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

BY

K. MAHLER

Reprinted from
THE JOURNAL OF THE AUSTRALIAN
MATHEMATICAL SOCIETY
Volume XVI, part 2, p.p. 176–184
1973

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 $h_1 \geqq 0$ exist such that

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

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,

$$\text{either } f_h = 0 \quad \text{or} \quad |f_h| \geqq e^{-ch(\log h)^2}.$$

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.

2

Denote by Ω 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 Ω satisfies an algebraic differential equation which has likewise coefficients in Ω, 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

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

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

$$0 \leqq \kappa_1 \leqq m, \cdots, 0 \leqq \kappa_N \leqq m; \ \kappa_1 \leqq \kappa_2 \leqq \cdots \leqq \kappa_N; \tag{2}$$

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

3

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

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

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

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

N being the same number of terms as in the system (κ).

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

(a) a polynomial $A(h) \not\equiv 0$ 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) $$A(h) \neq 0 \text{ and } A(h)f_h = \phi_h(f_0,f_1,\cdots,f_{h-1}) \quad \text{for } h \geqq h_0.$$

Here, by paper [1], the polynomial ϕ_h has the explicit form

(5) $$\phi_h(f_0,f_1,\cdots,f_{h-1}) = \sum_{\{v\}\in S_h} P_{\{v\},h} f_{v_1}\cdots f_{v_N},$$

where now N assumes at most the values $1,2,\cdots,n$; where S_h is a certain finite set of systems $\{v\} = \{v_1,\cdots,v_N\}$ of integers satisfying

(6) $$0 \leqq v_1 \leqq h-1,\cdots, 0 \leqq v_N \leqq h-1,\ v_1+\cdots+v_N \leqq h+c_1,$$

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) $$h_0 \geqq c_1 + 2.$$

4

From now on assume that the coefficients f_h of f are algebraic over the rational field $\boldsymbol{Q}$. Then, by the second relations (4), the infinite extension field

$$K = \boldsymbol{Q}(f_0,f_1,f_2,\cdots)$$

of $\boldsymbol{Q}$ is identical with the finite algebraic extension

$$K = \boldsymbol{Q}(f_0,f_1,\cdots,f_{h_0-1})$$

of $\boldsymbol{Q}$ and so is an algebraic number field of finite degree, D say, over $\boldsymbol{Q}$.

This number field K can then in D distinct ways be imbedded in the complex field $\boldsymbol{C}$, so generating the D conjugate real or complex algebraic number fields

$$K^{(1)},\cdots,K^{(D)} \quad \text{say.}$$

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

$$\overline{|a|} = \max(|a^{(1)}|,\cdots,|a^{(D)}|).$$

5

By hypothesis, f satisfies the algebraic differential equation (1), and this equation has rational coefficients. It follows then that the D power series

$$f^{(j)} = \sum_{h=0}^{\infty} f_h^{(j)} z^h \qquad (j = 1,2,\cdots,D)$$

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

$$\left|f_h^{(j)}\right| \leqq \gamma_1^{(j)}(h!)^{\gamma_2^{(j)}} \qquad \begin{bmatrix} j = 1, 2, \cdots, D \\ h = 0, 1, 2, \cdots \end{bmatrix}.$$

Therefore, on putting

$$\gamma_1 = \max_{j=1,2,\cdots,D} \gamma_1^{(j)} \text{ and } \gamma_2 = \max_{j=1,2,\cdots,D} \gamma_2^{(j)},$$

our hypothesis implies the infinite sequence of inequalities

(8) $$\overline{|f_h|} \leqq \gamma_1(h!)^{\gamma_2} \qquad (h = 0, 1, 2, \cdots).$$

6

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

(9) $$g_h = d_h f_h \qquad (h = 0, 1, 2, \cdots)$$

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

(10) $$g_h = \sum_{\{\nu\} \in S_h} P_{\{\nu\},h} \frac{d_h}{A(h)d_{\nu_1} \cdots d_{\nu_N}} g_{\nu_1} \cdots g_{\nu_N} \qquad \text{for } h \geqq h_0.$$

Here, for the first h_0 denominators

$$d_0, d_1, \cdots, d_{h_0-1},$$

choose the smallest positive rational integers for which the products

$$g_0, g_1, \cdots, g_{h_0-1}$$

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

$$h \geqq h_0$$

define d_h recursively as the smallest positive rational integer such that

(11) $A(h)d_{\nu_1} \cdots d_{\nu_N}$ is a divisor of d_h for all systems $\{\nu\} \in S_h$.

