A proof of Pisot's d^{th} root conjecture

By Umberto Zannier

Abstract

Let $\{b(n) : n \in \mathbf{N}\}$ be the sequence of coefficients in the Taylor expansion of a rational function $R(X) \in \mathbf{Q}(X)$ and suppose that $b(n)$ is a perfect d^{th} power for all large n. A conjecture of Pisot states that one can choose a dth root $a(n)$ of $b(n)$ such that $\sum a(n)X^n$ is also a rational function. Actually, this is the fundamental case of an analogous statement formulated for fields more general than $\mathbf{Q}$. A number of papers have been devoted to various special cases. In this note we shall completely settle the general case.

Introduction

Let $R(X) = \sum_{n=0}^{\infty} b(n)X^n$ represent a rational function in $k(X)$, where char $k = 0$. (This is equivalent to a linear recurrence $\sum_{i=0}^{t} c_i b(n + i) = 0$, valid for large n.) Suppose that there exists a field $F \supset k$, finitely generated over $\mathbf{Q}$, such that $b(n)$ is a perfect d^{th} power in F for all large n. Then, it is a generalization of a conjecture attributed to Pisot (see e.g. [B], [RvdP] and §6.4 of [vdP1]) that there exists a sequence $\{a(n)\}$ such that $a(n)^d = b(n)$ for large n and $\tilde{R}(X) := \sum a(n)X^n$ is again rational.

Let $\beta_1, \ldots, \beta_h$ be the poles of $R(X)$, of multiplicities $m_1, \ldots, m_h$ respectively. Then it is well-known that for large n, $b(n)$ may be expressed as an exponential polynomial

$$(1) \qquad b(n) = \sum_{i=1}^{h} B_i(n)\beta_i^n$$

for polynomials $B_i \in \bar{k}[T]$ of degrees resp. $\leq m_i - 1$. (The β_i are classically called the *roots* of the exponential polynomial.) The conjecture predicts that under the stated assumptions the right side of (1) is identically the dth power of a function of the same form.

Rumely and van der Poorten [RvdP, §7] refer to the above statement as the *Generalized Pisot d^{th} root conjecture*. In [RvdP, §6] they use specialization arguments to prove that it is actually sufficient to deal with the case when k is

a number field. Also, generalizing a previous argument in [PZ], they prove that it is also possible to assume $m_i = 1$ for $1 \le i \le h$, namely that all the B_i's are constant (see [RvdP, Prop. 3]). Theorem 2 of [RvdP] collects these facts. They prove in Theorem 1 that in the fundamental number field case, the conjecture is true provided there exists a unique pole β_i of maximal or minimal absolute value. This condition, though rather weak, plays a crucial role at one step in their arguments. In fact, the same type of condition, leading to the so-called *dominant root method*, had presented an obstacle also in several related investigations (e.g. on Pisot conjecture on the *Hadamard quotient*, studied by Pisot and finally solved by van der Poorten [vdP2] after an incomplete argument by Pourchet [P].) For a proof of the dth root conjecture under different additional assumptions, see [B].

Here we shall completely settle the fundamental case when k is a number field, by means of a method entirely different from those mentioned above. As we have noticed, the results in [RvdP] allow us to assume that the B_i are constant without loss of generality. However, since this assumption would only slightly simplify our proofs, we shall avoid it. By enlarging k we may suppose that $F = k$ and that the condition on $b(n)$ is true for all n. We have the following

THEOREM. *Let* $b(n) = \sum_{i=1}^{h} B_i(n)\beta_i^n$ *be an exponential polynomial, where* $B_i \in k[T]$ *and* $\beta_i \in k$, *for a field* k *finitely generated over* $\mathbf{Q}$. *Assume that* $b(n)$ *is a* d^{th} *power in* k *for* $n \in \mathbf{N}$. *Then there exists an exponential polynomial* $a(n) = \sum_{i=1}^{r} A_i(n)\alpha_i^n$, $A_i \in \bar{k}[T]$, $\alpha_i \in \bar{k}$, *such that* $b(n) = a(n)^d$ *for all* $n \in \mathbf{N}$.

