J. Austral. Math. Soc. (*Series A*) **37** (1984), 4–16

ARITHMETIC PROPERTIES OF CERTAIN RECURRENCE SEQUENCES

A. PERELLI and U. ZANNIER

(Received 4 June 1982)

Communicated by J. H. Loxton

Abstract

A classical theorem states that if a polynomial with integral coefficients is an mth power for every integral value of its argument, then it is the mth power of a polynomial with integral coefficients.

In this paper we deal with analogous problems concerning functions which arise as solutions of recurrence equations with constant coefficients.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 10 A 35.

1. Introduction and statement of the results

A classical theorem states that if a polynomial with integral coefficients is an mth power for every integral values of its argument, then it is the mth power of a polynomial with integral coefficients (see Pólya-Szegö [10] part VIII, Chapter 2). This theorem has been generalized and improved in various directions; we quote for example Davenport-Lewis-Schinzel [5], Ribenboim [11] and Perelli-Zannier [9].

In this paper we deal with analogous problems concerning functions, defined on the positive integers, $\mathbf{N}$, of the form

$$f(n) = \sum_{j=1}^{M} P_j(n) a_j^n, \tag{1}$$

where $P_j \in \mathbf{Z}[x]$, $a_j \in \mathbf{N}$. The interest of such functions arises also from the fact that they are solutions of recurrence equations with constant coefficients (see

Lemma 1). The particular case with the P_j constants has been dealt with by Lovasz [8].

We denote by A the integral domain of the functions f: $\mathbf{N} \to \mathbf{Z}$ of the form (1), by A^+ the subset of A consisting of the f such that $f(m) \geqslant 0$ for every $m \in \mathbf{N}$, and by K_A the quotient field of A. If $f \in A^+$ and $k \in \mathbf{N}$ we denote by $(f(m))^{1/k}$ the real kth root if k is odd and the positive real root if k is even. Let $B = \{g$: $\mathbf{N} \to \mathbf{R}$, $g(m) = \sum_{i=1}^{N} C_i (f_i(m))^{1/k_i}$, $C_i \in \mathbf{Z}$, $k_i \in \mathbf{N}$, $f_i \in A^+\}$; obviously B is a ring.

We say that a sequence of natural numbers is of type P if it intersects every arithmetic progression; it is easy to see that a P sequence contains infinitely many terms of every arithmetic progression.

Our results are the following:

THEOREM 1. *If $g \in K_A$ and $g(m) \in \mathbf{Z}$ for every $m \in \mathbf{N}$, $m > m_0$, then $Cg \in A$ for some integer C.*

THEOREM 2. *If $g \in B$ and $g(m) \in \mathbf{Z}$ for every m belonging to a fixed P sequence, then $Cg \in A$ for some integer C.*

The idea of considering P sequences in a similar problem concerning polynomials can be found in Davenport-Lewis-Schinzel [5].

We wish to thank Professor van der Poorten for useful comments. In his paper [12] he treats, among others, similar problems and he obtains independently our results using different methods. We point out that our method is completely elementary.

The referee pointed out that in the meantime Theorem 1 has been proved and to some extent generalized by Lewis and Morton [7]; anyway we still include it for sake of completeness.

Moreover in the paper of Benzaghou [1] there is a reference to an apparently unpublished proof by Pisot of the particular case of Theorem 2 in which the coefficient of the leading term of the exponential polynomial (1) is constant, and the P-sequence coincides with $\mathbf{N}$.

2. Preliminary lemmas

If $Q(y) = a_n y^n + a_{n-1} y^{n-1} + \cdots + a_0 \in \mathbf{C}[y]$ and f: $\mathbf{R} \to \mathbf{C}$ we set $[Tf](x) = f(x+1)$ and $Q(f, x) = [Q(T)f](x) = a_n f(x+n) + a_{n-1} f(x+n-1) + \cdots + a_0 f(x)$. As usual, if $x \in \mathbf{R}$, let $\|x\| = \min_{m \in \mathbf{Z}} |x - m|$, while if $\|x\| = |x - m_0|$ and $\|x\| \neq 1/2$ we put $(x) = x - m_0$ and otherwise $(x) = 1/2$.

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

We shall use the following lemma from the theory of finite-difference equations.

LEMMA 1. *Let* $f\colon \mathbf{N} \to \mathbf{C}$; *if there exists a polynomial* $Q \in \mathbf{C}[y]$,

$$Q(y) = Q_0 \prod_{j=1}^{R} (y - a_j)^{n_j+1}, \qquad a_i \neq a_j \text{ if } i \neq j, \tag{2}$$

satisfying $Q(f, m) = 0$ *for all* $m \in \mathbf{N}$, *then there exist* $P_1, P_2, \ldots, P_R \in \mathbf{C}[x]$, $\deg P_j \leqslant n_j$, *such that*

$$f(m) = \sum_{j=1}^{R} P_j(m) a_j^m \quad \text{for all } m \in \mathbf{N}. \tag{3}$$

Conversely, if f *is of the form* (3), *then* $Q(f, m) = 0$ *for all* $m \in \mathbf{N}$, *where* Q *is defined by* (2).

