Indag. Mathem., N.S., 9 (3), 317–332 September 28, 1998

Diophantine equations with power sums and Universal Hilbert Sets

by P. Corvaja and U. Zannier

Dipartimento di Matematica e Informatica, Via delle Scienze 206, Udine, Italy
D.C.A., Istituto Universitario di Architettura, Santa Croce, Venezia, Italy

Communicated by Prof. R. Tijdeman at the meeting of September 29, 1997

INTRODUCTION

In the present paper we shall deal with diophantine equations involving functions of $n \in \mathbf{N}$ of the form

$$(1) \qquad \alpha(n) = \sum_{i=1}^{h} c_i a_i^n$$

where the c_i are (nonzero) rational numbers and the a_i, called the *roots*, are in $\mathbf{Z}$. It is classical that such functions satisfy linear recurrence relations with constant coefficients, the general solutions being of the same form, but allowing the c_i to be polynomials in n and the $a_i \in \mathbf{C}$. The arithmetic properties of such general solutions, in the case e.g. of rational or algebraic coefficients, have been widely investigated. A number of results and conjectures have to do with assumptions involving all natural numbers n. We may mention for instance the solution by van der Poorten [vdP2] (after an incomplete argument by Pouchet [P]) of a conjecture by Pisot which, in its simplest form, roughly speaking predicts that a quotient of two solutions may have values in $\mathbf{Z}$ for all $n \in \mathbf{N}$ only when *this is obvious*, in the sense that it comes from an identical relation. Another instance, still open to our knowledge, is the problem of *Hadamard's d-th root*; i.e., is it true that if a solution of a recurrence relation as above is a d-th power for all $n \in \mathbf{N}$, then the function itself must be a d-th power of a function in the same form? (For conditional results see e.g. [P-Z], [R-vdP].) For an extended survey on such topics, see [vdP1].

On the other hand (as observed e.g. in §6.6 of [vdP1]) few general results seem to be known when assumptions of the mentioned type hold only for an infinite sequence of natural numbers n. We may mention for instance the paper by Shorey and Stewart [S-S], where however a fairly strong assumption on the roots is used. In the present paper we shall obtain such results in the particular cases when the solution of the linear recurrence is of the form (1); the fact that the c_i are constant and that the a_i may be assumed to have distinct absolute values has made this case much more tractable in all the mentioned investigations. For instance, Pisot's conjecture was known long ago before its complete solution, under these assumptions (with a simple proof, moreover). However we insist that we are dealing with general infinite sequences of solutions. Also, as remarked below, our proofs may be geralized to certain extent.

We shall first investigate (Theorem 1) the question whether the ratio of functions of the form (1) can be integral valued for an infinity of n; this is somewhat related with the Pisot conjecture (i.e. van der Poorten's theorem). Then (Theorem 2) we look at diophantine equations $F(\alpha(n), Y) = 0$ and (Theorem 3) at diophantine inequalities $|\alpha(n) - Y^d| \ll |Y|^{d-1-\epsilon}$.

As a simple application, we shall construct universal Hilbert sequences (or, equivalently, universal Hilbert sets) of exponentional type, i.e. sequences of the form (1) such that, for all irreducible $F \in \mathbf{Q}[X, Y]$, the polynomial $F(\alpha(n), Y)$ remains irreducible for all large n (depending on F). We give a necessary and sufficient condition on α (Theorem 4). Our Corollary 3, which originated with questions of Yasumoto [Y], substantially generalizes previous cases ([Theorem 2, D-Z]) and provides new concrete examples of universal Hilbert sequences.

Our proofs are simple and make use of the celebrated Schmidt's Subspace Theorem (in the form of recalled below). This result has long been known to be crucial in the investigation of recurrence sequences (see [vdP1]), but to our knowledge, somewhat surprisingly, the present application has not appeared before, notwithstanding its simplicity.

NOTATION AND STATEMENTS

For a ring $A \subset \mathbf{C}$, we let $\mathcal{E}_A$ denote the ring of complex functions on $\mathbf{N}$ of the form (1) where the $a_i \in A$, called the *roots* of α, are distinct and $c_i \in \mathbf{Q}$. If $K \subset \mathbf{C}$ is a field we define $K\mathcal{E}_A$ by the same formulas, but allowing $c_i \in K$.

Below, A will be usually either $\mathbf{Z}$ or $\mathbf{Q}$; moreover in that case we define by $K\mathcal{E}_A^+$ the subring formed by those functions having only positive roots. Working in this domain causes no loss of generality: the assumption of positivity of the roots may be achieved by writing $2n + r$ in place of n and considering the cases of $r = 0, 1$ separately.

Normally we shall denote such functions by greek letters. Also, we define $l(\alpha) = \max_{c_i \neq 0} |a_i|$. Our results provide relations between algebraic properties of any such a function α, viewed as an element of the ring $\mathcal{E}_{\mathbf{Z}}$, and arithmetic properties of its value set $\alpha(\mathbf{N})$.

We shall say that α is nondegenerate if there is an expression (1) with no quotient $a_i/a_j, i \neq j$, equal to a root of unity. Observe that, even if α is degenerate, there exists a positive integer d such that, writing $n = r + md$, α is nondegenerate as a function of m on each of the d arithmetic progressions with $0 \leq r < d$ (in the case of rational roots, it clearly suffices to take $d = 2$). Therefore, restricting to nondegenerate functions causes no substantial loss of generality.

Observe that if $\alpha \in K\mathcal{E}_{\mathbf{Q}}$ is nondegenerate and $\alpha(n) = 0$ for infinitely many positive integers n (or even $\alpha(t_n) = 0$ for any sequence of real numbers $t_n \to \infty$ in case α has only positive roots), then $\alpha = 0$ identically; for a proof consider e.g. leading terms.

Althought in this paper we shall work with $A = \mathbf{Z}$ or $A = \mathbf{Q}$, similar results hold more generally for functions of the form (1), but where the a_i are allowed to be algebraic numbers subject to the (crucial) restriction that there is a unique root (with nonzero coefficient) having maximum modulus (similarly to [R-vdP]). Also, some of the results hold by allowing the c_i to be polynomial functions of n, often with the restriction that the coefficient of the exponential term of maximum modulus is constant. The proofs of such generalizations do not involve any substantially new argument however, so we have preferred to avoid 'half' generalizations and to limit ourselves to the stated cases, both for the sake of simplicity and in order to obtain neater statements.

Theorem 1. *For $\alpha, \beta \in \mathcal{E}_{\mathbf{Z}}^{+}$, assume that $\alpha(n)/\beta(n)$ is an integer for all n in an infinite sequence Σ. Then there exists $\zeta \in \mathcal{E}_{\mathbf{Z}}^{+}$ such that $\alpha = \beta \cdot \zeta$.*

In particular, the set of natural numbers n such that $\alpha(n)/\beta(n)$ is an integer differs by a finite set from a finite union of arithmetic progressions.

The last conclusion (which follows at once from the rest) reminds of the Skolem–Mahler–Lech theorem (see e.g. [M-vdP]).

