ON PERFECT POWERS IN LINEAR RECURRENCE SEQUENCES OF INTEGERS

YANN BUGEAUD AND HAJIME KANEKO

Abstract. We prove that there are only finitely many perfect powers in any linear recurrence sequence of integers of order at least two and whose characteristic polynomial is irreducible and has a dominant root.

1. Introduction and main result

Let $(u_n)_{n\geq 0}$ be a linear recurrence sequence of integers with initial terms $u_0, \ldots, u_{k-1}$ and defined by the recurrence relation

$$u_{n+k} = t_1 u_{n+k-1} + t_2 u_{n+k-2} + \cdots + t_k u_n \tag{1.1}$$

for $n \geq 0$, where $k \geq 1$ is the order of $(u_n)_{n\geq 0}$ and $t_1, \ldots, t_k$ are integers with $t_k \neq 0$. We call the polynomial

$$X^k - t_1 X^{k-1} - \cdots - t_{k-1} X - t_k$$

the characteristic polynomial of $(u_n)_{n\geq 0}$ and its roots

$$\alpha_1, \ldots, \alpha_k, \quad \text{numbered such that } |\alpha_1| \geq \ldots \geq |\alpha_k|,$$

the roots of $(u_n)_{n\geq 0}$. We say that $(u_n)_{n\geq 0}$ has a dominant root if $|\alpha_1| > |\alpha_2|$. Furthermore, $(u_n)_{n\geq 0}$ is simple if all its roots are distinct. In the case where $(u_n)_{n\geq 0}$ is simple, we say that $(u_n)_{n\geq 0}$ is nondegenerate if α_i/α_j is not a root of unity for any $1 \leq i < j \leq k$.

In all what follows, for an integer $q \geq 2$, a q-th power is an integer of the form y^q, where y is in $\mathbb{Z}$. An integer is called a perfect power if it is a q-th power for some integer $q \geq 2$.

Perfect powers in terms of linear recurrence sequences $(u_n)_{n\geq 0}$ of integers have been widely studied, see e.g. [11] for references. The first general result, established in the early 80s independently by Shorey and Stewart [10] and Pethő [5, 6] asserts that if $(u_n)_{n\geq 0}$ has a dominant root and $u_n = y^q$ with integers $y, q, n > 1$, then q is less than an effectively computable positive number q_0 depending only on $(u_n)_{n\geq 0}$. The Diophantine ingredient of the proof is Baker's theory of linear forms in logarithms of algebraic numbers.

For fixed $q \geq 2$, Corvaja and Zannier [1] established in 2002 that, if $(u_n)_{n\geq 0}$ has a dominant root and u_n is a q-th power for infinitely many integers n, then this comes from an algebraic relation, that is, there exist an infinite arithmetic progression $\mathcal{P}$ and a linear recurrence sequence $(v_n)_{n\geq 0}$ such that $u_n = v_n^q$ for every n in $\mathcal{P}$. The

---

2010 *Mathematics Subject Classification.* 11D41, 11B37.

Key words and phrases. Diophantine equation, recurrence sequence, Diophantine approximation.

Diophantine ingredient of their proof is the Schmidt subspace theorem; see also [4, 3].

The combination of these two results gives much information on the perfect powers in terms of linear recurrence sequences of integers with a dominating root. More precisely, on page 59 of his monograph [12], Zannier attributes to Pethő the following remark:

Take a simple recurrence $(u_n)_{n\geq 0}$ *with a dominant root and at least another root; then, firstly one can apply the results in* [10] *to show that, for a certain computable* q_0*, the equation* $u_n = y^q$ *has only finitely many solutions in integers* $q > q_0$*,* n*, and* y*. And secondly one can apply Corollary IV.7 [of* [12]*] for each* $q \leq q_0$ *to obtain a complete description of the solutions, for variable* $q \geq 2$*.*

Indeed, Pethő [7] used [10] and the above mentioned result from [1] to prove the finiteness of the number of perfect powers in linear recurrence sequences of order three whose characteristic polynomial is irreducible and has a dominant root.

