^{-1} \), \( |I''|_p \leq X \), respectively, and let

\[ E(z) = (z-1) \ldots (z-X) \cdot X^{1+i}. \]

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

\[ \int_{r''} E(z) \Phi(z) \, dz = \frac{\Phi(r)}{E(r)} + \sum_{m=1}^{r} \sum_{m-1}^{X} \Phi_m(r) \int_{r''} (z-r)^{m-1} \frac{E(z)}{E(r)} \, dz. \]

For those \( z \) satisfying \( |z-r|_p = |I''|_p \), it is clear that

\[ 1/X \leq |r-r''|_p \leq X \]

\[ |z-r|_p = |z-r''|_p \]

\[ |z-r|_p = |z-r''|_p \leq \max (|z-r''|_p, |z-w|_p, |r|_p) = |z-w|_p, \]

whence

\[ \int_{r''} \frac{(z-r)^{m-1}}{(z-w) E(z)} \, dz \leq X^{1+i}. \]

Since \( X \leq H^{m-2k} \cdot 1/2 \), \( X+1 \leq k-H^{m-2k} \), and \( X-1 \leq k-H^{m-2k} \), 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 \( e^{-\frac{r}{2H}} \). Hence

\[ \frac{\Phi(r)}{E(r)} \leq \int_{r''} \frac{z \Phi(z)}{E(z)} \, dz + e^{-\frac{r}{2H}}. \]

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

\[ |E(z)|_p \geq p^{-n} \cdot X^{r+1} \geq |z-r|_p \geq p^{r+1} \]

\[ |\Phi(z)|_p \leq 1, \]

and thus estimating the integral we see that

\[ \frac{\Phi(r)}{E(r)} \leq p^{-n} \cdot X^{r+1} + e^{-\frac{r}{2H}}. \]

Now \( X \leq H^{m-2k} \cdot 1/2 \), \( X+1 \leq k \), whence it is clear (cf. again the proof of Lemma 4) that \( e^{-\frac{r}{2H}} < p^{r+1} \cdot X^{r+1} \), and so

\[ \frac{\Phi(r)}{E(r)} \leq 2p^{-n} \cdot X^{r+1}. \]

But, using the estimates

\[ X \geq \frac{1}{2} \cdot H^{m-2k} \cdot 1/2 \]

\[ X+1 \leq k \cdot 2^k \]

\[ |E(z)|_p \leq p^{X^{r+1}} \]

we conclude that

\[ |\Phi(\omega)|_p < e^{-r \cdot H^{m-2k} \cdot 1/2}. \]

The inequality (29) now follows easily from the integral formula (cf. [1], Theorem 3 of Appendix)

\[ \Phi_j(0) = \int_{0}^{1} \int_{0}^{1} \int_{0}^{1} \frac{\omega \Phi(z)}{\omega^{j+1}} \, dw \]  

where \( A \) denotes an element of \( \Omega \), satisfying \( A \omega = p \).

**Lemma 6.** Let \( t_1, t_2 \) be integers with absolute values at most \( T \), and let

\[ W = t_1 \log c_1 + \ldots + t_n \log c_n. \]

Then either \( W = 0 \) or

\[ |W|_p > (c_1 \cdot A \cdot \omega^{j+1})^{-d}. \]
Proof. Let \( a_j' \) (\( 1 \leq j \leq m \)) be the leading coefficient (supposed positive) of the minimal polynomial of \( a_j \) or \( a_j^{-1} \) according as \( t_j > 0 \) or \( t_j < 0 \). Then
\[
\omega = a_1^{a_1} \cdots a_m^{a_m}(\omega_1^{a_1} \cdots \omega_m^{a_m})^{-1}
\]
is an algebraic integer in \( K \). Further, any of its complex conjugates, obtained by substituting arbitrary complex conjugates for \( a_1, \ldots, a_m \), has absolute value at most \( c_1^{a_1}A^{a_m} \) (cf. [3], § 3). If \( \mathcal{W} \neq 0 \), then \( \omega \neq 0 \), and thus (4) implies that
\[
|\omega|_p \geq (c_1^{a_1}A^{a_m})^{-d}.
\]
Hence, on using (3), we obtain
\[
|\mathcal{W}|_p \geq |\omega_1^{a_1} \cdots \omega_m^{a_m}|_p |\mathcal{W}|_p = |\omega|_p \geq (c_1^{a_1}A^{a_m})^{-d},
\]
and this completes the proof of Lemma 6.