For the proof see, for example, Gelfond [6].

REMARK. Let Q and f be as in Lemma 1, $Q(f, m) = 0$ for all $m \in \mathbf{N}$; define, for $s = 1, 2, \ldots, R$, $Q_s(y) = Q(y)/(y - a_s) = \sum_{v=0}^{H} d_v y^v$, and $P_s(x) = b_s x^{n_s} + \cdots + b_0$. The operator defined from Q_s clearly annihilates all terms of f except the term $b_s x^{n_s} a_s^x$, whence

$$Q_s(f, m) = b_s a_s^m Q_s\big(t^{n_s} a_s^t, 0\big) = b_s a_s^m Q_s^{(n_s)}(a_s). \tag{4}$$

LEMMA 2. *Let* $P_1, P_2, \ldots, P_M \in \mathbf{R}[x]$, *let* $a_1 > a_2 > \cdots > a_{R-1} \geqslant 1 > a_R > \cdots > a_M > 0$ *be rational numbers and*

$$f(x) = \sum_{j=1}^{M} P_j(x) a_j^x, \qquad \deg P_j = n_j.$$

Suppose that, for integral $m \to \infty$, *we have* $\| f(m) \| \to 0$. *Then, for sufficiently large* m,

(i) $(f(m)) = \Sigma_{j \geqslant R} P_j(m) a_j^m$, *whence* $\Sigma_{j<R} P_j(m) a_j^m \in \mathbf{Z}$;
(ii) $a_1, \ldots, a_{R-1} \in \mathbf{Z}$;
(iii) $P_j(x) \in \mathbf{Q}[x]$ *if* $j \leqslant R - 1$.

PROOF. The lemma evidently follows from the special case where $a_j \geqslant 1$ for all j. Assume now that this applies. Let $Q(y) = Q_0 \prod_{j=1}^{M} (y - a_j)^{n_j+1}$ with Q_0 chosen so that $Q \in \mathbf{Z}[y]$. Writing $f(m) = N_f(m) + \theta_f(m)$, $\theta_f(m) = (f(m))$, we have by Lemma 1,

$$0 = Q(f, m) = Q\big(N_f, m\big) + Q\big(\theta_f, m\big).$$

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

But $Q(N_f, m)$ is an integer and $Q(\theta_f, m) \to 0$, so $Q(N_f, m) = Q(\theta_f, m) = 0$ if m is large enough. Again from Lemma 1 we obtain

$$\theta_f(m) = \sum_{j=1}^{M} V_j(m) a_j^m, \qquad V_j \in \mathbf{C}[x],$$

which implies $V_j = 0$, since $a_j \geqslant 1$ and $\theta_f(m) \to 0$. Thus, for sufficiently large m, $f(m)$ is in $\mathbf{Z}$ and, by repeated applications of (4), we see that all the coefficients of the $P_j(x)$ are rational numbers.

COROLLARY. *Let* $P_1(x), \ldots, P_M(x) \in (\overline{\mathbf{Q}} \cap \mathbf{R})(x)$ *be rational functions, let* $a_1, \ldots, a_M$ *be as in Lemma* 2 *and* $f(x) = \sum_{j=1}^{M} P_j(x) a_j^x$. *Suppose that* $m^N \| f(m) \| \to 0$, *where* N *is the degree of a common denominator* $V(x) \in \mathbf{Z}[x]$ *for* $P_1, \ldots, P_M$. *Then, for* m *large enough,*

(i) $(f(m)) = \sum_{j \geqslant R} P_j(m) a_j^m$;

(ii) $a_1, \ldots, a_{R-1} \in \mathbf{Z}$;

(ii) $P_1, \ldots, P_{R-1} \in \mathbf{Q}[x]$.

PROOF. We set $P_j(x) = Q_j(x)/V(x)$ and $F(x) = V(x)f(x)$. Obviously F satisfies the hypotheses of Lemma 2 and for large m we have, since $V(m) \in \mathbf{Z}$,

$$(F(m)) = V(m)(f(m)). \tag{5}$$

(i) and (ii) are immediately deduced, and we also obtain $P_j(x) \in \mathbf{Q}(x)$ for $j \leqslant R - 1$. From (i) we get

$$\sum_{j<R} P_j(m) a_j^m \in \mathbf{Z} \quad \text{for } m \text{ large enough.}$$