By what we have recalled above, it is sufficient to deal with the case when k is a number field, as we shall assume from now on. We remark that [CZ] contains proofs of analogous statements assuming the much weaker fact that $b(n)$ *is a* d^{th} *power for infinitely many* $n \in \mathbf{N}$. However, that method again requires (at least) the existence of a dominant β_i. On the other hand, the present method, of completely different nature, does not yield results under the weaker assumption.

Remark 1. The proof will give in fact the (apparently) stronger result stating that if the conclusion is not true, we may find an arithmetic progressions $\mathcal{A}$ and a prime ideal π of k such that $b(n)$ is not a dth power modulo π, for each $n \in \mathcal{A}$. In particular, it suffices that the assumption holds for a set of positive integers intersecting every arithmetic progression.

Remark 2. It should be rather straightforward to adapt the arguments to more general equations $f(y, b(n)) = 0$, $f \in k[x, y]$, monic in y. Assuming that for each $n \in \mathbf{N}$ the equation has a solution in k, one would obtain that there

exists an identical solution which is an exponential polynomial. (This would provide in particular a proof of conjectures mentioned in [vdP3].)

Proof of theorem. Here is a (very brief) outline of the method. First, we shall look at what happens upon replacing in the exponential polynomial the numbers β_i^n with suitable roots of unity of order dividing $p-1$, for a sufficiently large prime $p \equiv 1 \pmod{d}$. Assuming the conclusion to be false, we shall use congruences modulo p to show that the resulting algebraic number will not be a dth power in the corresponding cyclotomic extension of k. (More precisely, we shall use the Lang-Weil theorem for the number of points on varieties over finite fields.) Now Cebotarev's theorem will show that, for infinitely many prime ideals, the reduction of this algebraic integer will continue not to be a dth power in the residue field. By taking a suitable $n \in \mathbf{N}$, the effect of the reduction will just consist of replacing the mentioned roots of unity with the β_i^n. This will contradict the assumption that $b(n)$ is a dth power in k.

To begin the proof, we point out at once that it suffices to deal with the case when d is a prime number and k is normal over $\mathbf{Q}$, as we shall assume from now on.

We may assume that no β_i is zero, and we consider the multiplicative subgroup $\Gamma \subset k^*$ generated by the β_i's. We begin by proving that it is sufficient to deal with the case when Γ is torsion-free. Let N be the order of the torsion subgroup of Γ. For $r = 0, 1, \ldots, N-1$ we consider the exponential polynomial $b_r(n) := b(r + Nn)$. For an exponential polynomial $c(n) = \sum c_i(n)\gamma_i^n$, choose in some way N^{th} roots $\tilde{\gamma}_i$ for the γ_i's and put $\tilde{c}(n) = \sum c_i(\frac{n}{N})\tilde{\gamma}_i^n$. We have $\tilde{c}(nN) = c(n)$ for $n \in \mathbf{N}$.

Suppose now that we can prove the theorem for each $b_r(n)$, so that $b_r(n) = a_r(n)^d$ for suitable exponential polynomials $a_r(n)$, $0 \le r \le N-1$. Define $\phi(n) = (1/N)\sum_{\theta^N=1} \theta^n$, so $\phi(n)$ is 1 for $N|n$ and 0 otherwise. Then we find that

$$b(n) = \left(\sum_{r=0}^{N-1} \phi(n-r)\tilde{a}_r(n-r) \right)^d.$$

In fact, if $n = s + mN$, for integers m, s, $0 \le s \le N-1$, the right side equals $\tilde{a}_s(mN)^d = a_s(m)^d = b(s+mN) = b(n)$, as required. Since the expression into brackets in the right side is plainly an exponential polynomial, the theorem is proved for $b(n)$.

Therefore it suffices to prove the theorem for the $b_r(n)$. On the other hand, the roots of $b_r(n) = b(r + nN)$ are just the β_i^N, which clearly generate in k^* the torsion-free group Γ^N. Hence the above claim follows. Namely, in proving the theorem we can and shall assume that Γ is torsion-free.

