A p-ADIC ANALOGUE TO A THEOREM BY J. POPKEN

Dedicated to the memory of Hanna Neumann

K. MAHLER

(Received 27 April 1972)

Communicated by M. F. Newman

Abstract

It is proved that if

\[ f = \sum_{h=0}^{\infty} f_h z^h \]

is a formal power series with algebraic p-adic coefficients which satisfies an algebraic differential equation, then a constant \( \gamma_4 > 0 \) and a constant integer \( h_1 \geq 0 \) exist such that

either \( f_h = 0 \) or \( |f_h|_p \geq \exp^{-\gamma_4 h (\log h)^2} \) for \( h \geq h_1 \).

1

In his Ph.D. thesis, Jan Popken (1935) proved the following important result.

Theorem: Let

\[ f = \sum_{h=0}^{\infty} f_h z^h \]

be a formal power series with real or complex algebraic coefficients which satisfies an algebraic differential equation. Then a positive constant \( c \) exists such that, for all sufficiently large suffixes \( h \),

either \( f_h = 0 \) or \( |f_h| \geq e^{-c h (\log h)^2} \).

An analogous theorem for formal power series with p-adic coefficients will be established in the present paper. Its proof is based on results from two recent papers of mine, [1] and [2].

Popken's theorem can be proved quite similarly, and this proof would be slightly shorter than the original one.
Denote by $\Omega$ an arbitrary field of characteristic 0. If the formal power series

$$f = \sum_{h=0}^{\infty} f_h z^h$$

with coefficients $f_h$ in $\Omega$ satisfies an algebraic differential equation which has likewise coefficients in $\Omega$, then it is known that $f$ also satisfies such an algebraic differential equation with rational integral coefficients (Ritt and Gourin 1927; paper 2). Moreover, it evidently may be assumed that this differential equation does not explicitly involve the indeterminate $z$ and therefore is of the form

$$F((w)) \equiv F(w, w', \cdots, w^{(m)}) \equiv \sum_{(\kappa)} p_{(\kappa)} w^{(\kappa_1)} \cdots w^{(\kappa_N)} = 0.$$  \hspace{1cm} (1)

Here $m$ and $n$ are two fixed positive integers; $N$ depends on $(\kappa)$ and assumes only the values 0, 1, 2, $\cdots$, $n$; $(\kappa) = (\kappa_1, \cdots, \kappa_N)$ runs over finitely many systems of integers where

$$0 \leq \kappa_1 \leq m, \cdots, 0 \leq \kappa_N \leq m; \ k_1 \leq k_2 \leq \cdots \leq k_N;$$  \hspace{1cm} (2)

and the coefficients $p_{(\kappa)}$ are rational integers distinct from 0. There is at most one system $(\kappa)$ for which $N = 0$. This improper system will be denoted by $(\omega)$, and to it there corresponds the constant term $p_{(\omega)}$ on the right-hand side of (1).

On differentiating the equation (1) $h$ times and then putting $w = f$ and $z = 0$, we obtain by paper [1] the infinite system of equations

$$(3) \sum_{(\kappa)} \sum_{[\lambda]} p_{(\kappa)} \frac{(\kappa_1 + \lambda_1)!}{\lambda_1!} \cdots \frac{(\kappa_N + \lambda_N)!}{\lambda_N!} f_{k_1 + \lambda_1} \cdots f_{k_N + \lambda_N} = 0 \quad (h = 1, 2, 3, \cdots)$$

for the coefficients $f_h$ of $f$. Here in the second sum $[\lambda] = [\lambda_1, \cdots, \lambda_N]$ runs over all systems of $N$ integers satisfying

$$\lambda_1 \geq 0, \cdots, \lambda_N \geq 0, \lambda_1 + \cdots + \lambda_N = h,$$

$N$ being the same number of terms as in the system $(\kappa)$.