Let now $G(x)$ be a l.c.m. of the denominators of $P_1, \ldots, P_{R-1}$, such that $H_j(x) = G(x)P_j(x) \in \mathbf{Z}[x]$. Then G.C.D.$(H_1(x), \ldots, H_{R-1}(x), G(x)) = 1$. Suppose $\deg G > 0$; there exist $T_1, \ldots, T_{R-1}$, $T \in \mathbf{Z}[x]$ and an integer $A \neq 0$ such that

$$\sum_{j=1}^{R-1} T_j(x) H_j(x) + T(x)G(x) = A. \tag{6}$$

Let $p > \max(A, a_1, \ldots, a_{R-1})$ be a prime number such that $p \mid G(m_1)$ for some sufficiently large m_1 (see exercise 108, page 131 of [10]). From $\sum_{j<R} P_j(m_1) a_j^{m_1} \in \mathbf{Z}$ it follows that

$$\sum_{j<R} H_j(m_1 + up) a_j^{m_1+up} = G(m_1 + up) \sum_{j<R} P_j(m_1 + up) a_j^{m_1+up} \equiv 0 \pmod{p}$$

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

for every $u \in \mathbf{N}$, whence

$$\sum_{j \in R} H_j(m_1) a_j^{m_1} a_j^{up} \equiv 0 \pmod{p}, \qquad u = 0, 1, \ldots, R-1.$$

We consider these congruences as a linear system in $\mathbf{Z}/p\mathbf{Z}$ with unknowns $H_j(m_1)a_j^{m_1}$. The determinant is $\prod_{i<j}(a_i^p - a_j^p) \equiv \prod_{i<j}(a_i - a_j) \not\equiv 0 \pmod{p}$. Therefore $H_j(m_1) \equiv 0 \pmod{p}$ for all $j \leqslant R-1$ and, by (6), $p \mid A$, a contradiction.

LEMMA 3. *Let* $f(x) = \sum_{j=1}^{M} P_j(x) a_j^x$, $a_1 > \cdots > a_M \geqslant 1$, $P_j \in \mathbf{C}(x)$, $\delta > 0$. *Then there exist real numbers* $\lambda_1 = 1/a_1 > \lambda_2 > \cdots > \lambda_T > 0$ *and* $W_1(x) = 1/P_1(x)$, $W_2(x), \ldots, W_T(x) \in \mathbf{C}(x)$ *such that*

$$\frac{1}{f(x)} = \sum_{i=1}^{T} W_i(x) \lambda_i^x + O(\delta^x), \qquad x \to \infty.$$

Further, if $a_j \in \mathbf{Q}$ *and* $P_j \in \mathbf{Q}(x)$, *then we can take* $\lambda_i \in \mathbf{Q}$ *and* $W_i \in \mathbf{Q}(x)$.

PROOF. We have the identity

$$\begin{aligned} 1/f(x) &= 1/\left(P_1(x)a_1^x\right) + \left(-\sum_{j=2}^{M} P_j(x) a_j^x\right) / \left(P_1(x) a_1^x f(x)\right) \\ &= W_1(x)\lambda_1^x + g(x)/f(x). \end{aligned}$$

By iteration of this formula one obtains, for every $N \in \mathbf{N}$,

$$\begin{aligned} 1/f(x) = {} & W_1(x)\lambda_1^x + W_1(x)\lambda_1^x g(x) + \cdots \\ & + W_1(x)\lambda_1^x g^N(x) + g^{N+1}(x)/f(x). \end{aligned}$$

It is clear that $g(x) = O(\gamma^x)$, $0 < \gamma < 1$, and the lemma follows on choosing N large enough.

3. Proof of Theorem 1

Let $f(x) = \sum_{j=1}^{M} P_j(x) a_j^x$, $h(x) = \sum_{i=1}^{N} T_i(x) b_i^x$, $f,\ h \in A$, $g(x) = h(x)/f(x)$, $a_1 > \cdots > a_M > 0$, $b_1 > \cdots > b_N > 0$. Moreover let $\delta < 1/b_1$ and $\lambda_1, \ldots, \lambda_T$, $W_1, \ldots, W_T$ be determined as in Lemma 3. Then

$$\begin{aligned} g(x) &= \sum_{i=1}^{N} T_i(x) b_i^x \sum_{j=1}^{T} W_j(x) \lambda_j^x + O\left(T_1(x)(\delta b_1)^x\right) \\ &= \sum_{\nu=1}^{R} Q_\nu(x) \gamma_\nu^x + O(\gamma^x) = G(x) + O(\gamma^x), \end{aligned}$$

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

where $\gamma_\nu \geqslant 1$, $\gamma_\nu \in \mathbf{Q}$, $Q_\nu(x) \in \mathbf{Q}(x)$, $0 < \gamma < 1$. We have $\|G(m)\| \ll \gamma^m$, since $g(m) \in \mathbf{Z}$ if m is large. From the corollary to Lemma 2 it follows that $\gamma_\nu \in \mathbf{Z}$ and $Q_\nu(x) \in \mathbf{Q}[x]$. If $C \in \mathbf{Z}$ is such that $CQ_\nu(x) \in \mathbf{Z}[x]$ for all ν, we have

$$Cg(x) = CG(x) + O(\gamma^x) \quad \text{and} \quad CG \in A.$$

But $C(g(m) - G(m))$ is an integer which must be zero in view of the previous estimate, and the theorem is proved.