Replacing $\mathcal{E}_{\mathbf{Z}}^{+}$ with $\mathcal{E}_{\mathbf{Z}}$ leads to a false statement, since β may be degenerate; consider e.g. the case $\alpha(n) = 1$, $\beta(n) = 2^n + (-2)^n + 1$.

We observe that an entirely similar proof allows to generalize Theorem 1 to functions of type (1), but where the c_i are polynomials in n (see also Remark 1 below). The conclusion will be that α/β is of the form (1), but where now the c_i's are *rational functions of n* (this is in a sense best possible: observe in fact that $(1/n)a^n - (1/n)a \in \mathbf{Z}$ for n a prime). As pointed out above, however, the methods do not apply to the general case when the a_i are algebraic numbers. As mentioned in the Introduction, the general case has been treated by van der Poorten in his solution of Pisot's conjecture, but with the assumption holding *for all $n \in \mathbf{N}$*, not merely in an infinite sequence.

Theorem 2. *Let $F \in \mathbf{Q}[X, Y]$ be absolutely irreducible, of degree d in Y, d' in X, and $\alpha \in \mathcal{E}_{\mathbf{Z}}^{+}$. Assume that the equation $F(\alpha(n), Y) = 0$ has infinitely many solutions with $n \in \mathbf{N}$ and $Y = y_n \in \mathbf{Z}$. Then all the solutions but finitely many are*

given by $y_n = g(\pm c^{1/d} b^{n/d} \lambda(n))$ *where* $g \in \mathbf{Q}[T]$ *has degree* d', $c \in \mathbf{Q}^*$, $b \in \mathbf{N}$, $\lambda \in \mathcal{E}_{\mathbf{Z}}^+$, *for a real determination (resp. real positive) of* $c^{1/d}$ *(resp.* $b^{1/d}$*). Also,* cb^n *must be a d-th power.*[1] *If there are infinitely many solutions corresponding to a given choice of the sign, denoted* $\epsilon = \pm 1$, *then* $F(\alpha(n), g(\epsilon c^{1/d} b^{n/d} \lambda(n))) = 0$ *identically. Moreover,* $\alpha(n) = f(\epsilon c^{1/d} b^{n/d} \lambda(n))$ *identically, where* $f \in \mathbf{Q}[T]$ *has degree d and vanishing second coefficient. Finally, the natural numbers n such that* $F(\alpha(n), Y) = 0$ *has an integral solution make up a finite union of arithmetical progressions, made exception for a finite set.*

In the particular but interesting case of the polynomial $F(X, Y) = X - Y^d$, we shall obtain easily the following

Corollary 1. *Let* α *be a function in* $\mathcal{E}_{\mathbf{Z}}^+$, $d \geq 2$ *be an integer. If* $\alpha(n)$ *is the d-th power of an integer for infinitely many* $n \in \mathbf{N}$, *the there exist integers* $r \in \{0, \ldots, d-1\}$, $b \geq 1$ *and an element* $\beta \in \mathcal{E}_{\mathbf{Z}}^+$ *such that*

$$\alpha(n) = b^{n-r} \beta^d(n).$$

In particular one at least of the d functions $m \mapsto \alpha_h(m) = \alpha(md + h)$, $(h = 0, \ldots, d-1)$ *is a d-th power in the ring* $\mathcal{E}_{\mathbf{Z}}^+$ *and* $\alpha(n)$ *is a perfect d-th power for any n in a suitable arithmetic progression.*

Remark 1. One could prove that under the hypothesis of Corollary 2, α is a perfect power in the ring $\mathcal{E}_{\bar{\mathbf{Q}}}$ as in the following example: put

$$\alpha(n) = 18^n + 2 \cdot 6^n + 2^n = (\sqrt{2^n} + 3^n \sqrt{2^n})^2.$$

Then α is a square in $\mathcal{E}_{\bar{\mathbf{Q}}}$, but not in $\mathcal{E}_{\mathbf{Z}}$; the integer $\alpha(n)$ is a square in $\mathbf{Z}$ if and only if n is even and the function $n \mapsto \alpha(2n)$ is a square in the ring $\mathcal{E}_{\mathbf{Z}}$. In such examples the first two leading terms cannot be relatively prime (see Corollary 3).

A few remarks are in order. First, the condition that F is absolutely irreducible is not restrictive: this is shown by factoring F into absolutely irreducible factors and recalling the well known fact that factors whose coefficients span a $\mathbf{Q}$-vector space of dimension ≥ 2 produce finitely many solutions. (Write such a factor in the form $G(x, y) = \sum_{i=1}^{h} a_i g_i(x, y)$ for suitable a_i linearly independent over $\mathbf{Q}$ and $g_i \in \mathbf{Q}[x, y]$. For a rational solution (x_0, y_0) we must have $g_i(x_0, y_0) = 0$ for all i and the conclusion easily follows by applying Bezout's theorem and recalling that g is absolutely irreducible.)

Second, as in Theorem 1, the condition that the involved roots are positive may be removed simply by considering separately even and odd values of n. Also, we remark that the solutions with $y \in \mathbf{Q}$ instead of $y \in \mathbf{Z}$ can be classified starting from the theorem: if $a(x)$ is the leading coefficient of F, it suffices to consider $a(\alpha(n))y$ in place of y and $a(x)^{\deg_y F - 1} F(x, y/a(x))$ in place of F. Theorem 2 can be given a 'quantitative version', i.e. a lower bound for the values of $|F(\alpha(n), y_n)|$; for simplicity we restrict ourselves to its corollary; we prove

[1] This holds precisely when n lies in certain arithmetic progressions modulo d.

Theorem 3. *Let $\alpha \in \mathcal{E}_{\mathbf{Z}}^{+}, d, r$ be integers with $d \geq 2, 0 \leq r < d$. Let us suppose that there exists a real number $\rho < 1 - (1/d)$, and infinitely many pairs of positive integers (n, y_n) such that $n \equiv r \bmod d$ and*

$$|\alpha(n) - y_n^d| \ll |\alpha(n)|^{\rho}. \tag{2}$$

Then there exists an integer b and integral valued functions $\beta, \gamma \in \mathcal{E}_{\mathbf{Z}}$ such that

(i) $\alpha(n) = b^{n-r}\beta^d(n) + \gamma(n)$;

(ii) $y_n = b^{(n-r)/d}\beta(n)$ *for all but finitely many solutions (n, y_n) of (2);*

(iii) $|\gamma(n)| \ll |\alpha(n)|^{\rho}$.

Remark 2. The exponent $1 - (1/d)$ is best possible: every real number α can be approximated by a perfect d-th power y^d with an error $O(\alpha^{1-(1/d)})$. On the other hand $\alpha(n) = a^n + (a-1)^n$ would not satisfy the conclusion, for $r = 0$, as far as the integer a is sufficiently large with respect to d.

Also, observe that for every $n \equiv r \pmod d$ the integer $b^{n-r}\beta(n)^d$ is a perfect d-th power; thus under the hypothesis of Theorem 3, (2) is satisfied for *every* n in such an arithmetic progression.