We let $\gamma_1, \ldots, \gamma_r \in k^*$ be multiplicatively independent (i.e. free) generators for Γ. Then we may write

$$(2) \qquad\qquad b(n) = f(n, \gamma_1^n, \ldots, \gamma_r^n),$$

for a suitable rational function $f \in k[X_0, X_1, X_1^{-1}, \ldots, X_r, X_r^{-1}]$. Multiplying by a power of $(\gamma_1 \cdots \gamma_r)^{nd}$ does not affect the assumptions nor the conclusion, so we can assume that f is a polynomial in all the variables.

At this point we observe a technical fact, which shall be useful later. Let D be a positive integer and consider the polynomial

$$F(X_0, X_1, \ldots, X_r) = F_D(X_0, X_1, \ldots, X_r) := f(X_0, X_1^D, \ldots, X_r^D).$$

Suppose first that F is a dth power in $\overline{\mathbf{Q}}[X_0, \ldots, X_r]$, say $F = G^d$. Observe that F is invariant by every substitution ϕ, $X_i \mapsto \theta_i X_i$ where θ_i are D^{th} roots of unity and $\theta_0 = 1$. Therefore we have, for each such ϕ,

$$\phi(G) = \mu_\phi G,$$

where $\mu_\phi^d = 1$. From these equations we see at once that the quotient of any two monomials in G is invariant by all the substitutions ϕ. This means that G is of the form $X_1^{a_1} \cdots X_r^{a_r} H(X_0, X_1^D, \ldots, X_r^D)$, for $a_1, \ldots, a_r \in \mathbf{Z}$ and a polynomial $H \in \overline{\mathbf{Q}}[X_0, \ldots, X_r]$. Since $F = G^d$, we have $D | a_i d$ for all $i \geq 1$. Therefore $f(X_0, \ldots, X_r)$ may be written in the form $X_1^{b_1} \cdots X_r^{b_r} H^d(X_0, \ldots, X_r)$, where $a_i d = b_i D$. Now, if α is a dth root of $\gamma_1^{b_1} \cdots \gamma_r^{b_r}$ in $\bar{k}$, equation (2) gives $b(n) = (\alpha^n H(n, \gamma_1^n, \ldots, \gamma_r^n))^d$, providing a proof of the theorem.

In conclusion, we may suppose that for each positive integer D, F_D is not a dth power in $\overline{\mathbf{Q}}[X_0, \ldots, X_r]$. We proceed to derive a contradiction.

Before going on we shall establish the multiplicative independence of suitable elements of k^*, modulo certain powers. The following lemma will be helpful; it appears (in a more general form) in a forthcoming joint paper with E. Bombieri and D. Masser [BMZ, L. 6] (and perhaps elsewhere), but for completeness we give here the short proof of the case we need.

LEMMA 1.   *Let ℓ be a prime number such that k does not contain a primitive ℓ^{th} root of unity. Suppose that u lies in an abelian extension of k and that $u^\ell \in k^*$. Then there exists a root of unity ω such that $\omega u \in k^*$.*

Proof. We have $g(u) = 0$, where $g(X) := X^\ell - u^\ell \in k[X]$. Suppose first that g is reducible over k. Then it is classical that $u^\ell = v^\ell$ for some $v \in k^*$. In this case $u = \zeta v$ for some ℓ^{th} root of unity ζ, concluding the proof.

Therefore we may assume that g is irreducible, so $[k(u) : k] = \ell$. Observe that $k(u)/k$ is Galois, as a subextension of an abelian extension of k. Let σ

be a nontrivial element of the Galois group. Since $u^\ell \in k$ we have $\sigma(u) = \zeta u$ for some nontrivial (whence primitive) ℓ^{th} root of unity ζ. This shows that $\zeta \in k(u)$. Therefore $[k(\zeta) : k]$ divides both $[k(u) : k] = \ell$ and $[\mathbf{Q}(\zeta) : \mathbf{Q}] = \ell - 1$, so $\zeta \in k$, a contradiction.   □