As was proved in detail in paper [1], it can be deduced from (3) that there exist

(a) a polynomial $A(h) \neq 0$ in $h$ with rational integral coefficients;

(b) a polynomial $\phi_h(f_0, f_1, \cdots, f_{h-1})$ in $f_0, f_1, \cdots, f_{h-1}$, likewise with rational integral coefficients; and

(c) a positive integral constant $h_0$,

such that
\[(4) \quad A(h) \neq 0 \quad \text{and} \quad A(h) f_h = \phi_h(f_0, f_1, \ldots, f_{h-1}) \quad \text{for} \ h \geq h_0.\]

Here, by paper [1], the polynomial \(\phi_h\) has the explicit form
\[(5) \quad \phi_h(f_0, f_1, \ldots, f_{h-1}) = \sum_{\{v\} \in S_h} P_{\{v\}, h} f_{v_1} \cdots f_{v_N},\]
where now \(N\) assumes at most the values 1, 2, \ldots, \(n\); where \(S_h\) is a certain finite set of systems \(\{v\} = \{v_1, \ldots, v_N\}\) of integers satisfying
\[(6) \quad 0 \leq v_1 \leq h - 1, \ldots, 0 \leq v_N \leq h - 1, v_1 + \cdots + v_N \leq h + c_1,\]
\(c_1\) being a positive constant independent of \(h\) and \(\{v\}\); and where the coefficients \(P_{\{v\}, h}\) are rational integers which may depend on \(h\) and \(\{v\}\).

It is obvious that the relations (4) remain valid if \(h_0\) is increased. Let therefore, without loss of generality, \(h_0\) be so large that
\[(7) \quad h_0 \geq c_1 + 2.\]

4

From now on assume that the coefficients \(f_h\) of \(f\) are algebraic over the rational field \(\mathbb{Q}\). Then, by the second relations (4), the infinite extension field
\[K = \mathbb{Q}(f_0, f_1, f_2, \cdots)\]
of \(\mathbb{Q}\) is identical with the finite algebraic extension
\[K = \mathbb{Q}(f_0, f_1, \cdots, f_{h_0-1})\]
of \(\mathbb{Q}\) and so is an algebraic number field of finite degree, \(D\) say, over \(\mathbb{Q}\).

This number field \(K\) can then in \(D\) distinct ways be imbedded in the complex field \(\mathbb{C}\), so generating the \(D\) conjugate real or complex algebraic number fields
\[K^{(1)}, \ldots, K^{(D)}\]
say. If \(a\) is any element of the abstract algebraic field \(K\), denote by \(a^{(j)}\), where \(j = 1, 2, \cdots, D\), the image of \(a\) in \(K^{(j)}\). As is usual, we put
\[|a| = \max(|a^{(1)}|, \ldots, |a^{(D)}|).\]

5

By hypothesis, \(f\) satisfies the algebraic differential equation (1), and this equation has rational coefficients. It follows then that the \(D\) power series
\[f^{(j)} = \sum_{h=0}^{\infty} f_h^{(j)} z^h \quad (j = 1, 2, \cdots, D)\]
conjugate to \(f\) over \(K\) also satisfy the same differential equation (1).
Hence, by the main theorem of my paper [1], there exist for each \( j \) a pair of positive constants \( \gamma_1^{(j)} \) and \( \gamma_2^{(j)} \) such that

\[
|f_h^{(j)}| \leq \gamma_1^{(j)}(h!)^{\gamma_2^{(j)}} \quad \left[ j = 1, 2, \ldots, D \right] \quad \left[ h = 0, 1, 2, \ldots \right].
\]

Therefore, on putting

\[
\gamma_1 = \max_{j=1,2,\ldots,D} \gamma_1^{(j)} \quad \text{and} \quad \gamma_2 = \max_{j=1,2,\ldots,D} \gamma_2^{(j)},
\]

our hypothesis implies the infinite sequence of inequalities

\[
|f_h| \leq \gamma_1(h!)^{\gamma_2} \quad (h = 0, 1, 2, \ldots).
\]

6

In addition to this inequality for \( |f_h| \), we require an upper estimate for the denominators, \( d_h \) say, \( \circ \) the coefficients \( f_h \). Here \( d_h \) is a positive rational integer, by preference as small as possible, such that the product

\[
g_h = d_h f_h \quad (h = 0, 1, 2, \ldots)
\]

is an algebraic integer in \( K \).

An upper bound for such denominators \( d_h \) can be obtained by the following considerations which go back to Popken’s thesis.