Corollary 2. *Let $\alpha \in \bar{\mathbf{Q}}\mathcal{E}_{\mathbf{Z}}^{+}$ be given by*

$$\alpha(n) = c_1 a_1^n + c_2 a_2^n + \ldots + c_k a_k^n$$

where $k \geq 2, c_1, \ldots, c_k$ are non-zero algebraic numbers, $a_1 > a_2 > \ldots > a_k > 0$ are integers with a_1, a_2 coprime. Then for every integer $d \geq 2$ and every real $\epsilon > 0$,

$$\min_{y \in \mathbf{Z}} |\alpha(n) - y^d| > |\alpha(n)|^{1 - \frac{1}{d} - \epsilon} \tag{3}$$

for large n (depending on α, d, ϵ). In particular the equation

$$\alpha(n) = y^d$$

has only finitely many solutions $(n, y) \in \mathbf{N}^2$.

The following theorem and its corollary give a positive answer to a generalization of a question of Yasumoto.

Theorem 4. *For $\alpha \in \mathcal{E}_{\mathbf{Z}}$ the following conditions are equivalent:*

(i) $\alpha(\mathbf{N})$ *is a Universal Hilbert Set;*

(ii) *there exist no integer $d \geq 2$, a polynomial $P(X) \in \mathbf{Q}[X]$ of degree d and an element $\beta \in \mathcal{E}_{\mathbf{Z}}$ such that $\alpha' = P(\beta)$, where $\alpha'(m) = \alpha(md)$.*

Remark 3. If condition (ii) is not satisfied then α is of the form $P(\beta)$ for any $\beta \in \mathcal{E}_{\bar{\mathbf{Q}}}$. We observe without proof that also the converse indeed holds (as can be seen by conjugating the equation $P(\beta) = \alpha$ and applying the **Fact** remarked below, after equation (6)). We also point out that condition (ii) is easy to test effectively. In particular it always holds for those α having multiplicatively independent roots, as we show in the following

Corollary 3. *Let $\alpha \in \mathcal{E}_{\mathbf{Z}}^{+}$ be given by* (1) *with $h \geq 2$ and $a_1, \ldots, a_h$ multiplicatively independent. Then the set $\alpha(\mathbf{N})$ is a universal Hilbert set.*

The condition of multiplicative independence is also necessary for $h = 2$; in the case $h = 3$, without this condition, there are counter-examples to the conclusion even if two of the roots are multiplicatively independent.

PROOFS

For the reader's convenience we state a version of Schmidt's Subspace Theorem due to H.P. Schlickewei; we have borrowed it from [Sch2, Theorem 1E, p. 178] (a complete proof requires also [Sch1]).

Subspace Theorem. *Let S be a finite set of absolute values of $\mathbf{Q}$, including the infinite one and normalized in the usual way (i.e. $|p|_v = p^{-1}$ if $v|p$). Extend each $v \in S$ to $\bar{\mathbf{Q}}$ in some way. For $v \in S$ let $L_{1,v}, \ldots, L_{N,v}$ be N linearly independent linear forms in N variables with algebraic coefficients and let $\epsilon > 0$. Then the solutions $\mathbf{x} := (x_1, \ldots, x_N) \in \mathbf{Z}^N$ to the inequality*

$$\prod_{v \in S} \prod_{i=1}^{n} |L_{i,v}(\mathbf{x})|_v < \|\mathbf{x}\|^{-\epsilon}$$

where $\|\mathbf{x}\| := \max\{|x_i|\}$, are contained in finitely many proper subspaces of $\mathbf{Q}^N$.

Actually, the statement in [Sch2] is more precise, and quantifies the number of relevant subspaces (and a finite number of remaining exceptions) in terms of the linear forms. Correspondingly, it is possible to quantify some of our results.

The following lemmas are rather simple consequences of the deep Subspace Theorem. Lemma 1 is actually a special case of Theorem 1 and is used in the proof of Lemma 2, which plays a crucial role throughout the paper.

Lemma 1. *Let $\zeta \in \mathcal{E}_{\mathbf{Q}}$ be nondegenerate and such that $\zeta(n) \in \mathbf{Z}$ for infinitely many $n \in \mathbf{N}$. Then $\zeta \in \mathcal{E}_{\mathbf{Z}}$.*

Proof. It plainly suffices to prove that if $\zeta \in \mathcal{E}_{\mathbf{Z}}$ is given by (1) (with $c_1, \ldots, c_h \in \mathbf{Z} \setminus \{0\}$) and for infinitely many $n \in \mathbf{N}$ we have $p^n | \zeta(n)$, where p is a given prime, then $p | a_i$ for all i. We may plainly assume that none of the a_i's is divisible by p and derive a contradiction if $h > 0$.

We apply the Subspace Theorem taking $N = h$ and S to consist of ∞, all absolute values dividing some a_i and p. For $v \in S$, $v \neq p$, we put $L_{i,v}(\mathbf{X}) = X_i$ for $i = 1, \ldots, h$. Otherwise we put $L_{1,p}(\mathbf{X}) = L(\mathbf{X}) := \sum_{j=1}^{h} c_j X_j, L_{i,p}(\mathbf{X}) = X_i$ for $i = 2, \ldots, h$.

We let n be such that $p^n | \zeta(n)$ and put $x_j := a_j^n$. We have

$$\prod_{v \in S} \prod_{i=1}^{h} |L_{i,v}(\mathbf{x})|_v = \prod_{i=2}^{h} \Big(\prod_{v \in S} |x_i|_v \Big) \cdot |L(x)|_p \prod_{v \in S \setminus \{p\}} |x_1|_v.$$

Observe that $|x_i|_v = 1$ for $v \notin S$ or for $v = p$, whence, by the product formula,

$$\prod_{v \in S} \prod_{i=1}^{h} |L_{i,v}(\mathbf{x})|_v = |L(x)|_p \leq p^{-n} < \max\{|x_i|\}^{-\epsilon}$$

for $\epsilon < \log p / \log(\max a_i)$. From the Subspace Theorem we deduce that one at least of finitely many nontrivial relations of the type $\sum_{i=1}^{h} b_i a_i^n = 0$ holds. However, since ζ is nondegenerate, each such relation may hold only for a finite number of values of n, a contradiction. □

Lemma 2. *Let K be a number field (embedded in $\mathbf{C}$) and $\xi \in K\mathcal{E}_{\mathbf{Q}}$ be nondegenerate. Let $z(n)$, for n lying in an infinite sequence $\sum$ of natural numbers, be integers such that $|z(n) - \xi(n)| \ll l^n$, where $0 < l < 1$. Then there exists $\zeta \in \mathcal{E}_{\mathbf{Z}}$ such that $z(n) = \zeta(n)$ for all but finitely many $n \in \sum$. Moreover any root of ζ is a root of ξ.*

Proof. Write $\xi(n) = \sum_{i=1}^{h} c_i (a_i/b)^n$ where $c_i \in K^*$ and the a_i, b are integers, $b > 0$, and the a_i/b are nonzero distinct rational numbers.