4. Reduction of Theorem 2 to a particular case

We first require the following lemmas.

LEMMA 4. *Let* $f(x) = \sum_{j=1}^{M} P_j(x)a_j^x$, $P_j \in \mathbf{R}[x]$, $a_j \in \mathbf{R}$, $a_1 > a_2 > \cdots > a_n > 0$, *and let* $N = \sum_{j=1}^{M}(\deg P_j + 1)$. *Then, if* f *has* N *real zeros, all the* P_j *vanish identically.*

For the proof see [10], part V, Chapter 1, exercise 75.

LEMMA 5. *Let* $f_1(x), \ldots, f_R(x)$ *be of the same kind as* $f(x)$ *in Lemma* 4, *and suppose* $f_i(x) \geqslant 0$, *if* $x > x_0$. *Suppose that*

$$g(x) = \sum_{i=1}^{R} C_i \sqrt[k]{f_i(x)}, \qquad C_i \in \mathbf{R},\ x > x_0,$$

has arbitrarily large zeros. Then $g(x) = 0$ *identically.*

PROOF. Using Lemma 4, we may assume $f_i(x) > 0$ for $x > x_1$. We argue by induction on R. If $R = 1$, the conclusion follows from Lemma 4. If the lemma holds for $R \leqslant R_0 - 1$, let $h(x) = g(x)/f_1^{1/k}(x)$. Then $f^{(1+1/k)}(x)(\prod_{i=2}^{R_0} f_i(x))\, dh(x)/dx$ is of the same kind as $g(x)$ with $R = R_0 - 1$, and has, by Rolle's theorem, arbitrarily large zeros. From the induction hypothesis it follows that $dh/dx = 0$, whence $h(x) = C$ is a constant and $g(x) = Cf^{1/k}(x)$. This implies $g(x) = 0$.

We now show that the truth of Theorem 2 follows from a special case. Take g in B, say $g(m) = \sum_{i=1}^{N} C_i(f_i(m))^{1/k_i}$. We assume the theorem for $N = 1$, and work out the general case by induction.

We need the following corollary of a theorem of Besicovitch [2]: "If $\sum_{i=1}^{N} d_i \sqrt[k]{l_i} = 0$, where $l_i \in \mathbf{Q} - \{0\}$ and $l_i/l_j \notin \mathbf{Q}^k$, $i \neq j$, $d_i \in \mathbf{Q}$, then $d_i = 0$ for all i".

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

We may obviously assume, by replacing f_i with $f_i^{\prod_{j \neq i} k_j}$ if necessary, that $k_1 = \cdots = k_N = k$. For every fixed i we can write uniquely

$$f_i(m) = r_i^k(m) l_i(m) \quad \text{with } r_i, l_i \in \mathbf{Z} \text{ and } l_i \text{ } k\text{-free}.$$

Let $U(m, l) = \{i \leqslant N: l_i(m) = l\}$; clearly $\{1, \ldots, N\} = \bigcup_l U(m, l)$ for every m. We denote by S a P sequence such that $g(s) \in \mathbf{Z}$ for $s \in S$, and consider the following two cases:

(i) for every $s \in S$, $s > s_0$, we have $\{1, \ldots, N\} = U(s, 1)$. In this case, recalling that $\{s \in S: s > s_0\}$ is again a P sequence, Theorem 2 is a straightforward consequence of the induction hypothesis.

(ii) There exists an infinite subsequence S' of S such that $\{1, \ldots, N\} \neq U(s', 1)$, for every $s' \in S'$.

By Dirichlet's principle, there exist $T \in \mathbf{N}$ and non-empty disjoint sets $V_1, \ldots, V_T$ such that $\bigcup_{j=1}^T V_j = \{1, \ldots, N\}$ and there is an infinite subsequence S'' of S' such that, for every $s'' \in S''$ and every l satisfying $U(s'', l) \neq \varnothing$, there exists h with $U(s'', l) = V_h$.

We have, for every $s'' \in S''$,

$$g(s'') = \sum_{j=1}^{T} \sum_{i \in V_j} C_i \sqrt[k]{f_i(s'')} = \sum_{j=1}^{T} \sqrt[k]{l(j, s'')} \sum_{i \in V_j} C_i r_i(s''),$$

where $l(j, s'')$ is one of the $l_i(s'')$ for $i \in V_j$. Now it is plain that $l(j, s'')/l(h, s'') \notin \mathbf{Q}^k$ if $j \neq h$. Clearly, there exists at least a j such that $l(j, s'') \neq 1$; for every such j, by the above corollary to the theorem of Besicovitch, we deduce that $\Sigma_{i \in V_j} C_i r_i(s'') = 0$. This implies $\Sigma_{i \in V_j} C_i \sqrt[k]{f_i(s'')} = 0$ for all $s'' \in S''$. Then by Lemma 5 we get

$$\sum_{i \in V_j} C_i \sqrt[k]{f_i(s)} = 0 \quad \text{for every } s \in \mathbf{N}.$$