By (4), (5), and (9), \( g_h \) can be written in the explicit form

\[
g_h = \sum_{\{v_j\} \in S_n} P_{\{v_j, h\}} \frac{d_h}{A(h)d_{v_1} \cdots d_{v_N}} g_{v_1} \cdots g_{v_N} \quad \text{for} \quad h \geq h_0.
\]

Here, for the first \( h_0 \) denominators

\[
d_0, d_1, \ldots, d_{h_0-1},
\]

choose the smallest positive rational integers for which the products

\[
g_0, g_1, \ldots, g_{h_0-1}
\]

as defined in (9) are algebraic integers in \( k \), and then, for each larger suffix

\[
h \geq h_0
\]

define \( d_h \) recursively as the smallest positive rational integer such that

\[
A(h)d_{v_1} \cdots d_{v_N} \text{ is a divisor of } d_h \text{ for all systems } \{v\} \in S_h.
\]

By complete induction on \( h \) it is then immediately obvious from (10) that also all the products \( g_h \) with \( h \geq h_0 \) become algebraic integers in \( K \).
7

It is now convenient to split every system \( \{v\} \) in \( S_h \) into two subsystems
\[
\{ \xi_1, \ldots, \xi_X \} \quad \text{and} \quad \{ \xi_1, \ldots, \xi_Y \}
\]
where the \( \xi \)'s are those \( v \)'s which are \( \leq h_0 - 1 \), while the \( \zeta \)'s are the \( v \)'s which are \( \geq h_0 \). For reasons which will soon become clear, we further put
\[
\eta_1 = \zeta_1 - (h_0 - 1), \quad \eta_2 = \zeta_2 - (h_0 - 1), \ldots, \quad \eta_Y = \zeta_Y - (h_0 - 1),
\]
so that \( \eta_1, \ldots, \eta_Y \) are \textit{positive} integers. With the \( \zeta \)'s and \( \eta \)'s so defined, the system \( \{v\} \) will from now on be written as
\[
\{v\} = \{ \xi | \eta \} = \{ \xi_1, \ldots, \xi_X | \eta_1, \ldots, \eta_Y \}.
\]
Here the numbers \( X \) and \( Y \) are such that
\[
0 \leq X \leq N \leq n, \quad 0 \leq Y \leq N \leq n, \quad 1 \leq X + Y = N \leq n.
\]

We further put
\[
d(k) = d_{k+h_0-1} \quad (k = 1, 2, 3, \ldots)
\]
and define \( S(k) \) as the set of all subsystems \( \{ \eta \} \) to which there exists at least one system
\[
\{v\} \quad \text{in} \quad S_{k+h_0-1} \quad \text{such that} \quad \{v\} = \{ \xi | \eta \}.
\]

8

If \( \{v\} = \{ \xi | \eta \} \) lies in \( S_{k+h_0-1} \), both the factors \( d_{\xi_i} \) and the number \( X \) of these factors in the product
\[
d_{\xi_1} \cdots d_{\xi_X}
\]
are bounded. Hence there exists a positive integral constant \( d^* \) such that
\[
(12) \quad d_{\xi_1} \cdots d_{\xi_X} \text{ is a divisor of } d^* \text{ whenever } \{ \xi | \eta \} \in S_{k+h_0-1} \text{ and } k \geq 1.
\]

Let us then replace \( A(h) \) by the new polynomial
\[
(13) \quad a(k) = A(k + h_0 - 1)d^*
\]
in \( k \). Also \( a(k) \) has rational integral coefficients, and the first formula (4) implies that
\[
(14) \quad a(k) \neq 0 \text{ for } k = 1, 2, 3, \ldots.
\]

In the new notation, the conditions (11) for \( d_h \) are equivalent to the conditions for \( d(k) \), as follows,
A(k + h_0 - 1)d_{\xi_1} \cdots d_{\xi_N} d(\eta_1) \cdots d(\eta_Y) \text{ divides } d(k) \text{ for all } \{\xi \mid \eta\} \in S_{k+h_0-1} \\
\text{and all } k \geq 1.

Further these new conditions are certainly satisfied if
\[(15) \quad a(k)d(\eta_1) \cdots d(\eta_Y) \text{ is a divisor of } d(k) \text{ for all } \{\eta\} \in S(k) \text{ and all } k \geq 1,\]
as will from now be assumed.

We had seen that
\[(6) \quad 0 \leq v_1 \leq h - 1, \cdots, 0 \leq v_N \leq h - 1, \quad v_1 + \cdots + v_N \leq h + c_1 \quad \text{if } \{v\} \in S_h.

