BULL. AUSTRAL. MATH. SOC. 11B37, 11D61, 11D88
VOL. 46 (1992) [401–412]

ON THE NUMBER OF ZEROS OF EXPONENTIAL POLYNOMIALS AND RELATED QUESTIONS

A.J. VAN DER POORTEN AND I.E. SHPARLINSKI

We apply Straßmann's theorem to p-adic power series satisfying linear differential equations with polynomial coefficients and note that our approach leads to our estimating the number of integer zeros of polynomials on a given interval and thence to an investigation of the number of p-adic small values of a function on such an interval, that is, of the number of solutions of a congruence modulo p^r.

0. INTRODUCTION

We extend the scope of the p-adic method based on Straßmann's theorem for estimating the number of zeros of exponential polynomials (and hence of recurrence sequences) applied in [3, 5, 6].

Accordingly, let $\mathbb{K}$ be an algebraic number field and $p \geqslant 3$ a rational prime.

Firstly, we show that Straßmann's theorem can be applied in a broad class of situations, namely to the class of function satisfying p-adic linear differential equations with polynomial coefficients. We provide a general bound for the number of zeros of such functions.

The class of functions under consideration includes generalised exponential polynomials

$$E(z) = \sum_{i=1}^{m} F_i(z)\phi_i^{s_i(z)} \tag{1}$$

with *roots* ϕ_i in $\mathbb{K}$, polynomial coefficients $F_i(z)$ in $\mathbb{K}[z]$, and exponents $s_i(z)$ in $\mathbb{Z}[z]$. Such functions are considered in [13], where bounds for their number of zeros in a given disc in the complex plane are stated. We get a bound for the total number of their integer zeros.

The idea of our method is to reduce the given function to a product of a polynomial and a function without zeros in the ring of p-adic integers $\mathbb{Z}_p$. Thus our problem becomes that of bounding the degree of the polynomial factor, since that plainly bounds

Received 18th November, 1991
Work supported in part by grants from the Australian Research Council

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

the number of integer zeros of the function. Moreover, we remark that we readily move from those considerations to the problem of estimating the number of integer zeros of polynomials on a given interval and thence to the question of finding the number of p-adic small values of a function on such an interval, that being the number of solutions of a congruence modulo p^n.

We consider in greater detail the interesting special case of recurrence sequences (a_h) of integers

$$a_{h+n} = s_1 a_{h+n-1} + \dots + s_n a_h\,, \quad h = 1, 2, \dots \,. \tag{2}$$

We confine ourselves to *nondegenerate* recurrence sequences, those being nonzero sequences with characteristic polynomial

$$S(X) = X^n - s_1 X^{n-1} - \dots - s_n \in \mathbb{Z}[X]\,,$$

with $s_n \neq 0$ and so that no quotient α_i/α_j of two of its distinct zeros is a root of unity.

Upper bounds for the number of solution of a general congruence $a_h \equiv 0 \pmod{\mathfrak{a}}$, with $h = 1, \dots, H$ and $\mathfrak{a}$ an integral ideal of $\mathbb{K}$ are known; [**8**, **11**]. However, the estimates proved here are new for interesting ranges of the parameters.

We conclude by giving some applications of our bounds to an asymptotic formula for the average value of the p-adic order of the terms of a recurrence sequence.

Throughout $\mathbb{K}$ is an algebraic number field of degree d over $\mathbb{Q}$, and $\mathfrak{p}$ a prime ideal of $\mathbb{K}$ lying over the rational prime p. We denote by e and f, respectively its ramification index and the residue class degree. As usual $\mathbb{Q}_p$ denotes the p-adic completion of the field of rationals $\mathbb{Q}$, and $\mathbb{C}_p$ the completion of its algebraic closure; $\mathbb{K}_\mathfrak{p}$ is the completion of $\mathbb{K}$ at p. We write in terms of the additive valuation $\operatorname{ord}_p t$ normalised by $\operatorname{ord}_p p = 1$, and will suppress the subscript henceforth. The ring of p-adic integers $\mathbb{Z}_p$ is the set $\{t \in \mathbb{Q}_p : \operatorname{ord} t \geqslant 0\}$ and $\mathbb{Z}_\mathfrak{p} = \{t \in \mathbb{K}_\mathfrak{p} : \operatorname{ord} t \geqslant 0\}$. We denote the unit disc $\{t \in \mathbb{C}_p : \operatorname{ord} t \geqslant 0\}$ by U_p.

