

APPLICATIONS OF p -ADIC INTERPOLATION TO EXPONENTIAL POLYNOMIALS AND SUMS OF POWERS

VICHIAN LAOHAKOSOL and JANE PITMAN

(Received 8 January 1980)

Communicated by A. J. van der Poorten

Abstract

An approach to p -adic interpolation via divided differences is used to give alternative proofs of results of van der Poorten on p -adic exponential polynomials and to derive a p -adic analogue of Turán's first main theorem on sums of powers.

980 *Mathematics subject classification (Amer. Math. Soc.)*: primary 12 B 40; secondary 10 F 45.

1. Introduction

As can be seen, for example, from Gelfond (1960) or Baker (1975), an important part in the theory of transcendence is played by auxiliary results about classical exponential polynomials

$$E(z) = \sum_{i=1}^m \sum_{j=0}^{\rho(i)-1} a_{ij} z^j \exp(\omega_i z) \quad (z \in C),$$

where the frequencies $\omega_1, \dots, \omega_m$ and the coefficients a_{ij} , for $i = 1, \dots, m$ and $j = 0, \dots, \rho(i) - 1$, belong to the complex field C . These auxiliary results give upper bounds for the ratio $M(R)/M(r)$, where $0 < r < R$ and

$$M(R) = \max\{|E(z)|; |z| = R\},$$

and hence for the number of zeros of E in a certain disk and for the absolute values of its coefficients under certain conditions. Proofs of such results typically involve the use of interpolation, and recent work of this kind is described, for example, in van der Poorten (1977) and also in Balkema and Tijdeman (1973),

where an interpolation method is used to obtain an upper bound for $M(R)/M(r)$ and also to prove refinements of Turan’s theorems on sums of powers.

In 1972, Shorey (1972 a and b) initiated the investigation of corresponding results and their applications for p -adic exponential polynomials, that is, exponential polynomials over Ω_p , the completion (with respect to the p -adic valuation $|\cdot|_p$) of the algebraic closure of the p -adic field \mathbb{Q}_p , for a given prime p . Shorey used p -adic interpolation methods modelled on the classical case, with Schnirelman integrals in place of contour integrals. Van der Poorten (1976 a and b) applied different methods and (1976b) obtained more refined estimates by using a precise form of the Hermite interpolation formula. Subsequently Robba, in a paper (1977) which came to our notice only after the present paper was completed, gave a very simple and elegant proof, depending on the Newton polygon, the differential equation and the power series, of van der Poorten’s theorem on zeros.

In this paper we present a different approach to p -adic interpolation and apply it (in sections 4 and 5) to obtain alternative proofs of theorems on exponential polynomials corresponding to those of van der Poorten. We also use it (in section 6) to obtain a p -adic analogue of the version of Turan’s first main theorem considered by Balkema and Tijdeman (1973), and we indicate how a corresponding approach simplifies their proof of the complex version of this theorem. The essence of our approach is that it avoids complicated interpolation formulae by depending heavily on divided differences.

To indicate the kind of result obtainable by this approach, we now give, in a slightly weakened form, our main result on exponential polynomials (Theorem 2 below), which is very close to the corresponding result on page 13 of van der Poorten (1976b).

For fixed positive real θ , and positive integral $m, \rho(1), \rho(2), \dots, \rho(m)$, let $n = \sum_{i=1}^m \rho(i)$, let $\omega_1, \dots, \omega_m$ be distinct elements of Ω_p such that

$$|\omega_i|_p \leq p^{-1/(p-1)-\theta} \quad (i = 1, \dots, m),$$

and let E be a fixed exponential polynomial function of the form

$$E(z) = \sum_{i=1}^m \sum_{j=0}^{\rho(i)-1} a_{ij} z^j \exp(\omega_i z) \quad (|z|_p < p^\theta),$$

where

$$a_{ij} \in \Omega_p \quad (i = 1, \dots, m, j = 0, \dots, \rho(i) - 1).$$

Further, for fixed positive integral l and non-negative integral s_1, s_2, \dots, s_l , let

$$s = \sum_{i=1}^l s_i,$$

and let β_1, \dots, β_l be distinct elements of Ω_p such that

$$|\beta_i|_p \leq 1 \quad (i = 1, \dots, l).$$

Let w, b, B be real numbers such that $w > 0, b > 0,$

$$|\omega_i - \omega_j|_p \geq w \quad (i \neq j),$$

$$|\beta_i - \beta_j|_p \geq b \quad (i \neq j),$$

$$|E^{(j)}(\beta_i)/j!|_p \leq B \quad (0 \leq j \leq s_i - 1, 1 \leq i \leq l).$$

If $n > 1$ and

$$(1.1) \quad s > (n - 1) + ([\log_p(n - 1)] + 1 - 1/(p - 1))/\theta,$$

then for each pair of integers M, N such that $1 \leq M \leq m, 0 \leq N \leq \rho(M) - 1,$ we have

$$|N!a_{MN}|_p \leq w^{-n+1+N}b^{1-s}B,$$

where a_{MN} is the coefficient of $z^N \exp(\omega_M z)$ in $E(z)$.

By applying the above theorem to an exponential polynomial with at least s zeros in the unit circle where s satisfies (1.1), we see that the right-hand side of (1.1) also gives an upper bound for the number of zeros in the unit circle of an exponential polynomial which does not vanish identically. This theorem on zeros can also be proved directly, without recourse to Theorem 2, and it will appear as Theorem 1 below.

The work described here originated in the idea, which was due to Vichian Laohakosol, of finding p -adic analogues of the methods of Balkema and Tijdemann (1973) and using them to improve the results of Shorey (1972a, b) on exponential polynomials. A more detailed discussion of p -adic interpolation, including an account of an earlier version of this work, is given in Laohakosol (1978).

