GLASNIK MATEMATIČKI
Vol. 44(64)(2009), 285 – 307

ARITHMETIC PROPERTIES OF THE INTEGER PART OF THE POWERS OF AN ALGEBRAIC NUMBER

Florian Luca and Maurice Mignotte
Universidad Nacional Autónoma de México, Mexico and Université Louis Pasteur, France

Abstract. For a real number x, we let $\lfloor x \rceil$ be the closest integer to x. In this paper, we look at the arithmetic properties of the integers $\lfloor \theta^n \rceil$ when $n \geq 0$, where $\theta > 1$ is a fixed algebraic number.

1. Introduction

For any real number x we let $\lfloor x \rfloor$, $\lceil x \rceil$ and $\lfloor x \rceil$ be the largest integer $\leq x$, the smallest integer $\geq x$ and the closest integer to x respectively. When x is not an integer but $2x$ is we let $\lfloor x \rceil = \lfloor x \rfloor$. We also put $\{x\} = x - \lfloor x \rfloor$ and $||x|| = |x - \lfloor x \rceil|$ for the fractional part of x and the distance from x to the nearest integer, respectively.

We let $\theta > 1$ be an algebraic number. Although there are several results in the literature concerning the behavior of the numbers $||\theta^n||$ and $\{\theta^n\}$, many problems remain unsolved. For example, a famous question of Mahler whether there exists a real number $\alpha > 0$ such that $\{\alpha(3/2)^n\} \in (0, 1/2)$ holds for all $n > 0$ has not yet been answered.

In this note, we look at the arithmetic properties of the sequences of integers $(\lfloor \theta^n \rfloor)_{n \geq 0}$, $(\lceil \theta^n \rceil)_{n \geq 0}$, and $(\lfloor \theta^n \rceil)_{n \geq 0}$, respectively. We study their digital properties, the size and number of their prime factors, as well as whether or not such numbers can be perfect powers.

Some of our results work only for Pisot numbers θ (i.e., real algebraic integers $\theta > 1$ all whose conjugates lie inside the unit disk), some other ones work for arbitrary real algebraic numbers and finally some of them work only for a certain class of algebraic numbers including the ones having the property

2000 *Mathematics Subject Classification.* 11D45, 11D75.
Key words and phrases. Powers of algebraic numbers, digital representations, applications of linear forms in logarithms and the subspace theorem.

that none of their powers is either an integer, or a Pisot number. Our methods use classical techniques from Diophantine equations and Diophantine approximations. These techniques are summarized in Section 2. Section 3 contains our results and their proofs. We briefly mention here our main results. Let A_n be one of the numbers $\lfloor \theta^n \rfloor$, $\lceil \theta^n \rceil$, $\lfloor \theta^n \rceil$ when $n \geq 0$. Assume that $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ. Then the sum of the digits of A_n with respect to an integer base $b > 1$ is $\gg \log n / \log\log n$; this is also true if $\theta^\ell \in \mathbb{Z}$ for some positive integer ℓ but with θ and b multiplicatively independent instead (Theorem 3.1). The largest prime divisor of A_n is $\gg \log n \log\log n / \log\log\log n$ for all positive integers n and $\gg \log n \log\log n$ for almost all positive integers n (Theorem 3.3). Moreover, if additionally θ^ℓ is not a Pisot number or a Salem number whose minimal polynomial is congruent to a monomial modulo some prime, then the total number of prime divisors of A_n counted by multiplicity is $o(n)$ as $n \to \infty$ (Theorem 3.5). We show that the assumptions here are indeed necessary (see the discussion before Theorem 3.5). Finally, if θ is a Pisot number, then A_n is a perfect power only for finitely many n (Theorem 3.8).

Throughout this paper, we use the Vinogradov symbols $\ll$, $\gg$ and $\asymp$ and the Landau symbols O and o with their usual meaning. We write $P(n)$ for the largest prime factor of the integer n with the convention that $P(0) = P(\pm 1) = 1$. For a positive real number x we write $\log x$ for the maximum between the natural logarithm of x and 1. We denote by $2 = p_1 < p_2 < \cdots < p_k < \cdots$ the increasing sequence of prime numbers. We also write $c_1,\ c_2,\ c_3,\ \ldots$ for positive computable constants depending on θ and b.

2. Preparations

In this section, we recall some results from Diophantine approximations and Diophantine equations which are needed throughout the paper.

We start with a quantitative version of the Subspace Theorem of W. Schmidt as formulated by Evertse ([4]).

We normalize absolute values and heights as follows. Let $\mathbb{K}$ be an algebraic number field of degree d. Let $M(\mathbb{K})$ denote the set of places on $\mathbb{K}$. For x in $\mathbb{K}$ and a place v in $M(\mathbb{K})$ define the absolute value $|x|_v$ by

(i) $|x|_v = |\sigma(x)|^{1/d}$ if v corresponds to the embedding $\sigma : \mathbb{K} \hookrightarrow \mathbb{R}$;
(ii) $|x|_v = |\sigma(x)|^{2/d} = |\overline{\sigma}(x)|^{2/d}$ if v corresponds to the pair of conjugate complex embeddings $\sigma, \overline{\sigma} : \mathbb{K} \hookrightarrow \mathbb{C}$;
(iii) $N_{\mathbb{K}/\mathbb{Q}}(\pi)^{-\mathrm{ord}_\pi(x)/d}$ if v corresponds to the prime ideal π of $\mathcal{O}_\mathbb{K}$.

These absolute values satisfy the product formula

$$\prod_{v \in M(\mathbb{K})} |x|_v = 1 \qquad \text{for } x \in \mathbb{K}^*.$$

Let $n \geq 2$ and $\mathbf{x} = (x_1, \ldots, x_n)$ be in $\mathbb{K}^n$ with $\mathbf{x} \neq \mathbf{0}$. For a place v in $M(\mathbb{K})$ put

$$\begin{aligned} |\mathbf{x}|_v &= \left(\sum_{i=1}^{n} |x_i|_v^{2d} \right)^{1/(2d)} && \text{if } v \text{ is real infinite;} \\ |\mathbf{x}|_v &= \left(\sum_{i=1}^{n} |x_i|_v^{d} \right)^{1/d} && \text{if } v \text{ is complex infinite;} \\ |\mathbf{x}|_v &= \max\{|x_1|_v, \ldots, |x_n|_v\} && \text{if } v \text{ is finite.} \end{aligned}$$

Now define the *height* of $\mathbf{x}$ by

$$H(\mathbf{x}) = H(x_1, \ldots, x_n) = \prod_{v \in M(\mathbb{K})} |\mathbf{x}|_v.$$

We stress that $H(\mathbf{x})$ depends only on $\mathbf{x}$ and not on the choice of the number field $\mathbb{K}$ containing the coordinates of $\mathbf{x}$ (see e.g. [4]). If $L(\mathbf{x}) = a_1 x_1 + \cdots + a_n x_n$ is a linear form with algebraic coefficients in $\mathbf{x}$, we write $H(L)$ for the height of its normal vector $H(a_1, \ldots, a_n)$.

We use the following formulation of the Subspace Theorem. In the sequel, we assume that the algebraic closure of $\mathbb{K}$ is $\overline{\mathbb{Q}}$. We choose for every place v in $M(\mathbb{K})$ a continuation of $|\cdot|_v$ to $\overline{\mathbb{Q}}$ that we denote also by $|\cdot|_v$.

THEOREM 2.1. *Let $\mathbb{K}$ be an algebraic number field. Let $m \geq 2$ be an integer. Let $\mathcal{S}$ be a finite set of places on $\mathbb{K}$ of cardinality s containing all infinite places. For each v in $\mathcal{S}$ let $L_{1,v}, \ldots, L_{m,v}$ be linearly independent linear forms in m variables with algebraic coefficients. Let ε be real with $0 < \varepsilon < 1$. Then the set of solutions $\mathbf{x} \in \mathbb{K}^m$ to the inequality*

$$\prod_{v \in \mathcal{S}} \prod_{i=1}^{m} \frac{|L_{i,v}(\mathbf{x})|_v}{|\mathbf{x}|_v} \leq \prod_{v \in S} \left(|\det(L_{1,v}, \ldots, L_{m,v})|_v \right) H(\mathbf{x})^{-m-\varepsilon} \tag{2.1}$$

lies in finitely many proper subspaces of $\mathbb{K}^m$. Furthermore, if H and D are such that

$$H(L_{i,v}) \leq H \qquad \text{and} \qquad [\mathbb{K}(L_{i,v}) : \mathbb{K}] \leq D \qquad \text{for all } i = 1, \ldots, m,\ v \in \mathcal{S}, \tag{2.2}$$

then the following two assertions hold:

(i) *There exist proper linear subspaces $T_1, \ldots, T_{t_1}$ of $\mathbb{K}^m$ with*

$$t_1 \leq \left(2^{60m^2} \epsilon^{-7m} \right)^s \log 4D \log\log 4D,$$

such that every solution $\mathbf{x} \in \mathbb{K}^m$ with $H(\mathbf{x}) \geq H$ of inequality (2.1) belongs to $T_1 \cup \cdots \cup T_{t_1}$.