1. Zeros of solutions of differential equations

We consider power series $f(t) = \sum_{h=0}^{\infty} f_h t^h$ with coefficients f_h in $\mathbb{Z}_\mathfrak{p}$, converging in the unit disc U_p, and satisfying a differential equation

$$d^m f(t)/dt^m = \sum_{i=0}^{m-1} q_{m-i}(t) d^i f(t)/dt^i$$

of order m with polynomial coefficients $q_j(t) \in \mathbb{Z}_\mathfrak{p}[t]$ of respective degrees n_j.

Let $\mathcal{M} = \mathcal{M}(F)$ denote the number of zeros of f in the ring $\mathbb{Z}_\mathfrak{p}$. Our main tools to bound $\mathcal{M}$ are the following two statements:

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

Lemma 1. (Straßmann's Theorem) *Let*

$$g(t) = \sum_{h=0}^{\infty} g_h t^h$$

be a power series with coefficients in $\mathbb{Z}_\mathfrak{p}$ *and converging on the unit disc* U_p. *Suppose (as we may after multiplying by a nonzero constant if necessary) that some coefficient* g_l, *say, has* $\operatorname{ord} g_l = 0$. *Set*

$$M = \max\{h : \operatorname{ord} g_h = 0\}.$$

Then there is a factorisation

$$g(t) = P(t)U(t)$$

where $P(t) \in \mathbb{Z}_\mathfrak{p}[t]$ *is a polynomial of degree* M *and the series* $U(t)$ *satisfies* $\operatorname{ord} U(t) = 0$ *for* $t \in U_p$.

Remark. This is just the p-adic Weierstraß preparation theorem as stated by Straßmann [**12**]. There is an elementary proof in [**3**]; see also [**6**] and [**5**].

Set $n = \max\{m - j + n_j : j = 1, \ldots, m\}$.

Lemma 2. *For each* $k \in \mathbb{Z}_\mathfrak{p}$ *the function* $g(t) = f(pt + k)$ *satisfies the conditions of Lemma 1 with* $M \leqslant n(p-1)/(p-2)$.

Proof: It is easy to check that $g(t)$ satisfies the differential equation

$$d^m g(t)/dt^m = \sum_{i=0}^{m-1} r_{m-i}(t) d^i g(t)/dt^i, \tag{3}$$

of order m with polynomial coefficients

$$r_j(t) = p^j \sum_{i=0}^{n_j} p^i t^i q_j^{(i)}(k)/i! \in \mathbb{Z}_\mathfrak{p}[t], \quad j = 1, \ldots, m.$$

Indeed, in the sequel we need only that $r_j(t) = \sum_{i=0}^{n_j} a_{i,j} t^i$ with $\operatorname{ord} a_{i,j} \geqslant i + j$.

The function $g(t)$ can be represented in the form

$$g(t) = b \sum_{h=0}^{\infty} g_h t^h$$

where the multiplier b is choosen such that $\min\{\operatorname{ord} g_h : h = 0, 1, \ldots\} = 0$. Set $c_h = g_h h!$. Then

$$d^i g(t)/dt^i = b \sum_{h=0}^{\infty} c_{h+i} t^h / h!.$$

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

From equation (3) we get the recurrence relation

$$c_{h+m} = \sum_{j=0}^{m-1} \sum_{i=0}^{n_j} a_{i,m-j} c_{h-i+j} h!/(h-i)!\,.$$

Thus for $h = 0, 1, \ldots$

$$\operatorname{ord} c_{h+m} \geqslant \min_{0 \leqslant j < m; 0 \leqslant i \leqslant n_j} (\operatorname{ord} c_{h-i+j} + m + i - j),$$

or

$$\operatorname{ord} c_h \geqslant \min_{0 \leqslant j < m; 0 \leqslant i \leqslant n_j} (\operatorname{ord} c_{h-m-i+j} + m + i - j)\,. \tag{4}$$