2. Preliminaries on p -adic analysis.

Throughout sections 2 to 5, p is a fixed prime, and $\mathcal{Q}_p, |\cdot|_p, \Omega_p$ are as defined in section 1, and all functions considered have domain and range contained in Ω_p . For $r > 0$ and a function f bounded on $|z|_p = r$, we write

$$M_f(r) = \max\{|f(z)|_p; |z|_p = r\}.$$

We assume the basic results on p -adic analysis, most of which are set out in Adams (1966), and, in particular we need the following results.

LEMMA 1 (maximum modulus theorem). For given $R > 0$, let f be analytic in $|z|_p < R$,

$$f(z) = \sum_{j=0}^{\infty} c_j z^j \quad (|z|_p < R).$$

Then for any r such that $0 < r < R$

$$(2.1) \quad |f(z)|_p \leq M_f(r) \quad \text{for all } z \text{ such that } |z|_p \leq r,$$

$$(2.2) \quad M_f(r) = \max_{j \geq 0} |c_j|_p r^j,$$

$$(2.3) \quad |f^{(j)}(0)|_p \leq |j!|_p M_f(r) r^{-j} \quad (j = 0, 1, 2, \dots).$$

PROOF. See the lemma following the statement of Theorem 1 of Adams and Straus (1971) and Theorem 9 of Adams (1966).

LEMMA 2. For any positive integer m , let $s(m)$ denote the sum of the p -adic digits of m ,

$$s(m) = a_0 + a_1 + \dots + a_t,$$

where

$$m = a_t p^t + a_{t-1} p^{t-1} + \dots + a_1 p + a_0, \quad 0 \leq a_i \leq p - 1 \quad (i = 0, \dots, t).$$

Then

$$|m!|_p = p^{(-m + s(m))/(p-1)}.$$

PROOF. See Lemma 3.1 of Bachman (1964).

It then follows (see, for example, page 306 of Adams (1966) or Theorem 3.1 of Bachman (1964)) that the p -adic exponential function defined by

$$\exp z = e^z = \sum_{i=0}^{\infty} \frac{z^i}{i!} \quad (|z|_p < p^{-1/(p-1)})$$

is well-defined and analytic on $|z|_p < p^{-1/(p-1)}$, and

$$(2.4) \quad |e^z - 1|_p = |z|_p \quad (|z|_p < p^{-1/(p-1)}).$$

At one point we shall use the *Schnirelman integral* of f on the circle $|z|_p = R$, where f is analytic on $|z|_p < \rho$ and $0 < R < \rho$. This integral, which is defined on page 298 of Adams (1966), is denoted by

$$\int_{0,R} f(z) dz.$$

It is easily shown (see, for example, Theorem 1 of Adams (1966)) that

$$(2.5) \quad \left| \int_{0,R} f(z) dz \right|_p \leq M_f(R).$$

3. Basic results on p -adic interpolation

3.1 Throughout section 3, the following notation will be used: m, n are fixed positive integers, $\rho(i)$ ($i = 1, \dots, m$) are fixed positive integers such that

$$n = \sum_{i=1}^m \rho(i),$$

α_i ($i = 1, \dots, m$) are distinct fixed elements of Ω_p , and for $i = 1, \dots, m$ we write α_i for the $\rho(i)$ -dimensional vector with all components equal to α_i , so that

$$\alpha_i = (\alpha_i, \alpha_i, \dots, \alpha_i) \in \Omega_p^{\rho(i)}.$$

As in the classical case (see, for example, Gelfond (1971)), for any given set of elements c_{ij} ($j = 0, \dots, \rho(i) - 1, i = 1, \dots, m$) of Ω_p , there is a unique polynomial P (over Ω_p) of the form

$$P(z) = \sum_{k=0}^{n-1} p_k z^k,$$

which we shall say is “of degree at most $n - 1$ ”, such that

$$(3.1) \quad P^{(j)}(\alpha_i) = c_{ij} \quad (j = 0, \dots, \rho(i) - 1, i = 1, \dots, m).$$

In particular, for each pair M, N such that

$$(3.2) \quad 1 \leq M \leq m, \quad 0 \leq N \leq \rho(M) - 1$$

we denote by Q_{MN} the unique polynomial of degree at most $n - 1$ such that for i, j as above

$$(3.3) \quad Q_{MN}^{(j)}(\alpha_i) = \begin{cases} 1 & \text{if } (i, j) = (M, N) \\ 0 & \text{otherwise.} \end{cases}$$

Clearly the unique polynomial P satisfying (3.1) is then given by

$$(3.4) \quad P(z) = \sum_{i=1}^m \sum_{j=0}^{\rho(i)-1} c_{ij} Q_{ij}(z).$$

3.2 We shall be concerned with the unique interpolation polynomial P of degree at most $n - 1$ such that

$$(3.5) \quad P^{(j)}(\alpha_i) = f^{(j)}(\alpha_i) \quad (j = 0, \dots, \rho(i) - 1, i = 1, \dots, m),$$

where f is analytic in $|z|_p < \rho$ and

$$\max_i |\alpha_i|_p < \rho.$$

We write

$$\begin{aligned} (\eta_0, \eta_1, \dots, \eta_{n-1}) &= (\alpha_1, \alpha_2, \dots, \alpha_m) \\ &= (\alpha_1, \dots, \alpha_1, \alpha_2, \dots, \alpha_2, \dots, \alpha_m, \dots, \alpha_m), \end{aligned}$$

where, in the vector on the right, each α_i is repeated $\rho(i)$ times, and we write