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

7

It is now convenient to split every system $\{\nu\}$ in S_h into two subsystems

$$\{\xi_1, \cdots, \xi_X\} \text{ and } \{\zeta_1, \cdots, \zeta_Y\}$$

where the ξ's are those ν's which are $\leqq h_0 - 1$, while the ζ's are the ν's which are $\geqq h_0$. For reasons which will soon become clear, we further put

$$\eta_1 = \zeta_1 - (h_0 - 1), \eta_2 = \zeta_2 - (h_0 - 1), \cdots, \eta_Y = \zeta_Y - (h_0 - 1),$$

so that $\eta_1, \cdots, \eta_Y$ are *positive* integers. With the ξ's and η's so defined, the system $\{\nu\}$ will from now on be written as

$$\{\nu\} = \{\xi \,|\, \eta\} = \{\xi_1, \cdots, \xi_X \,|\, \eta_1, \cdots, \eta_Y\}.$$

Here the numbers X and Y are such that

$$0 \leqq X \leqq N \leqq n, \; 0 \leqq Y \leqq N \leqq n, \; 1 \leqq X + Y = N \leqq n.$$

We further put

$$d(k) = d_{k+h_0-1} \qquad (k = 1, 2, 3, \cdots)$$

and define $S(k)$ as the set of all subsystems $\{\eta\}$ to which there exists at least one system

$$\{\nu\} \text{ in } S_{k+h_0-1} \text{ such that } \{\nu\} = \{\xi \,|\, \eta\}.$$

8

If $\{\nu\} = \{\xi \,|\, \eta\}$ lies in S_{k+h_0-1}, both the factors d_{ξ_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) $d_{\xi_1} \cdots d_{\xi_X}$ *is a divisor of* d^* *whenever* $\{\xi \,|\, \eta\} \in S_{k+h_0-1}$ *and* $k \geqq 1$.

Let us then replace $A(h)$ by the new polynomial

(13) $$a(k) = A(k + h_0 - 1)d^*$$

in k. Also $a(k)$ has rational integral coefficients, and the first formula (4) implies that

(14) $$a(k) \neq 0 \text{ for } k = 1, 2, 3, \cdots.$$

In the new notation, the conditions (11) for d_h are equivalent to the conditions for $d(k)$, as follows,

$A(k+h_0-1)d_{\xi_1}\cdots d_{\xi_X}d(\eta_1)\cdots d(\eta_Y)$ *divides* $d(k)$ *for all* $\{\xi \mid \eta\} \in S_{k+h_0-1}$ *and all* $k \geqq 1$.

Further these new conditions are certainly satisfied if

(15) $a(k)d(\eta_1)\cdots d(\eta_Y)$ *is a divisor of* $d(k)$ *for all* $\{\eta\} \in S(k)$ *and all* $k \geqq 1$,

as will from now be assumed.

We had seen that

$$(6)\qquad 0 \leqq v_1 \leqq h-1, \cdots, 0 \leqq v_N \leqq h-1,\ v_1+\cdots+v_N \leqq h+c_1 \text{ if } \{v\} \in S_h.$$

By the decomposition of $\{v\}$, this implies in particular that

$$0 \leqq \zeta_1 \leqq k+h_0-2, \cdots, 0 \leqq \zeta_Y \leqq k+h_0-2,\ \zeta_1+\cdots+\zeta_Y \leqq k+h_0+c_1-1 \quad \text{if } \{v\} \in S_{k+h_0-1},$$

and hence that

$$1 \leqq \eta_1 \leqq k-1, \cdots,\ 1 \leqq \eta_Y \leqq k-1,\ \eta_1+\cdots+\eta_Y \leqq k+h_0+c_1-1-Y(h_0-1) \quad \text{if } \{\eta\} \in S(k).$$

If $Y \geqq 2$, it follows then, by (7), that

$$(16)\qquad 1 \leqq \eta_1 \leqq k-1, \cdots, 1 \leqq \eta_Y \leqq k-1,\ \eta_1+\cdots+\eta_Y \leqq k-1 \text{ if } \{\eta\} \in S(k).$$

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

$$(17)\qquad d[k] = \prod_{j=1}^{k} |a(j)|^{\left[\frac{(n-1)k+1}{(n-1)j+1}\right]} \qquad (k = 1,2,3,\cdots),$$

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 $k \geqq 1$ be chosen as the integer

$$(18)\qquad d(k) = d[k] \qquad (k = 1,2,3,\cdots),$$

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

$$\left[\frac{(n-1)\eta_1+1}{(n-1)j+1}\right]+\cdots+\left[\frac{(n-1)\eta_Y+1}{(n-1)j+1}\right] \leqq \left[\frac{(n-1)k+1}{(n-1)j+1}\right] \tag{19}$$

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

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

$$= (n-1)(\eta_1+\cdots+\eta_Y)+Y \leqq (n-1)(k-1)+Y \leqq (n-1)k+1$$

because

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

and so the assertion (19) follows at once.