Now, if $V_j = \{1, \ldots, N\}$, we have $g(s) = 0$ for all $s \in \mathbf{N}$, whence $g \in A$; if $V_j \neq \{1, \ldots, N\}$, then the induction hypothesis applies to

$$\sum_{i \notin V_j} C_i \sqrt[k]{f_i(s)} = g(s) - \sum_{i \in V_j} C_i \sqrt[k]{f_i(s)} = g(s).$$

This completes the induction.

Now we only have to prove

THEOREM 2'. *Let $g \in B$, $g(m) = C_0 \sqrt[k]{f(m)}$ with C_0 in $\mathbf{Z}$ and f in A^+. If $g(m) \in \mathbf{Z}$ for every m belonging to a fixed P sequence, then $Cg \in A$ for some integral C.*

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

We now prove that we may further restrict ourselves to the following

THEOREM 2″. *Let* $g \in B$, $g(m) = C_0\sqrt[k]{f(m)}$ *as before. If* $g(m) \in \mathbf{Z}$ *for every* $m \in \mathbf{N}$, *then* $Cg \in A$ *for some integral* C.

First of all we show that if $f(s) \in \mathbf{Z}^k$ for every $s \in S$, then there exist $a, b \in \mathbf{Z}$ such that $f(am + b) \in \mathbf{Z}^k$ for every $m \in \mathbf{N}$. We set $f(m) = d^m f^*(m)$, where $d = (a_1, \ldots, a_M)$, whence $f^*(m) = \Sigma_{j=1}^M P_j(m) b_j^m$ with $(b_1, \ldots, b_M) = 1$. Further, let $\mathcal{P}_0 = \{p\colon p \text{ prime}, p \mid b_j \text{ for some } j\}$ and, for $p \in \mathcal{P}_0$, let $J(p) = \{j \leqslant M\colon p \nmid b_j\}$, and $f_p^*(m) = \Sigma_{j \in J(p)} P_j(m) b_j^m$. From Lemma 4 it follows that there exists $r \in \mathbf{N}$, $r \equiv 0 \pmod k$, such that

$$f_p^*(r) \neq 0 \quad \text{for every } p \in \mathcal{P}_0.$$

For $p \in \mathcal{P}_0$ let $p^{h(p)} \| f_p^*(r)$. If $c > h(p)$ for all $p \in \mathcal{P}_0$ we have, for $m \geqslant 1$:

$$f^*(r + m(p-1)p^c) \equiv f_p^*(r + m(p-1)p^c) \equiv f_p^*(r) \pmod{p^c},$$

whence $p^{h(p)} \| f^*(r + m(p-1)p^c)$ for $m \geqslant 1$. Setting $L = k(\prod_{p \in \mathcal{P}_0}(p-1)p^c)$ we have, for $m \geqslant 1$, $p^{h(p)} \| f^*(r + mL)$. Thus we can write

$$f(r + mL) = \prod_{p \in \mathcal{P}_0} p^{h(p)} d^{r+mL} y(m), \quad \text{where } \left(y(m), \prod_{p \in \mathcal{P}_0} p\right) = 1.$$

We will show that if $q^s \| y(m)$, and q is prime, then $s \equiv 0 \pmod k$, thereby proving that $y(m) \in \mathbf{Z}^k$. Assume the contrary, that is, $tk < s < (t+1)k$; if $c > s$ and $v \in \mathbf{N}$, we have

$$f^*(r + Lm + Lv(q-1)q^c) \equiv f^*(r + Lm) \pmod{q^c},$$

whence $q^s \| f^*(r + Lm + Lv(q-1)q^c)$ for every $v \in \mathbf{N}$. Now $r + Lm + Lv(q-1)q^c$ is an arithmetic progression and so $f(r + Lm + Lv_0(q-1)q^c) \in \mathbf{Z}^k$ for some v_0. Hence $f^*(r + L_m + Lv_0(q-1)q^c) \in \mathbf{Z}^k$ since $f(kn)/f^*(kn) \in \mathbf{Z}^k$, and this contradiction proves the statement. We can now write

$$f(r + mL) = \prod_{p \in \mathcal{P}_0} p^{h(p)} y_1^k(m), \qquad m \geqslant 1, y_1(m) \in \mathbf{Z}.$$

With the same arguments as before we see that $h(p) \equiv 0 \pmod k$ for all $p \in \mathcal{P}_0$ whence $f(r + mL) \in \mathbf{Z}^k$ for every $m \geqslant 1$.