Lemma 7. Let \( d_1, \ldots, d_m \) be any \( m \geq 2 \) numbers in \( \Omega_p \), and let \( a_1, \ldots, a_m \) be \( m \) distinct numbers in \( \Omega_p \) with \( |a_i|_p \leq 1 \) (\( 1 \leq i \leq m \)). Let \( g(z) \) denote the function
\[
\sum_{j=1}^{m} d_i \exp(a_i z),
\]
where \( g(z) \) denotes the \( j \)-th derivative of \( g(z) \).

Proof. For each suffix \( i \) with \( 1 \leq i \leq m \), let the numbers \( c_{ij} \) be defined by the equation
\[
\prod_{j=1}^{m}(z - a_j) / \prod_{j=1}^{m}(a_j - a_i) = \sum_{j=1}^{m} c_{ij} z^j.
\]
It is clear from this definition that
\[
\sum_{j=1}^{m} c_{ij} a_j^{a_i} = \begin{cases} 0 & \text{if } i \neq f, \\ 1 & \text{if } i = f, \end{cases}
\]
whence
\[
\sum_{j=1}^{m} c_{ij} d_i = \sum_{j=1}^{m} d_j a_j^{a_i} = d_i.
\]
Thus we have
\[
\max_{a_i \in \Omega_p} |g_{ij}(0)|_p \geq |d_i|_p \max_{a_i \in \Omega_p} |\sigma_{ij}|_p.
\]
But since \( |a_i|_p \leq 1 \), it is evident from (33) that
\[
\max_{a_i \in \Omega_p} |\sigma_{ij}|_p \leq 1 / \prod_{j=1}^{m}(a_j - a_i) \quad (1 \leq i \leq m).
\]
On combining these last two estimates, we obtain Lemma 7.
But \( n < \frac{1}{2}(r - 1) + 1 + \frac{1}{2} \), 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 the coefficient of \( x^r \) 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 \( a^{q-1}f(x, y) = F(X, Y) \), 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 \( (x, y, p_1, \ldots, p_s) = 1 \), satisfying the equation (1), then plainly

\[
F(X/b, Y/b) = a^{r-\nu}m/b^n,
\]

where \( b \) denotes the largest integer, comprised solely of powers of \( p_1, \ldots, p_s \), which divides both \( X \) and \( Y \). Since \( (X/b, Y/b, p_1, \ldots, p_s) = 1 \), 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 now make a modification in the equation (1). Recall that \( m \) is the largest integer, comprised solely of powers of \( p_1, \ldots, p_s \), which divides \( m \). Suppose that \( m = p_1^{\nu_1} \cdots p_s^{\nu_s} \), where \( \nu_1, \ldots, \nu_s \) are non-negative integers. Dividing each of these exponents by \( n \), we have \( m = p_1^{\nu_1/n} \cdots p_s^{\nu_s/n} \), where \( \nu_1, \ldots, \nu_s \) are integers such that \( 0 \leq \nu_i < n \) for \( 1 \leq i \leq s \). Thus, if we define

\[
x' = x/p_1^{\nu_1} \cdots p_s^{\nu_s}, \quad y' = y/p_1^{\nu_1} \cdots p_s^{\nu_s}, \quad m' = m/p_1^{\nu_1} \cdots p_s^{\nu_s},
\]

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

\[
f(x', y') = m'.
\]

Here the integer \( m' \) has the important property that

\[
|m'|_{p_i} \geq p_i^{\nu_i-n} \quad (1 \leq i \leq s),
\]

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 \( p_1, \ldots, p_s \).

Before proceeding to our principal argument, we introduce more notation and recall several facts from algebraic number theory. Put \( \sigma = s+1 \), and let \( |r_1|, |r_2|, \ldots, |r_s| \) denote respectively the valuations of \( |a|, |b_1|, \ldots, |b_s| \) of \( Q \), the field of rational numbers. In a similar notation to that used above, let \( \Omega_i \) denote the completion of the algebraic closure of the completion of \( Q \) with respect to \( |r_i| \). Thus, in particular, \( \Omega_1 \) is the field of complex numbers. Plainly, \( f(x', y') \) will factorize in each \( \Omega_i \) into a product of linear factors of the form

\[
f(x', y') = (x' - a_i^{(i)}y') \cdots (x' - a_i^{(m)}y') \quad (1 \leq i \leq s),
\]

where \( a_i^{(1)}, \ldots, a_i^{(m)} \) are distinct elements of \( \Omega_i \). Let \( R \) be the number field which is obtained by adjoining \( a = a_i^{(1)} \) to \( Q \). Clearly the \( n \) subfields of \( \Omega_i \), which are isomorphic to \( R \), are the fields which are obtained by adjoining the \( n \) numbers \( a_i^{(1)} \) (1 \( \leq i \leq n \)) to \( Q \). If \( \xi \) is any element of \( R \), we shall denote by \( \xi^{(1)} \) the image of \( \xi \) under that embedding of \( R \) in \( \Omega_i \), which is defined by mapping \( a \) to \( a_i^{(1)} \).