We now choose once and for all a large prime number β, such that $\beta, \gamma_1, \ldots, \gamma_r$ are multiplicatively independent. Also, let $h_1, \ldots, h_r$ be integers (which shall be specified later) and put

$$(3) \qquad\qquad \delta_i := \gamma_i \beta^{-h_i}, \qquad i = 1, \ldots, r.$$

Define $\mathbf{Q}_c$ to be the maximal cyclotomic extension of $\mathbf{Q}$ and $k_c := k\mathbf{Q}_c$. We have

LEMMA 2. *There exists a number L depending only on k and $\beta, \gamma_1, \ldots, \gamma_r$, with the following property. Let M be a positive integer and let ℓ be a prime number $> L$. Then β^M does not lie in the group generated by the δ_i and by $k_c^{*\ell M}$.*

Proof. Assume that the conclusion is false and that we have integers $a_1, \ldots, a_r$ such that

$$\beta^M \delta_1^{a_1} \cdots \delta_r^{a_r} = v^{\ell M},$$

where $v \in k_c^*$. Suppose also that this M is minimal among such equalities. We write it as

$$\beta^{a_0} \gamma_1^{a_1} \cdots \gamma_r^{a_r} = v^{\ell M},$$

where $a_0 = M - \sum_{i=1}^r a_i h_i$. The left side lies in k^*. Therefore, if ℓ is large enough with respect to k, we may apply Lemma 1 and suppose that $u := v^M = \omega\nu$ for a root of unity ω and a $\nu \in k^*$.

Let Q be a positive integer. By a well-known easy result in diophantine approximation, we may find a positive integer $b \leq Q^{r+1}$ and integers p_i such that, putting $b_i := ba_i - \ell p_i$, we have $|b_i| \leq \ell Q^{-1}$ for $i = 0, 1, \ldots, r$. (Apply, e.g., Thm. 1A, p. 27 of [Schm1].)

Raising both sides of the last displayed equation to the bth power we obtain

$$\beta^{b_0} \gamma_1^{b_1} \cdots \gamma_r^{b_r} = \omega^{\ell b} \rho^\ell$$

with $\rho \in k^*$ (we take $\rho = \nu^b (\beta^{p_0} \gamma_1^{p_1} \cdots \gamma_r^{p_r})^{-1}$). Taking Weil heights we get

$$\ell h(\rho) \leq \max_i(|b_i|) \left(h(\beta) + \sum_{i=1}^r h(\gamma_i) \right) \ll \frac{\ell}{Q},$$

where the implied constant depends only on β and the γ_i's. Choosing, e.g., $Q = \lceil \ell^{\frac{1}{r+2}} \rceil$, we see that $h(\rho) \ll \ell^{\frac{-1}{r+2}}$ and $0 < b \leq Q^{r+1} < \ell$ for large ℓ. On

the other hand the Weil height has a positive lower bound on k^*, outside the roots of unity. For large enough ℓ our inequality thus forces ρ to be a root of unity. From the multiplicative independence of $\beta, \gamma_1, \ldots, \gamma_r$ we thus obtain $b_0 = b_1 = \ldots = b_r = 0$. Since $1 \leq b < \ell$ we deduce that a_i is a multiple of ℓ for all $i = 0, 1, \ldots, r$. In particular ℓ divides M. Writing $M = \ell M'$, $a_i = \ell a_i'$ we have

$$\beta^{M'} \delta_1^{a_1'} \cdots \delta_r^{a_r'} = (v\theta)^{\ell M'}$$

for some root of unity θ. This however contradicts the minimality of M and concludes the proof. $\square$

In the sequel ζ_s will denote a primitive s^{th} root of unity. Take L as in Lemma 2; without loss we can assume $L > d$. Let D be an integer divisible by all the primes $\leq L$. We may also assume that $\mathbf{Q}(\zeta_D)$ contains the maximal cyclotomic subfield $\mathbf{Q}_c \cap k$ of k.