Theorem 2″ implies the existence of $g \in A$, $g(m) = \Sigma_{j=1}^T Q_j(m) l_j^m$ such that $H^k f(r + xL) = g^k(x)$ for some integer H and $x \in \mathbf{R}$. For fixed $l \in \mathbf{N}$, $0 < l < L$ we have

$$H^k f(r + l + mL) = g^k(m + l/L),$$

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

hence there exist infinitely many integers $m_1, m_2, \ldots$, such that $g(m_v + l/L) \in \mathbf{Z}$. Setting $Q_j(m + l/L) = \sum_{i=0}^{N_j} c_{j,i} m^i$, $c_{j,i} \in \mathbf{Q}$, we have

$$g(m_v + l/L) = \sum_{j=1}^{T} \sum_{i=0}^{d_j} c_{j,i} m_v^i l_j^{m_v l/L}.$$

Consider the following linear system, with unknowns $y_{i,j}$:

$$\sum_{j=1}^{T} \sum_{i=0}^{d_j} m_v^i l_j^{m_v} y_{i,j} = g(m_v + l/L) \qquad (\in \mathbf{Z}) \quad \text{if } v = 1, \ldots, \sum_{j=1}^{T} (d_j + 1).$$

Its determinant is non-zero, for otherwise there would exist $x_{i,j}$ not all zero such that

$$\sum_{j=1}^{T} \sum_{i=0}^{d_j} m_v^i l_j^{m_v} x_{i,j} = 0$$

for $\sum_{j=1}^{T}(d_j + 1)$ distinct values of m_v, which is impossible by Lemma 4. By Cramer's rule we have $y_{i,j} \in \mathbf{Q}$. But the system has the unique solution $y_{i,j} = c_{j,i} l_j^{l/L}$, and so $l_j^{l/L} \in \mathbf{Q}$ for all j. Taking $l = 1$ we deduce $l_j = h_j^L$, where $h_j \in \mathbf{Q}$. Writing

$$h(m) = g(m/L) = \sum_{j=1}^{T} Q_j(m/L) h_j^m$$

we have $H^k f(m + r) = h^k(m) \in \mathbf{Z}$, whence $h(m) \in \mathbf{Z}$. Either by Lemma 2 or by an even simpler argument, we obtain $h_j \in \mathbf{Z}$. Thus there exists an integer C such that $Ch \in A$, whence $C^k H^k f \in A^k$.

5. Proof of Theorem 2″

We require some more lemmas.

LEMMA 6. *Let* $f(x) = P_1^k(x) a_1^x + \sum_{j=2}^{M} P_j(x) a_j^x$, *where* $P_1 \in (\overline{\mathbf{Q}} \cap \mathbf{R})[x]$, $a_1 > a_2 > \cdots > a_M \geqslant 1$, $a_i \in \mathbf{Z}$, $P_j \in \mathbf{Q}[x]$ *if* $j \geqslant 2$. *Suppose that, for* m *large,* $f(m) \in \mathbf{Z}^k$. *Then there exists an integer* C *such that* $Cf \in A^k$.

PROOF. We let $F(x) = f(kx)$; $F^{1/k}(x)$ is defined for large x, and

$$F^{1/k}(x) = P_1(kx) a_1^x (1 + h(x))^{1/k}$$

where $h(x) \ll \delta x$ with $0 < \delta < 1$. Expanding $(1 + h(x))^{1/k}$ as a power series of $h(x)$, when x is large, we see that for every $\eta > 0$ there exists $U(x) = \sum_{j=1}^{T} Q_j(x) l_j^x$,

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

$Q_j \in (\overline{\mathbf{Q}} \cap \mathbf{R})(x)$, $l_j \in \mathbf{Q}$, such that

$$F^{1/k}(x) = U(x) + O(\eta^x), \qquad x \to \infty.$$

But for $m \in \mathbf{Z}$, m large, $F^{1/k}(m) \in \mathbf{Z}$, whence $\|U(m)\| \ll \eta^m$. Choose $\eta < 1$. Since $F^{1/h}(m)$ is in $\mathbf{Z}$ for m large, the corollary to Lemma 2 gives

$$F^{1/k}(m) = \sum_{j=1}^{N} \tilde{Q}_j(m)\tilde{l}_j^m, \qquad \tilde{Q}_j \in \mathbf{Q}[x], \qquad \tilde{l}_j \in \mathbf{Z}, \tilde{l}_1 > \tilde{l}_2 > \cdots > \tilde{l}_N > 0.$$

Hence there exists an integer C such that $Cf(km) = g^k(m) \in A^k$.

Noting that $Cf(m) = g^k(m/k)$ is integral for m large, we obtain the lemma by the same argument used at the end of the previous section.