$$(3.6) \quad P \equiv f \pmod{\eta_0, \dots, \eta_{n-1}}$$

if and only if (3.5) holds. The *divided differences* $[\eta_i, \eta_{i+1}, \dots, \eta_{i+j}; f]$ are defined as follows:

$$[\eta_i; f] = f(\eta_i) \quad (0 \leq i \leq n - 1),$$

and, for $0 \leq i < i + j < n$ and $\eta_i \neq \eta_{i+j}$,

$$(3.7) \quad [\eta_i, \dots, \eta_{i+j}; f] = \frac{[\eta_i, \dots, \eta_{i+j-1}; f] - [\eta_{i+1}, \dots, \eta_{i+j}; f]}{\eta_i - \eta_{i+j}};$$

while, for $0 \leq i < i + j < n$ and $\eta_i = \eta_{i+j}$,

$$[\eta_i, \dots, \eta_{i+j}; f] = \lim_{\eta \rightarrow \eta_i} \frac{[\eta_i, \dots, \eta_{i+j-1}; f] - [\eta_{i+1}, \dots, \eta_{i+j-1}, \eta; f]}{\eta_i - \eta}.$$

For $(\eta_0, \dots, \eta_{n-1})$ and f as above, if $\eta_i = \eta_{i+j}$, then we have

$$\eta_i = \eta_{i+1} = \dots = \eta_{i+j-1} = \eta_{i+j},$$

and it is easily shown that

$$[\eta_i, \dots, \eta_{i+j}; f] = [\eta_i, \eta_i, \dots, \eta_i; f] = f^{(j)}(\eta_i)/j!$$

3.3 As with Newton's formula in the classical case, it is easily shown that the interpolation polynomial P of degree at most $n - 1$ such that (3.5), or equivalently (3.6), holds, satisfies

$$(3.8) \quad P(z) = \sum_{j=0}^{n-1} [\eta_0, \dots, \eta_j; f](z - \eta_0) \cdots (z - \eta_{j-1}),$$

$$(3.9) \quad f(z) - P(z) = [z, \eta_0, \dots, \eta_{n-1}; f](z - \eta_0) \cdots (z - \eta_{n-1}).$$

Moreover, if

$$\max_i |\alpha_i|_p = \max_i |\eta_i|_p < R < \rho$$

then for f as above it is easily shown by induction that

$$[\eta_0, \dots, \eta_i; f] = \int_{0,R} \frac{f(z)z \, dz}{(z - \eta_0) \cdots (z - \eta_i)}.$$

It then follows from (3.9) that if

$$\max_i |\eta_i|_p \leq |z|_p < R < \rho,$$

then

$$f(z) - P(z) = \int_{0,R} \prod_{i=0}^{n-1} \left(\frac{z - \eta_i}{u - \eta_i} \right) \frac{f(u)u}{(u - z)} \, du.$$

By applying (2.5) to this integral, we obtain the following estimate of the error.

LEMMA 3. Suppose that

$$|\alpha_i|_p \leq |z_0|_p < R < \rho \quad (i = 1, \dots, m),$$

and P is the interpolation polynomial of degree at most $n - 1$ such that (3.5) holds, where f is analytic on $|z|_p < \rho$. Then

$$|f(z_0) - P(z_0)|_p \leq |z_0|_p^n R^{-n} M_f(R).$$

3.4 The following lemmas give some further results on divided differences and interpolation polynomials which will be used later.

LEMMA 4. For integral j , let I^j be the function defined by

$$(3.10) \quad I^j(z) = z^j,$$

and let η_0, \dots, η_k be given, for non-negative integral k .

(i) Suppose that $|\eta_i|_p \leq A$ for $i = 0, \dots, k$, and $j \geq k$; then

$$|[\eta_0, \eta_1, \dots, \eta_k; I^j]|_p \leq A^{j-k},$$

(ii) Suppose that η_0, \dots, η_k are distinct, $|\eta_i|_p \geq 1$ for $i = 0, \dots, k$ and $j \geq 1$; then

$$|[\eta_0, \eta_1, \dots, \eta_k; I^{-j}]|_p \leq |\eta_0 \eta_1 \cdots \eta_k|_p^{-1}.$$

PROOF. It is easily verified that for $j \geq k$

$$[\eta_0, \dots, \eta_k; I^j] = \sum_s \eta_0^{s_0} \eta_1^{s_1} \cdots \eta_k^{s_k},$$

where the summation is extended over all non-negative integers s_0, \dots, s_k such that

$$s_0 + s_1 + \cdots + s_k = j - k,$$

and (i) then follows. For any function f and distinct η_0, \dots, η_k , we have, as in the classical case,

$$[\eta_0, \dots, \eta_k; f] = \sum_{i=0}^k \frac{f(\eta_i)}{\prod_{r \neq i} (\eta_i - \eta_r)};$$

by applying this to both the relevant divided differences we obtain

$$[\eta_0^{-1}, \dots, \eta_k^{-1}; I^{j+k-1}] = (-1)^k \eta_0 \cdots \eta_k [\eta_0, \dots, \eta_k; I^{-j}],$$

and by using (i) and the condition $|\eta_i^{-1}|_p \leq 1$ we get (ii).