Let S be the set of absolute values of $\mathbf{Q}$ consisting of ∞ and all primes dividing some of the a_i or b. Extend each value in S to K in some way, the infinite value being extended so to coincide with the complex absolute value in the given embedding of K in $\mathbf{C}$. Define the linear forms $L_{i,v}$ for $v \in S$ and $i = 0, 1, \ldots, h$ as follows: $L_{0,\infty} = L := X_0 - \sum_{i=1}^{h} c_i X_i$, $L_{i,\infty} = X_i$ for $i = 1, \ldots, h$, while for $v \in S$, $v \neq \infty$, put $L_{i,v} = X_i$ for $i = 0, 1, \ldots, h$. Consider, for $n \in \sum$, the vector $\mathbf{x}_n = (b^n z(n), a_1^n, \ldots, a_h^n) \in \mathbf{Z}^{h+1}$. We have

$$\prod_{v \in S} \prod_{i=0}^{h} |L_{i,v}(\mathbf{x}_n)|_v = \prod_{i=1}^{h} \Big(\prod_{v \in S} |a_i^n|_v \Big) \cdot |L(\mathbf{x}_n)| \prod_{v \in S \setminus \{\infty\}} |b^n z(n)|_v.$$

By the product formula and the choice of S we have $\prod_{v \in S} |a_i^n|_v = 1$ for $i = 1, \ldots, h$. By our assumptions we have $|L(\mathbf{x}_n)| \ll (bl)^n$. Finally, S includes all finite absolute values nontrivial on b and the $z(n)$ are integers, so, by the product formula,

$$\prod_{v \in S \setminus \{\infty\}} |b^n z(n)|_v \leq \prod_{v \in S \setminus \{\infty\}} |b^n|_v = |b|^{-n}.$$

On the other hand $\|\mathbf{x}_n\| \ll A^n$ for some $A > 0$ independent of n. Combining such estimates we get

$$\prod_{v \in S} \prod_{i=0}^{h} |L_{i,v}(\mathbf{x}_n)|_v < \|\mathbf{x}_n\|^{-\epsilon}$$

for large $n \in \sum$, provided $\epsilon < \log(1/l)/\log A$. By the Subspace Theorem there exist finitely many nonzero rational linear forms $\Lambda_j(X_0, \ldots, X_h)$ such that each vector $\mathbf{x}_n$ as above is a zero of some Λ_j. Suppose first Λ_j does not depend on X_0. Then, if $\Lambda_j(\mathbf{x}_n) = 0$ we have a nontrivial relation $\sum_{i=1}^{h} u_i (a_i/b)^n = 0$, for constant rational u_i; however this can hold for a finite number of n at most, since ξ is supposed to be nondegenerate. Hence there is some rational linear form Λ,

depending on X_0, such that $\Lambda(\mathbf{x}_n) = 0$ holds for infinitely many $n \in \sum$. We may write

$$\Lambda(X_0, \ldots, X_h) = X_0 - \sum_{i=1}^{h} \upsilon_i X_i, \qquad \upsilon_i \in \mathbf{Q}$$

whence $z(n) = \zeta(n) := \sum_{i=1}^{h} \upsilon_i (a_i/b)^n \in \mathcal{E}_{\mathbf{Q}}$ for n lying in an infinite subsequence $\sum_1$ of $\sum$. Since $|z(n) - \xi(n)| \ll l^n$ for $n \in \sum$, where $l < 1$, we see that $\upsilon_i = c_i$ for i such that $|a_i/b| \geq 1$. By definition any root of ζ is a root of ξ. In particular ζ is nondegenerate and takes integer values on $\sum_1$ whence, by Lemma 1, $\upsilon_i = 0$ if a_i/b is not an integer, so $\zeta \in \mathcal{E}_{\mathbf{Z}}$. In particular $\upsilon_i = 0$ if $|a_i/b| < 1$. We conclude that the linear form Λ is determined in terms of ξ only and the lemma follows. □

Remark 4. A similar result holds (with an entirely analogous proof) by allowing the $c_i = c_i(n)$ to be constant times integer valued functions of n such that $|c_i(n)| \ll \exp(\epsilon n)$ for all $\epsilon > 0$. For instance, taking $c_i(n) = c_i \cdot n^{e_i}$, $c_i \in K, e_i \in \mathbf{N}$, we recover all cases with polynomial coefficients.

Proof of Theorem 1. Write $\beta(n) = \sum_{i=1}^{h} c_i a_i^n$ with nonzero c_i's and $a_1 > a_2 > \ldots > a_h > 0$. Put $\sigma := -\sum_{i=2}^{h} (c_i/c_1)(a_i/a_1)^n \in \mathcal{E}_{\mathbf{Q}}$. We have $\sigma(n) \ll |a_2/a_1|^n$, so we may write

$$\frac{1}{\beta(n)} = (c_1 a_1)^{-n}(1 - \sigma(n))^{-1} = (c_1 a_1)^{-n} \sum_{r=0}^{\infty} \sigma(n)^r$$

the expansion being convergent for large enough n. Say that $|\alpha(n)| \ll A^n$ for a positive number A and pick R such that $l := A|a_2/a_1|^R < 1$. Set $\eta(n) := (c_1 a_1)^{-n} \sum_{r=0}^{R} \sigma(n)^r \in \mathcal{E}_{\mathbf{Q}}$ and observe that $\alpha\eta \in \mathcal{E}_{\mathbf{Q}}$ is nondegenerate (because has positive roots), while $|\frac{\alpha(n)}{\beta(n)} - \alpha(n)\eta(n)| \ll l^n$. Setting $z(n) := \alpha(n)/\beta(n)$ for $n \in \sum$, $\xi := \alpha\eta$, we may thus apply Lemma 2, obtaining that for all but finitely many $n \in \sum$ we have $\alpha(n)/\beta(n) = \zeta(n)$, where $\zeta \in \mathcal{E}_{\mathbf{Z}}$ has only positive roots. Hence $\alpha - \beta\zeta \in \mathcal{E}_{\mathbf{Z}}$ has only positive roots and vanishes on an infinite set, whence must vanish identically. This proves the first part.

For completeness we give the easy argument for the last part. By the first part it suffices to show that the set $\{n \in \mathbf{N} | \gamma(n) \in \mathbf{Z}\}$, where $\gamma \in \mathcal{E}_{\mathbf{Z}}$, differs by a finite set from a finite union of arithmetic progressions. In turn, this is equivalent to derive the same conclusion for the set of $n \in \mathbf{N}$ such that $\phi(n) := \sum_{i=1}^{h} c_i a_i^n \equiv 0 \pmod{M}$; here the $a_i, c_i \in \mathbf{Z}$ and M is a given positive integer. It suffices to consider the case $M = p^k$, a prime power, and to restrict to $n \geq k$, which means that we may further assume that no a_i is a multiple of p. In that case the congruence $\phi(n + p^{k-1}(p-1)) \equiv \phi(n) \pmod{p^k}$ proves the assertion. □

Proof of Theorem 2. As e.g. in [D-Z], Siegel's theorem implies that all solutions but finitely many are given by

$$(2) \qquad \alpha(n) = f(x_n), \quad y_n = g(x_n), \quad n \in \sum$$

for some $x_n \in \mathbf{Q}$ (uniquely determined by (n, y_n) apart from a finite number of possible exceptions). Here $f, g \in \mathbf{Q}(T)$ are such that $\mathbf{C}(f(T), g(T)) = \mathbf{C}(T)$ and f has at most two poles. Accordingly, we consider two cases.