(ii) *There exist proper linear subspaces $S_1, \ldots, S_{t_2}$ of $\mathbb{K}^m$ with*

$$t_2 \leq \left(150 m^4 \varepsilon^{-1} \right)^{ms+1} (2 + \log\log 2H),$$

such that every solution $\mathbf{x} \in \mathbb{K}^m$ *with* $H(\mathbf{x}) < H$ *of inequality* (2.1) *belongs to* $S_1 \cup \cdots \cup S_{t_2}$.

For a proof of Theorem 2.1 the reader is directed to [4].

In the case when all the components of $\mathbf{x}$ are algebraic integers and if one is not interested in effective bounds for the number of subspaces involved, then the above statement can be simplified as follows.

THEOREM 2.2. *Let* $\mathbb{K}$ *be an algebraic number field. Let* $m \geq 2$ *be an integer. Let* $\mathcal{S}$ *be a finite set of places on* $\mathbb{K}$ *of cardinality* s *containing all infinite places. For each* v *in* $\mathcal{S}$ *let* $L_{1,v}, \ldots, L_{m,v}$ *be linearly independent linear forms in* m *variables with algebraic coefficients. Let* ε *be real with* $0 < \varepsilon < 1$. *Then, the set of solutions* $\mathbf{x} \in \mathcal{O}_{\mathbb{K}}^m$ *to the inequality*

$$\prod_{v \in \mathcal{S}} \prod_{i=1}^{m} |L_{i,v}(\mathbf{x})|_v < H(\mathbf{x})^{-\varepsilon}$$

is contained in the union of finitely many proper subspaces of $\mathcal{O}_{\mathbb{K}}^m$.

Let $\mathcal{S}$ be as in Theorem 2.1. Recall that an $\mathcal{S}$-unit is an element of $x \in \mathbb{K}$ such that $|x|_v = 1$ for all $v \notin \mathcal{S}$. We shall need the following version of a theorem of Evertse ([3]) on $\mathcal{S}$-unit equations.

LEMMA 2.3. *Let* $a_1, \ldots, a_N \in \mathbb{K}$ *be nonzero. Then the equation*

$$\sum_{i=1}^{N} a_i u_i = 1$$

in $\mathcal{S}$*-unit unknowns* u_i *for* $i = 1, \ldots, N$ *such that* $\sum_{i \in I} a_i u_i \neq 0$ *for each nonempty proper subset* $I \subset \{1, \ldots, N\}$ *has only finitely many solutions* $(u_1, \ldots, u_N)$.

Recall that an exponential polynomial is a sequence whose general term has the form $u_n = \sum_{i=1}^{s} \gamma_i \alpha_i^n$, where $\gamma_1, \alpha_1, \ldots, \gamma_s, \alpha_s$ are nonzero algebraic numbers. We assume that $\alpha_1, \ldots, \alpha_s$ are distinct and that

$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_s|.$$

The numbers $\gamma_1, \ldots, \gamma_s$ are called the *coefficients* and the numbers $\alpha_1, \ldots, \alpha_s$ are called the *roots* of the exponential polynomial, respectively. The sequence $(u_n)_{n \geq 0}$ is linearly recurrent with characteristic polynomial

$$f(X) = \prod_{i=1}^{s} (X - \alpha_i).$$

One well-known consequence of Theorem 2.2 and Lemma 2.3 is the following statement regarding the number of zeros and the rate of growth of exponential polynomials which was first proved independently by Evertse ([3]) and van der Poorten and Schlickewei ([13]) (this appears also as Theorem 2.3 on page 32 in [2]).

LEMMA 2.4. *Let $\alpha_1, \ldots, \alpha_s$ be nonzero algebraic numbers such that the number α_i/α_j is not a root of unity for any $i \neq j$ in $\{1, \ldots, s\}$. Then the following hold:*

(i) *The set of n such that $u_n = 0$ is finite.*
(ii) *Given any $\varepsilon > 0$, the set of n such that $|u_n| < |\alpha_1|^{(1-\varepsilon)n}$ is finite.*

Note that (ii) above implies (i) but we have also included (i) since it will be used in what follows.

Finally, we will need lower bounds for linear forms in complex logarithms, due to Matveev ([10]). To formulate them, we recall that if α is an algebraic number the naïve height of α denoted by $h(\alpha)$ is the maximum between 3 and the absolute values of the coefficients of the minimal nonzero primitive polynomial with integer coefficients having α as a root.

LEMMA 2.5. *Let $a_1, \ldots, a_N \in \mathbb{K}$ be nonzero and, for $1 \leq i \leq N$, let A_i be an upper bound for $h(a_i)$. Let $x_1, \ldots, x_N$ be integers such that $a_1^{x_1} \cdots a_N^{x_N} \neq 1$. Let $X \geq \max\{|x_i| : i = 1, \ldots, N\}$. Then, the inequality*

$$\log |a_1^{x_1} \cdots a_N^{x_N} - 1| > -C^N (\log A_1) \cdots (\log A_N)(\log X),$$

holds, where C is a constant which depends only on the degree d of $\mathbb{K}$.

3. Results

Let $b > 1$ be a positive integer. For a positive integer n we write $s_b(n)$ for the sum of the digits of n when written in base b. Our first result gives a lower bound for $s_b(m)$ as m runs through positive integers of the form $\lfloor \theta^n \rfloor$. Versions of this result have appeared in [8] and [16].

THEOREM 3.1. *Assume that $\theta > 1$ is algebraic. Assume further that $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ. Then, the inequality*

$$s_b(\lfloor \theta^n \rfloor) \gg \frac{\log n}{\log \log n}$$

holds for all $n > 1$. The same result holds with $\lfloor \cdot \rfloor$ replaced by $\lceil \cdot \rceil$, or $\lfloor \cdot \rceil$. Furthermore, the same inequality holds when $\theta^\ell \in \mathbb{Z}$ holds for some positive integer ℓ if one further assumes that θ and b are multiplicatively independent.

PROOF. We assume that $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ. Write

$$\theta^n + \lambda_n = a_0 b^{t_0} + a_1 b^{t_1} + \cdots + a_k b^{t_k}, \tag{3.1}$$

where $a_i \in \{1, \ldots, b-1\}$ are nonzero digits in basis b of the number on the left and

$$0 < |\lambda_n| \leq 1. \tag{3.2}$$

Here, $t_0 > t_1 > \cdots > t_k \geq 0$. Of course, $k,\ a_0,\ t_0,\ a_1,\ t_1, \ldots,\ a_k,\ t_k$ depend on n. We write n_0 for a large positive integer depending on θ and b not necessarily the same at each occurrence. Clearly, $a_0 \neq 0$ if $n > n_0$. Since

$$b^{t_0} \leq \theta^n + 1 \qquad \text{and} \qquad \theta^n - 1 \leq (b-1)(b^{t_0+1} - 1),$$

we get easily that

$$t_0 = n\frac{\log \theta}{\log b} + O(1) \tag{3.3}$$

as $n \to \infty$. Relation (3.1) can be rewritten as

$$\left|a_0 b_0^{t_0} \theta^{-n} - 1\right| \leq \frac{a_1 b^{t_1} + \cdots + a_k b^{t_k} + |\lambda_n|}{\theta^n} < \frac{2b}{b^{t_0 - t_1}} \tag{3.4}$$

provided that $n > n_0$. For $n > n_0$, the expression on the left above is not zero. Furthermore, also for $n > n_0$, estimate (3.3) shows that

$$t_0 \leq n^2. \tag{3.5}$$

Taking logarithms in the inequality (3.4) and applying Lemma 2.5 together with estimate (3.5), we get

$$-c_1 (\log b)^2 (\log h(\theta)) \log n \leq -(t_0 - t_1) \log b + \log(2b),$$

where $c_1 > 0$ is some constant depending only on the degree of θ. For $n > n_0$, the above inequality implies that

$$t_0 - t_1 \leq c_2 \log n, \tag{3.6}$$

where one can take $c_2 = 2c_1 (\log b) \log h(\theta)$ provided that $n > n_0$.

We now show that there exists a constant $c_3 > 0$ such that the inequality

$$t_0 - t_i < (c_3 \log n)^i \tag{3.7}$$

holds for all $i = 1, \ldots, k$. Inequality (3.6) proves that inequality (3.7) holds at $i = 1$ when $n > n_0$ with any constant $c_3 \geq c_2$. Assume that it holds with some $i \in \{1, \ldots, k-1\}$ and let us prove that it holds with i replaced by $i+1$.