The aim of the present note is to extend Pethő's result to linear recurrence sequences of arbitrary order at least two, with a dominant root and whose characteristic polynomial is irreducible. This boils down to exclude the putative algebraic relations occurring in the conclusion of Corvaja and Zannier's result [1] mentioned above.

THEOREM 1.1. *Let* $(u_n)_{n\geq 0}$ *be a linear recurrence sequence of integers of order at least two and such that its characteristic polynomial is irreducible and has a dominant root. Then there are only finitely many perfect powers in* $(u_n)_{n\geq 0}$*. Moreover, their number can be bounded by an effectively computable number.*

Let $\alpha_1, \dots, \alpha_k$ be the roots of the (irreducible) characteristic polynomial of $(u_n)_{n\geq 0}$ in Theorem 1.1, numbered such that $|\alpha_1| > |\alpha_2| \geq \dots \geq |\alpha_k|$. We note that, for every i, j with $1 \leq i < j \leq n$, the ratio α_i/α_j is not a root of unity. In particular, $\alpha_1, \dots, \alpha_k$ are all distinct. Indeed, suppose on the contrary that $(\alpha_i/\alpha_j)^h = 1$ for some positive integer h. Taking an automorphism σ of $\mathbb{Q}(\alpha_1, \dots, \alpha_k)/\mathbb{Q}$ such that $\sigma(\alpha_i) = \alpha_1$, we get that $1 = |\alpha_1^h/\sigma(\alpha_j)^h| > 1$, a contradiction.

Consider the recurrence sequence $(u_n)_{n\geq 0}$ defined by $u_0 = 0, u_1 = 1, u_2 = 1$, and

$$u_{n+3} = 2(u_{n+2} + u_{n+1}) - u_n, \quad \text{for } n \geq 0.$$

We check that u_n is equal to the square of the n-th Fibonacci number for every $n \geq 0$. The characteristic polynomial of $(u_n)_{n\geq 0}$ factors as

$$X^3 - 2X^2 - 2X + 1 = (X + 1)(X^2 - 3X + 1).$$

This and similar examples show that the assumption of irreducibility of the characteristic polynomial cannot be removed in the statement of Theorem 1.1.

Relaxing the dominant root assumption remains a challenging open problem. It seems to be currently out of reach of the ineffective techniques (based on the subspace theorem) and of the effective methods (based on the theory of linear forms in logarithms).

2. Linear recurrences of rational numbers

Let $(u_n)_{n\geq 0}$ be a simple linear recurrence sequence of rational numbers satisfying (1.1), where $t_1, \dots, t_k$ are rational numbers with $t_k \neq 0$. It can be written as

$$u_n = \beta_1 \alpha_1^n + \cdots + \beta_k \alpha_k^n \tag{2.1}$$

for any $n \geq 0$, where $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k$ are nonzero algebraic numbers and $\alpha_1, \dots, \alpha_k$ are distinct. For convenience, if $k = 0$, then (2.1) means that $u_n = 0$ for any nonnegative integer n.

If $\alpha_1, \dots, \alpha_k$ are the Galois conjugates of α_1, then we call $(u_n)_{n\geq 0}$ an atom. If $(u_n)_{n\geq 0}$ is an atom, then, we say for $i = 1, \dots, k$ that $(u_n)_{n\geq 0}$ includes α_i.

Let $\mathcal{R}$ denote the set of simple linear recurrence of rational numbers. Then $\mathcal{R}$ is a ring with usual addition and multiplication of sequences, namely, we have

$$(u_n)_{n\geq 0} + (v_n)_{n\geq 0} = (u_n + v_n)_{n\geq 0},$$
$$(u_n)_{n\geq 0}(v_n)_{n\geq 0} = (u_n v_n)_{n\geq 0},$$

for all $(u_n)_{n\geq 0}$ and $(v_n)_{n\geq 0}$ in $\mathcal{R}$.