Now set

$$\Delta = \max\{k - \operatorname{ord} c_k : k = 0, \ldots, n-1\}\,.$$

Since for any h we have $\operatorname{ord} c_h \geqslant \operatorname{ord} g_h \geqslant 0$, then $\Delta < n$. Furthermore, by (4) and induction, we get

$$\operatorname{ord} c_h \geqslant h - \Delta, \quad h = n, n+1, \ldots\,.$$

But it is well known that $\operatorname{ord} h! \leqslant h/(p-1)$. Hence

$$\operatorname{ord} g_h \geqslant \operatorname{ord} c_h - h/(p-1) \geqslant h(p-2)/(p-1) - \Delta > h(p-2)/(p-1) - n > 0$$

for $h \geqslant n(p-1)/(p-2)$, and we are done. □

Theorem 1. *If $\mathcal{M} < \infty$ then we have the bound*

$$\mathcal{M} \leqslant 2p^d n\,.$$

Proof: It is evident that each $t \in \mathbb{Z}_\mathfrak{p}$ can be uniquely represented in the form $t = px + k$ where $x \in \mathbb{Z}_\mathfrak{p}$ and k is taken from a complete residue system of $\mathbb{Z}_\mathfrak{p}$ modulo p.

Accordingly, we fix k and consider the function $g(t) = f(px + k)$. By Lemma 2 we see that the function $g(t)$ has at most $n(p-1)/(p-2) \leqslant 2n$ zeros. But a complete residue system modulo p has $\operatorname{Norm} p = p^d$ elements, proving the theorem. □

Corollary. *Let $\mathcal{M}$ be the number of integer zeros of a nonzero exponential polynomial (1) with polynomials $F_i(x) \in \mathbb{K}[x]$, $s_i(x) \in \mathbb{Z}[x]$, $i = 1, \ldots, m$ of degrees at most F and s respectively. If $\mathcal{M} < \infty$ then*

$$\mathcal{M} \leqslant 2^{8d+1} m F s (d + \omega)^{4d},$$

where ω is the number of different prime ideal divisors of the ϕ_i, $i = 1, \ldots, m$, in $\mathbb{K}$.

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

PROOF: We select the rational prime p so that $p > d+1$ and p is prime to each of the ϕ_i. It is shown in [6] that such a prime can be selected with

$$p < 16(d+\omega)^2 . \tag{5}$$

For each i set $\phi_i^{p^f-1} = \exp \Phi_i$. We then see that each of the $p^f - 1$ functions

$$v_k(t) = E\big((p^f-1)t+k\big) = \sum_{i=1}^{m} F_i\big((p^f-1)t+k\big)\phi_i^{s_i(k)} \exp\big(\Phi_i r_{i,k}(t)\big) ,$$

where

$$r_{i,k}(t) = \big[s_i\big((p^f-1)t+k\big) - s_i(k)\big] \,/ (p^f-1), \quad i = 1,\dots,m; \quad k = 1,\dots,p^f-1,$$

has a power series expansion converging in the unit disk U_p.

Let D denote the differential operator $D = d/dt$. Then, as shown in [12], Theorem 1, each function $v_k(t)$ satisfies the differential equation

$$\left[\prod_{i=1}^{m}\Big(D - \big(r'_{i,k}(t)\big)^{\deg F_i}\Big)\right] v_k(t) = 0 ,$$

of order at most mF whose coefficients are polynomials over $\mathbb{K}_{\mathfrak{p}}$ and which have respective degrees at most $mF(s-1)$. Thus we can apply Theorem 1 to each of the $p^f - 1$ functions $v_k(t)$, with $n \leqslant mF + mF(s-1) = mFs$.