LEMMA 5. For $m, n, \rho(1), \dots, \rho(m), \alpha_1, \dots, \alpha_m$ as in subsection 3.1 and given positive A and ρ , suppose that

$$\max_i |\alpha_i|_p \leq A < \rho$$

and that f is analytic in $|z|_p < \rho$ with power series

$$f(z) = \sum_{j=0}^{\infty} c_j z^j.$$

Let P be the unique polynomial of degree at most $n - 1$ such that (3.5) holds, and write

$$P(z) = \sum_{k=0}^{n-1} p_k z^k.$$

Then

$$|p_k - c_k|_p \leq \max_{j > n} |c_j|_p A^{j-k} \quad (0 \leq k \leq n - 1).$$

PROOF. Taking $\eta_0, \dots, \eta_{n-1}$ as in subsection 3.2, we see from the properties of power series that

$$[\eta_0, \dots, \eta_i; f] = \sum_{j=0}^{\infty} c_j [\eta_0, \dots, \eta_i; I^j] \quad (0 \leq i \leq n - 1),$$

where I^j is as in (3.10). By (3.8), it follows that

$$P(z) = \sum_{j=0}^{\infty} c_j P_j(z) = \sum_{j=0}^{n-1} c_j z^j + \sum_{j=n}^{\infty} c_j P_j(z),$$

where

$$P_j(z) = \sum_{i=0}^{n-1} [\eta_0, \dots, \eta_i; I^j] (z - \eta_0) \cdots (z - \eta_{i-1}),$$

that is, P_j is the unique polynomial of degree at most $n - 1$ such that

$$P_j \equiv I^j \pmod{\eta_0, \dots, \eta_{n-1}}.$$

As $|\eta_i|_p \leq A$ for all i , the p -adic value of the coefficient of z^k in $(z - \eta_0) \cdots (z - \eta_{i-1})$ for $i - 1 \geq k$ is at most A^{i-k} . Also, by Lemma 4 (i)

$$|[\eta_0, \dots, \eta_i; I^j]|_p \leq A^{j-i}.$$

Multiplying, we see that the p -adic value of the coefficient of z^k in $c_j P_j(z)$ for $j \geq n$ is at most

$$|c_j|_p A^{j-i} A^{i-k} = |c_j|_p A^{j-k},$$

and the required inequality follows.

LEMMA 6. For $m, n, \rho(1), \dots, \rho(m), \alpha_1, \dots, \alpha_m$ as in subsection 3.1, suppose further that

$$(3.11) \quad |\alpha_i|_p \leq 1 \quad (i = 1, \dots, m), \quad |\alpha_i - \alpha_j|_p \geq a \quad (i \neq j).$$

For given M, N satisfying (3.2), let $Q = Q_{MN}$ be the unique polynomial of degree at most $n - 1$ such that (3.3) holds, and write

$$Q(z) = \sum_{k=0}^{n-1} q_k z^k.$$

Then

$$|N!q_k|_p \leq a^{-n+1+N} \quad (k = 0, \dots, n - 1).$$

PROOF. Without loss of generality, suppose $M = 1$ and hence $N \leq \rho(1) - 1$. We define $\eta_0, \dots, \eta_{n-1}$ as in subsection 3.2 (so that $\eta_i = \eta_0 = \alpha_1$ for $0 \leq i \leq \rho(1) - 1$), and note that the $[\eta_i, \eta_{i+1}, \dots, \eta_{i+j}; Q]$ are uniquely determined by the conditions (3.3). Therefore the identity corresponding to (3.8) holds with P and f replaced by Q , and since $|\eta_i|_p \leq 1$ for all i it follows that for all k

$$(3.12) \quad |q_k|_p \leq \max\{ |[\eta_0, \dots, \eta_j; Q]|_p; 0 \leq j \leq n - 1 \}.$$

By subsection 3.2 (applied to Q) and (3.3) with $M = 1$, we see that if $\eta_{i+j} = \eta_i$ then

$$[\eta_i, \dots, \eta_{i+j}; Q] = \frac{Q^{(j)}(\eta_i)}{j!} = \begin{cases} \frac{1}{N!} & \text{if } \eta_i = \alpha_1, j = N \\ 0 & \text{otherwise.} \end{cases}$$

By using (3.7) when $\eta_{i+j} \neq \eta_i$, we see that the divided differences before the N th are all zero, and that for $0 \leq i \leq n - 1 - N$ the N th differences satisfy

$$[\eta_i, \dots, \eta_{i+N}; Q] = \begin{cases} \frac{1}{N!} & \text{if } i \leq \rho(1) - 1 - N \\ 0 & \text{otherwise.} \end{cases}$$

Since $1 \geq |\eta_{i+j} - \eta_i|_p \geq a$ if $\eta_{i+j} \neq \eta_i$, it follows by induction on j (starting with $j = N$) that for $0 \leq j \leq n - 1$ and $0 \leq i \leq n - 1 - j$,

$$|N![\eta_i, \dots, \eta_{i+j}; Q]|_p \leq a^{-j+N} \leq a^{-n+1+N},$$

and (3.12) now yields the required result.

By a more careful argument along the same lines, it can be shown that for $i + j \geq \rho(1)$ and $i \leq \rho(1) - 1 - N$

$$|N![\eta_i, \dots, \eta_{i+j}; Q]|_p \leq a^{1+i+N-\rho(1)} \prod_{k=\rho(1)}^{i+j} |\eta_0 - \eta_k|_p^{-1}.$$

This leads to the more precise inequality

$$(3.13) \quad |N!q_k|_p \leq a^{-\rho(M)+1+N} \prod_{j \neq M} |\alpha_M - \alpha_j|_p^{-\rho(j)}.$$

The following lemma is an immediate consequence of Lemma 6 and (3.4).