Rewrite (3.1) as

$$\left|(a_0 b^{t_0 - t_i} + \cdots + a_i) b^{t_i} \theta^{-n} - 1\right| \leq \frac{a_{i+1} b^{t_{i+1}} + \cdots + a_k b^{t_k} + |\lambda_n|}{\theta^n} \leq \frac{2b}{b^{t_0 - t_{i+1}}} \tag{3.8}$$

for $n \geq n_0$. Assume first that the expression on the left is nonzero. Then Lemma 2.5 together with estimate (3.5) imply that

$$-c_1 (\log n)(\log b)(\log h(\theta)) \log(b^{t_0 - t_i + 1}) \leq -(t_0 - t_{i+1}) \log b + \log(2b).$$

We may assume that $t_{i+1} - t_0 \geq 4$, otherwise the desired inequality (3.7) holds with i replaced by $i+1$ provided that $n \geq n_0$. Thus,

$$(t_{i+1} - t_i) \log b \geq 4 \log b \geq 2 \log(2b).$$

Since also

$$\log(b^{t_0-t_i+1}) \le 2(t_0-t_i)\log b \le 2(\log b)(c_3\log n)^i,$$

we get that

$$\begin{aligned} -(2c_1(\log b)^2\log h(\theta))(c_3\log n)^i(\log n) &\le -(t_0-t_{i+1})\log b + \log(2b) \\ &\le -\frac{(t_0-t_{i+1})}{2}\log b, \end{aligned}$$

giving

$$t_0 - t_{i+1} \le (4c_1\log b\log h(\theta))(c_3\log n)^i(\log n).$$

Hence, choosing $c_3 = 2c_2$, we note that $c_3 > c_2$ and that inequality (3.7) with i implies the same inequality with i replaced by $i+1$. This conclusion was drawn under the assumption that

$$\theta^n - \left(a_0b^{t_0} + \cdots + a_ib^{t_i}\right) \ne 0, \tag{3.9}$$

which is true because $\theta^n \notin \mathbb{Z}$. Hence, inequality (3.7) holds for all $i = 1, \ldots, k$. We now rewrite again (3.1) as

$$\left|(a_0b^{t_0-t_k} + \cdots + a_k)b^{t_k}\theta^{-n} - 1\right| \le \frac{1}{\theta^n}. \tag{3.10}$$

The left hand side above is $\lambda_n\theta^{-n} \ne 0$. Applying again Lemma 2.5 and estimate (3.5), we get that

$$-c_1(\log b)(\log h(\theta))(\log n)\log(b^{t_0-t_k+1}) \le -n\log\theta,$$

giving

$$n\log\theta \le c_1(\log b)^2(\log h(\theta))(\log n)(t_0-t_k+1) \le (c_4\log n)^{k+1}, \tag{3.11}$$

where we can take $c_4 = c_3\log b$. This last inequality obviously leads to the conclusion that

$$k \ge (1+o(1))(\log n)/\log\log n \quad \text{as} \quad n \to \infty,$$

which is slightly more than what we wanted to prove.

The above argument deals with the statement of the theorem when $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ by taking λ_n to be $\theta^n - \lfloor\theta^n\rfloor$, or $\theta^n - \lceil\theta^n\rceil$, or the minimum between the above two expressions, respectively. Minor modifications deal with the case when $\theta^\ell \in \mathbb{Z}$ for some positive integer ℓ. Indeed, the fact that $\theta^\ell \notin \mathbb{Z}$ was only used to justify that the expression (3.9) is nonzero. Assume, with the previous notations, that

$$(c_3\log n)^k \le \frac{n}{\log n}, \tag{3.12}$$

since otherwise the desired inequality is true. If the expression appearing at (3.9) is zero for some $i \le k$, it then follows, in particular, that $\theta^n \in \mathbb{Z}$. Letting ℓ be the minimal positive integer such that $\theta^\ell \in \mathbb{Z}$, we conclude that $\ell \mid n$. Thus, we may replace θ by θ^ℓ and therefore assume that $\ell = 1$; i.e., $\theta \in \mathbb{Z}$. Let $i \le k$ be minimal such that the expression shown at (3.9) is zero. Note

that for $i = n$ this expression is zero anyway since $\theta^n \in \mathbb{Z}$. Then the above inductive argument gives $t_0 - t_i \le (c_3 \log n)^i$. Let $q_1, \ldots, q_s$ be all the distinct primes dividing θb and write

$$\theta = \prod_{j=1}^{s} q_j^{u_j} \qquad \text{and} \qquad b = \prod_{j=1}^{s} q_j^{v_j}$$

for some nonnegative exponents $u_1, v_1, \ldots, u_s, v_s$. Then the relation

$$\theta^n = b^{t_i}(a_0 b^{t_0 - t_i} + \cdots + a_i)$$

together with estimate (3.12) shows that

$$u_j = v_j t_i + O\left(\frac{n}{\log n}\right)$$

holds for $j = 1, \ldots, s$, where the constant implied by the above O depends on θ and b. In particular, $u_j \ne 0$ if and only if $v_j \ne 0$ holds for $n > n_0$. Thus, $u_j v_j \ne 0$ for all $j = 1, \ldots, s$ and

$$\left|\frac{u_j}{v_j} - \frac{t_i}{n}\right| = O\left(\frac{1}{\log n}\right) \qquad \text{for all } j = 1, \ldots, s.$$

Thus, if j_1, j_2 are in $\{1, \ldots, s\}$, we then get that

$$\left|\frac{u_{j_1}}{v_{j_1}} - \frac{u_{j_2}}{v_{j_2}}\right| = O\left(\frac{1}{\log n}\right).$$

For $n > n_0$, the above estimates imply that

$$\frac{u_{j_1}}{v_{j_1}} = \frac{u_{j_2}}{v_{j_2}} \qquad \text{for all } j_1,\ j_2 \in \{1, \ldots, s\}.$$

Writing u/v for the common value of all u_j/v_j for $j = 1, \ldots, s$, we get that $\theta^n = b^v$, which contradicts the fact that θ and b are not multiplicatively independent.

□

REMARK 3.2. The same conclusion remains true if the sequences of general term $u_n = \lfloor \theta^n \rfloor$, etc., from the statement of Theorem 3.1 are replaced by sequences of integers $(u_n)_{n \ge 1}$ of the form

$$u_n = \theta^n + \lambda_n \qquad \text{for all } n \ge 0$$

with an algebraic number $\theta > 1$ satisfying the following conditions:

(i) either $\theta^n \notin \mathbb{Z}$ for any $n > 0$, or $\theta^\ell \in \mathbb{Z}$ for some positive integer ℓ but θ and b are multiplicatively independent.

(ii) There exists $\epsilon > 0$ and n_0 such that

$$|\lambda_n| < \theta^{(1-\epsilon)n} \qquad \text{holds for all } n > n_0.$$

Indeed, in this case, with the notation from the proof of Theorem 3.1, we assume additionally that

$$(c_3 \log n)^k < \frac{\epsilon \log \theta}{2 \log b},$$

since otherwise the desired inequality holds. Then

$$b^{t_0 - t_k} \leq \theta^{\epsilon n/2},$$

therefore the inequality

$$b^{t_k} \geq \theta^n - \theta^{(1-\epsilon)n} b^{(t_0 - t_k + 1)} \geq \frac{\theta^{(1-\epsilon/2)n}}{2b} > \theta^{(1-\epsilon)n} > |\lambda_n|$$

holds for $n > n_0$. Thus, estimates (3.4) and (3.8) hold. Estimate (3.10) also holds up to replacing n by ϵn in the exponent of θ appearing in the denominator in the right hand side, which in turn leads to an inequality similar to (3.11), except that its left hand side is now smaller by a factor of ϵ. This still implies the desired estimate.

THEOREM 3.3. *Let again $\theta > 1$ be an algebraic number such that $\theta^\ell \notin \mathbb{Z}$ for any positive integer $\ell > 0$. Then the inequality*

$$P(\lfloor \theta^n \rfloor) \gg \frac{\log n \log \log n}{\log \log \log n} \tag{3.13}$$

holds for all positive integers n, while the inequality

$$P(\lfloor \theta^n \rfloor) \gg \log n \log \log n \tag{3.14}$$

holds for almost all positive integers n. The same estimates hold with $\lfloor \theta^n \rfloor$ replaced by $\lceil \theta^n \rceil$, or by $\lfloor \theta^n \rceil$, respectively.