PROPOSITION 2.1. *Any element $(u_n)_{n\geq 0}$ of $\mathcal{R}$ can be uniquely expressed as a sum of linearly independent atoms (over $\mathbb{Q}$) in $\mathcal{R}$. We denote the number of atoms in $(u_n)_{n\geq 0}$ by $\Lambda(u_n)$.*

Proof. The uniqueness is clear. Let $(u_n)_{n\geq 0}$ be as in (2.1). We prove the existence of a representation by induction on k. The case of $k = 0$ is clear. Assume that $k \geq 1$. Let σ be any element of the absolute Galois group of $\mathbb{Q}$ satisfying $\sigma(\alpha_1) = \alpha_1$. Since u_n is rational for any nonnegative integer n, we have $u_n - \sigma(u_n) = 0$. Thus, we see that $\sigma(\beta_1) = \beta_1$, and so β_1 is in $\mathbb{Q}(\alpha_1)$ because σ is an arbitrary element with $\sigma(\alpha_1) = \alpha_1$.

Let $\alpha_1, \gamma_2, \dots, \gamma_s$ be the Galois conjugates of α_1. For $2 \leq j \leq s$, let σ_j be an element of the absolute Galois group of $\mathbb{Q}$ satisfying $\sigma_j(\alpha_1) = \gamma_j$. Since $u_n - \sigma_j(u_n) = 0$ for any nonnegative integer n, there exists $2 \leq i(j) \leq k$ with $\alpha_{i(j)} = \gamma_j, \beta_{i(j)} = \sigma_j(\beta_1)$. Using that β_1 is in $\mathbb{Q}(\alpha_1)$, we get that

$$a_n := \beta_1 \alpha_1^n + \sum_{j=2}^{s} \sigma_j(\beta_1 \alpha_1^n) \in \mathcal{R}$$

is a subsum (2.1). Applying the inductive hypothesis to $(u_n - a_n)_{n\geq 0}$, we deduce Proposition 2.1. □

By a theorem proved independently by van der Poorten and Schlickewei [8] and Evertse [2], for any nondegenerate linear recurrence sequence $(w_n)_{n\geq 0}$ of integers, for any positive ε, we have

$$|w_n| > A^{n(1-\varepsilon)}, \quad \text{for every sufficiently large integer } n, \tag{2.2}$$

where A denotes the maximum of the moduli of the roots of the characteristic polynomial of $(w_n)_{n\geq 0}$.

Let us also recall effective upper bounds for the number of zeros (the zero multiplicity) in nondegenerate linear recurrences obtained by Schmidt [9]. Let $(v_n)_{n\geq 0}$ be a linear recurrence of complex numbers of order k. If $(v_n)_{n\geq 0}$ is simple and nondegenerate, then the number of nonnegative n with $v_n = 0$ is at most

$$e^{(7k)^{8k}}. \tag{2.3}$$

3. Proof of the main theorem

Let $(u_n)_{n\geq 0}$ be a linear recurrence sequence of integers as in the statement of the theorem.

By the results of Shorey and Stewart [10] and Pethő [5, 6] mentioned in the beginning of Section 1, it is sufficient to show that, for any fixed integer $q>1$ and any sufficiently large integer n, the n-th term u_n of the linear recurrence sequence is not a q-th power.

Let $(u_n)_{n\geq 0}$ be as in (2.1). Recall that, for any i,j with $1\leq i<j\leq k$, the quotient α_i/α_j is not a root of unity. In particular, for any positive integer m and $1\leq i<j\leq k$, two numbers α_i^m and α_j^m are distinct.

Let q be an integer with $2\leq q\leq q_0$. In what follows, the implicit constants in the symbols $\ll$, $\gg$ are positive, effectively computable, and depend only on $(u_n)_{n\geq 0}$. We denote by Card $\mathcal{S}$ the cardinality of a finite set $\mathcal{S}$. Let

$$\mathcal{A} := \{n\in\mathbb{N} \ : \ u_n \text{ is a } q\text{-th power}\}.$$

Our aim is to show that Card $\mathcal{A}\ll 1$. The proof of Theorem 2.1 in [3] implies that there exist a subset $\mathcal{B}\subset\mathcal{A}$, a positive integer $l\ll 1$, distinct nonzero algebraic numbers $\delta_1,\ldots,\delta_l$, and nonzero algebraic numbers $d_1,\ldots,d_l$ satisfying the following:

(1) For any n in $\mathcal{B}$, we have

$$u_n=\left(\sum_{i=1}^{l} d_i\delta_i^n\right)^q. \tag{3.1}$$

(2) $\delta_1,\ldots,\delta_l$ are effectively determined by $(u_n)_{n\geq 0}$.
(3) There is a finite field extension $K/\mathbb{Q}$ effectively determined by $(u_n)_{n\geq 0}$ such that $d_1,\ldots,d_l$ are in K.
(4) For any $R>0$, there is an effectively computable positive constant $C=C((u_n)_{n\geq 0};R)$, depending only on $(u_n)_{n\geq 0}$ and R, such that if Card $\mathcal{A}\geq C$, then Card $\mathcal{B}\geq R$. In what follows, we say that if Card $\mathcal{A}\gg 1$, then Card $\mathcal{B}\gg 1$.

If necessary, changing $d_1,\ldots,d_l$ and $\mathcal{B}$, we may assume by (3.1) that

$$v_n:=\sum_{i=1}^{l} d_i\delta_i^n \text{ is an integer,}$$

for any n in $\mathcal{B}$. Since $l\ll 1$ and $\delta_1,\ldots,\delta_l$ are effectively determined by $(u_n)_{n\geq 0}$, there is a positive integer $M\ll 1$ such that

$$\left(u_{Mn+i}-v_{Mn+i}^q\right)_{n\geq 0} \text{ is nondegenerate or identically zero,} \tag{3.2}$$

for any $0\leq i<M$. By the pigeon hole principle, there exists an $0\leq i_0<M$ such that

$$\text{Card }\{n\in\mathcal{B}\mid n\equiv i_0 \ (\mathrm{mod}\ M)\}\geq \frac{1}{M}\text{Card }\mathcal{B}.$$

Let

$$\mathcal{P}:=\{n\in\mathbb{N}\mid n\equiv i_0 \ (\mathrm{mod}\ M)\},\quad \mathcal{A}':=\mathcal{B}\cap\mathcal{P}.$$

Then we see that v_n is an integer for any n in $\mathcal{A}'$, and if Card $\mathcal{A}\gg 1$, then Card $\mathcal{A}'\gg 1$. Thus, using (3.2) and the upper bound (2.3) for the zero multiplicity of nondenegerate linear recurrences, we deduce that

$$u_n = v_n^q$$

for any n in $\mathcal{P}$.

LEMMA 3.1. *If Card $\mathcal{A} \gg 1$, then there exists an arithmetic progression $\mathcal{Q} = \{bn + c \mid n = 0, 1, \ldots\}$ included in $\mathcal{P}$ such that v_n is an integer for any n in $\mathcal{Q}$.*

Proof. Let K' be the Galois closure of a field extension $K(\delta_1, \ldots, \delta_l)/\mathbb{Q}$ and let $G = \{\sigma_1, \ldots, \sigma_D\}$ the Galois group of $K'/\mathbb{Q}$. Note that K' and G are effectively determined by $(u_n)_{n\geq 0}$. Let $w_n := v_n - \sigma_1(v_n)$. Note that $w_n = 0$ for any n in $\mathcal{A}'$. In the same way as the construction of $\mathcal{A}'$ and $\mathcal{P}$, we see by (2.3) that if Card $\mathcal{A} \gg 1$, then there exist a subset $\mathcal{A}''$ of $\mathcal{A}'$ with Card $\mathcal{A}'' \gg 1$ and an arithmetic progression

$$\mathcal{P}' = \{MM'n + i_0' \ : \ n \in \mathbb{N}\} \subset \mathcal{P}$$

with $M' \ll 1$ and $0 \leq i_0' < MM'$ satisfying $\mathcal{A}'' \subset \mathcal{P}'$ and $w_n = 0$ for any n in $\mathcal{P}'$.