LEMMA 7. For $m, n, \rho(1), \dots, \rho(m), \alpha_1, \dots, \alpha_m$ as in Lemma 6 (so that (3.11) holds), and c_{ij} ($1 \leq i \leq m, 0 \leq j \leq \rho(i) - 1$) such that

$$\left| \frac{c_{ij}}{j!} \right|_p \leq C \quad (1 \leq i \leq m, 0 \leq j \leq \rho(i) - 1),$$

let P be the unique polynomial of degree at most $n - 1$ such that

$$P^{(j)}(\alpha_i) = c_{ij} \quad (1 \leq i \leq m, 0 \leq j \leq \rho(i) - 1).$$

If $|z|_p \geq 1$, then

$$|P(z)|_p \leq Ca^{1-n}|z|_p^{n-1}.$$

4. Zeros of p -adic exponential polynomials

We shall use Lemma 5 to prove the following theorem.

THEOREM 1. For given positive real θ and positive integral $m, \rho(1), \dots, \rho(m)$, such that

$$n = \sum_{i=1}^m \rho(i) > 1,$$

let $\omega_1, \dots, \omega_m$ be distinct elements of Ω_p such that

$$(4.1) \quad \max_i |\omega_i|_p = W < p^{-1/(\rho-1)-\theta}$$

and let E be an exponential polynomial of the form

$$E(z) = \sum_{i=1}^m \sum_{j=0}^{\rho(i)-1} a_{ij} z^j \exp(\omega_i z) \quad (|z|_p < p^\theta),$$

where

$$a_{ij} \in \Omega_p \quad (i = 1, \dots, m, j = 0, \dots, \rho(i) - 1).$$

If E does not vanish identically, then the number zeros of E (counted with multiplicity) in $|z|_p \leq 1$ is at most H , where

$$(4.2) \quad H = n - 1 + \max_{1 < j < n-1} \left(\frac{s(j) - 1}{(p - 1)\theta} \right),$$

and $s(j)$ denotes the sum of the p -adic digits of j , as in Lemma 2.

The value of H given here is the same as that obtained by Robba (1977), whereas van der Poorten (1976b) gives

$$(4.3) \quad H \leq n - 1 + \max_{0 < r < p-1} \left\{ \left[\log_p(n + r) \right] - \frac{r}{p - 1} \right\} \frac{1}{\theta},$$

which is very close to (4.2), since $s(j) \leq ([\log_p j] + 1)(p - 1)$.

Our estimate of the number of zeros of E will be derived by obtaining upper and lower bounds for $M_E(R)/M_E(r)$ for suitable R, r such that $1 < r < R < p^\theta$, and, as in the classical case, the required upper bound is obtained by using an appropriate interpolation polynomial, which we now introduce.

For fixed $v \in \Omega_p$ such that

$$|v|_p = R < p^\theta,$$

let f be the function analytic in $|z|_p \leq p^{-1/(p-1)-\theta}$ defined by

$$f(z) = \exp(vz).$$

Let P be the unique polynomial of degree at most $n - 1$ such that for i, j as in Theorem 1

$$P^{(j)}(\omega_i) = (D^{(j)}(\exp vz))_{z=\omega_i} = v^j \exp(v\omega_i) = f^{(j)}(\omega_i).$$

The following lemma gives the connection between E and P .

LEMMA 8. *Let $v, E(z), P(z)$ be as above and let*

$$P(z) = \sum_{j=0}^{n-1} p_j z^j.$$

Then

$$E(v) = \sum_{j=0}^{n-1} p_j E^{(j)}(0).$$

PROOF. The proof is as in the classical case, for example, see in the proof of Lemma 1 page 121 of Baker (1975).

We now use this lemma to get our upper bound for $M_E(R)/M_E(r)$.

LEMMA 9. *Let θ, W , and E be as in Theorem 1, so that (4.1) holds, and let r and R be such that*

$$1 < r < R < p^\theta.$$

Then

$$M_E(R) \leq M_E(r) R \max_{1 \leq j \leq n-1} r^{-j} W^{1-j} |j!|_p.$$

In particular, for given positive θ and ϵ such that $\theta > 2\epsilon$, we have

$$M_E(p^{\theta-\epsilon}) < p^K M_E(p^\epsilon),$$

where

$$(4.4) \quad K = \max_{1 < j < n-1} \left\{ \frac{s(j) - 1}{p - 1} + j(\theta - \epsilon) \right\} \\ \leq (n - 1)(\theta - \epsilon) + \max_{1 < j < n-1} \frac{s(j) - 1}{p - 1}.$$

PROOF. By applying Lemma 8 with v such that $|v|_p = R$ and using (2.3) of Lemma 1, we deduce that

$$(4.5) \quad M_E(R) \leq \max_{0 < j < n-1} |p_j E^{(j)}(0)|_p \leq \max_{0 < j < n-1} (|p_j j!|_p r^{-j}) M_E(r).$$

By applying Lemma 5 and using the facts that $|\omega_i|_p \leq W$ (from (4.1)) and that

$$f(z) = \exp(vz) = \sum_{j=0}^{\infty} \frac{v^j}{j!} z^j,$$

with $|v|_p = R$, we see that

$$(4.6) \quad |p_j j!|_p \leq \max \left(R^j, \max_{i > n} |j!|_p \frac{R^i W^{i-j}}{|i!|_p} \right).$$

Now as $n > 1$, it follows from (2.2) of Lemma 1 and (2.4) and (4.1) that

$$\max_{i > n} \frac{(RW)^i}{|i!|_p} \leq \max\{|e^z - 1|_p; |z|_p = RW\} = RW.$$

Moreover, since $RW < p^{-1/(p-1)}$ by (4.1), Lemma 2 implies that for $j \geq 1$

$$R^j \leq |j!|_p RW^{1-j}.$$

Thus the required inequality for $M_E(R)$ and $M_E(r)$ now follows from (4.5) and (4.6), on noting that, by (4.6), $|p_0 0!|_p r^{-0} \leq 1 < Rr^{-1}$.