By the decomposition of \{v\}, this implies in particular that
\[
0 \leq \zeta_1 \leq k + h_0 - 2, \cdots, 0 \leq \zeta_Y \leq k + h_0 - 2, \quad \zeta_1 + \cdots + \zeta_Y \leq k + h_0 + c_1 - 1
\]
if \{v\} \in S_{k+h_0-1},

and hence that
\[
1 \leq \eta_1 \leq k - 1, \cdots, 1 \leq \eta_Y \leq k - 1, \quad \eta_1 + \cdots + \eta_Y \leq k + h_0 + c_1 - 1 - Y(h_0 - 1)
\]
if \{\eta\} \in S(k).

If \(Y \geq 2\), it follows then, by (7), that
\[(16) \quad 1 \leq \eta_1 \leq k - 1, \cdots, 1 \leq \eta_Y \leq k - 1, \quad \eta_1 + \cdots + \eta_Y \leq k - 1 \quad \text{if } \{\eta\} \in S(k).

These inequalities evidently remain valid also if \(Y = 1\); and they are without content if \(Y = 0\), a case which may be excluded.

9

As usual, denote by \([x]\) the integral part of the positive number \(x\). Further put
\[(17) \quad d[k] = \prod_{j=1}^{k} |a(j)\left[ \frac{(n-1)k+1}{(n-1)j+1} \right] \quad (k = 1, 2, 3, \cdots),\]

so that
\[d(1) = |a(1)|.

We assert that the denominator \(d(k) = d_{k+h_0-1}\) of \(f_{k+h_0-1}\) may for all \(k \geq 1\) be chosen as the integer
\[(18) \quad d(k) = d[k] \quad (k = 1, 2, 3, \cdots),\]

but we do not assert that this is always the smallest possible choice of \(d(k)\).

The assertion (18) is by (15) and (16) certainly true for \(k = 1\) because \(S(1)\) is the empty set and we may therefore take \(d(1) = |a(1)|\). Assume next that (18)
has already been established for all values of $k$ less than some integer $K^*$. We shall now show that then (18) is valid also for $k = K^*$ and so is always true.

To carry out this proof, it suffices by (17) to prove that

$$
\left[ \frac{(n-1)\eta_1 + 1}{(n-1)j + 1} \right] + \cdots + \left[ \frac{(n-1)\eta_Y + 1}{(n-1)j + 1} \right] \leq \left[ \frac{(n-1)k + 1}{(n-1)j + 1} \right]
$$

for all integers $j \geq 1$, for all integers $k = 1, 2, \cdots, K^*$, and for all systems $\{\eta\}$ in $S(k)$. But for such values of the parameters,

$$
\{(n-1)\eta_1 + 1\} + \cdots + \{(n-1)\eta_Y + 1\} \leq (n-1)(\eta_1 + \cdots + \eta_Y) + Y \leq (n-1)(k-1) + Y \leq (n-1)k + 1
$$

because

$$
Y \leq n = (n-1) + 1,
$$

and so the assertion (19) follows at once.

10

This proof has established that we may choose

$$
d_{k+h_0-1} = d(k) = \prod_{j=1}^{k} [a(j) \left[ \frac{(n-1)k + 1}{(n-1)j + 1} \right]]
$$

as an admissible denominator of the coefficients $f_{k+h_0-1}$ if $k \geq 1$. We next determine an upper estimate for this product.

There evidently exist positive constants $c_2, c_3, c_4, c_5$ independent of $j$ and $k$ such that

$$
|a(j)| \leq c_2 j^{c_3} \quad (j = 1, 2, 3, \cdots);
$$

$$
\frac{(n-1)k + 1}{(n-1)j + 1} \leq \frac{k}{j} \quad \text{if } 1 \leq j \leq k \text{ and } k \geq 1;
$$

$$
\sum_{j=1}^{k} \frac{1}{j} \leq c_4 + \log k; \quad \sum_{j=1}^{k} \frac{\log j}{j} \leq c_5 + (\log k)^2.
$$

It thus follows from (20) that

$$
1 \leq d_{k+h_0-1} \leq \prod_{j=1}^{k} (c_2 j^{c_3})^{k/j} \leq c_2^{k(c_4 + \log k)} \cdot e^{c_3 k(c_5 + (\log k)^2)}.
$$