PROOF. Assume that the largest prime factor of $\lfloor \theta^n \rfloor$ is p_t. Then

$$\lfloor \theta^n \rfloor = p_1^{a_{1,n}} \cdots p_t^{a_{t,n}},$$

therefore

$$\left| 1 - \theta^{-n} p_1^{a_{1,n}} \cdots p_t^{a_{t,n}} \right| = O(\theta^{-n}). \tag{3.15}$$

Applying Lemma 2.5 to get a lower bound on the left hand side of estimate, together with the trivial estimate $a_i \ll n$, and taking logarithms of both sides, we get that there exists a computable absolute constant $c_1 > 0$ such that

$$n \log \theta < c_1^t (\log h(\theta)) \prod_{i=1}^{t} (\log p_i) \log n \qquad \text{for } n > n_0.$$

Since $p_i < i^2$ holds for all $i \geq 2$, we get that

$$\frac{n \log \theta}{(\log n) \log h(\theta)} \leq (2c_1 \log t)^t. \tag{3.16}$$

After taking logarithms, this last inequality leads to

$$(1+o(1))\log n \le t\log\log t$$

as $n\to\infty$. The last estimate above leads to the conclusion that the inequality $t > (1+o(1))(\log n)/(\log\log\log n)$ holds as $n\to\infty$. By the Prime Number Theorem, we get that

$$p_t = P(\lfloor \theta^n \rfloor) > (1+o(1))\frac{\log n\log\log n}{\log\log\log n} \qquad \text{as } n\to\infty,$$

which obviously implies estimate (3.13). Note that the implied constant in (3.13) can be taken to be any positive constant < 1 and the resulting inequality then holds once n is sufficiently large.

For the second inequality, we take $\mathbb{K} = \mathbb{Q}[\theta]$ and let d be its degree. We assume that X is a large positive real number. We let t be a function of X to be determined later and let

$$\mathcal{N} = \{X^{1/2} \le n \le X : P(\lfloor \theta^n \rfloor) \le p_t\}.$$

We may assume that t is sufficiently large such that p_t exceeds both the numerator and the denominator of the rational number $N_{\mathbb{K}/\mathbb{Q}}(\theta)$. Then

$$\left|\theta^n - \prod_{i=1}^{t} p_i^{a_{i,n}}\right| = |\lambda_n| < 1 \qquad \text{for } n\in\mathcal{N}. \tag{3.17}$$

We let $\mathcal{S}$ be the set of all valuations v of $\mathbb{K}$ such that $|p_i|_v \ne 1$ for some $i = 1,\dots,t$. Clearly, $|\mathcal{S}| = s \le d(t+1)$. We select the infinite valuation of $\mathcal{S}$ corresponding to the conjugation that sends θ to itself and we denote this valuation by w (note that θ is real, so $|\theta|_w = |\theta|^{1/d}$). We let $m = 2$ and for $\mathbf{x} = (x_1, x_2)$, we let $L_{i,v}(\mathbf{x}) = x_i$ for $(i,v)\in\{1,2\}\times\mathcal{S}$ except for $(i,v) = (2,w)$ for which we put $L_{2,w} = x_1 - x_2$. It is easy to see that $L_{1,v}(\mathbf{x})$ and $L_{2,v}(\mathbf{x})$ are linearly independent over $\mathbb{K}$ for all $v\in\mathcal{S}$. One also checks easily that condition (2.2) holds for our system of forms $L_{i,v}(\mathbf{x})$ for $i = 1,2$ and $v\in\mathcal{S}$ with $H = D = 1$. Furthermore,

$$|\det(L_{1,v}, L_{2,v})|_v = 1 \qquad \text{for all } v\in\mathcal{S}.$$

We now let $\mathbf{x} = (\theta^n, p_1^{a_{1,n}}\cdots p_t^{a_{t,n}})$, where $n\in\mathcal{N}$. It is then easy to see that

$$\begin{aligned}\prod_{v\in\mathcal{S}}\prod_{i=1}^{2}|L_{i,v}(\mathbf{x})|_v &= |\theta^n - p_1^{a_{1,n}}\cdots p_t^{a_{t,n}}|^{1/d}\prod_{v\in\mathcal{S}}|\theta^n|_v\prod_{v\in\mathcal{S}\setminus\{w\}}|p_1^{a_{1,n}}\cdots p_t^{a_{t,n}}|_v \\ &\ll (p_1^{a_{1,n}}\cdots p_t^{a_{t,n}})^{-1/d} \ll \theta^{-n/d}.\end{aligned} \tag{3.18}$$

Since $|x_2|_v \le 1$ for all finite valuations $v \in \mathcal{S}$ and $|x_1|_v = |x_2|_v = 1$ for all valuations v of $\mathbb{K}$ which are not in $\mathcal{S}$, one gets easily that

$$H(\mathbf{x}) \asymp H(\theta^n) = H(\theta)^n.$$

Let $\delta > 0$ be such that $\theta = H(\theta)^\delta$. Relation (3.18) now shows that

$$\prod_{v\in\mathcal{S}} \prod_{i=1}^{2} |L_{i,v}(\mathbf{x})|_v \ll H(\mathbf{x})^{-\delta/d},$$

therefore

$$\prod_{v\in\mathcal{S}} \prod_{i=1}^{2} \frac{|L_{i,v}(\mathbf{x})|_v}{|\mathbf{x}|_v} \ll H(\mathbf{x})^{-\delta/d} \left(\prod_{v\in\mathcal{S}} |\mathbf{x}|_v \right)^{-2} \le H(\mathbf{x})^{-2-\delta/d}, \tag{3.19}$$

where the last inequality follows from the fact that

$$H(\mathbf{x}) \le \prod_{v\in\mathcal{S}} |\mathbf{x}|_v,$$

which in turn holds because $\mathcal{S}$ contains all valuations v of $\mathbb{K}$ such that $|\mathbf{x}|_v \ge 1$. It thus follows that inequality (2.1) is satisfied for $m = 2$, our finite set of valuations $\mathcal{S}$ and system of linear forms $L_{i,v}(\mathbf{x})$ for $i = 1, 2$ and $v \in \mathcal{S}$ with $\varepsilon = \delta/2d$ assuming that X is large. For such large X, the argument from the end of the proof of Theorem 3.1 shows that $H(\mathbf{x}) > 1$. Now Theorem 2.1 shows that $\mathcal{N}$ is contained in at most

$$(2^{240}(d\delta^{-1})^{14})^{d(t+1)} \log 4d \log\log 4d$$

nontrivial subspaces. Note that a vector $\mathbf{x} = (x_1, x_2)$ to belong to a proper a subspace of $\mathbb{K}^2$ just means that $x_1/x_2 = \gamma$ has fixed value. If γ is fixed, then since $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ, it follows that there can exist at most one positive integer $n \in \mathcal{N}$ such that $\theta^n/(p_1^{a_{1,n}} \cdots p_t^{a_{t,n}}) = \gamma$. This shows that for large X we have

$$|\mathcal{N}| \le (2^{240}(d\delta^{-1})^{14})^{d(t+1)} \log 4d \log\log 4d.$$

If

$$t + 1 \le \frac{\log(2^{240}(d\delta^{-1})^{14})}{2d} \log X,$$

we then get that $|\mathcal{N}| \le X^{1/2} \log 4d \log\log 4d = o(X)$ as $X \to \infty$. Thus, for most n, the inequality

$$t + 1 \ge \frac{\log(2^{240}(d\delta^{-1})^{14})}{2d} \log n$$

holds. This implies, via the Prime Number Theorem, that the inequality

$$p_t \gg \log n \log\log n$$

holds for most positive integers n. Taking λ_n to be $\theta^n - \lfloor \theta^n \rfloor$, or $\theta^n - \lceil \theta^n \rceil$, or the minimum of the two, respectively, we get the desired estimates. □

REMARK 3.4. As Theorem 3.1, Theorem 3.3 also holds under slightly more general assumptions. Namely, both statements asserted by Theorem 3.3 remain true if the sequence of general term $u_n = \lfloor \theta^n \rfloor$ is replaced by a sequence of general term

$$u_n = \theta^n + \lambda_n,$$

where $\theta > 1$ is an algebraic number such that θ^ℓ is irrational for all positive integers ℓ and there exist $\epsilon > 0$ and $n > n_0$ such that

$$0 < |\lambda_n| < \theta^{(1-\epsilon)n} \qquad \text{holds for all } n \geq n_0.$$

Indeed, in this case, the right hand side of inequality (3.15) is replaced by $O(\theta^{\epsilon n})$. In turn, this leads to an inequality similar to (3.16) except that its left hand side is smaller by a factor of ϵ. This does not change the desired conclusion about p_t. For the second inequality, the right hand side of inequality (3.17) becomes $\theta^{(1-\epsilon)n}$. In turn, this implies that inequality (3.19) holds with the exponent of $H(\mathbf{x})$ equal to $-2 - \epsilon\delta/d$. This leads to the conclusion that for large X, the inequality (2.1) from the statement of Theorem 2.1 holds for $m = 2$, our set of valuations $\mathcal{S}$ and our system of linear forms $L_{i,v}(\mathbf{x})$ for $i = 1, 2$ and $v \in \mathcal{S}$ with $\varepsilon = \epsilon\delta/(2d)$. This leads to the desired conclusion except that the constant implied by the symbol $\gg$ in $p_t = P(u_n)$ also depends on ϵ. We give no further details.