Hence $\mathcal{M} \leqslant 2p^d(p^f-1)mFs < 2p^{2d}mFs$, and recalling ineouality (5), we have the claim. □

2. NUMBER OF SOLUTIONS OF CERTAIN CONGRUENCES

It is evident that using the representation of a generalised exponential polynomial (1) as in the proof of Corollary to Theorem 1 and utilising bounds for the number of solutions of polynomial congruences leads to bounds for the number of solutions of congruences involving these generalised exponential polynomials.

Let $\mathfrak{O}_{\mathbf{K}}$ be the ring of integers of K and let $\mathfrak{a}$ be an integral ideal of $\mathfrak{O}_{\mathbb{K}}$.

Let $M_k(\mathfrak{O}_{\mathbf{K}}, \mathfrak{a})$ denote the set of polynomials

$$P(t) = a_0t^k + a_1t^{k-1} + \ldots + a_k \in \mathfrak{O}_{\mathbf{K}}[t]$$

of degree at most k and with $\gcd(a_0,\dots,a_k)$ prime to $\mathfrak{a}$. Set

$$\tau_k(\mathfrak{O}_{\mathbf{K}}, H, \mathfrak{a}) = \max\{\rho(P, H, \mathfrak{a}) : P \in M_k(\mathfrak{O}_{\mathbf{K}}, \mathfrak{a})\}$$

where $\rho(P, H, \mathfrak{a})$ is the number of solutions of the congruence

$$P(t) \equiv 0 \pmod{\mathfrak{a}}, \quad t = 1, \dots, H.$$

In the case $\mathbb{K} = \mathbb{Q}$, when we have congruences modulo a positive integer $q \in \mathbb{Z}$, bounds for $\tau_k(H, q) = \tau_k(\mathbb{Z}, H, q)$ are established in [10]: For any $\varepsilon > 0$ we have

$$\tau_k(H, q) = O\Big(H^{\varepsilon}\Big(H^{1-1/k-\theta_k} + Hq^{-1/k}\Big)\Big),$$

where $\theta_k = (k-1)/k\big(k^3 - k^2 + 1\big)$; and for small H there is the sharper bound

$$\tau_k(H, q) = O\Big(Hq^{-2/k(k+1)} + 1\Big),$$

with the constants implied in the O-symbol depending only on k and ε.

We obtain a bound for congruences modulo a power of a prime ideal $\mathfrak{a} = \mathfrak{p}^r$, which is new even in the case $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{p} = p$.

LEMMA 3. *There exists a constant C, depending only on the ramification index e and on k, such that*

$$\tau_k(\mathfrak{O}_{\mathbb{K}}, H, \mathfrak{p}^r) \leqslant C\Big(Hp^{-r/ek} + 1\Big).$$

PROOF: Consider a polynomial $P \in M_k(\mathfrak{O}_{\mathbb{K}}, \mathfrak{p}^r)$. Plainly, it suffices to show, with $U = \lfloor p^{-r/ek} \rfloor$, and for integers v, that the congruence

$$P(v + u) \equiv 0 \pmod{\mathfrak{p}^r}, \quad u = 1, \dots, U$$

has at most k solutions.

Suppose there are $k+1$ solutions $1 \leqslant u_1 < \dots < u_{k+1} \leqslant U$ of the congruence. Thus

$$\operatorname{ord} P(u_j) \geqslant r/e, \quad j = 1, \dots, k+1.$$

On the one hand, by the Lagrange interpolation formula we have

$$P(u) = \sum_{j=1}^{k+1} \frac{\prod\limits_{i \neq j} (u - u_i)}{\prod\limits_{i \neq j} (u_j - u_i)} P(u_j),$$

and on the other hand, for each $j = 1, \dots, k+1$

$$0 < \Big|\prod_{i \neq j} (u_j - u_i)\Big| \leqslant (U-1)^k < p^{r/e}.$$

That is absurd because $P \in M_k(\mathfrak{O}_{\mathbb{K}}, \mathfrak{p}^r) = M_k(\mathfrak{O}_{\mathbb{K}}, \mathfrak{p})$. □

Given a generalised exponential polynomial (1) and an integral ideal $\mathfrak{a}$, denote by $\mathcal{M}(N, \mathfrak{a})$ the number of solutions of the congruence $E(n) \equiv 0 \pmod{\mathfrak{a}}, \quad n = 1, \dots, N$.