LEMMA 7. *Let $f(x) = \sum_{j=1}^{M} P_j(x)a_j^x \in A$ such that $f(m) \in \mathbf{Z}^k$ for m large, and let $f_i(x) = \sum_{j=1}^{M} P_j^{(i)}(x)a_j^x$. Let q be a prime number and let m_1 be an integer such that $q \mid f(m_1)$. Then if $q > \max(a_1, \ldots, a_M, k)$ we have $q \mid f_i(m_1)$ for $i = 0, 1, \ldots, k - 1$.*

PROOF. Let $a_j^{q-1} = 1 + qA_j$. We have

$$\begin{aligned} P_j(m_1 + tq(q-1))a_j^{tq(q-1)} &= \left(P_j(m_1) + tq(q-1)P_j'(m_1) + \cdots\right) \\ &\quad \times \left(1 + qA_j\binom{tq}{1} + q^2A_j^2\binom{tq}{2} + \cdots\right) \\ &\equiv C_{0,s,j} + tC_{1,s,j} + \cdots + t^{s-1}C_{s-1,s,j} \pmod{q^s} \end{aligned}$$

for every $s \leqslant k$. It is well known that $\binom{tq}{j}$ is a polynomial in t with coefficients divisible by q if $j < q$. Hence

$$C_{s-1,s,j} \equiv q^{s-1}P_j^{(s-1)}(m_1)(q-1)^{s-1}/(s-1)! \pmod{q^s}.$$

From these congruences we obtain

$$\begin{aligned} (7)\quad f(m_1 + tq(q-1)) &\equiv C'_{0,s} + tC'_{1,s} + \cdots \\ &\quad + t^{s-1}q^{s-1}(q-1)^{s-1}f_{s-1}(m_1)/(s-1)! \pmod{q^s}. \end{aligned}$$

Now $f(m_1 + tq(q-1)) \equiv f(m_1) \equiv 0 \pmod{q}$ and, since $f(m_1 + tq(q-1)) \in \mathbf{Z}^k$, we have

$$(8)\qquad f(m_1 + tq(q-1)) \equiv 0 \pmod{q^k}$$

for every sufficiently large integer t.

From (7) and (8) we obtain finally $f_{s-1}(m_1) \equiv 0 \pmod{q}$ if $s \leqslant k$.

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

We now introduce the following polynomials

$$F_s(x) = \sum_{j=1}^{M} P_j(s-x)a_j^s. \tag{9}$$

LEMMA 8. *Under the same hypotheses as Lemma 7, every root of $F_s(x)$ has multiplicity $\geqslant k$, for all $s \in \mathbf{N}$.*

PROOF. We note that $f_r(s+(q-1)h) \equiv \sum_{j=1}^{M} P_j^{(r)}(s-h)a_j^s \equiv (-1)^r F_s^{(r)}(h) \pmod q$, $h \in \mathbf{N}$, if $q > \max(a_1, a_2, \ldots, a_M)$. For fixed s, let q be a sufficiently large prime satisfying $q \mid F_s(h)$ for some h. This implies $q \mid f(s+(q-1)h)$, whence $q \mid f_r(s+(q-1)h)$ by Lemma 7, for $r = 0, 1, \ldots, k-1$. Hence $q \mid F_s^{(r)}(h)$ for $0 \leqslant r \leqslant k-1$.

Let now $F_s(x) = Q_1^{u_1}(x) \cdots Q_b^{u_b}(x)$ with $Q_u \in \mathbf{Z}[x]$, Q_u irreducible over $\mathbf{Q}$ and $Q_i \neq Q_j$ for $i \neq j$. We claim that $u_i \geqslant k$ $(i = 1, \ldots, b)$. If, for example, we had $0 < u_1 < k$, then G.C.D.$(F_s(x), F_s'(x), \ldots, F_s^{(k-1)}(x), Q_1(x)) = 1$ and there would exist $V_1, \ldots, V_{k-1}, V \in \mathbf{Z}[x]$ and an integer $D \geqslant 0$ such that

$$\sum_{i=0}^{k-1} V_i(x)F_s^{(i)}(x) + V(x)Q_1(x) = D.$$

Then the previous remark, where q is a large prime number dividing $Q_1(h)$ gives a contradiction.

We can now give the proof of Theorem 2''.

For $f(n) = \sum_{j=1}^{M} P_j(n)a_j^j \in A$ we put $\deg f = \max \deg P_j$. We denote by E the subring of A consisting of the f such that $\deg f = 0$, and by K_E its quotient field.