For a positive integer $n = \prod_{i=1}^t q_i^{a_i}$, where $q_1 < \cdots < q_t$ are primes and a_i are positive integers for $i = 1, \ldots, t$, we write $\Omega(n) = \sum_{i=1}^t a_i$ for the total number of prime factors of n, including repetition. It is known that the maximal order of $\Omega(n)$ is $\log n / \log 2$ (see Lemma 3.7 below). Next, we ask whether this order of magnitude can be attained by a subsequence of the form $(\lfloor \theta^n \rfloor)_{n \geq 0}$, where $\theta > 1$ is an algebraic number. Considering the following scenarios:

1. Assume that $\theta^\ell \in \mathbb{Z}$ holds for some positive integer ℓ. Clearly, $\theta^\ell > 1$. Let p be a prime factor of θ^ℓ. Then, if n is any multiple of ℓ, we have that

$$\lfloor \theta^n \rfloor = \lceil \theta^n \rceil = \lfloor \theta^n \rceil = \theta^n \equiv 0 \pmod{p^{n/\ell}},$$

therefore

$$\Omega(\lfloor \theta^n \rfloor) = \Omega(\lceil \theta^n \rceil) = \Omega(\lfloor \theta^n \rceil) \gg n \gg \log(\theta^n)$$

holds for infinitely many n.

2. Assume that $\theta > 1$ is such that for some positive integer ℓ we have that $\theta^\ell = \eta$, where η is a Pisot number of degree e_1 whose minimal polynomial is congruent to $X^{e_1} \pmod{p}$ for some prime number p. In this case, we let $\eta_1 (= \eta),\ \eta_2,\ \ldots,\ \eta_{e_1}$ be all the conjugates of η. Clearly,

$$u_n = \sum_{i=1}^{e_1} \eta_i^n \in \mathbb{Z}$$

and $\sum_{i=2}^{e_1} \eta_i^n = o(1)$ as $n \to \infty$. Thus, if n is sufficiently large, then $u_n = \lfloor \eta^n \rceil = \lfloor \theta^{\ell n} \rceil$. Now note that since the minimal polynomial of η is congruent to $X^{e_1} \pmod{p}$, it follows that p divides $\eta_i^{e_1}$ for all $i = 1, \ldots, e_1$. In particular,

$$p^{\lfloor n/e_1 \rfloor} \mid \sum_{i=1}^{e_1} \eta_i^n = u_n.$$

Thus,

$$\Omega(\lfloor \theta^{\ell n} \rceil) \geq \lfloor n/e_1 \rfloor \gg \log(\theta^{\ell n})$$

holds for all sufficiently large n.

As an example, we leave it to the reader to verify that if p is any prime and d is odd and large with respect to p, then the polynomial

$$f_{p,d}(X) = X^d - 2pX - p$$

is a Pisot polynomial (i.e., the minimal polynomial of a Pisot number).

The next result shows that up to allowing also Salem numbers, the above two cases are the only ones for which $\lfloor \theta^n \rfloor$, or $\lceil \theta^n \rceil$, or $\lfloor \theta^n \rceil$ can have a very large total number of prime factors for infinitely many n. The precise statement is as follows. Recall that a Salem number is an algebraic integer $\theta > 1$ all whose conjugates are inside or on the unit circle and at least one of them has absolute value one. Now the precise statement of the result is as follows.

THEOREM 3.5. *Let $\theta > 1$ be an algebraic number such that neither $\theta^\ell \notin \mathbb{Z}$ for a positive integer ℓ, nor is θ^ℓ a Pisot or a Salem number whose minimal polynomial is congruent to a monomial modulo some prime number. Then the estimate*

$$\Omega(\lfloor \theta^n \rfloor) = o(n)$$

holds as $n \to \infty$. The same conclusion holds when $\lfloor \theta^n \rfloor$ is replaced by $\lceil \theta^n \rceil$, or $\lfloor \theta^n \rceil$, respectively.

In order to prove Theorem 3.5, we need the following technical result.

THEOREM 3.6. *Let $\theta > 1$ be any algebraic number such that either $\theta^\ell \notin \mathbb{Z}$ for any positive integer ℓ, or θ^ℓ is not some Pisot or Salem number whose minimal polynomial is congruent to a monomial modulo some prime number. Then, for every finite set of places $\mathcal{S}$ of $\mathbb{K} = \mathbb{Q}[\theta]$ and for every $\epsilon > 0$ there are only finitely positive integers n such that*

$$\prod_{v \in \mathcal{S}} |\lfloor \theta^n \rfloor|_v < \frac{1}{\theta^{n\epsilon}}. \tag{3.20}$$

The same conclusion holds if one replaces $\lfloor \theta^n \rfloor$ by $\lceil \theta^n \rceil$, or $\lfloor \theta^n \rceil$, respectively.

PROOF. We assume that there are infinitely many values of n for which inequality (3.20) holds and we shall reach a contradiction.

We let d be the degree of θ and let $\theta_1(=\theta), \theta_2, \ldots, \theta_d$ be all its conjugates. Let $\mathbb{L} = \mathbb{Q}[\theta_1, \ldots, \theta_d]$ be the normal closure of $\mathbb{K} = \mathbb{Q}[\theta]$. We let $\overline{\mathcal{S}}$ be the set of valuations of $\mathbb{L}$ consisting of the following ones:

(i) valuations v of $\mathbb{L}$ extending some valuation of $\mathbb{K}$ from $\mathcal{S}$;
(ii) valuations v of $\mathbb{L}$ sitting above some prime p_i for $i = 1, \ldots, t$, where t is a sufficiently large positive integer such that p_t exceeds the largest prime factor of both the numerator and the denominator of the rational number $N_{\mathbb{K}/\mathbb{Q}}(\theta)$.

It is clear that if n is such that inequality (3.20) holds, then the same inequality also holds when v runs in the subset of all the finite valuations of $\mathbb{L}$. We let $\mathcal{N}$ be the set of positive integers n such that inequality (3.20) is fulfilled. Let U be the group of roots of unity inside $\mathbb{L}$ and let M be its cardinality. Assume that $\{\theta_1^M, \ldots, \theta_d^M\}$ has precisely d_1 distinct elements. Up to relabeling the conjugates $\theta_2, \ldots, \theta_d$ of θ_1, we may assume that $\theta_1^M, \ldots, \theta_{d_1}^M$ are distinct. Put $\alpha_i = \theta_i^M$ for $i = 1, \ldots, d_1$. By Galois theory, α_1 has degree d_1 and all its conjugates are $\alpha_1, \ldots, \alpha_{d_1}$. Let us note that α_i/α_j is not a root of 1 for any $i \neq j$ in $\{1, \ldots, d_1\}$. Indeed, assume that α_i/α_j is a root of 1. Then $(\theta_i/\theta_j)^M$ is a root of 1, therefore θ_i/θ_j is also a root of 1. Since $\theta_i/\theta_j \in \mathbb{L}$, we get that this root of 1 is in U, a group of order M. But then $(\theta_i/\theta_j)^M = 1$, therefore $\alpha_i = \alpha_j$, which is not allowed. So far, we know that α_i/α_j is not a root of 1 for any $i \neq j$ in $\{1, \ldots, d_1\}$.

Assuming that the inequality (3.20) is fulfilled for infinitely many positive integers n, we conclude that there exists $a \in \{0, 1, \ldots, M-1\}$ and infinitely many positive integers n such that inequality (3.20) holds with n replaced by $a + Mn$.

Now let $m = d_1 + 1$, put $\mathbf{x} = (x_1, \ldots, x_m)$ and the system of forms $L_{i,v}(\mathbf{x})$ for $i = 1, \ldots, m$ and $v \in \overline{\mathcal{S}}$ given as follows:

(i) $L_{i,v}(\mathbf{x}) = \theta_{i_v}^a x_i$ for all $i = 1, \ldots, d_1$ and all $v \in \overline{\mathcal{S}}$;
(ii) $L_{m,v}(\mathbf{x}) = x_m$ for all finite valuations $v \in \overline{\mathcal{S}}$;
(iii) For any infinite valuation $v \in \overline{\mathcal{S}}$ corresponding to some automorphism of $\mathbb{L}$ into itself, let $i_v \in \{1, \ldots, d\}$ be such that θ_{i_v} is mapped via this automorphism to θ_1. Let $j_v \in \{1, \ldots, d_1\}$ be such that $\theta_{i_v}^M = \theta_{j_v}^M$. Then put $L_{m,v}(\mathbf{x}) = \theta_{i_v}^a x_{j_v} - x_m$.