Theorem 2. *Suppose that the generalised exponential polynomial (1) with coefficients $F_i(x) \in \mathbb{K}[x]$ of degree at most F and exponents $s_i(x) \in \mathbb{Z}[x]$ of degree at most s, has only a finite number of zeros in $\mathbb{Z}_p$. Select the rational prime p so that it is relatively prime to each of the roots ϕ_i. Then there is a constant c depending only on E and p such that*

$$\mathcal{M}(N, \mathfrak{p}^r) \leqslant c\Big(Np^{-r/L} + 1\Big), \tag{6}$$

where $L = mFs - 1$.

Proof: It is clear that we can choose θ positive such that

$$\operatorname{ord}\Big(\phi^{(p^f-1)p^\theta} - 1\Big) > mFs/(p-1).$$

Accordingly, set $H = \lfloor N/p^\theta(p^f - 1)\rfloor + 1$. For $k \in \mathbb{Z}_\mathfrak{p}$ we consider the function

$$v_k(t) = E\big(p^\theta(p^f - 1)t + k\big);$$

$P_k(t) \in \mathbb{Z}_\mathfrak{p}[t]$ denotes the polynomial $P(t)$ determined by Lemmas 1 and 2.

Then we can proceed as in the proof of the Corollary to Theorem 1 and in the proof of Lemma 2 of [**6**], but with $\varepsilon = (mFs - 1)/(p-1)$. Thus we see that the degree of the polynomial $P_k(t)$ does not exceed $\deg P_k(t) \leqslant mFs - 1 + (mFs - 2)/\varepsilon(p-1) < mFs$.

Suppose γ_k is the largest p-adic order of the coefficients of P_k. It is clear that as k varies in a complete residue system modulo $p^\theta\big(p^f - 1\big)$ the γ_k are bounded by some constant γ that depends only on E and p, and not on r.

Then, if $r > \gamma$,

$$\mathcal{M}(N, \mathfrak{p}^r) \leqslant \sum_{k \pmod p} \rho\big(P_k p^{-\gamma_k}, H, p^{r-\gamma_k}\big).$$

Evidently, the polynomials $P_k p^{-\gamma_k}$ satisfy the conditions of Lemma 3 and we have the bound (6). □

3. Congruences for recurrence sequences

We obtain more precise bounds for the case of recurrence sequences.

Let (a_h) be a nondegenerate recurrence sequence of integers of $\mathbb{K}$ given by (2). It is well known that its terms can be represented in the form

$$a_h = \sum_{i=1}^{m} A_i(h)\alpha_i^h$$

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

where $\alpha_i \in \mathbb{K}$ are the distinct roots of the characteristic polynomial and their respective multiplicities n_i control the polynomial coefficients $A_i(h) \in \mathbb{K}[h]$, which have degrees respectively at most $n_i - 1$.

Given an integral ideal $\mathfrak{a}$ of $\mathbb{K}$, denote by $\mathcal{R}(H,\mathfrak{a})$ the number of solutions of the congruence

$$a_h \equiv 0 \pmod{\mathfrak{a}}, \quad h = 1, \dots, H.$$

In [8] it is established that

$$\mathcal{R}(H,\mathfrak{a}) < CH/\log\big(\operatorname{Norm}\mathfrak{a} + 1\big), \tag{7}$$

with a constant $C > 0$ depending only on the recurrence relation, and not on the initial values of the sequence. It is a simple matter to give an explicit expression for the constant C using a bound on the number of zeros of recurrence sequences.

Notwithstanding its simplicity and generality, the bound (7) is nontrivial for all H and $\mathfrak{a}$ and it yields useful results on the arithmetical structure of recurrence sequences; for such see [9].