Since \( f(x', y') \) is irreducible over \( Q \), \( R \) has degree \( n \) over \( Q \). Thus there are at most \( n \) valuations of \( R \) extending any given valuation of \( Q \), and hence there will be at most \( n \) elements in the set \( S = \{ |r_1|, \ldots, |r_s| \} \) of valuations of \( R \) extending the set \( S = \{ |r_1|, \ldots, |r_s| \} \) of valuations of \( Q \). It will be assumed that the reader is familiar with the fact (cf. [8], p. 30) that every valuation \( |r| \) of \( R \) extending the valuation \( |r_i| \) of \( Q \) is given by

\[
|r| = |\xi r_i|_{r_i} \quad (\xi \in R)
\]

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

\[
\sum_{\xi \in R} |r| = n, \quad \prod_{\xi \in R} |\xi r_i|_{r_i} = |\xi|_{r_i}^{n-1},
\]

where \( n \) denotes the degree of the completion of \( R \) at \( |r_i| \) over the completion of \( Q \) at \( |r_i| \), and both the sum and the product are taken over all valuations of \( R \) extending \( |r_i| \) (cf. § III).

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

\[
\prod_{\eta \in R} |\eta|_S = 1.
\]

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

\[
\Delta = \begin{vmatrix}
\log|\eta_1|_{r_1} & \cdots & \log|\eta_{q-1}|_{r_1} \\
\cdots & \cdots & \cdots \\
\log|\eta_1|_{r_{q-1}} & \cdots & \log|\eta_{q-1}|_{r_{q-1}}
\end{vmatrix}
\]

is equal to 1.
is not zero. Further, $\eta_1, \ldots, \eta_{g-1}$ can be chosen so that not only is $J \neq 0$, but also
\begin{equation}
|J| \geq C_{\lambda_1} \quad |\log \eta_j|_{\mathfrak{p}_1} \leq C_2 \quad (1 \leq i \leq q-1, 1 \leq j \leq q-1),
\end{equation}
where $C_1, C_2$ denote positive numbers, which can be specified explicitly in terms of $n_1$ the coefficients of $f(x', y')$, and $p_1, \ldots, p_2$. As remarked earlier, we shall use the equation (38), rather than the original equation (1). Thus $x', y'$ will denote rational numbers satisfying (36), whose denominators are composed solely of powers of $p_1, \ldots, p_2$. We put
\begin{equation}
\beta = x' - ay'.
\end{equation}
By the factorization (37), and the fact that $f(x', y') = m'$, we have
\begin{equation}
|\beta|^{\hslash_1} \beta^{(\hslash_2)_{\hslash_2}} = |m'|_{\mathfrak{p}_2} \quad (1 \leq i \leq \sigma).
\end{equation}
Multiplying these $\sigma$ equations together and using (38), we obtain
\begin{equation}
\prod_{\mathfrak{p}_2} |\beta|_{\mathfrak{p}_2}^{n_2} = \prod_{i=1}^{\sigma} |m'|_{\mathfrak{p}_i},
\end{equation}
and, taking logarithms and again using (38), it follows that
\begin{equation}
\sum_{\mathfrak{p}_2} n_2 \log |\gamma|_{\mathfrak{p}_2} = 0,
\end{equation}
where, for brevity, we have written $\gamma$ for $\prod_{\mathfrak{p}_2} |\beta|_{\mathfrak{p}_2}$. Note that the number on the right of (41) is precisely $|m'|_{\mathfrak{m}_1}$; 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 $|\mathfrak{m}_1|$ which leads to the more general form of Theorem 1.