Taking $R = p^{\theta-\epsilon}$ and $r = p^\epsilon$ and using Lemma 2 again to estimate $|j!|_p$, we obtain the final result.

PROOF OF THEOREM 1. We now suppose that E does not vanish identically and hence has a finite number, h , say, of zeros in $|z|_p \leq 1$ (as follows, for example, from Theorem 14 of Koblitz (1977)). Let $\alpha_1, \dots, \alpha_h$ be all zeros of $E(z)$ in $|z|_p \leq 1$. Define the function g by

$$g(z) = \frac{E(z)}{(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_h)}.$$

Clearly, g is analytic in $|z|_p < p^\theta$. Hence, for any r, R such that $1 < r < R < p^\theta$, we have, using Lemma 1,

$$M_g(r) = \frac{M_E(r)}{r^h} \leq M_g(R) = \frac{M_E(R)}{R^h},$$

and hence

$$\left(\frac{R}{r}\right)^h \leq \frac{M_E(R)}{M_E(r)}.$$

For fixed ϵ satisfying $0 < \epsilon < \frac{1}{2}\theta$, take $R = p^{\theta-\epsilon}$, $r = p^\epsilon$. Then by Lemma 9

$$\left(\frac{R}{r}\right)^h = p^{(\theta-2\epsilon)h} < p^K,$$

where K is given by (4.4). It follows that

$$h \leq \frac{K}{\theta - 2\epsilon} \leq (n - 1) \frac{\theta - \epsilon}{\theta - 2\epsilon} + \frac{1}{\theta - 2\epsilon} \max\left(\frac{s(j) - 1}{p - 1}\right).$$

Letting $\epsilon \rightarrow 0$, we obtain

$$h \leq n - 1 + \max_{1 < j < n-1} \left(\frac{s(j) - 1}{(p - 1)\theta}\right),$$

as required.

If $j \leq n - 1 < p$, then $s(j) = j$. Hence we obtain

COROLLARY 1. *Let the hypotheses of Theorem 1 be satisfied. If $n \leq p$, then the number of zeros, h , of E in $|z|_p \leq 1$ satisfies*

$$h \leq n - 1 + \frac{n - 2}{(p - 1)\theta}.$$

For all n , we have

$$h \leq n - 1 + ([\log_p(n - 1)] + 1 - 1/(p - 1))/\theta.$$

We note also that exclusion of the case $n = 1$ from the above results does no harm, since by (2.4) we already know that if $n = 1$ then $|E(z)|_p = |a_0|_p$ for all z such that $|z|_p < p^\theta$.

5. Coefficients of p -adic exponential polynomials

As a further application of our bound for $M_E(R)/M_E(r)$ in Lemma 9, we prove the following theorem, which is independent of Theorem 1 but uses, in addition, Lemmas 3, 6 and 7.

THEOREM 2. *Let θ, W and E be as in Theorem 1, so that (4.1) holds, and for given positive integral l and non-negative integral s_1, \dots, s_l , let*

$$s = \sum_{i=1}^l s_i,$$

and let β_1, \dots, β_l be distinct elements of Ω_p such that

$$|\beta_i|_p \leq 1 \quad (i = 1, \dots, l).$$

Let w, b, B be real numbers such that $w > 0, b > 0$,

$$|\omega_i - \omega_j|_p \geq w \quad (i \neq j), \quad |\beta_i - \beta_j|_p \geq b \quad (i \neq j),$$

$$|E^{(j)}(\beta_i)/j!|_p \leq B \quad (0 \leq j \leq s_i - 1, 0 \leq i \leq l).$$

If $s > H$, where H is given by (4.2), as in Theorem 1, then for each pair of integers M, N such that

$$1 \leq M \leq m, \quad 0 \leq N \leq \rho(M) - 1,$$

we have

$$|N!a_{MN}|_p \leq w^{1+N-n}b^{1-s}B,$$

(where a_{MN} is the coefficient of $z^N \exp(\omega_M z)$ in $E(z)$).

In order to estimate the coefficient a_{MN} , we use the following lemma.

LEMMA 10. *For fixed positive integers M, N , let*

$$Q(z) = Q_{MN}(z) = \sum_{j=0}^{n-1} q_j z^j$$

be the unique polynomial of degree at most $n - 1$ such that

$$Q^{(j)}(\omega_i) = \begin{cases} 1 & \text{if } i = M, j = N \\ 0 & \text{otherwise,} \end{cases}$$

where i runs from 1 to m and j runs from 0 to $\rho(i) - 1$ with

$$\rho(1) + \dots + \rho(m) = n.$$

Then

$$a_{MN} = \sum_{j=0}^{n-1} q_j E^{(j)}(0).$$

PROOF. See section 5 pages 87–88 of Mahler (1967).