Moreover, it is shown in [8] that the bound (7) cannot be improved for general ideals $\mathfrak{a}$. The simplest example is $\mathbb{K} = \mathbb{Q}$, $a_h = 3^h - 2^h$, and the congruence is taken modulo $q = 3^m - 2^m$; that is, $\mathfrak{a}$ is the principal ideal (q) in $\mathbb{Z}$.

However, for the case of a prime ideal $\mathfrak{a} = \mathfrak{p}$, and constant coefficients $A_i(h)$, a different bound follows from the general bound proved in [11] for the number of zeros of exponential polynomials over an arbitary ring R without zero-divisors.

For $i = 1, \dots, n$ let $A_i, \alpha_i \in R$ be nonzero elements of R and let t be the smallest positive integer so that, for $i \neq j$, $\alpha_i^t = \alpha_j^t$; if there is no such integer t set $t = \infty$.

Define the sequence of rational numbers (δ_k) by $\delta_2 = 1$ and the recurrence

$$\delta_k = \delta_{\lfloor (k+2)/2 \rfloor} / \lfloor (k+2)/2 \rfloor \quad k = 3, 4, \dots .$$

Then the number $\mathcal{M}(H)$ of solutions of the equation

$$A_1\alpha_1^h + \dots + A_n\alpha_n^h = 0, \quad h = 1, \dots, H$$

does not exceed

$$\mathcal{M}(H) \leqslant 2n\big(H^{1-\delta_n} + Ht^{-\delta_n}\big); \tag{8}$$

of course $t = \infty$ means our omitting the second term on the right.

Now, suppose that the constant coefficient s_n of the characteristic polynomial $S(X)$ and p are co-prime. We take τ to be the smallest positive integer with $\alpha_i^\tau \equiv \alpha_j^\tau \pmod{\mathfrak{p}}$ for some $i \neq j$.

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

Suppose that at least one term of the sequence (a_h) is prime to p. Then

$$\mathcal{R}(H,p) \leqslant 2n\left(H^{1-\delta_n} + H\tau^{-\delta_n}\right). \tag{9}$$

This bound seems stronger than (7) but the difficulty lies in obtaining a lower bound for τ. Of course we have $\tau > c\log p$ with some positive constant depending on $\alpha_1, \dots, \alpha_n$, but such an estimate yields a weaker bound than (7). We also note that $\delta_l > \exp\left(-c\log^2 l\right)$ where $c > 0$ is some absolute constant and that a similar bound to (9) can be proved for an arbitrary ideal $\mathfrak{a}$ at the cost of a more complicated definition for τ.

The bound (8) is applied in [11] to a problem in computational number theory on constructing primitive normal bases in finite fields.

Theorem 3. *Let (a_h) be a nondegenerate recurrence sequence given by (2). Suppose that $\mathfrak{p}$ is prime to s_n. Then there exists a constant $c > 0$ depending only on (a_h) and $\mathfrak{p}$ such that for each natural number r,*

$$\mathcal{R}(H,\mathfrak{p}^r) \leqslant c\left(Hp^{-r/e(n-1)} + 1\right). \tag{10}$$

Proof: We recall that a nondegenerate recurrence sequence always has only a finite number of zeros; see [**4**, **6**].

Consider the functions

$$v_k(t) = \sum_{i=1}^{m} A_i\left((p^f-1)p^\theta t + k\right)\alpha_i^{(p^f-1)p^\theta t+k}.$$

It is plain that for θ large enough we have

$$\operatorname{ord}\left(\alpha_i^{(p^f-1)p^\theta} - 1\right) > n/(p-1), \quad i = 1, \dots, m.$$

Hence, if for $i = 1, \dots, m$ we define the frequencies ω_i by the equations

$$\exp\omega_i = \alpha_i^{(p^f-1)p^\theta},$$

then we have $\operatorname{ord}\omega_i > n/(p-1)$, as in [**6**, Section 3].