1st case: f has one pole. We may then assume the pole is ∞, i.e. that f is a polynomial with rational coefficients. The degree of f is the degree of the function X on the curve determined by F, i.e. $\deg f = \deg_Y F = d$. The equation $\alpha(n) = f(x_n)$ implies that x_n is a rational number with denominator independent of n. Since y_n is an integer, the rational function g takes integral values at the infinitely many 'almost' integral arguments x_n. It follows easily that g too must be a polynomial. As above, its degree must be the degree in X of F. As in [D-Z], after a translation on X we may write

$$f(X) = aX^d + R(X), \quad a \in \mathbf{Q}^*, \quad R \in \mathbf{Q}[X], \quad \deg R \leq d - 2.$$

Let us first deal with the solutions (n, y_n) such that x_n is positive, the argument being symmetrical in the other case. We may suppose that their set is still infinite and continue to denote by $\sum$ the set of corresponding n. Since we have infinitely many solutions (n, y_n), α is not constant, so $|\alpha(n)| \gg 2^n$. Since $f(x_n) = \alpha(n)$ we have $|x_n| \sim |\alpha(n)/a|^{1/d}$ and therefore, for $n \in \sum$,

$$(3) \qquad |x_n - (\frac{\alpha(n)}{a})^{1/d}| \ll |\alpha(n)^{\frac{1}{d}-1} x_n^{d-2}| \ll |\alpha(n)^{\frac{1-d}{d}+\frac{d-2}{d}}| \ll 2^{-n/d}$$

where we choose the d-th root which is real and positive[2]. Let $w > 0$ be a common denominator for all the x_n, put $z(n) = wx_n$ and write

$$\eta(n) := w^d \alpha(n)/a = \sum_{i=1}^{h} c_i a_i^n, \quad c_i \neq 0, \quad a_1 > a_2 > \ldots > a_h > 0.$$

Now we devide n by d: $n = md + r, 0 \leq r < d$, and partition $\sum$ in the d subsets $\sum_0 = \{n \in \sum : n \equiv 0 \pmod d\}, \ldots, \sum_{d-1} = \{n \in \sum : n \equiv d - 1 \pmod d\}$, where r is fixed. For given r and sufficiently large n we may write

$$\eta(n)^{1/d} = (\sum_{i=1}^{h} (w^d c_i/a) a_i^n)^{1/d} = w(c_1 a_1^r/a)^{1/d} a_1^m (1 + \sigma(n))^{1/d}$$

where $\sigma(n) = \sigma_r(n) := \sum_{i=2}^{h} (\frac{c_i}{c_1})(a_i/a_1)^n \in \mathcal{E}_{\mathbf{Q}}$[3], and where all involved d-th roots are those on the positive real line. Here we observe that for n large enough, $|\sigma(n) < 1|$. Since $a_1 > a_i$ for $i > 1$, for large m we may expand the d-th root by the binomial theorem and find for any positive integer R,

$$(1 + \sigma(n))^{1/d} = \sum_{j=0}^{R} \binom{1/d}{j} \sigma(n)^j + O(|a_2/a_1|^{Rn}) = \sum_{i=1}^{H} u_i b_i^n + O(|a_2/a_1|^{Rn})$$

---

[2] Which is certainly possible.

[3] Both as a function of n and of m.

where H is a positive integer (depending on R), while $\gamma(n) = \gamma_R(n) := \sum_{i=1}^{H} u_i b_i^n \in \mathcal{E}\mathbf{Q}$ is nondegenerate: in fact the b_i's are positive, since the a_i's are. We have

$$|\eta(n)^{1/d} - (w^d c_1 a_1^r/a)^{1/d} a_1^m \gamma(n)| \ll |a_1|^m |a_2/a_1|^{Rn}. \tag{4}$$

Choose R so large that $|a_1| \cdot |a_2/a_1|^{Rd} < 1$ and set $l := \max\{|a_1||a_2/a_1|^{Rd}, 1/2\}$, $\xi(m) := (w^d c_1 a_1^r/a)^{1/d} a_1^m \gamma(n)$. Then, by (3) and (4), for $n = dm + r \in \sum_r$,

$$|z(n) - \xi(m)| \ll l^m.$$

We may view the relevant functions as depending on m and, since ξ is nondegenerate (as it has positive roots), we may apply Lemma 2 as soon as $\sum_r$ is infinite; we let $\mathcal{R}$ be the set of such r. For $r \in \mathcal{R}$

$$z(n) = wx_n = \zeta_r(m)$$

where $\zeta_r \in \mathcal{E}_{\mathbf{Z}}$ (as a function of m) has roots which are a subset of those of ξ, whence is of type

$$\zeta_r(m) = (w^d c_1 a_1^r/a)^{1/d} a_1^m \delta_r(n)$$

where $\delta_r \in \mathcal{E}_{\mathbf{Q}}$.

We claim that δ_r does not depend on $r \in \mathcal{R}$. In fact we may write, for $r \in \mathcal{R}$ and large $n \in \sum_r$,

$$x_n = \zeta_r(m)/w = (c_1/a)^{1/d} a_1^{n/d} \delta_r(n) \tag{5}$$

where both $(c_1/a)^{1/d}$ and $a_1^{1/d}$ have the real positive determination. Write $n = td$ in (5). Then the right side of (5), as a function $\phi_r(t)$ of t (recall that δ_r has only positive roots, so this makes sense), satisfies formally $f(\phi_r(t)) = \alpha(dt)$, and the same relation thus must hold for all large positive t. But the equation $f(X) = T$ has at most one positive solution X, for large $|T|$, so, since $\phi_r(t)$ is positive for large $t > 0$, we have that $\phi_r(t)$ itself is independent of $r \in \mathcal{R}$ and our assertion follows. We may thus write, for large $n \in \sum$,

$$x_n = c^{1/d} a_1^{n/d} \delta(n)$$

where $c \in \mathbf{Q}^*$, $\delta \in \mathcal{E}_{\mathbf{Q}}$. Let $r \in \mathcal{R}$, $n \in \sum_r$ and write $n = dm + r$. Then $(ca_1^r)^{1/d} a_1^m \delta(dm + r)$ assumes integral values for infinitely many m. It follows at once that ca_1^r is the d-th power of a rational number and Lemma 1 implies that $a_1/v^d := b$, say, is an integer if $v > 0$ is a common denominator for the roots of δ. Hence we may write

$$x_n = c^{1/d} b^{n/d} \lambda(n) = \theta(n), \tag{6}$$

say, where $\lambda(n) = v^n \delta(n) \in \mathcal{E}_{\mathbf{Z}}$.