Define $k_1 = k(\zeta_D)$. If $\ell \leq L$ is a prime we have that $k_1(\zeta_{\ell D})/k_1$ is cyclic of order ℓ. In fact, $\ell | D$ and $[k_1(\zeta_{\ell D}) : k_1] = [\mathbf{Q}(\zeta_{\ell D}) : \mathbf{Q}(\zeta_D)] = \ell$; this is because $[\mathbf{Q}(\zeta_{\ell D}) : \mathbf{Q}_c \cap k] = [k(\zeta_{\ell D}) : k]$ and $[\mathbf{Q}(\zeta_D) : \mathbf{Q}_c \cap k] = [k_1 : k]$.

Let k_2 be the compositum of the fields $k_1(\zeta_{\ell D})$ for all primes $\ell \leq L$. Then the Galois group $\mathrm{Gal}(k_2/k_1)$ is a product of cyclic groups of pairwise coprime orders and is thus cyclic. Pick a generator σ of $\mathrm{Gal}(k_2/k_1)$. Then σ does not induce the identity on any field $k_1(\zeta_{\ell D})$ as above.

Let p be a prime number which splits completely in $k_1/\mathbf{Q}$, and such that, for some $\mathcal{B}$ in k_2 above p, the Frobenius automorphism of $\mathcal{B}$ in $\mathrm{Gal}(k_2/k_1)$ is σ. Cebotarev's theorem guarantees the existence of infinitely many such primes. Since $\mathbf{Q}(\zeta_D) \subset k_1$, p splits completely also in $\mathbf{Q}(\zeta_D)/\mathbf{Q}$ and hence $p \equiv 1 \pmod{D}$.

On the other hand, p cannot split completely in any $\mathbf{Q}(\zeta_{\ell D})$ for a prime $\ell \leq L$. (Otherwise it would split completely in $k_1(\zeta_{\ell D})$ and σ would be the identity on this field.) In turn, this means that $p \not\equiv 1 \pmod{\ell D}$. In conclusion we get infinitely many primes p with the following properties.

(a) $p = 1 + Dm$, where the least prime factor of m is $> L > d$.

(b) p splits completely in k_1.

Put, as above, $F(X_0, \ldots, X_r) = f(X_0, X_1^D, \ldots, X_r^D)$. We have seen that it is possible to assume that F is not a dth power in $\overline{\mathbf{Q}}[X_0, \ldots, X_r]$. Therefore (by Kummer theory) the polynomial

(4) $$S(X_0, \ldots, X_r, Y) = Y^d - F(X_0, \ldots, X_n)$$

is absolutely irreducible. Pick now a large prime p with the properties (a),(b) and consider a prime ideal factor $\mathcal{P}$ of p in k_1. For large p we may look at

the reduction $\tilde{S} \in \mathbf{F}_p[X_0, \ldots, X_r, Y]$ of S modulo $\mathcal{P}$. Also, for large p a well-known theorem due to Ostrowski (see e.g. [Schm2, p. 193]) guarantees that $\tilde{S}$ is absolutely irreducible. We now apply the Lang-Weil theorem, as stated e.g. in [Schm2, Thm. 5A, p. 210 or Cor. 5C, p. 213] or [Se, p. 184]. We deduce that the number $N(p)$ of solutions $(\mathbf{x}, y) := (x_0, \ldots, x_r, y) \in \mathbf{F}_p^{r+2}$ to $\tilde{S}(\mathbf{x}, y) = 0$ satisfies

$$N(p) = p^{r+1} + O(p^{r+\frac{1}{2}}).$$

Recall that $d|D$, so $p \equiv 1 \pmod{d}$. Hence, for each $\mathbf{x} \in \mathbf{F}_p^{r+1}$ which corresponds to a solution $(\mathbf{x}, y)$ with $F(\mathbf{x}) \not\equiv 0 \pmod{\mathcal{P}}$, we find d distinct solutions to be counted in $N(p)$. But the number of solutions of $F(\mathbf{x}) \equiv 0$ $\pmod{\mathcal{P}}$ in $\mathbf{F}_p^{r+1}$ is trivially $O(p^r)$. Therefore the number of $\mathbf{x} \in \mathbf{F}_p^{r+1}$ such that $\tilde{F}(\mathbf{x})$ is a dth power in $\mathbf{F}_p$ is at most $(p^{r+1}/d) + O(p^{r+\frac{1}{2}}) \le 2p^{r+1}/3$, say, for large enough p.[1]

In particular, if p has been chosen large enough, we may find

$$\mathbf{x} = (x_0, \ldots, x_r) \in \mathbf{F}_p^{r+1}$$

such that $x_0 \cdots x_r \ne 0$ and $\tilde{F}(x_0, \ldots, x_r)$ is not a dth power in $\mathbf{F}_p$.