By repeating this argument, we end up with an arithmetic progression $\mathcal{Q}$ included in $\mathcal{P}$ such that $\sigma_i(v_n) = v_n$ for any $i = 1, \ldots, D$ and n in $\mathcal{Q}$. This establishes the lemma. □

We are now in position to complete the proof of Theorem 1.1. Assume that Card $\mathcal{A} \gg 1$ and let $\mathcal{Q}$ be as given by Lemma 3.1. Put

$$u_{bn+c} = \sum_{j=1}^{k} \beta_j' \alpha_j'^n =: u_n' \in \mathcal{R},$$

where $\beta_j' = \beta_j \alpha_j^c, \alpha_j' = \alpha_j^b$ for $j = 1, \ldots, k$, and

$$v_{bn+c} = \sum_{i=1}^{l'} d_i' \delta_i'^n =: v_n' \in \mathcal{R},$$

where $d_1', \ldots, d_{l'}', \delta_1', \ldots, \delta_{l'}'$ are nonzero algebraic numbers and $\delta_1', \ldots, \delta_{l'}'$ are distinct. By considering, if necessary, an arithmetic progression $\mathcal{Q}'$ included in $\mathcal{Q}$, we may assume that δ_i'/δ_j' is not a root of unity for any $1 \leq i < j \leq l'$.

Observe that $(u_n')_{n\geq 0}$ is a linear recurrence sequence of order $k(> 1)$. Moreover, the characteristic polynomial of $(u_n')_{n\geq 0}$ is irreducible and has a dominant root. Thus,

$$\Lambda(u_n') = 1. \tag{3.3}$$

In what follows, we get a contradiction, calculating $\Lambda(v_n'^q)(= \Lambda(u_n'))$. Renumber $\delta_1', \ldots, \delta_{l'}'$ so that

$$|\delta_1'| = \cdots = |\delta_{i_1}'| > |\delta_{1+i_1}'| = \cdots = |\delta_{i_2}'| > \cdots > |\delta_{1+i_{p-1}}'| = \cdots = |\delta_{i_p}'|,$$

where p is the number of distinct values among $|\delta_1'|, \ldots, |\delta_{l'}'|$ and $i_p = l'$. Moreover, we may assume that α_1' is the dominant root of the characteristic polynomial of $(u_n')_{n\geq 0}$. Observe that $|\alpha_1'| = |\delta_1'|^q$. Put

$$D_1(n) := \sum_{i=1}^{i_1} d_i' \delta_i'^n, \ D_2(n) := \sum_{i=1+i_1}^{i_p} d_i' \delta_i'^n.$$

Using

$$\sum_{j=1}^{k} \beta'_j \alpha'^n_j = (D_1(n) + D_2(n))^q \tag{3.4}$$

we get

$$\beta'_1 \alpha'^n_1 - D_1(n)^q = \sum_{i=1}^{q} \binom{q}{i} D_1(n)^{q-i} D_2(n)^i - \sum_{j=2}^{k} \beta'_j \alpha'^n_j.$$

We argue as in the proof of Theorem 6 in [7]. Let ε be a positive real number. By (2.2), the left-hand side of the last equality is, if nonzero, greater than $|\alpha'_1|^{n(1-\varepsilon)}$, for n large enough, while its right-hand side is bounded from above by some constant times $\max\{|\alpha'_2|^n, |\alpha'_1|^{(q-1)n/q}\}$, again for n large enough. Since $|\alpha'_2| < |\alpha'_1|$, there exists $1 \le i \le i_1$ satisfying

$$\beta'_1 \alpha'^n_1 = D_1(n)^q = d'^q_i \delta'^{qn}_i$$

for infinitely many integers $n \ge 0$. Without loss of generality, we may assume that $i = 1$. Thus, there exists a q-th root ζ of unity such that

$$d'_1(1-\zeta)\delta'^n_1 + d'_2 \delta'^n_2 + \cdots + d'_{i_1} \delta'^n_{i_1} = 0 \tag{3.5}$$

for infinitely many integers $n \ge 0$. Since δ'_i/δ'_j is not a root of unity for any $1 \le i < j \le i_1$, we see by the Skolem-Mahler-Lech theorem that (3.5) holds for any nonnegative integer n. Thus, we get $\zeta = 1, i_1 = 1$, and $p \ge 2$ by (3.4) and $k > 1$.

Now, we bound from below the number of atoms in $(v'^q_n)_{n\ge0}$. First, we observe that there exists an atom $(a_n)_{n\ge0}$ in $(v'^q_n)_{n\ge0}$ including δ'^q_1 because $d'^q_1 \delta'^{qn}_1$ cannot be vanished by other terms in $(v'^q_n)_{n\ge0}$.