We now prove Theorem 2, and so we suppose that $s > H$, where H is given by (4.2). By Lemma 10 and (2.3) of Lemma 1 we have that for any r such that

$$1 < r < \rho^\theta,$$

$$|N!a_{MN}|_p \leq \max_{0 < j < n-1} |N!q_j|_p r^{-j} |j!|_p M_E(r).$$

By Lemma 6, it follows that

$$(5.1) \quad |N!a_{MN}|_p \leq w^{1+N-n} M_E(r).$$

We must now estimate $M_E(r)$ and to do this we use an interpolation polynomial P , the unique polynomial of degree at most $s - 1$ such that

$$P^{(i)}(\beta_i) = E^{(i)}(\beta_i) \quad (i = 1, \dots, l; j = 0, \dots, s_i - 1).$$

By Lemma 3, for any R such that $1 < r < R < p^\theta$, we have for $|z|_p = r$,

$$|E(z) - P(z)|_p \leq \left(\frac{r}{R}\right)^s M_E(R).$$

For any ϵ such that $0 < \epsilon < \frac{1}{2}\theta$, we may take $R = p^{\theta-\epsilon}$, $r = p^\epsilon$. Then it follows from the above inequality and Lemma 9 that for $|z|_p = p^\epsilon$,

$$|E(z) - P(z)|_p \leq p^{-s(\theta-2\epsilon)} M_E(R) \leq p^L M_E(r),$$

where

$$L = -s(\theta - 2\epsilon) + (n - 1)(\theta - \epsilon) + \max_{1 < j < n-1} \frac{s(j) - 1}{p - 1}.$$

Since $s > H$, where H is given by (4.2), it follows that if ϵ is sufficiently small, then $L < 0$ and so

$$|E(z) - P(z)|_p < M_E(r),$$

and hence, by the strong triangle inequality

$$M_E(r) = M_P(r).$$

Also, by Lemma 7, since $r > 1$, we have

$$M_P(r) \leq Bb^{1-s}r^{s-1}.$$

We now see, by (5.1), that for all $\epsilon > 0$ sufficiently small

$$|N!a_{MN}|_p \leq w^{1+N-n} b^{1-s} p^{\epsilon(s-1)} B,$$

from which the required result follows by letting $\epsilon \rightarrow 0$.

A more precise result could clearly be obtained (as is done in Laohakosol (1978)), at the price of more notational complexity, by using the more precise version (3.13) of the inequality in Lemma 6 and a corresponding refinement of Lemma 7. The result of van der Poorten (1976b) corresponding to the above theorem again has H defined by (4.3).

6. Turan’s first main theorem on sums of powers

In order to derive a p -adic version of Turan’s first main theorem, we shall require the following lemma, which follows easily from the strong triangle inequality.

LEMMA 11. *Let $Q(z) = \sum_{k=0}^n q_k z^k$ be a p -adic polynomial. Then for any two sequences $\eta_0, \eta_1, \dots, \eta_r$ and b_0, b_1, \dots, b_r of elements of Ω_p , we have*

$$\left| \sum_{k=0}^r b_k Q(\eta_k) \right|_p \leq \left(\max_{0 < h < n} |q_h|_p \right) \left(\max_{0 < i < n} \left| \sum_{k=0}^r b_k \eta_k^i \right|_p \right).$$

PROOF. See Shorey (1972b), Lemma 6.

We shall now prove

THEOREM 3 (p-adic analogue of Turan’s first main theorem). *Let m, n be two non-negative integers, and let b_0, \dots, b_n and η_0, \dots, η_n be two sequences of elements of Ω_p . Then there exists an integer ν with $m + 1 < \nu < m + n + 1$ such that*

$$\left| \sum_{k=0}^n b_k \eta_k^\nu \right|_p \geq \left| \sum_{k=0}^n b_k \right|_p \min_{0 < i < n} |\eta_i|_p^\nu.$$

PROOF. We may suppose without loss of generality that

$$\min_{0 < i < n} |\eta_i|_p = 1,$$

and by using continuity we may also suppose that η_0, \dots, η_n are distinct. Thus we must show that there exists an integer ν with $m + 1 < \nu < m + n + 1$ such that

$$\left| \sum_{k=0}^n b_k \eta_k^\nu \right|_p \geq \left| \sum_{k=0}^n b_k \right|_p,$$

where η_0, \dots, η_n are distinct. Using the notation (3.10), let Q be the unique polynomial of degree at most n such that

$$(6.1) \quad Q \equiv I^{-m-1} \pmod{\eta_0, \dots, \eta_n}.$$

By (3.8), we have

$$(6.2) \quad Q(z) = \sum_{k=0}^n [\eta_0, \dots, \eta_k; I^{-m-1}](z - \eta_0) \cdots (z - \eta_{k-1}) = \sum_{k=0}^n q_k z^k,$$

say. Lemma 4 (ii) shows that

$$|[\eta_0, \dots, \eta_k; I^{-m-1}]|_p \leq |\eta_0 \cdots \eta_k|_p^{-1} \quad (0 < k < n),$$

and hence, using the condition $|\eta_i|_p \geq 1$, we see that

$$|q_k|_p \leq 1 \quad (0 \leq k \leq n).$$

Since $Q(\eta_i) = \eta_i^{-m-1}$, it now follows from Lemma 11 that

$$\left| \sum_{k=0}^n b_k \eta_k^{-m-1} \right|_p \leq \left(\max_{0 < i < n} \left| \sum_{k=0}^n b_k \eta_k^i \right|_p \right).$$

Writing $b_k \eta_k^{m+1}$ for b_k , we get the required result.

In fact, as we shall now show, the above approach also leads to simplification of the proof in the complex case by Balkema and Tijdeman (1973) of the version of Turan's first main theorem due to de Bruijn (1960) and Makai (1959), which appears as Theorem C of Balkema and Tijdeman.

THEOREM 3'. *Let m and n be non-negative integers, and let b_0, \dots, b_n and η_0, \dots, η_n be sequences of complex numbers. Then there exists an integer ν with $m + 1 \leq \nu \leq m + n + 1$ such that*

$$\left| \sum_{k=0}^n b_k \eta_k^\nu \right| \geq \left(\sum_{h=0}^n \binom{m+h}{h} 2^h \right)^{-1} \left| \sum_{k=0}^n b_k \right| \min_{0 < i < n} |\eta_i|^\nu.$$

The proof depends on the following classical analogue of Lemma 4, which is proved in the same way as Lemma 4, except that the ordinary triangle inequality must now be used.