Now I assert that we can find integers $b_1, \ldots, b_{q-1}$ such that
\begin{equation}
\gamma = b_1^{(\hslash_2)_{\hslash_2}} \ldots b_{q-1}^{(\hslash_2)_{\hslash_2}}
\end{equation}
satisfies
\begin{equation}
|\log (\gamma^{-1})|_{\mathfrak{p}_2} \leq C_1 \quad (1 \leq i \leq q).
\end{equation}
To prove this, we observe that, since $J \neq 0$, there exist real numbers $b_1, \ldots, b_{q-1}$ such that
\begin{equation}
\sum_{1}^{\sigma} |b_i|_{\mathfrak{p}_i} \log |b_i|_{\mathfrak{p}_i} + \log (\gamma^{-1})_{\mathfrak{p}_2} = 0 \quad (1 \leq i \leq q-1),
\end{equation}
whence, choosing integers $b_1, \ldots, b_{q-1}$ so that $|b_i - b_i| \leq 1/2$ for $1 \leq i \leq q-1$, it is clear that the element $\gamma$ of $\mathfrak{R}$ defined above satisfies
\begin{equation}
|\log (\gamma^{-1})|_{\mathfrak{p}_2} \leq (q-1)C_2 + 1 \quad (1 \leq i \leq q-1).
\end{equation}
But, since $\eta_1, \ldots, \eta_{q-1}$ are $\mathfrak{S}$-units, we have
\begin{equation}
\prod_{\mathfrak{p}_2} |\beta|_{\mathfrak{p}_2} = \prod_{\mathfrak{p}_2} |\eta_j|_{\mathfrak{p}_2},
\end{equation}
and so it follows from (41) that
\begin{equation}
\sum_{\mathfrak{p}_2} n_2 \log (\gamma^{-1})_{\mathfrak{p}_2} = 0.
\end{equation}
Now (44) and (45) together plainly imply (43).

We next obtain an upper estimate for the height of $\gamma$. Let
\begin{equation}
g(x) = d(x - \gamma^{(\hslash_2)_{\hslash_2}}) \ldots (x - \gamma^{(\hslash_2)_{\hslash_2}}),
\end{equation}
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 $p_1, \ldots, p_2$, the valuations of $\beta$, and so also of $\gamma$, are at most equal to 1 for every valuation of $\mathfrak{R}$ which does not belong to $\mathfrak{S}$. Thus there exists an integer $d'$, composed solely of powers of $p_1, \ldots, p_2$, with the property that $d'\gamma$ is an algebraic integer in $\mathfrak{R}$. Let $d$ divides $d'$, and therefore $d$ is composed solely of powers of $p_1, \ldots, p_2$, whence
\begin{equation}
|d| = 1 \prod_{\mathfrak{p}_2} |d|_{\mathfrak{p}_2}.
\end{equation}
We now obtain a lower bound for the $|d|_{\mathfrak{p}_2}$. If $h(x)$ denotes a polynomial with coefficients in $\mathfrak{B}_2$, we define $|h|_{\mathfrak{p}_2}$ to be the maximum of the valuations of the coefficients of $h(x)$. Since $|\mathfrak{p}_2$ is a non-archimedean valuation for $2 \leq i \leq \sigma$, the same argument as that used to prove the lemma of Gauss (cf. [2], p. 20) shows that $|h|_{\mathfrak{p}_2} = |h|_{\mathfrak{p}_2} |h|_{\mathfrak{p}_2}$ for any two polynomials $h_1(x), h_2(x)$. Hence, applying this result to the polynomial
\begin{equation}
g(x) = d(x - \gamma^{(\hslash_2)_{\hslash_2}}) \ldots (x - \gamma^{(\hslash_2)_{\hslash_2}}) \quad (2 \leq i \leq \sigma),
\end{equation}
we obtain that
\begin{equation}
|g|_{\mathfrak{p}_2} = |d|_{\mathfrak{p}_2} \prod_{\mathfrak{p}_2} \max (1, |\gamma^{(\hslash_2)_{\hslash_2}}|_{\mathfrak{p}_2}) \quad (2 \leq i \leq \sigma).
\end{equation}
But $|\mathfrak{p}_2| = 1$ for $2 \leq i \leq \sigma$, since the coefficients of $g(x)$ are, by hypothesis, relatively prime integers. Thus, by virtue of (43),
\begin{equation}
|d|_{\mathfrak{p}_2} \geq c^{-d} \psi^{-\sigma} \quad (2 \leq i \leq \sigma),
\end{equation}
and so it follows from (46) that
\[ |d| \leq \delta^{\nu q^{(n-1)}}. \]

Now the minimal polynomial of \( \gamma \) divides \( \gamma(x) \). The roots of this minimal polynomial are a subset of \( \gamma^{(n)}(1), \ldots, \gamma^{(n)}(n) \), and its highest coefficient divides \( d \). Hence (43) and (47) clearly imply that the height of \( \gamma \) is at most \( C_q \delta^{q^m} \). But by definition
\[ \delta^{q^m} = \prod_{\nu=1}^{n} |\nu|_{1, \nu} = |\nu|_{1, \nu} \]
and thus the height of \( \gamma \) is at most \( C_q |\nu|_{1, \nu} \).