As to the solutions with negative x_n, either they are finite in number or we again may write $x_n = \theta'(n)$, where θ' has the same form as θ. Now we observe the following simple

Fact: If $f(\mu(n)) = f(\nu(n))$ identically, where $\mu, \nu \in \bar{\mathbf{Q}}\mathcal{E}_{\mathbf{Z}}$ are nonconstant and have positive roots, then $\mu = w\nu$, where w is a d-th root of unity, and $f(X) = f(wX)$.

To prove the claim observe that $1 < l(\mu) = l(\nu) = L$[4], say, and write the equation as $a(\mu^d - \nu^d) = R(\nu) - R(\mu)$. The right side has leading term at most L^{d-2}. The left side equals $a\prod_{w^d=1}(\mu - w\nu)$. If it is zero we are done. Otherwise the leading term of each factor but one is L. The leading term of the remaining factor is ≥ 1, since all the involved roots are integral. Hence the left side has leading term $\geq L^{d-1}$, a contradiction.

To apply the observation, recall that both $\theta(dn), \theta'(dn) \in \bar{\mathbf{Q}}\mathcal{E}_{\mathbf{Z}}$ are nonconstant and that $f(\theta(dn)) = f(\theta'(dn)) = \alpha(dn)$. Therefore $\theta(n) = -\theta'(n)$, since θ, θ' are distinct and have real coefficients and roots.

Observe that, by (6), x_n is rational precisely when n lies in certain arithmetic progressions modulo d and, by the proof of Corollary 1, wx_n will be integral for n in a union of arithmetical progressions, made exception for a finite set. For n such that wx_n is integral, we apply the same considerations to $g(x_n)$. We find that $g(x_n)$ will be integral for n lying in a set of the same form. This proves the theorem when f has one pole.

2nd case: f has precisely two poles. As in [D-Z] we let K be the field generated over $\mathbf{Q}$ by the two poles and conclude that it must be a real quadratic field. Allowing f to have coefficients in K we may assume that the poles are 0, ∞ and write

$$f(X) = F(X)/X^s = \frac{(F_0X^d + F_1X^{d-1} + \ldots + F_d)}{X^s}, \quad F_j \in K,$$
$$F_0F_d \neq 0, \quad s, d-s > 0.$$

Moreover, as proved in [D-Z], x_n must be of the form

$$x_n = tu^e$$

where $t \in K$ has finitely many possibilities, $u > 1$ is the fundamental unit of K and $e \in \mathbf{Z}$. Let us study the solutions with fixed $t \neq 0$ and $e \geq 0$, the argument being symmetrical in case $e < 0$ (as in [D-Z]). If we write α in the form (1) with nonzero c_i's and $a_1 > a_2 > \ldots > a_h > 0$, the equation $f(x_n) = \alpha(n)$ implies

$$|F_0t^{d-s}u^{e(d-s)} - c_1a_1^n| \ll \max\{u^{e(d-s-1)}, a_2^n\}.$$

Arguing as in [D-Z] we observe that, since $u \neq a_1$, the theory of linear forms in three logarithms provides the bound

$$|F_0t^{d-s}u^{e(d-s)} - c_1a_1^n| \gg \max\{u^{e(d-s)}, a_1^n\}^{1-\epsilon}$$

for any $\epsilon > 0$. Choosing $1 - \epsilon > \max\{\frac{\log a_2}{\log a_1}, \frac{d-s-1}{d-s}\}$ we obtain that both n and e are bounded. Hence only finitely many solutions may arise in this way.

This completes the proof of Theorem 2. □

---

[4] $l(\alpha)$ denotes as before the leading root of α.

Remark 5. As pointed out above, the method of proof leads of generalizations. For instance we could allow $\alpha(n)$ to be of the form $a_1^n + c_2(n)a_2^n + \ldots + c_h(n)a_h^n$, where the $c_i(n)$, $i = 2, \ldots, h$ are polynomials with complex algebraic coefficients and the a_i are complex algebraic numbers such that $|a_1| > \max_{i \geq 2}\{|a_i|\}$. We briefly indicate the main necessary modifications, which are rather small. In the first place an analogue of Lemma 2 will be needed, where $z(n)$ will be now an algebraic integer in some fixed number field L and ξ will be of the same form as α. (The analogue is needed mainly due to the fact that the a_i's are no more supposed to be rational. The complication caused by the polynomial coefficients is of a milder nature – see also Remark 4.) Again the Subspace Theorem (in a general formulation for solutions in a number field) will yield a similar conclusion, but we shall now need a better upper bound for l to kill the contribution given by the $z(n)$ at the remaining archimedean absolute values. (This contribution would appear in the analogue of the second displayed formula in the proof of Lemma 2.) In particular, we will need an exponential estimate A^n for the conjugates of $z(n)$ and a corresponding upper bound for l (it will suffice if $l < A^{-[L:\mathbf{Q}]}$)[5].

Second, we again will have to consider the equation $f(x_n) = \alpha(n)$, where now $x_n \in L$ will have fixed denominator. To follow the present proof, i.e. to apply to this equation the mentioned analogue of Lemma 2, we will have to approximate x_n by functions of the required form, but, due to the observation just made, we will need an exponential estimate for the conjugates of x_n and a sufficiently good error term. The first goal is achieved just by conjugating $f(x_n) = \alpha(n)$. The second one, by considering sufficiently many terms in the full Puiseux expansions in $T^{1/d}$ of the solutions of $f(X) = T$. (Taking just the d-th root, as in the above proof, corresponds to stopping at the constant term.) Another point to be observed is that also the case of two poles will lead sometimes to infinitely many solutions (look e.g. at Pell's equation).

Proof of Corollary 1. Applying Theorem 2 to the polynomial $F(X, Y) = X - Y^d$ we obtain the existence of $\lambda \in \mathcal{E}_{\mathbf{Z}}^+$ and $g \in \mathbf{Q}[X]$ such that $\alpha(n) = (g(\epsilon c^{1/d} b^{n/d} \lambda(n)))^d$ identically, for some $\epsilon \in \{\pm 1\}$, some positive rational c and some $b \in \mathbf{N}$. Since however by the same Theorem 2 the degree of g must be $\deg_X F = 1$ in the present case, we have identically

$$\alpha(n) = (Ac^{1/d} b^{n/d} \lambda(n) + B)^d$$

for some come constants $A, B \in \mathbf{Q}$. Moreover, again by Theorem 2, there exists a polynomial f of degree d with vanishing second coefficient such that $\alpha(n) = f(c^{1/d} b^{n/d} \lambda(n))$; since λ is non degenerate (having positive roots), it follows that $f = g^d$, hence $B = 0$. Therefore we have $\alpha(n) = cb^n (A\lambda(n))^d$. Taking n such that $\alpha(n)$ is a d-th power we see that we may write $c = b^{-r} c_1^d$ for some