Observe that p splits completely in $\mathbf{Q}(\zeta_{p-1})$, so it splits completely in $k_3 := k_1(\zeta_{p-1}) = k(\zeta_{p-1})$. Let $\mathcal{Q}$ be a prime ideal of k_3 above $\mathcal{P}$. Observe that the reduction of ζ_{p-1} generates the group of nonzero classes modulo $\mathcal{Q}$. So we may choose integers $h_0, \ldots, h_r$ such that $\zeta_{p-1}^{h_i} \equiv x_i \pmod{\mathcal{Q}}$. We determine ζ_m by putting $\zeta_m = \zeta_{p-1}^D$. What we have proved implies the following

Claim. $\Psi := F(\zeta_{p-1}^{h_0}, \ldots, \zeta_{p-1}^{h_r}) = f(\zeta_{p-1}^{h_0}, \zeta_m^{h_1}, \ldots, \zeta_m^{h_r})$ is not a dth power in k_3.

Consider now the field $K := k(\zeta_{p-1}, \beta^{1/m}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$, where the δ_i are defined by (3). Plainly $\Psi \in K$.

Suppose that K has degree $< m$ over $k(\zeta_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$. Then, Kummer theory for K/k_3 shows that β belongs to the multiplicative group generated by $\delta_1^{\frac{\ell}{m}}, \ldots, \delta_r^{\frac{\ell}{m}}$ and the ℓth powers in $k(\zeta_{p-1})^*$, for some prime ℓ dividing m. However this contradicts Lemma 2 (with $M = \frac{m}{\ell}$), since each prime divisor of m is $> L$ by property (a) above.

Therefore $K/k(\zeta_{p-1}, \delta_1^{1/m}, \ldots, \delta_r^{1/m})$ is cyclic of degree m. We let τ be a generator of the Galois group.

Recall that Ψ is not a dth power in $k_3 = k(\zeta_{p-1})$. We contend now that Ψ is not a dth power in K. In fact, the degree of K over $k(\zeta_{p-1})$ divides a power

---

[1] This argument goes back to M. Eichler and has been used by S. D. Cohen in the context of large sieve applied to Hilbert's Irreducibility Theorem. See [Se, Ch. 13].

of m, while $k(\zeta_{p-1})(\Psi^{1/d})$ $k(\zeta_{p-1})$ has degree d. But each prime factor of m is $> L > d$, proving the contention.

Let ξ be an element of $\mathrm{Gal}(K(\Psi^{1/d})/k(\zeta_{p-1}))$ which induces τ on K and is not the identity on $\Psi^{1/d}$. We let Π be the set of primes of $k(\zeta_{p-1})$ of degree 1 over $\mathbf{Q}$ and whose Frobenius in $K(\Psi^{1/d})$ is ξ. (Note that we are dealing with an abelian extension.) Cebotarev's theorem guarantees that Π is infinite. For $\pi \in \Pi$, let $\mathbf{F}_q$ be the residue field of π. For almost all $\pi \in \Pi$ we may reduce $\beta^{\pm 1}$, $\gamma_i^{\pm 1}$, $\delta_i^{\pm 1}$, f and Ψ modulo π. Observe that

(i) Since the Frobenius of π does not fix $\Psi^{1/d}$, we have that Ψ is not a dth power modulo π.

(ii) Since ξ induces τ, which fixes $\delta_i^{1/m}$, we have that each δ_i is an mth power modulo π, so

(5) $$\delta_i^{\frac{q-1}{m}} \equiv 1 \pmod{\pi}.$$

(iii) Since ξ induces τ, which sends $\beta^{1/m}$ to $\zeta_m^a \beta^{1/m}$ for some a coprime with m, we have that

(6) $$\beta^{\frac{q-1}{m}} \equiv \zeta_m^a \pmod{\pi}.$$

(iv) Since π has degree 1 over $\mathbf{Q}$, there exists an integer $n_0 \in \mathbf{Z}$ such that $n_0 \equiv \zeta_{p-1} \pmod{\pi}$.