From the definition of \( \gamma \) it is clear that
\[ \log |\gamma_{1, \gamma}| = -b_1 \log |\nu_{1, \gamma}| - \cdots - b_{q-1} \log |\nu_{q-1, \gamma}| \quad (1 \leq j \leq q-1), \]
whence, solving these equations, we obtain
\[ -b_k = \sum_{\nu=1}^{q-1} A_{\nu k} \log |\gamma_{1, \nu}| \quad (1 \leq k \leq q-1), \]
where \( A_{\nu k} \) denotes the cofactor of the element in the \( j \)th row and \( k \)th column of the determinant \( A \). Thus, if \( H \) denotes the maximum of the absolute values of \( b_1, b_2, \ldots, b_{q-1} \), at least one of the numbers
\[ |\log |\gamma_{1, \nu}|| \quad (1 \leq j \leq q-1) \]
must exceed \( C_q H \). Let this maximum be given by \( j = J \). Then, by (43),
\[ |\log |\gamma_{1, \nu}|| = |\log |\gamma_{1, \nu}|| - \log |\gamma_{1, J}|| \geq C_q H - C_q, \]
and this inequality together with (49) plainly implies that there is a suffix \( I_j \) with \( 1 \leq I_j \leq \sigma \\) such that
\[ |\log |\gamma_{1, \nu}||| \leq - (C_q H - C_q)(|w|_{\nu} - 1). \]

But, as was remarked earlier, \( |\gamma_{1, \nu}| < 2^{2^\nu \cdot \sigma_{\nu}} \) for some pair of indices \( i, j \) with \( 1 \leq i < \sigma \) and \( 1 < j \leq n \), and thus we have shown that
\[ |\log |\gamma_{1, \nu}|| \leq - (C_q H - C_q)(|w|_{\nu} - 1). \]
In particular, this implies that \( |\gamma_{1, \nu}| \leq 2^{2^\nu \cdot \sigma_{\nu}} \), and so it follows from (40) and the inequality \( |\mu|_{1, \nu} \geq \mu_{1, \nu}^{\nu_{1, \nu}} \) that
\[ |\gamma_{1, \nu}| \geq C_q \delta^{q_\nu \cdot \nu_{1, \nu}^{\nu_{1, \nu}}} \]
for some superscript \( k \neq j \). Let \( h \) denote any superscript other than \( k \) or \( j \). Since \( \nu \geq 3 \), such a superscript certainly exists.