[5] It is to be observed that without any such assumption, no analogue of Lemma 2 would hold generally.

natural number r and some rational c_1. Defining $\beta(n) := c_1 A\lambda(n)$ gives what we need. □

Proof of Theorem 3. We suppose that inequality (2) is satisfied for infinitely many pairs (n, y_n). Since the roots of α are positive we may also assume, changing sign if necessary, that $\alpha(n) > 0$ for all large n. We factorize

$$\alpha(n) - y_n^d = (\alpha(n)^{1/d} - y_n) \cdot (\alpha(n)^{(d-1)/d} + \alpha(n)^{(d-2)/d} y_n + \ldots + y_n^{d-1}).$$

Here, as in the proof of Theorem 2, we take the positive real determination of the d-th root. Since the last factor is $\geq |\alpha(n)|^{(d-1)/d}$, we get from (2)

$$|\alpha(n)^{1/d} - y_n| \ll |\alpha(n)|^{-\epsilon},$$

for any $\epsilon < 1 - \frac{1}{d} - \rho$. Write $\alpha(n) = \sum_{i=0}^{k} c_i a_i^n$ with $a_0 > \ldots > a_k > 0$. Applying the binomial theorem as before, we expand the function $(1+x)^{1/d}$ around the origin:

$$(1+x)^{1/d} = \sum_{j=0}^{R} \binom{1/d}{j} x^j + O(x^R)$$

where $R \geq 1$ is any integer. For $\alpha(n)^{1/d}$ we obtain

$$\alpha(n)^{1/d} = (c_0 a_0^n)^{1/d} \left[1 + \sum_{j=1}^{R} \binom{1/d}{j} \cdot \left(\sum_{i=1}^{k} \frac{c_i a_i^n}{c_0 a_0^n} \right)^j + O\left(\frac{a_1^{nR}}{a_0^{nR}} \right) \right].$$

In particular, for $R > \max\{1, (\frac{1}{d} + \epsilon)(\log a_0/(\log a_0/a_1))\}$ the remainder term $O((a_1^{nR}/a_0^{nR}) \cdot a_0^{n/d})$ is $\ll a_0^{-n\epsilon} \ll |\alpha(n)|^{-\epsilon}$. Now putting

$$\alpha'(m) = (c_0 a_0^r)^{1/d} \cdot a_0^m \left[1 + \sum_{j=1}^{R} \binom{1/d}{j} \cdot \left(\sum_{i=1}^{k} \frac{c_i a_i^{md+r}}{c_0 a_0^{md+r}} \right)^j \right]$$

where again we write $n = md + r$ with $n \in \mathbf{N}$, $r \in \{0, \ldots, d-1\}$; we see that $\alpha' \in \mathbf{Q}((c_0 a_0^r)^{1/d}) \mathcal{E}_{\mathbf{Q}}$ and

$$|a'(m) - y_{md+r}| < l^m$$

for infinitely many m and for a suitable $l < 1$ (in fact any real $l > a_0^{-\epsilon}$ would work). Applying Lemma 2 we obtain the existence of $\beta' \in \mathcal{E}_{\mathbf{Z}}^+$ with $\beta'(m) = y_{md+r}$ for all but finitely many m such that $(md + r, y_{md+r})$ satisfies (2). Let β' be given by

$$\beta'(m) = \sum_{i=0}^{h} c_i b_i^m, \quad b_0 > b_1 > \ldots > b_h > 0$$

then put

$$\beta_1(n) = \sum_{i=0}^{h} c_i b_i^{-r/d} b_i^{n/d}.$$

Then clearly $\beta_1(md + r) = \beta'(m)$ for every m; moreover if we put

$\gamma(n) = \alpha(n) - \beta_1^d(n)$ then properties (i), and (ii) of Theorem 3 would be proved provided that the exponential functions β_1, γ verify

(i) β_1 is of the form $b^{n/d}\beta(n)$ with $\beta \in \mathcal{E}_{\mathbf{Z}}$ and $b \in \mathbf{Z}$,

(ii) $\gamma \in \mathcal{E}_{\mathbf{Z}}$.

It is easy to see that (ii) is a consequence of (i), so we have only to prove (i). But from the fact that $\rho < 1 - \frac{1}{d}$ we obtain for $n \equiv r(\mathrm{mod}.\, d)$

$$|\beta_1^d(n) - \alpha(n)| < |\alpha(n)|^{\rho} \ll |\beta_1^{d-1}(n)| \tag{7}$$

and this must also hold for any n. Observe that by expanding β_1^d we get a linear combination of terms $((b_0^{1/d})^{k_0} \ldots (b_h^{1/d})^{k_h})^n$ with $k_0 + \ldots + k_h = d$. The terms with $k_0 = d$ or $k_0 = d - 1$, namely the terms b_0 or $(b_0^{(d-1)/d} b_i^{1/d})^n$, are all distinct and larger than any other term. Hence they cannot be cancelled out and must actually appear as roots of β_1^d. Also, they are obviously larger than any root of β_1^{d-1}. Therefore, by inequality (7), all such terms must appear in the development of α, whence they are integers. This means that $b_0^{-1/d} b_i^{1/d}$ are rational for every $i = 0, \ldots, h$, so the function $\beta(n) = b_0^{n/d}\beta_1(n)$ belongs to $\mathcal{E}_{\mathbf{Z}}$. This achieves the proof of (i) and (ii). To prove (iii), just notice that $|\gamma(n)| < |\alpha(n)|^{1-\frac{1}{d}-\epsilon}$ for large values of n with $n \equiv r(\mathrm{mod}.\, d)$, so it holds for every large n. □

Proof of Corollary 2. We argue by contradiction. If (3) does not hold, then for infinitely many pairs (n, y_n)

$$|\alpha(n) - y_n^d| < |\alpha(n)|^{1-\frac{1}{d}-\epsilon};$$

then Theorem 3 gives the existence of exponential functions $\beta, \gamma \in \mathcal{E}_{\mathbf{Z}}$ and integers r, b with

$$\gamma(n) = \alpha(n) - b^{-r} b^n \beta(n)^d$$

and $|\gamma(n)| \ll |\alpha(n)|^{1-\frac{1}{d}-\epsilon}$. Let us write

$$\beta(n) = d_0 b_0^n + \ldots + d_h b_h^n$$

for integers b_i's in decreasing order. Then

$$\beta^d(n) = d_0^d (b_0^d)^n + (d_0^{d-1} d_1)(b_0^{d-1} b_1)^n + o((b_0^{d-1} b_1)^n);$$

since $\gamma(n) = o\left(\alpha(n)^{1-\frac{1}{d}}\right)$, the first two leading terms of α are the leading terms of β^d, which are not relatively prime. This contradiction proves the corollary. □

Proof of Theorem 4. The implication *(i)* ⇒ *(ii)* is clear: if such a polynomial $P(X)$ exists, then the polynomial $F(X, Y) = P(X) - Y$, irreducible in $\mathbf{Q}[X, Y]$, defines by specialization $Y \mapsto \alpha(n)$ for any n in an arithmetic progression a reducible polynomial in $\mathbf{Q}[X]$, having a rational root $\beta(n)$.