LEMMA 4'. *For integral j , let I^j be defined by*

$$I^j(z) = z^j \quad (z \in C),$$

and let η_0, \dots, η_k be given elements of C , for non-negative integral k .

(i) *Suppose that $|\eta_i| \leq A$ for $i = 0, \dots, k$, and $j \geq k$; then*

$$|[\eta_0, \dots, \eta_k; I^j]| \leq \binom{j}{k} A^{j-k}.$$

(ii) *Suppose that η_0, \dots, η_k are distinct, $|\eta_i|_p \geq 1$ for $0 \leq i \leq k$, and $j \geq 1$; then*

$$|[\eta_0, \eta_1, \dots, \eta_k; I^{-j}]| \leq \binom{j+k-1}{k} |\eta_0 \cdots \eta_k|^{-1}.$$

We now prove Theorem 3'. As before, it is sufficient to prove that if η_0, \dots, η_k are distinct and $|\eta_i| \geq 1$ for all i , then the given inequality holds with 1 in place of $\min|\eta_i|^\nu$, for some ν such that $m + 1 \leq \nu \leq m + n + 1$. Once again

we take Q as the unique polynomial of degree at most n such that (6.1) holds (in the classical sense), we write

$$Q(z) = \sum_{k=0}^n q_k z^k,$$

and Q is again of the form (6.2). By Lemma 4',

$$|[\eta_0, \dots, \eta_k; I^{-m-1}]| \leq \binom{m+k}{k} |\eta_0 \cdots \eta_k|^{-1} \quad (0 < k < n),$$

and so it follows from (6.2) and the condition $|\eta_i| \geq 1$ that

$$\begin{aligned} \sum_{k=0}^n |q_k| &\leq \sum_{k=0}^n \binom{m+k}{k} \left(1 + \frac{1}{|\eta_0|}\right) \cdots \left(1 + \frac{1}{|\eta_{k-1}|}\right) \\ &\leq \sum_{k=0}^n \binom{m+k}{k} 2^k = C_n, \end{aligned}$$

say. It is easily seen (as in Balkema and Tijdeman (1973), Lemma 1) that

$$\left| \sum_{k=0}^n b_k Q(\eta_k) \right| \leq \sum_{k=0}^n |q_k| \max_{0 < j < n} \left| \sum_{k=0}^n b_k \eta_k^j \right|,$$

and since $Q(\eta_i) = \eta_i^{-m-1}$, we obtain

$$\left| \sum_{k=0}^n b_k \eta_k^{-m-1} \right| \leq C_n \max_{0 < j < n} \left| \sum_{k=0}^n b_k \eta_k^j \right|,$$

which gives the required result as before.

References

- W. W. Adams (1966), 'Transcendental numbers in the p -adic domain', *Amer. J. Math.* **88**, 279–308.
 W. W. Adams and E. G. Straus (1971), 'Non-archimedean analytic functions taking the same value at the same points', *Illinois J. Math.* **15**, 418–424.
 G. Bachman (1964), *Introduction to p -adic numbers and valuation theory* (Academic Press, New York).
 A. Baker (1975), *Transcendental number theory* (Cambridge University Press, Cambridge).
 A. A. Balkema and R. Tijdeman (1973), 'Some estimates in the theory of exponential sums', *Acta Math. Acad. Sci. Hungar.* **24**, 115–133.
 N. G. de Bruijn (1960), 'On Turan's first main theorem', *Acta Math. Acad. Sci. Hungar.* **11**, 213–216.
 A. O. Gelfond (1960), *Transcendental and algebraic numbers* (Dover, New York).
 A. O. Gelfond (1971), *Calculus of finite differences* (Hindustan Publishing Corporation, Delhi).
 N. Koblitz (1977), *p -adic numbers, p -adic analysis and zeta functions* (Springer, New York).
 V. Laohakosol (1978), *Two topics in p -adic approximation* (M.Sc. Thesis, University of Adelaide, South Australia).
 K. Mahler (1967), 'On a class of entire functions', *Acta Math. Acad. Sci. Hungar.* **18**, 83–96.
 E. Makai (1959), 'The first main theorem of Turan', *Acta Math. Acad. Sci. Hungar.* **10**, 405–411.
 P. Robba (1977), 'Nombre de zéros des fonctions exponentielles-polynômes', *Groupe d'étude d'Analyse ultramétrique 4e année*, no. 9, pp. 1–3 (Secrétariat Mathématique, Paris).

- T. N. Shorey (1972a), 'Algebraic independence of certain numbers in the p -adic domain', *Nederl. Akad. Wetensch. Proc. Ser. A.* **75**, 423–435 (= *Indag. Math.* **34**, 423–435).
- T. N. Shorey (1972b), ' P -adic analogue of a theorem of Tijdeman and its application', *Nederl. Akad. Wetensch. Proc. Ser. A.* **75**, 436–442 (= *Indag. Math.* **34**, 436–442).
- A. J. van der Poorten (1976a), 'Zeros of p -adic exponential polynomials', *Nederl. Akad. Wetensch. Proc. Ser. A.* **79**, 46–49 (= *Indag. Math.* **38**, 46–49).
- A. J. van der Poorten (1976b), 'Hermite interpolation and p -adic exponential polynomials', *J. Austral. Math. Soc. Ser. A.* **22**, 12–26.
- A. J. van der Poorten (1977), 'On the number of zeros of functions', *Enseignement Math.* **23**, 19–38.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801
U.S.A.

Department of Mathematics
University of Adelaide
Adelaide, South Australia 5001
Australia