One checks easily that the system of forms $L_{i,v}(\mathbf{x})$ for $i = 1, \ldots, m$ consists of m linearly independent linear forms for all $v \in \overline{\mathcal{S}}$. Further, the condition (2.2) holds for our system of forms with $H = H(\theta_1, \cdots, \theta_d)^M$ and $D = d!/d_1$ although these parameters will not be needed in the proof that follows. We write again

$$\theta^n + \lambda_n = u_n,$$

where $0 < |\lambda_n| < 1$. For our system of forms with

$$\mathbf{x} = (\alpha_1^n, \alpha_2^n \cdots, \alpha_{d_1}^n, u_{a+Mn}) \qquad \text{and} \qquad a + Mn \in \mathcal{N},$$

we have the following estimate

$$\begin{aligned}\prod_{i=1}^{m}\prod_{v\in\mathcal{S}}|L_{i,v}(\mathbf{x})|_v &= \prod_{i=1}^{d_1}\prod_{v\in\overline{\mathcal{S}}}|\theta_i^a\alpha_i^n|_v\prod_{\substack{v\in\overline{\mathcal{S}}\\ v \text{ finite}}}|u_{a+Mn}|_v\\ &\quad\times\prod_{\substack{v\in\overline{\mathcal{S}}\\ v \text{ infinite}}}|\theta_{i_v}^n\alpha_{j_v}^n-u_{a+Mn}|_v\\ &= |\theta^{a+Mn}-u_{a+Mn}|\prod_{\substack{v\in\overline{\mathcal{S}}\\ v \text{ finite}}}|u_{a+Mn}|_v\\ &\ll \theta^{-nM\epsilon}\ll\alpha_1^{-n\epsilon}.\end{aligned}$$

As in the proof of Theorem 3.3, the above inequality implies that

$$\prod_{i=1}^{m}\prod_{\nu\in\mathcal{S}}\frac{|L_{i,v}(\mathbf{x})|_v}{|\mathbf{x}|_v}\ll H(\mathbf{x})^{-m-n\epsilon\delta},$$

where $\delta>0$ is such that $\theta=H(\theta)^{\delta}$. Theorem 2.2 now tells us that $\mathcal{N}$ is contained in finitely many nontrivial subspaces of $\mathbb{L}^m$. Let one such nontrivial subspace be given by an equation of the form

$$\sum_{i=1}^{m}\gamma_i x_i=0,$$

where not all coefficients $\gamma_1,\ldots,\gamma_m$ are zero. Hence, we have arrived to the equation

$$\sum_{i=1}^{d_1}\gamma_i\alpha_i^n+\gamma_{d_1+1}u_{a+Mn}=0. \tag{3.21}$$

If $\gamma_{d_1+1}=0$, we then get that

$$\sum_{i=1}^{d_1}\gamma_i\alpha_i^n=0 \tag{3.22}$$

and not all γ_i for $i=1,\ldots,d_1$ are equal to zero. Since α_i/α_j is not a root of unity for any $i\neq j$, Lemma 2.4 (i) shows that there can be only finitely many positive integers n such that relation (3.22) holds.

Assume next that $\gamma_{d_1+1}\neq 0$. Suppose that $d_1=1$. Then writing $\gamma=\gamma_{d_1+1}/\gamma_1$ (note that $\gamma_1\neq 0$), we then get that $\alpha_1^n=\gamma u_n$. If this equation has at least two positive integer solutions n, we then get that there exists a positive integer ℓ such that $\alpha_1^{\ell}\in\mathbb{Q}$ (here, we can take ℓ to be the difference between two solutions for n, say n_1 and n_2). If furthermore this equation has infinitely many positive integer solutions n, it follows that there exists $b\in\{0,1,\ldots,\ell-1\}$ such that infinitely many of these solutions will have $n\equiv b\pmod{\ell}$. Write $n=b+\ell n_1$. Then, writing $\gamma'=\gamma/\alpha_1^b$, we get that

$(\alpha_1^\ell)^{n_1} = \gamma' u_{b+\ell n_1}$ holds for infinitely many positive integers n_1. In turn, this is possible only if $\alpha_1^\ell \in \mathbb{Z}$ (since the numbers of the form $\gamma' u_{b+\ell n_1}$ have bounded denominators independently of n_1). Thus, we have arrived at the conclusion that $\theta^{M\ell}$ is an integer, which was excluded.

Assume next that still $\gamma_{d_1+1} \neq 0$ but $d_1 \geq 2$. Write $\gamma_i' = \gamma_i/\gamma_{d_1+1}$. Conjugating the relation

$$\sum_{i=1}^{d_1} \gamma_i' \alpha_i^n = u_{a+Mn} \tag{3.23}$$

by an appropriate Galois automorphism of $\mathbb{L}$, we may assume that $\gamma_1' \neq 0$. Using also the fact that $u_n = \theta^a \alpha_1^n + \lambda_n$, we have

$$(\gamma_1' - \theta_1^a)\alpha_1^n + \sum_{i=2}^{d_1} \gamma_i' \alpha_i^n = \lambda_{a+Mn} = O(1).$$

Since $|\alpha_1| > 1$, (ii) of Lemma 2.4 shows that unless $\gamma_1' = \theta_1^a$, the above estimate is possible only for finitely many values of n. Knowing that $\gamma_1' = \theta_1^a$, we claim that $\gamma_j' = \theta_j^a$ holds for all $j = 1, \ldots, d_1$. Indeed, to see why this is true, note that if

$$\sum_{i=1}^{d_1} \widehat{\gamma}_i \alpha_i^n = u_{a+nM} \tag{3.24}$$

holds with some algebraic coefficients $\widehat{\gamma}_i$ for $i = 1, \ldots, d_1$, then necessarily $\widehat{\gamma}_i = \gamma_i'$ for all $i = 1, \ldots, d_1$. Indeed, this can be noticed by subtracting the above relation from (3.23) getting

$$\sum_{i=1}^{d_1} (\gamma_i' - \widehat{\gamma}_i)\alpha_i^n = 0,$$

relation which, by (i) of Lemma 2.4, has only finitely many positive integer solutions n provided that at least one of the coefficients $\gamma_i' - \widehat{\gamma}_i$ is not zero. With this observation, let σ be some Galois automorphism of $\mathbb{L}$ mapping θ_1 to θ_j. Conjugating relation (3.23) by σ, we get a relation like (3.24) where $\widehat{\gamma}_j = \theta_j^a$. Hence, $\gamma_j' = \theta_j^a$. We record this as follows.

$$\sum_{i=1}^{d_1} \theta_i^{a+Mn} = u_{a+Mn}.$$

In particular, $\gamma_j' \neq 0$ for any $j = 1, \ldots, d_1$. Replacing again u_{a+Mn} by $\theta_1^a \alpha_1^n + \lambda_{a+Mn}$, we get that $\sum_{j=2}^{d_1} \gamma_j' \alpha_j^n = O(1)$ holds for infinitely many n. Now (ii) of Lemma 2.4 implies that $|\alpha_j| \leq 1$ holds for all $j = 2, \ldots, d_1$. Furthermore, it is well-known and again a consequence of the Subspace Theorem 2.2, that the fact that $\sum_{i=1}^{d_1} \gamma_i' \alpha_i^n$ is an integer for infinitely many n implies that α_1 is an algebraic integer (see, for example, [1]). Let us briefly sketch the details

of such a deduction. Assume on the contrary that the denominator of α_1 is $D > 1$. Let $\beta_i = D\alpha_i \in \mathcal{O}_{\mathbb{L}}$ for $i = 1, \dots, d_1$ and write

$$(D) = \prod_{\pi \in \mathcal{P}} \pi^{a_\pi}$$

for a certain finite set of prime ideals $\mathcal{P}$ of $\mathcal{O}_{\mathbb{K}}$, where a_π is a positive integer for each $\pi \in \mathcal{P}$. If for each $\pi \in \mathcal{P}$ we have that $\pi^{a_\pi} \mid \beta_i$ for all $i = 1, \dots, d_1$, we conclude that $D = \prod_{\pi \in \mathcal{P}} \pi^{a_\pi}$ divides β_i for all $i = 1, \dots, d_1$. In particular, $\alpha_i = \beta_i / D \in \mathcal{O}_{\mathbb{K}}$ for all $i = 1, \dots, d_1$, contradicting the minimality of the positive integer D with such a property. Thus, there exist $\pi_0 \in \mathcal{P}$ and $i_0 \in \{1, \dots, d_1\}$ such that $\pi_0^{b_{\pi_0}} \| \beta_0$, where b_{π_0} is some positive integer strictly less that a_{π_0}. Note that