Now let us see that condition (ii) is also sufficient. Classical reduction steps (see e.g. [Schi]) show that it is enough to prove that, for all absolutely irreducible $F \in \mathbf{Q}[X, Y]$ of degree $d \geq 2$ in Y, the equation $F(\alpha(n), Y) = 0$ has an

integral solution $Y = y_n$ only for finitely many n. Suppose this does not hold for a certain F and apply Theorem 2. We conclude that the exist an identical equation $\alpha(n) = f(c^{1/d} b^{n/d} \lambda(n))$, where $f \in \mathbf{Q}[T]$ has degree d, $c \in \mathbf{Q}$, $b \in \mathbf{N}$, $\lambda \in \mathcal{E}_{\mathbf{Z}}^{+}$. Put $\beta(n) := b^n \lambda(nd)$, $P(T) := f(c^{1/d} X)$. Then $\alpha'(n) := \alpha(nd) = P(\beta(n))$. From this equation it is easy to see that P has rational coefficients (by e.g. conjugating or using decreasing induction on the terms of various degrees), so (ii) would be contradicted. □

Proof of Corollary 3. We show that condition (ii) of Theorem 4 is verified for α. Since any substitution $m \mapsto md$ does not affect the assumptions of corollary we have only to show that α is not of the form $P(\beta)$. This follows from the following

Lemma 3. *For any polynomial $P(X) \in \mathbf{C}[X]$ of degree $d \geq 2$ and any $\beta \in \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+}$ with positive roots, either $\alpha = P(\beta)$ has only one root or its roots are multiplicatively dependent.*

Proof. Suppose by contradiction that $\alpha(n)$ is given by (1) with $h \geq 2$ and $a_1, \ldots, a_h$ multiplicative independent; we can also suppose without loss of generality, by applying a suitable translation, that P has a vanishing second coefficient. Let $\{p_1, \ldots, p_k\}$ be the set of primes dividing $a_1 \ldots a_h$ and $\mathbf{i}_1, \ldots \mathbf{i}_h$ be the vectors in $(\mathbf{N} \cup \{0\})^k$ of the exponents in the factorization of $a_1, \ldots, a_h$. That is, for $j \in \{1, \ldots, h\}$, we have

$$a_j = p_1^{i_{j1}} \ldots p_k^{i_{jk}},$$

where $\mathbf{i}_j = (i_{j1}, \ldots, i_{jk})$. The multiplicative independence of $a_1, \ldots, a_h$ is equivalent to the linear independence (over the rationals) of $\mathbf{i}_1, \ldots, \mathbf{i}_h$. Hence, under this hypothesis, there exists a vector $\mathbf{l} = (l_1, \ldots, l_k) \in \mathbf{Z}^k$ and a positive integer N such that $< \mathbf{i}_j, \mathbf{l} > = N$ for all j ($< ., . >$ standing for the usual scalar product). Since the functions $n \mapsto p_i^n$ are algebraically independent, there exists a morphism of $\mathbf{C}$-algebras $\Phi : \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+} \to \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+}[T, T^{-1}]$ sending the function $p_i^n \mapsto T^{l_i} p_i^n$, such that $\Phi(\alpha) = T^N \alpha$. From $\alpha = P(\beta)$ we get

$$\alpha T^N = P(f(T)),$$

where $f(T) = \Phi(\beta) \in \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+}[T, T^{-1}]$ must in fact be a polynomial in T. Write $P(X) = a \cdot \prod_{i=1}^{d} (X - r_i), a, r_1, \ldots, r_d \in \mathbf{C}$. Then $\alpha T^N = a \cdot \prod_{i=1}^{d} (f(T) - r_i)$; whence all the r_i must be equal ($f(T) - r$ is coprime with $f(T) - r'$ if $r \neq r'$.) Then P is a constant time a pure power: $P(X) = a \cdot X^d$. We then obtain $\alpha = a \cdot \beta^d$, with $a \in \mathbf{C}$. By choosing $\mathbf{l} = (l_1, \ldots, l_k) \in \mathbf{Z}^k$ such that $< \mathbf{i}, \mathbf{l} > = N$ and $< \mathbf{i}_j, \mathbf{l} > = M$ for $j = 2, \ldots, h$, where $M > N \geq 1$ we obtain similarly as above another morphism $\Psi : \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+} \to \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+}[T, T^{-1}]$ such that $\Psi(\alpha) = \alpha_1 T^N + \alpha_2 T^M$ with $\alpha_1, \alpha_2 \in \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+} \setminus \{0\}$. Then

$$\alpha_1 T^N + \alpha_2 T^M = (g(T))^d$$

with $g(T) = \Psi(f(T)) \in \mathbf{C}\mathcal{E}_{\mathbf{Z}}^{+}[T]$, and a contradiction arises easily from the fact that all the roots of the right hand term have multiplicity $\geq d \geq 2$. This proves Lemma 3 and Corollary 4. □

REFERENCES

[D-Z] Dèbes, P. and U. Zannier – Universal Hilbert subsets. To appear in Math. Proc. Camb. Phil. Soc.

[M-vdP] Myerson, G. and A.J. van der Poorten – Some problems concerning recurrence sequences. American Math Monthly **102**, 698–705 (1995).

[P-Z1] Perelli, A. and U. Zannier – Arithmetic properties of certain recurrence sequences. J. Austral. Math. Soc. **37**, (Series *A*), 4–16 (1984).

[P] Pourchet, Y. – Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles. C. R. Acad. Sci. Paris **288**, Série *A*, 1055–1057 (1979).

[R-vdP] Rumely, R.S. and A.J. van der Poorten – A note on the Hadamard k-th root of a rational function. J. Austral. Math. Soc. **43**, (Series *A*), 314–327 (1987).

[Schi] Schinzel, A. – Selected topics on polynomials. The University of Michigan Press, Ann Arbor (1982).

[Sch1] Schmidt, W.M. – Diophantine Approximation. Springer Verlag, LN **785** (1980).

[Sch2] Schmidt W.M. – Diophantine Approximations and Diophantine Equations. Springer Verlag, LN **1467** (1991).

[S-S] Shorey, T.N. and C.L. Stewart – Pure Powers in Recurrent Sequences and Some Related Diophantine Equations. J. Number Theory **27**, 324–352 (1987).

[Y] Yasumoto, M. – Hilbert Irreducibility Sequences and Nonstandard Arithmetic. J. Number Theory **26** (1987).

[vdP1] van der Poorten, A.J. – Some facts that should be better known, especially about rational functions. Macquarie Mathematics Report No. **88-0022**, June (1988).

[vdP2] van der Poorten, A.J. – Solution de la conjecture de Pisot sur le quationt de Hadamard de deux fractions rationnelles. C. R. Acad. Sci. Paris, t. **306**, Série I, 97–102 (1988).

Received January 27, 1997; revised September 8, 1997