Thus we can apply Lemma 2 of [**6**] with $\varepsilon = n/(p-1) - 1/(p-1) = (n-1)/(p-1)$. By [**6**, Lemma 2] we see that the degrees of the polynomials P_k corresponding to the polynomial $P(t)$ of Lemma 2 do not exceed

$$\deg P_k \leqslant n - 1 + (n-2)/\varepsilon(p-1) = n - 1/(n-1) < n.$$

Now we can repeat the proof of Theorem 2 *mutatis mutandis* using in the corresponding places the bound $\deg P_k \leqslant n-1$. ▯

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

4. Average p-adic order of a recurrence sequence

Suppose that a recurrence sequence (a_h) has no zeros and denote by $\chi_p(H)$ the average p-adic order of $a_1, \dots, a_H$; that is,

$$\chi_p(H) = H^{-1} \sum_{h=1}^{H} \operatorname{ord} a_h .$$

Theorem 4. *Let (a_h) be a nondegenerate recurrence sequence given by (2). Suppose that p is prime to s_n. Then there exists a constant χ_p depending only on (a_h) and p such that as $H \to \infty$, $\chi_p(H) = \chi_p + o(1)$.*

Proof: Let $\beta_p(H) = \max\{\operatorname{ord} a_h : h = 1, \dots, H\}$. It is clear that

$$\chi_p(H) = H^{-1} \sum_{\beta=1}^{\beta_p(H)} \mathcal{R}(H, p^\beta) .$$

Let $\tau(p^\beta)$ denote the smallest period of the sequence (a_h) modulo p^β. Then

$$\mathcal{R}(H, p^\beta) = \frac{H}{\tau(p^\beta)} \mathcal{R}(\tau(p^\beta), p^\beta) + O(\tau(p^\beta)) .$$

It is known that there exist positive constants c_1, c_2 depending on (a_h) and p only, so that

$$c_1 p^\beta < \tau(p^\beta) < c_2 p^\beta .$$

Thus for arbitrary integral positive γ we have

$$\chi_p(H) = \sum_{\beta=1}^{\gamma} \mathcal{R}(\tau(p^\beta), p^\beta)/\tau(p^\beta) + O(H^{-1} p^\gamma) + H^{-1} \sum_{\beta=\gamma+1}^{\beta_p(H)} \mathcal{R}(H, p^\beta) .$$

It follows from the bound (10) of Theorem 3 that

$$\sum_{\beta=1}^{\infty} \mathcal{R}(\tau(p^\beta), p^\beta)/\tau(p^\beta)$$

converges to a finite value that we denote by χ_p. Moreover

$$\sum_{\beta=1}^{\gamma} \mathcal{R}(\tau(p^\beta), p^\beta)/\tau(p^\beta) = \chi_p + O\left(p^{-\gamma/e(n-1)}\right) ,$$

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

where $L = d(n-1)$. Applying the bound (10) to the second sum we get

$$H^{-1}\sum_{\beta=\gamma+1}^{\beta_p(H)} \mathcal{R}(H,p^\beta) = O\Big(p^{-\gamma/e(n-1)} + H^{-1}\beta_p(H)\Big).$$

Thus $\chi_p(H) = \chi_p + O(p^{-\gamma/e(n-1)} + H^{-1}p^\gamma + H^{-1}\beta_p(H))$.

If we choose γ so that $p^\gamma \leqslant H^{e(n-1)/(en-e+1)} < p^{\gamma+1}$, then we obtain

$$\chi_p(H) = \chi_p + O\Big(H^{-1/(en-e+1)} + H^{-1}\beta_p(H)\Big).$$

For the final step we need the deep result that it can be shown that

$$\beta_p(H) = o(H).$$

For this and related results see [**7**] or [**2**]; and [**4**] and its references. □

The main disadvantage of the theorem is its ineffectivity; the upper bound $\beta_p(H) = o(H)$ is not effectively computable. On the other hand we can use a trivial effective upper bound of the kind $\beta_p(H) = O(H)$ and prove that the average value $\chi_p(H)$ is bounded by some effective constant C depending only on (a_h) and p.