As an immediate consequence of the identity
\[ (a_0^{(n)} - a_0^{(n)})^{(n)} - (a_0^{(n)} - a_0^{(n)})^{(n)} = (a_0^{(n)} - a_0^{(n)})^{(n)}, \]
we obtain the equation
\[ a_1^{(n)} \cdots a_{q-1}^{(n)} - a_q = a_n, \]
where
\[ a_g = \frac{(a_0^{(n)} - a_0^{(n)})^{(n)}}{(a_0^{(n)} - a_0^{(n)})^{(n)}}, \quad a_q = \frac{a_0^{(n)}}{a_0^{(n)}} \quad (1 \leq g \leq q-1). \]
Now by virtue of the inequalities (43), (48) and (49) and the definition of \( \nu_{\nu} \), it is clear that
\[ \theta < |\nu|_{1, \nu} < C_q \delta^{q_\nu \cdot \nu_{1, \nu}^{\nu_{1, \nu}}} \]
Further, as it was shown earlier that the height of \( \gamma \) is at most \( C_q |\nu|_{1, \nu} \), it is easily verified (cf. [3], § 6) that
\[ \log A \leq C_q (1 + \log |\nu|_{1, \nu}), \]
where \( A \) denotes the height of \( \gamma \). Also we have by (43)
\[ C_q \delta^{\nu_{1, \nu}} < |\nu|_{1, \nu} < C_q \delta^{\nu_{1, \nu}}. \]
We are now in a position where we can apply either Theorem 3 of the present paper or Theorem 3 of [3], according to \( H \), in a \( p \)-adic field or the complex field. In either case we shall deduce that
\[ H < \max \{ C_{13}, C_{14} \mu(\log |\nu|_{1, \nu}) \}. \]
Here \( x' = \frac{1}{2}(x + n(s+1)+1) \), and \( s \) 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
\[ 0 < |\nu|_{1, \nu} < \frac{C_q}{q_{13}}, \]
for (53) is certainly true if \( C_q \delta^{q_\nu \cdot \nu_{1, \nu}^{\nu_{1, \nu}} - 1} \geq 1 \).
We now proceed to verify (53). We assume first that \( \nu \) is a \( p \)-adic field. Let \( K \) be the number field which is obtained by adjoining \( a_0^{(n)}, \ldots, a_0^{(n)} \) to \( Q \). Then \( K \) has degree at most \( \sigma_{\nu}^{\nu_{1, \nu}} \), and is generated over \( Q \) by an element \( \theta \) 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 \( \gamma \) shows that
each of $a_1, \ldots, a_n$, has height at most $C_{10}$. Let $p$ be the set of all algebraic integers $\xi$ in $K$ satisfying $|\xi|_c < 1$. Then $p$ is clearly a prime ideal, and the valuation of $K$ determined by $p$ is none other than $| \cdot |_p$. Let $2 = \max (C_{10}, C_{11}, c^{(3)})$. Then, by virtue of (39), (50), (54), and (52) and the fact that $n' > n(s+1)+1$, all the hypotheses of Theorem 3 are satisfied with $a_1, \ldots, a_n$ replaced by $a_1, \ldots, a_n$, $x$ replaced by $C_{10}/2$, and $x$ replaced by $x'$. Note that the inequality $x' > p+1$ is valid since plainly $p < n(s+1)+1$. The assertion (53) then follows from the conclusion of Theorem 3 and (51).

We suppose next that $G_{11}$ is the complex field. Then, as above, each of $a_1, \ldots, a_n$ has height at most $C_{10}$. Let $2 = \max (C_{16}, C_{19})$. Thus, by (52), (54) and the inequality $n' > n(s+1)+1$, it is clear that all the hypotheses of Theorem 3 are satisfied with $a_1, \ldots, a_n$ replaced by $a_1, \ldots, a_n$, $x$ replaced by $C_{10}/2$, and $x$ replaced by $x'$. Note that $n' > p+1$ or $n' > p+2$ according as $a_1, \ldots, a_n$ are or are not all real, since for these two cases we have the respective inequalities $p < n(s+1)+1$, $p < n(s+1)+1$. The assertion (53) then follows from the conclusion of Theorem 3 of [3] and (51).

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

$$|z|^{|i|_e} = |z|^{|i|_e} |y|^{p(j - j')}^2 \cdots |y|^{p(j - j')^2} C_{10} e^{O_{e}}(m(m(m)))^{m'} (1 \leq i \leq \sigma, 1 \leq j \leq s).$$

Hence the identities

$$x'' = \frac{-d_0(d_0 - d_0^h)}{d_0 - d_0^h}, \quad y'' = \frac{-d_0 - d_0^h}{d_0 - d_0^h} (1 \leq i \leq \sigma, 1 \neq j)$$

imply that

$$|z'|_{<e} < C_{10} e^{O_{e}(m(m)))^{m'}}, \quad |y'|_{<e} < C_{10} e^{O_{e}(m(m)))^{m'}} (1 \leq i \leq \sigma).$$

But

$$z'' = \langle x, p_1, \ldots, p_s \rangle, \quad y'' = \langle y, p_1, \ldots, p_s \rangle,$$

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

$$|z|_e < C_{10} e^{O_{e}(m(m)))^{m'}} (1 \leq i \leq s).$$

Applying (55) again, we obtain

$$|z| = |z|^{|i|_e} |y|^{p(j - j')}^2 \cdots |y|^{p(j - j')^2} C_{10} e^{O_{e}(m(m)))^{m'}},$$

$$|y| = |y|^{|i|_e} |y|^{p(j - j')}^2 \cdots |y|^{p(j - j')^2} C_{10} e^{O_{e}(m(m)))^{m'}}.$$

If $\log(|m(m))^{m'} = (s+1)C_{10}$, these inequalities clearly imply that

$$\max (|z|, |y|) < C_{10},$$

and so the conclusion of Theorem 1 is certainly valid; and it is again obvious if $\log(|m(m))^{m'} > (s+1)C_{10}$, the proof of Theorem 1 is therefore complete.