Put

$$\left(d'_1 \delta'^n_1 + \sum_{i=2}^{i_2} d'_i \delta'^n_i + \sum_{i=1+i_2}^{i_p} d'_i \delta'^n_i \right)^q$$

$$=: (d'_1 \delta'^n_1)^q + q(d'_1 \delta'^n_1)^{q-1} \left(\sum_{i=2}^{i_2} d'_i \delta'^n_i \right) + \rho,$$

where ρ is the remaining term. Any algebraic number included in $(a_n)_{n\ge0}$ is of the form δ'^q, where δ' is a conjugate of δ'_1. Thus, for any i with $2 \le i \le i_2$, $\delta'^{q-1}_1 \delta'_i$ is not included in $(a_n)_{n\ge0}$. In fact, we see by $q \ge 2$ that $|\delta'^{q-1}_1 \delta'_i| \ne |\delta'^q|$ for any conjugate δ' of δ'_1 because δ'_1 is the dominant root of the characteristic polynomial of $(v'_n)_{n\ge0}$. Here, we have used that $i_1 = 1$.

Moreover, for any summand $s\theta^n$ in ρ, we see that $|\delta'^{q-1}_1 \delta_i| > |\theta|$ for any $2 \le i \le i_2$. Thus, $q d'^{q-1}_1 d'_i (\delta'^{q-1}_1 \delta_i)^n$ cannot be vanished by terms in ρ. Hence, there exists an atom in $(v'^q_n - a_n)_{n\ge0}$. Therefore, we conclude that $\Lambda(v'^q_n) \ge 2$, which contradicts (3.3).

This implies that Card $\mathcal{A} \ll 1$. The proof of Theorem 1.1 is complete.

Acknowledgements

The second author was supported by JSPS KAKENHI Grant Number 15K17505. The authors are grateful to Umberto Zannier for detailed comments.

References

[1] P. Corvaja and U. Zannier, *Some new applications of the subspace theorem*, Compositio Math. 131 (2002), 319-340.
[2] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. 53 (1984), 225–244.
[3] C. Fuchs, *Polynomial-exponential equations and linear recurrences*, Glas. Mat. Ser. III 38 (2003), 233–252.
[4] C. Fuchs and R. F. Tichy, *Perfect powers in linear recurring sequences*, Acta Arith. 107 (2003), 9–25.
[5] A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory 15 (1982), 5–13.
[6] A. Pethő, *Perfect powers in second order recurrences.* In: Topics in Classical Number Theory, Proceedings of the Conference in Budapest 1981, Colloq. Math. Soc. János Bolyai 34, pp. 1217–1227, North–Holland, Amsterdam, 1984.
[7] A. Pethő, *Diophantine properties of linear recursive sequences. II*, Acta Math. Acad. Paedagog. Nyházi. (N.S.) 17 (2001), 81–96.
[8] A. J. van der Poorten and H. P. Schlickewei, *The growth condition for recurrence sequences*, Macquarie University Math. Rep. 82-0041 (1982).
[9] W. M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. 182 (1999), 243–282.
[10] T. N. Shorey and C. L. Stewart, *On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand. 52 (1983), 24–36.
[11] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations.* Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986.
[12] U. Zannier, Some applications of Diophantine Approximation to Diophantine Equations. Udine: Forum Editrice, 2003.

Yann Bugeaud
Institut de Recherche Mathématique Avancée, U.M.R. 7501
Université de Strasbourg et C.N.R.S.
7, rue René Descartes
67084 Strasbourg, FRANCE
e-mail : bugeaud@math.unistra.fr

Hajime Kaneko
Institute of Mathematics, University of Tsukuba, 1-1-1
Tennodai, Tsukuba, Ibaraki, 305-8571, JAPAN
Research Core for Mathematical Sciences
University of Tsukuba, 1-1-1
Tennodai, Tsukuba, Ibaraki, 305-8571, JAPAN
e-mail: kanekoha@math.tsukuba.ac.jp