5. Remarks

It is not difficult to see that more complicated computations would allow one to improve and generalise some of the bounds presented here. However, it is not clear whether it is possible to omit the condition that p be prime to all the α_i without a quite new idea. Were this achieved it would yield a solution to a longstanding conjecture to the effect that the number of zeros of a recurrence sequence can be bounded in terms of (the field of definition and) its order n only. In this sense, in the bound $(n-1)\big(4(d+\omega)\big)^{2(d+1)}$, the 'bad' parameter is ω, the number of different prime divisors of the roots α_i. Using the ideas suggested by Cassels [**1**], it is possible to replace the bound by one of the shape

$$C(\mathbb{K})n\omega\log\omega.$$

This result would be better with respect to ω other than that it contains a large, though effectively computable, constant $C(\mathbb{K})$ depending on $\mathbb{K}$.

Another problem is to get an effective upper bound for the constant in Theorem 2; recall that in Theorem 3 this is possible since we have the bound (7). With that done one would obtain a lower bound for the number of different prime divisors of general exponential polynomials; compare [**8, 9**]. Also, it would be useful to prove (9)

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press

for arbitrary nondegenerate recurrence sequences, that is, to omit the condition that the characteristic polynomial has distinct zeros.

It would also be interesting to consider recurrence sequences over other rings, for example, over function fields; here it seems feasible to utilise the bound (8).

Probably the most serious unsolved problem in the study of arithmetical properties of recurrence sequences is obtaining a nontrivial effective upper bound for the function $\beta_p(H)$ used in the proof of Theorem 4; relevant sources include [2] or [7], and [4].

References

[1] J.W.S. Cassels, 'An embedding theorem for fields', *Bull. Austral. Math. Soc.* **14** (1976), 193–198.

[2] J.-H.Evertse, 'On sums of S-units and linear recurrences', *Comp. Math.* **53** (1984), 225–244.

[3] A.J. van der Poorten, 'Zeros of p-adic exponential polynomials', *Indag. Math.* **38** (1976), 46–49.

[4] A.J. van der Poorten, 'Some facts that should be better known, especially about rational functions', *Number theory and applications*, Editor R. A. Mollin, pp. 497–528 (Kluwer Academic Publ., The Netherlands, 1989).

[5] A.J. van der Poorten and R. Rumely, 'Zeros of p-adic exponential polynomials II', *J. London Math. Soc.* **36** (1987), 1–15.

[6] A.J. van der Poorten and H.P. Schlickewei, 'Zeros of recurrence sequences', *Bull. Austral Math. Soc.* **44** (1991), 215–223.

[7] A.J. van der Poorten and H.P.Schlickewei, 'Additive relations in fields', *J. Austral Math. Soc.* **51** (1991), 154–170.

[8] I.E. Shparlinski, 'O числе различных простых делителеи рекуррентных последовательностеи ', Мат. Заметки **42**, pp. 494–507. 'On the number of different prime divisors of recurrence sequences', *Matem. Notes* **42** (1987), 773–780.

[9] I.E. Shparlinski, 'O некоторых арифметических своиствах рекуррентных последовательностеи ', Матем. Заметки, **47** (1990), 124-131, 'On some arithmetical properties of recurrence sequences', *Matem. Notes* **47** (1990).

[10] I.E. Shparlinski, 'O полиномиальных сравнениях' ('On polynomial congruences'), *Acta Arith.* **58** (1991), 153–156.

[11] S.A. Stepanov and I.E. Shparlinski, 'On the construction of primitive elements and primitive normal bases in a finite field', in *Computational number theory*, pp. 1–14 (Walter de Gruyter & Co., Berlin, 1991).

[12] R. Straßmann, 'Uber den Wertevorrat von Potenzreihen im Gebiet der $\mathfrak{p}$-adischen Zahlen', *J. für Math.* **159** (1928), 13–28.

[13] M. Voorhoeve, A. J. van der Poorten and R. Tijdeman, 'On the number of zeros of certain functions', *Indag. Math.* **37** (1975), 405-414.

Centre for Number Theory Research
Macquarie University NSW 2109
Australia
alf@macadam.mpce.mq.edu.au

Mosfilmovskaja Str dom 2 kv 41
Moscow 119285
Russia

https://doi.org/10.1017/S0004972700012065 Published online by Cambridge University Press