$$\sum_{i=1}^{d_1} \gamma_i' \beta_i^n = D^n u_{a+nM}$$

is divisible by $\pi^{na_\pi - c_0}$, where $c_0 > 0$ is some constant depending on the denominators of γ_i' for $i = 1, \dots, d_1$. We now take $m = d_1$ and $\mathcal{T}$ be all the valuations of $\mathbb{L}$ which are either infinite or correspond to prime ideals in $\mathcal{O}_{\mathbb{L}}$ which divide $DN_{\mathbb{L}/\mathbb{Q}}(\beta_1)$. Write v_0 for the valuation corresponding to π_0. Put $L_{i,m}(\mathbf{x}) = x_i$ for all $(i, v) \in \{1, \dots, d_1\} \times \mathcal{T}$ except for $(i, v) = (i_0, v_0)$, where we put $L_{i_0,v_0}(\mathbf{x}) = \sum_{i=1}^{d_1} c_i' x_i$. Evaluating the double product for our system of forms and valuations in $\mathbf{x} = (\beta_1^n, \dots, \beta_{d_1}^n)$ and using the fact that $\mathcal{T}$ consists of all possible valuations v of $\mathbb{L}$ such that $|\beta_i|_v \neq 1$ for some $i = 1, \dots, d_1$, we get that

$$\prod_{v \in \mathcal{T}} |L_{i,v}(\mathbf{x})|_v = |\sum_{i=1}^{d_1} \gamma_i' \beta_i^n|_{w_0} |\beta_{i_0}^n|_{w_0}^{-1} \ll \pi_0^{-n(a_{\pi_0} - b_{\pi_0})} \ll H(\mathbf{x})^{-\delta}$$

for some suitable number δ. We can take

$$\delta = \frac{d_1 \log(H(\beta_1, \dots, \beta_{d_1}))}{(a_{\pi_0} - b_{\pi_0}) \log p_0},$$

where p_0 is that prime number such that $N_{\mathbb{L}/\mathbb{Q}}(\pi_0)$ is a power of p_0. Theorem 2.2 now implies that $(\beta_1^n, \dots, \beta_{d_1}^n)$ can lie in only finitely many subspaces of $\mathcal{O}_{\mathbb{L}}$ and (i) of Lemma 2.4 shows the each of such subspaces can contain only finitely many of such vectors. Hence, there are only finitely many possibilities for n altogether, which is a contradiction.

In particular, θ_1 is an algebraic integer and θ_1^M is either a Pisot or a Salem number.

Returning to estimate (3.20), it follows easily that there exists a constant $\delta > 0$ depending on ε, $\mathcal{S}$ and θ and a prime ideal $\pi_0 \in \mathcal{O}_{\mathbb{L}}$, such that for infinitely many n, we have that $\pi_0^{\lfloor \delta n \rfloor} \mid u_{a+Mn}$. Indeed, let $\mathcal{P}$ be the set of all prime ideals corresponding to all the finite valuations of $\overline{\mathcal{S}}$. Put P for the

maximal prime number appearing in the factorization of $N_{\mathbb{L}/\mathbb{Q}}(\pi)$ for $\pi \in \mathcal{P}$ and t for the number of finite valuations in $\overline{\mathcal{S}}$. Then, writing

$$(u_{a+Mn}) = \prod_{\pi \in \mathcal{P}} \pi^{a_\pi} V,$$

where V is an ideal such that $|V|_\pi = 1$ for all $\pi \in \overline{\mathcal{S}}$, we get that if we put

$$a(n) = \max\{a_\pi : \pi \in \mathcal{P}\},$$

then the product appearing on the left of (3.20) exceeds $P^{-ta(n)/d_1}$. Inequality (3.20) implies that $a(n) \gg n$, where the constant understood in $\gg$, which we denote by δ, depends on P, d_1, θ and ϵ. Since we have infinitely many values for n and only finitely many elements in $\mathcal{P}$, it follows that we may assume that $a(n) = a_{\pi_0}$ holds for infinitely many n. Then

$$\sum_{i=1}^{d_1} \gamma_i' \alpha_i^n \equiv 0 \pmod{\pi_0^{\delta n}}$$

holds for infinitely many n. An argument similar to the one used to prove that α_i is an algebraic integer based on the Subspace Theorem now shows that $\pi_0 \mid \alpha_i$ must hold for all $i = 1, \ldots, d_1$. But this shows that the minimal polynomial $f(X)$ of α_1 is congruent to X^{d_1} modulo π_0 and, in particular, it is also congruent to X^{d_1} modulo p_0, where p_0 is the prime number such that $N_{\mathbb{L}/\mathbb{Q}}(\pi_0)$ is a power of p_0. Now θ is a root of $f(X^M)$, a polynomial congruent to $X^{Md_1} \pmod{p_0}$. Since the minimal polynomial of θ divides $f(X^M)$ and has degree d, we conclude that this polynomial must be $X^d \pmod{p_0}$, which finishes the proof. □

Now Theorem 3.5 is an immediate consequence of Theorem 3.6 and of the following lemma which has previously appeared in [9] concerning the structure of positive integers n with a large $\Omega(n)$.

LEMMA 3.7. (1) *The inequality* $\Omega(n) \le \dfrac{\log n}{\log 2}$ *holds for all positive integers* n.

(2) *Let* K *be any positive real number in the interval* $\left(0, \dfrac{1}{\log 2}\right)$ *and let* A_K *be the set of all positive integers* n *such that* $\Omega(n) \ge K \log n$. *Then* A_K *is infinite and there exist two computable positive constants* L *and* δ *with* $\delta < 1$ *depending only on* K *such that if* $n \in A_K$, *then there exists a prime number* $p < L$ *such that if we write* $n = p^{\alpha_p} m$ *where* $\gcd(p, m) = 1$, *then*

$$\log m < \delta \log n.$$

Finally, we look at the perfect powers in the sequence $(\lfloor \theta^n \rfloor)_{n \ge 0}$.

THEOREM 3.8. *Assume that $\theta > 1$ is a Pisot number. Then the equation*

$$x^k = \lfloor \theta^n \rfloor$$

has only finitely many positive integer solutions (x, k, n) with $x > 1$ and $k > 1$. The same conclusion remains true when $\lfloor \theta^n \rfloor$ is replaced by $\lceil \theta^n \rceil$, or $\lfloor \theta^n \rceil$, respectively.

PROOF. Write again

$$\theta^n + \lambda_n = x^k,$$

where $0 < |\lambda_n| < 1$. Then

$$|\theta^n - x^k| = O(1).$$

A result of Shorey and Stewart from [15] implies that k is bounded.

Now assume that $k \geq 2$ is fixed. We show that the equation $\lfloor \theta^n \rfloor = x^k$ has only finitely many positive integer solutions (n, x). Assume that this is not so. Since θ is Pisot, it follows that if we write $\theta_1 = \theta, \ldots, \theta_d$ for all the conjugates of θ (including itself), then

$$\sum_{\ell \geq 2} \theta_\ell^n = o(1)$$

as $n \to \infty$. In particular,

$$\lfloor \theta^n \rfloor = \sum_{\ell=1}^{d} \theta_\ell^n + \delta, \qquad \text{where } \delta \in \{-1, 0\}.$$

Since there are infinitely many pairs (n, x), we may assume that δ is common for infinitely many values of n. The sequence

$$u_n = \sum_{\ell=1}^{d} \theta_\ell^n + \delta$$

is a linearly recurrent sequence of order d, or $d+1$, according to whether $\delta = 0$, or -1, respectively, which has a dominant root θ. Theorem 2 on page 322 of [1] (for more general statements of this type see [5–7]) shows that there exists $a \in \{0, 1, \ldots, k-1\}$, an integer $s \geq 1$, and numbers $\alpha_1,\ \beta_1,\ \ldots, \alpha_s,\ \beta_s \in \overline{\mathbb{Q}}$ such that the identity

$$u_{kn+a} = \left(\sum_{\ell=1}^{s} \alpha_i \beta_i^n \right)^k$$

holds for all n. Further, a close analysis of the arguments used to prove the above statement, shows that there exist rational numbers $a_{i,j}$ whose denominators divide k such that $\beta_i = \prod_{j=1}^{d} \theta_i^{a_{i,j}}$ for all $i = 1, \ldots, s$. Thus, taking

$n = 2km$, and writing $\gamma_i = \beta_i^{2k}$, we get that

$$\sum_{i=1}^{d} (\theta_i)^a (\theta_i^m)^{2k^2} + \delta = u_{2k^2m+a} = \left(\sum_{i=1}^{s} \alpha_i \gamma_i^m \right)^{2k^2} \tag{3.25}$$

holds for all positive integers m. A result of Mignotte ([11]), shows that there is no nontrivial multiplicative relation among the θ_i's. By a trivial multiplicative relation, we mean that it could happen that $N_{\mathbb{K}/\mathbb{Q}}(\theta) = \pm 1$, in which case $\prod_{i=1}^{d} \theta_i = \pm 1$ is a trivial multiplicative relation on the θ_i's.