If $F_s(x)$ is defined by (9) then, using the euclidean algorithm, which involves only rational operations, we can write

$$R_s(x) = \text{G.C.D.}\left(F_s(x), F_s'(x)\right) = x^n + C_{n-1,s}x^{n-1} + \cdots + C_{0,s} \tag{10}$$

where $C_{i,s} \in K_E$, $i = 0, 1, \ldots, n-1$. If $F_s(x) = F(s)\prod_{i=1}^{M}(x-\beta_{i,s})^{v_{i,s}}$, $\beta_{i,s} \neq \beta_{j,s}$, $i \neq j$. Then, since $v_{i,s} \geqslant k \geqslant 2$ by Lemma 8, we have $R_s(x) = \prod_{i=1}^{M}(x-\beta_{i,s})^{v_{i,s}-1}$, whence

$$F_s(x)/R_s(x) = \prod_{i=1}^{M}(x-\beta_{i,s})F(s) = W_s(x).$$

Using again the euclidean algorithm, we see that $W_s(x)$ is of the form (10). By Lemma 8, $F_s(x)$ is divisible by $W_s^k(x)$ and their quotient, $Q_s(x)$, is again of the form (10). On multiplying $F_s(x) = W_s^k(x)Q_s(x)$ by a common denominator $D^k(s) \in E$ of the coefficients, we obtain

$$D^k(s)F_s(x) = B_s^k(x)T_s(x), \tag{11}$$

https://doi.org/10.1017/S1446788700021704 Published online by Cambridge University Press

where B_s and T_s are of the form (10). Putting $x = 0$ in (11) and noting that $F_s(0) = f(s)$, we have

$$D^k(s)f(s) = B_s^k(0)T_s(0),$$

where $D \in E$, and $B_s(0)$, $T_s(0) \in A$.

If s is large enough, then $D(s) \in \mathbf{Z}$, $f(s) \in \mathbf{Z}^k$, whence $T(s) = T_s(0) \in \mathbf{Z}^k$, and, since obviously $\deg B > 0$, we have $\deg T < \deg f$. Thus, after a finite number of steps we obtain an identity of the form

$$\tilde{D}^k(s)f(s) = \tilde{B}^k(s)\tilde{T}(s),$$

where $\tilde{D}$, $\tilde{T} \in E$ and $\tilde{B} \in A$. If

$$\tilde{D}^k(s) = \sum_{j=1}^{M_{\tilde{D}}} D_j d_j^s, \qquad d_1 > d_2 > \cdots > d_{\tilde{D}},$$

$$\tilde{B}(s) = \sum_{j=1}^{M_{\tilde{B}}} \tilde{B}_j(s) b_j^s, \quad b_1 > b_2 > \cdots > b_{\tilde{B}},$$

$$\tilde{T}(s) = \sum_{j=1}^{M_{\tilde{T}}} T_j t_j^s, \qquad t_1 > t_2 > \cdots > t_{\tilde{T}},$$

we finally obtain $D_1 P_1(s) = B_1^k(s)T_1$. By Lemma 6 the proof is complete.

Final remarks

(1) The introduction of the polynomials $F_s(x)$ is motivated by the following remark: if $f \in A^k$, $f(n) = (\sum_{i=1}^N H_i(n)b_i^n)^k = \sum_{j=1}^M P_j(n)a_j^n$ then it is easy to see that $(\sum_{i=1}^N H_i(m)b_i^n)^k = \sum_{j=1}^M P_j(m)a_j^n$ for every m, n, and the polynomials in m $\sum_{j=1}^M P_j(m)a_j^n$ are kth powers.

(2) It may be worth noting that A is a unique factorization domain; this follows from the "Principal Theorem" of Cashwell-Everett [3], concerning the unique factorization problem for a certain class of rings.

References

[1] B. Benzaghou, 'Algèbres de Hadamard,' *Bull. Soc. Math. France* **98** (1970), 209–252.
[2] A. S. Besicovitch, 'On the linear independence of fractional powers of integers,' *J. London Math. Soc.* **15** (1940), 3–6.
[3] E. D. Cashwell and C. J. Everett, 'Formal power series,' *Pacific J. Math.* **13** (1963), 45–64.
[4] J. W. S. Cassels, *An introduction to diophantine approximation* (Cambridge Univ. Press, 1957).

[5] H. Davenport, D. J. Lewis and A. Schinzel, 'Polynomials of certain special types,' *Acta Arith.* **9** (1964), 107–116.
[6] A. O. Gelfond, *Calcul des différences finites* (Dunod, 1963).
[7] D. J. Lewis and P. Morton, 'Quotients of polynomials and a theorem of Pisot and Cantor,' *J. Fac. Sci. Univ. Tokyo* **28** (1982), 813–822.
[8] L. Lovasz, 'On finite Dirichlet series', *Acta Math. Acad. Sci. Hungar.* **22** (1972), 227–231.
[9] A. Perelli and U. Zannier, 'Una proprietà aritmetica dei polinomi,' *Boll. Un. Mat. Ital. A* **17** (1980), 199–202.
[10] G. Pólya and G. Szegö, *Problems and theorems in analysis*, vol. II (Springer-Verlag, 1976).
[11] P. Ribemboim, 'Polynomials whose values are powers,' *J. Reine Angew. Math.* **268/269** (1974), 34–40.
[12] A. J. van der Poorten, 'Some problems of recurrent interest,' to appear in the Proceedings of the János Bólyai Colloquium, 1981.

Scuola Normale Superiore
56100 Pisa
Italy