10

This proof has established that we may choose

$$d_{k+h_0-1} = d(k) = \prod_{j=1}^{k} \left|a(j)\right|^{\left[\frac{(n-1)k+1}{(n-1)j+1}\right]} \tag{20}$$

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

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

$$\left|a(j)\right| \leqq c_2 j^{c_3} \qquad (j = 1, 2, 3, \cdots);$$

$$\frac{(n-1)k+1}{(n-1)j+1} \leqq \frac{k}{j} \text{ if } 1 \leqq j \leqq k \text{ and } k \geqq 1;$$

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

It thus follows from (20) that

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

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 γ_3 and a positive integer h_1 such that the denominator d_h of f_h satisfies the inequality

(21) $$1 \leqq d_h \leqq e^{\gamma_3 h(\log h)^2} \qquad \textit{for all suffixes } h \geqq h_1.$$

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

11

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

Denote by

$$u_h(x) = x^{\Delta} + u_{h1}x^{\Delta-1} + \cdots + u_{h\Delta} \qquad (h = 0, 1, 2, \cdots)$$

the irreducible polynomial with rational coefficients for which

$$u_h(f_h) = 0 \qquad (h = 0, 1, 2, \cdots);$$

here Δ may depend on h. The further polynomial defined by

$$U_h(x) = \prod_{j=1}^{D} (x - f_h^{(j)}) = x^D + U_{h1}x^{D-1} + \cdots + U_{hD} \qquad (h = 0, 1, 2, \cdots)$$

is then a positive integral power of $u_h(x)$, and therefore also

$$U_h(f_h) = 0 \qquad (h = 0, 1, 2, \cdots).$$

Denote again by d_h the denominator of f_h and then put

$$V_h(x) = d_h^D \cdot U_h(x/d_h) \qquad (h = 0, 1, 2, \cdots).$$

Then $V_h(x)$ has the explicit form

$$V_h(x) = x^D + V_{h1}x^{D-1} + \cdots + V_{hD}$$

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_{hD}*.

Here

$$V_{hD} = (-1)^D \prod_{j=1}^{D} (d_h f_h^{(j)}),$$

whence, by (8) and (21),

$$|V_{hD}| \leqq \left(e^{\gamma_3 h(\log h)^2} \cdot \gamma_1 (h!)^{\gamma_2}\right)^D \qquad \text{for } h \geqq h_1.$$

This estimate implies that there exists a positive constant γ_4 independent of h such that

(22) $$|V_{hD}| \leqq e^{\gamma_4 h(\log h)^2} \qquad \text{for } h \geqq h_1.$$

12

Assume finally that both $h \geqq h_1$ and

$$f_h \neq 0.$$

Then also

$$f_h^{(j)} \neq 0 \text{ for } j = 1, 2, \cdots, D,$$

hence

$$V_{hD} \neq 0,$$

whence, by (22),

$$\left| V_{hD} \right|_p \geqq e^{-\gamma_4 h(\log h)^2} \quad \text{for } h \geqq h_1. \tag{23}$$

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

$$\left| d_h f_h \right|_p \geqq \left| V_{hD} \right|_p. \tag{24}$$

Further d_h is a positive rational integer and therefore satisfies

$$\left| d_h \right|_p \leqq 1. \tag{25}$$

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 γ_4 and a positive integer h_1 exist such that

$$\text{either } f_h = 0 \text{ or } \left| f_h \right|_p \geqq e^{-\gamma_4 h(\log h)^2} \quad \text{for } h \geqq h_1.$$

It would have great interest to decide whether this estimate is best possible; but I rather doubt it.

References

[1] K. Mahler, *Atti della Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*, 50 (1971) 36–49.
[2] K. Mahler, *Atti della Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*, 50 (1971) 174–184.
[3] J. Popken, Ph. D. Thesis, N.V. Noord-Hollandsche Uitgeversmaatschappij (1935).
[4] J. F. Ritt and E. Gourie, *Bull. Amer. Math. Soc.*, 33 (1927), 182–184.

Department of Mathematics
Institute of Advanced Studies
Australian National University
Canberra