Assume first that $N_{\mathbb{K}/\mathbb{Q}}(\theta) \neq \pm 1$. In this case, the d functions $m \mapsto \theta_i^m$ are multiplicatively independent, and by a theorem of Ritt ([14]) (see also 3.2 in [12]), it follows that there exists a polynomial $P(X_1, \ldots, X_d) \in \overline{\mathbb{Q}}[X_1, \ldots, X_d]$ such that

$$\sum_{i=1}^{d} \delta_i X_i^{2k^2} + \delta = P(X_1, \ldots, X_d)^{2k^2}, \tag{3.26}$$

where we have put $\delta_i = \theta_i^a$ for all $i = 1, \ldots, d$. Since $d \geq 2$, the polynomial on the left is a binomial polynomial of the form $\delta_1 X_1^{2k^2} + Q(X_2, \ldots, X_m)$ as a polynomial in X_1, where $\delta_1 Q(X_2, \ldots, X_m)$ is nonzero. Of course, such a polynomial cannot have a double root (as a polynomial in the variable X_1), showing that relation (3.26) with $k \geq 2$ is impossible.

Assume finally that $N_{\mathbb{K}/\mathbb{Q}}(\theta) = \pm 1$. Then

$$\theta_d = \pm (\theta_1 \cdots \theta_{d-1})^{-1},$$

and the functions $m \to \theta_i^m$ are multiplicatively independent for $i = 1, \ldots, d-1$. Ritt's theorem tells us now that relation (3.25) implies that the rational function

$$\sum_{i=1}^{d-1} \delta_i X_i^{2k^2} + \delta_d \prod_{i=1}^{d-1} X_i^{-2k^2} + \delta$$

is the kth power of a rational function in $\overline{\mathbb{Q}}(X_1, \ldots, X_{d-1})$. In particular,

$$\prod_{i=1}^{d-1} X_i^{2k^2} \left(\sum_{i=1}^{d-1} \delta_i X_i^{2k^2} + \delta \right) + \delta_d = R(X_1, \ldots, X_{d-1})^k$$

for some $R(X_1, \ldots, X_{d-1}) \in \overline{\mathbb{Q}}[X_1, \ldots, X_{d-1}]$. As a polynomial in X_1, the polynomial on the left above is of the form

$$Q(X_1, \ldots, X_{d-1}) = AX_1^{4k^2} + BX_1^{2k^2} + C,$$

where

$$A = \delta_1 \prod_{i=2}^{d-1} X_i^{2k^2}, \qquad B = \prod_{i=2}^{d-1} X_i^{2k^2} \left(\sum_{i=2}^{d-1} \delta_i X_i^{2k^2} + \delta \right), \qquad C = \delta_d$$

are all three nonzero in $\overline{\mathbb{Q}}[X_2, \ldots, X_d]$. Such a polynomial does not have triple roots. It can have double roots only if

$$\Delta = B^2 - 4AC = 0,$$

in which case

$$Q(X_1, \ldots, X_{d-1}) = A(X^{2k^2} - Y)^2,$$

where $Y \in \overline{Q}[X_2, \ldots, X_{d-1}]$ is such that

$$AX_1^2 + BX_1 + C = A(X_1 - Y)^2.$$

For us,

$$\Delta = (X_2 \cdots X_{d-1})^{2k^2} \left(\left(\sum_{i=2}^{d-1} \delta_i X_i^{2k^2} + \delta \right)^2 - 4\delta_d \delta_1 \right).$$

Clearly, the above polynomial is never zero for $d \geq 3$. Thus, it remains to treat the case $d = 2$, $k = 2$. In this case, θ is a quadratic unit and $k = 2$. We can assume that θ is a fundamental unit. Write $\mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{D}]$ for some squarefree positive integer D. Let

$$\theta^n = X_n + \sqrt{D} Y_n,$$

where X_n and Y_n are positive integers. Then

$$X_n^2 - DY_n^2 = \pm 4, \ \pm 1,$$

according to whether $D \equiv 1 \pmod 4$ or not. Furthermore,

$$X_n = \frac{\theta_1^n + \theta_2^n}{2}.$$

Hence, $\theta_1^n + \theta_2^n = 2X_n$. It thus follows that

$$\lfloor \theta_1^n \rfloor = \theta_1^n + \theta_2^n + \delta = 2X_n + \delta,$$

where $\delta \in \{0, -1\}$. Thus, $\lfloor \theta^n \rfloor = x^2$ implies that $X_n = (x^2 - \delta)/2$, where $\delta \in \{0, -1\}$. Hence,

$$DY_n^2 = X_n^2 - \lambda = \left(\frac{x^2 - \delta}{2} \right)^2 - \lambda = \frac{x^4 - 2\delta x^2 + \delta^2 - 4\lambda}{4},$$

where $\delta \in \{0, -1\}$ and $\lambda \in \{\pm 1, \pm 4\}$. The discriminant of the quadratic polynomial $x^4 - 2\delta x^2 + (\delta^2 - 4\lambda)$ is $16\lambda \neq 0$. Thus, this polynomial has four simple roots. A well-known theorem of Siegel implies that the Diophantine equation

$$Dy^2 = \frac{x^4 - 2\delta x^2 + (\delta^2 - 4\lambda)}{2}$$

has only finitely many integer solutions (y, x) for each of the finitely many possibilities for the couple (δ, λ). Thus, even in the case $k = d = 2$ and $N_{\mathbb{K}/\mathbb{Q}}(\theta) = \pm 1$, there can be only finitely many n such that $\lfloor \theta^n \rfloor$ is a perfect power of exponent k. This takes care of the case $d = 2, \ k = 2$.

Similar arguments can be used to deal with the sequences of general term $\lceil \theta^n \rceil$, or $\lfloor \theta^n \rceil$, respectively (i.e., one only has to also allow for the possibility $\delta = 1$, which does not affect the preceding arguments). This completes the proof of Theorem 3.8. □

Acknowledgements.

The authors thank the anonymous referee for a careful reading of the manuscript and for suggestions that improved the quality of the paper. They are also grateful to Christian Mauduit who posed them many of the questions treated in this paper, and who encouraged them during its preparation, and to Yann Bugeaud for several suggestions and advice. Both authors were supported in part by the joint Project France-Mexico ANUIES-ECOS M01-M02.

References

[1] P. Corvaja and U. Zannier, *Some new applications of the subspace theorem*, Compositio Math. **131** (2002), 319-340.

[2] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, Recurrence sequences, Mathematical Surveys and Monographs **104**, American Mathematical Society, Providence, 2003.

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

[4] J.-H. Evertse, *An improvement of the quantitative subspace theorem*, Compositio Math. **101** (1996), 225-311.

[5] C. Fuchs, *Polynomial–exponential equations and linear recurrences*, Glas. Mat. Ser. III **38(58)** (2003), 233-252.

[6] C. Fuchs, *Polynomial-exponential equations involving multirecurrences*, Studia Sci. Math. Hungar. **46** (2009), 377-398.

[7] C. Fuchs and A. Scremin, *Polynomial-exponential equations involving several linear recurrences*, Publ. Math. Debrecen **65** (2004), 149-172.

[8] F. Luca, *Distinct digits in base b expansions of linear recurrence sequences*, Quaest. Math. **23** (2000), 389-404.

[9] F. Luca, *Arithmetic properties of positive integers with fixed digit sum*, Rev. Mat. Iberoam. **22** (2006), 369-412.

[10] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125-180. English transl. in Izv. Math. **64** (2000), 1217-1269.

[11] M. Mignotte, *Sur les conjugués des nombres de Pisot*, C. R. Acad. Sci. Paris Sér. I Math. **298** (1984), 21.

[12] A. J. van der Poorten, *Some facts that should be better known especially about rational functions*, in: Number Theory and its Applications, R. A. Mollin (Ed.), Kluwer Acad. Publ., Dordrecht, 1989, 497-528.

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

[14] J. F. Ritt, *A factorization theory for functions* $\sum_{i=1}^{n} a_i e^{\alpha_i z}$, Trans. Amer. Math. Soc. **29** (1927), 584-596.

[15] T. N. Shorey and C. L. Stewart, *Pure powers in recurrence sequences and some related Diophantine equations*, J. Number Theory **27** (1987), 324-352.

[16] C. L. Stewart, *On the representation of an integer in two different bases*, J. Reine Angew. Math. **319** (1980), 63-72.

F. Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán
México
E-mail: fluca@matmor.unam.mx

M. Mignotte
Université Louis Pasteur
UFR de mathématiques
7 rue René Descartes
67084 Strasbourg
France
E-mail: mignotte@math.u-strasbg.fr

Received: 5.11.2008.
Revised: 15.2.2009.