We can now obtain the desired contradiction as follows. By (5) and (6) we have

$$\gamma_i^{\frac{q-1}{m}} \equiv \beta^{h_i \frac{q-1}{m}} \equiv \zeta_m^{a h_i} \pmod{\pi}.$$

Therefore, for an integer a' such that $aa' \equiv 1 \pmod{m}$,

$$\gamma_i^{a' \frac{q-1}{m}} \equiv \zeta_m^{h_i} \pmod{\pi}.$$

Choose now an integer $n \in \mathbf{N}$ such that

$$n \equiv n_0^{h_0} \pmod{q}, \qquad n \equiv a' \frac{q-1}{m} \pmod{q-1}.$$

These congruences imply

$$f(\zeta_{p-1}^{h_0}, \zeta_m^{h_1}, \ldots, \zeta_m^{h_r}) \equiv f(n_0^{h_0}, \gamma_1^{a' \frac{q-1}{m}}, \ldots, \gamma_r^{a' \frac{q-1}{m}})$$
$$\equiv f(n, \gamma_1^n, \ldots, \gamma_r^n) = b(n) \pmod{\pi}.$$

On the other hand the left side is Ψ and the right side is a dth power in k by assumption. Since $b(n)$ is π-integral for almost all π, we may reduce and get a contradiction with (i) above.

Added in proof. The principle of replacing powers α^n with roots of unity by reduction is used also in [BBS].

Istituto Universitario di Architettura di Venezia, Venezia, Italy
E-mail address: zannier@iuav.unive.it

References

[BBS]   D. Barsky, J.-P. Bèzivin, and A. Schinzel, Une caractérisation arithmétique de suites récurrentes linéaires, *J. reine angew. Math.* **494** (1998), 73–84.

[B]   J.-P. Bézivin, Sur les propriétés arithmétiques du produit de Hadamard, *Ann. Fac. Sci. Toulouse Math.* **11** (1990), 7–19.

[BMZ]   E. Bombieri, D. Masser, and U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups, *Int. Math. Res. Notices*, to appear.

[CZ]   P. Corvaja and U. Zannier, Diophantine equations with power sums and universal Hilbert sets, *Indag. Mathem.* **9** (1998), 317–332.

[PZ]   A. Perelli and U. Zannier, Arithmetic properties of certain recurrent sequences, *J. Austral. Math. Soc.* (Ser. A) **37** (1984), 4–16.

[P]   Y. Pourchet, Solution du problème arithmétique du quotient de Hadamard de deux fractions rationelles, *C. R. Acad. Sci. Paris*, Sér. *A* **288** (1979), A1055–A1057.

[RvdP]   R. Rumely and A. J. Van der Poorten, A note on the Hadamard k^{th} root of a rational function, *J. Austral. Math. Soc.* (Ser. A) **43** (1987), 314–327.

[Schm1]   W. M. Schmidt, *Diophantine Approximation, Lecture Notes in Math.* **785**, Springer-Verlag, New York, 1980.

[Schm2]   _____, *Equations over Finite Fields. An Elementary Appraoch, Lecture Notes in Math.* **536**, Springer-Verlag, New York, 1976.

[Se]   J-P. Serre, *Lectures on the Mordell-Weil Theorem, Aspects of Math.* **E15**, Friedr. Viewer and Sohn, Braunschweig, 1990.

[vdP1]   A. J. Van der Poorten, Some facts that should be better known, especially about rational functions, in *Number Theory and Applications* (Banff, AB, 1988), 497–528, Kluwer Acad. Publ., Dordrecht, 1989.

[vdP2]   _____, Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationelles, *C. R. Acad. Sci. Paris*, Série I **306** (1988), 97–102.

[vdP3]   _____, A note on Hadamard roots of rational functions, *Rocky Mountain J. Math.* **26** (1996), 1183–1197.