On replacing here $k + h_0 - 1$ again by $h$, we arrive then at the result that

There exists to the series $f$ a positive constant $\gamma_3$ and a positive integer $h_1$ such that the denominator $d_h$ of $f_h$ satisfies the inequality
$$1 \leq d_h \leq e^{\gamma_3(h \log h)^2} \quad \text{for all suffixes } h \geq h_1.$$  

This result certainly holds if all the coefficients $f_h$ of $f$ lie in the formal algebraic number field $K$ of degree $D$ over $\mathbb{Q}$. It still remains valid if we imbed $K$ in any one of the $D$ possible ways in the complex number field $\mathbb{C}$, or if we imbed $K$ for any prime $p$ in some finite algebraic extension of the $p$-adic field $\mathbb{Q}_p$.

11

We apply the last remark to the case when all the coefficients $f_h$ are algebraic $p$-adic numbers.

Denote by
$$u_h(x) = x^D + u_{h_1}x^{D-1} + \cdots + u_{h_D} \quad (h = 0, 1, 2, \ldots)$$
the irreducible polynomial with rational coefficients for which
$$u_h(f_h) = 0 \quad (h = 0, 1, 2, \ldots);$$
here $\Delta$ may depend on $h$. The further polynomial defined by
$$U_h(x) = \prod_{j=1}^{D} (x - f_h^{(j)}) = x^D + U_{h_1}x^{D-1} + \cdots + U_{h_D} \quad (h = 0, 1, 2, \ldots)$$
is then a positive integral power of $u_h(x)$, and therefore also
$$U_h(f_h) = 0 \quad (h = 0, 1, 2, \ldots).$$

Denote again by $d_h$ the denominator of $f_h$ and then put
$$V_h(x) = d_h^D \cdot U_h(x/d_h) \quad (h = 0, 1, 2, \ldots).$$

Then $V_h(x)$ has the explicit form
$$V_h(x) = x^D + V_{h_1}x^{D-1} + \cdots + V_{h_D}$$
with rational integral coefficients. All the zeros of $V_h(x)$ are therefore algebraic integers, and hence the algebraic integer $d_h f_h$ is a divisor of $V_{h_D}$.

Here
$$V_{h_D} = (-1)^D \prod_{j=1}^{D} (d_h f_h^{(j)}),$$
whence, by (8) and (21),
$$|V_{h_D}| \leq \left( e^{\gamma_3(h \log h)^2} \cdot \gamma_1(h!)^{\gamma_2} \right)^D \quad \text{for } h \geq h_1.$$

This estimate implies that there exists a positive constant $\gamma_4$ independent of $h$ such that

$$|V_{h_D}| \leq e^{\gamma_4 h (\log h)^2} \quad \text{for } h \geq h_1.$$
Assume finally that both \( h \geq h_1 \) and
\[
f_h \neq 0.
\]
Then also
\[
f_h^{(j)} \neq 0 \text{ for } j = 1, 2, \ldots, D,
\]
hence
\[
V_{hD} \neq 0,
\]
whence, by (22),
\[
|V_{hD}|_p \geq e^{-\gamma_4 h (\log h)^2} \text{ for } h \geq h_1.
\]

The algebraic integer \( d_h f_h \) is also a \( p \)-adic integer, and it is a divisor of \( V_{hD} \neq 0 \). This implies that
\[
|d_h f_h|_p \geq |V_{hD}|_p.
\]
Further \( d_h \) is a positive rational integer and therefore satisfies
\[
|d_h|_p \leq 1.
\]
On combining these three inequalities (23), (24), and (25), we arrive then finally at the following analogue of Popken's theorem.

**Theorem.** Let \( p \) be a fixed prime, and let
\[
f = \sum_{h=0}^{\infty} f_h z^h
\]
be a formal power series with \( p \)-adic algebraic coefficients which satisfies an algebraic differential equation. Then a positive constant \( \gamma_4 \) and a positive integer \( h_1 \) exist such that
\[
either f_h = 0 or |f_h|_p \geq e^{-\gamma_4 h (\log h)^2} \text{ for } h \geq h_1.
\]
It would have great interest to decide whether this estimate is best possible; but I rather doubt it.

**References**


Department of Mathematics
Institute of Advanced Studies
Australian National University
Canberra