Bull Braz Math Soc, New Series 41(4), 551-566

On the intersection of infinite geometric and arithmetic progressions

Artūras Dubickas and Jonas Jankauskas

Abstract. We prove that the intersection $\mathcal{G} \cap \mathcal{A}$ of an infinite geometric progression $\mathcal{G} = u, uq, uq^2, uq^3, \ldots$, where $u > 0$ and $q > 1$ are real numbers, and an infinite arithmetic progression $\mathcal{A}$ contains at most 3 elements except for two kinds of ratios q. The first exception occurs for $q = r^{1/d}$, where $r > 1$ is a rational number and $d \in \mathbb{N}$. Then this intersection can be of any cardinality $s \in \mathbb{N}$ or infinite. The other (possible) exception may occur for $q = \beta^{1/d}$, where $\beta > 1$ is a real cubic algebraic number with two nonreal conjugates of moduli distinct from β and $d \in \mathbb{N}$. In this (cubic) case, we prove that the intersection $\mathcal{G} \cap \mathcal{A}$ contains at most 6 elements.

Keywords: arithmetic and geometric progression, fractional part, algebraic number, linear recurrence, zero multiplicity.

Mathematical subject classification: 11B25, 11B37, 11J71, 11R04, 11R06, 12D10.

1 Introduction

Let

$$\mathcal{G} = \mathcal{G}(u, q) := u, uq, uq^2, uq^3, \ldots \tag{1}$$

be an infinite geometric progression with the first term $u > 0$ and the ratio $q > 1$. Let also

$$\mathcal{A} = \mathcal{A}(v, D) := v, v + D, v + 2D, v + 3D, \ldots \tag{2}$$

be an infinite arithmetic progression with the first term $v \geqslant 0$ and the difference $D > 0$. Arithmetic and geometric progressions appear everywhere from elementary mathematics to the celebrated Green-Tao theorem on prime numbers that are consecutive terms of arithmetic progressions of arbitrary finite length. Obviously, for every $\mathcal{G}$ given in (1), there is an $\mathcal{A}$, where, e.g., $v := u$ and $D := u(q - 1)$, as in (2) such that the intersection $\mathcal{G} \cap \mathcal{A}$ contains at least 2

Received 16 March 2010.

elements. In this paper we are interested in the following natural question: *how large can the intersection $\mathcal{G} \cap \mathcal{A}$ be?*

It is easily seen that $\mathcal{G} \cap \mathcal{A}$ contains at most two elements if the ratio q of $\mathcal{G}$ is a transcendental number. Indeed, suppose that uq^a, uq^b, uq^c, where $0 \leqslant a < b < c$ are integers, are three elements of the arithmetic progression $v + Dm$, $m = 0, 1, 2, \ldots$, with indices $m_1 < m_2 < m_3$. Then

$$\frac{q^{c-a} - 1}{q^{b-a} - 1} = \frac{uq^c - uq^a}{uq^b - uq^a} = \frac{m_3 - m_1}{m_2 - m_1} \in \mathbb{Q}.$$

Thus q is a root of a polynomial in $\mathbb{Z}[x]$ which means that q must be an algebraic number over $\mathbb{Q}$.

The following result is a consequence of [7] and formula (5). It is stated here only for the sake of completeness.

Theorem 1. *For any geometric progression $\mathcal{G}$ with ratio $q > 1$, we have $|\mathcal{G} \cap \mathcal{A}| = \infty$ for some arithmetic progression $\mathcal{A}$ if and only if $q = m^{1/d}$ for some integers $m \geqslant 2$ and $d \geqslant 1$.*

The next result covers the ratios $q = r^{1/d}$, where $r > 1$ is a rational number and $d \in \mathbb{N}$. It shows that $|\mathcal{G} \cap \mathcal{A}|$ can take any nonnegative integer value:

Theorem 2. *Suppose that $r > 1$ is a rational non-integer number, $d \in \mathbb{N}$ and $q = r^{1/d}$. Then, for every nonnegative integer s, there is a geometric progression $\mathcal{G}$ with ratio q which contains exactly s positive integers, so that $|\mathcal{G} \cap \mathbb{N}| = s$.*

The main theorems of this paper are the following:

Theorem 3. *Suppose that the ratio $q > 1$ is not of the form $\beta^{1/d}$, where $d \in \mathbb{N}$ and where $\beta > 1$ is either a rational number or a cubic algebraic number with two nonreal conjugates over $\mathbb{Q}$ of moduli distinct from β. Then $|\mathcal{G} \cap \mathcal{A}| \leqslant 3$ for each $\mathcal{G} = \mathcal{G}(u, q)$ and each $\mathcal{A}$.*

Moreover, for every integer $s \geqslant 2$, there exist an algebraic number $q > 1$ of degree s (satisfying $q \neq \beta^{1/d}$ for $s \neq 3$) and a positive real number $u \in \mathbb{Q}(q)$ such that $|\mathcal{G} \cap \mathcal{A}| = 3$ for the geometric progression $\mathcal{G} = \mathcal{G}(u, q)$ and some arithmetic progression $\mathcal{A}$.

Theorem 4. *For $q = \beta^{1/d}$, where $d \in \mathbb{N}$ and $\beta > 1$ is a cubic algebraic number with two nonreal conjugates of moduli distinct from β, we have $|\mathcal{G} \cap \mathcal{A}| \leqslant 6$ for each $\mathcal{G} = \mathcal{G}(u, q)$ and each $\mathcal{A}$.*

In the proof of Theorem 4 we use a deep (and sharp!) result of Beukers [4] on the zero multiplicity of ternary recurrence sequences. Unlike in all other cases, we do not have any examples with $|\mathcal{G} \cap \mathcal{A}|$ equal to $4, 5$ or 6 under conditions of Theorem 4. So we conjecture that the sharp upper bound on $|\mathcal{G} \cap \mathcal{A}|$, where $q = \beta^{1/d}$ with a cubic β and d as in Theorem 4, should be 3, the same as in Theorem 3.

The problems on the intersection of $\mathcal{G}$ and $\mathcal{A}$ can be easily transformed into the language of multiplicities of fractional parts. This will be explained in Section 2, where we give some additional motivation for the study of those problems and also remind some earlier relevant results. In particular, the reduction of the problem on the size of $|\mathcal{G} \cap \mathcal{A}|$ to the corresponding problem on multiplicities of the fractional parts of the geometric sequence $\mathcal{G}$ shows that the result given in [7] implies Theorem 1. The proofs of Theorems 2, 3, 4 will be given in Section 4 after stating all necessary auxiliary lemmas and other results in Section 3.

2 Fractional parts of geometric progressions

Throughout, let $\{y\}$ be the fractional part of a real number y. Let also $\xi > 0$, $\alpha > 1$ and $t \in [0, 1)$ be arbitrary real numbers. We shall consider the fractional parts of powers $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$. Let $M_{\xi,\alpha}(t)$ (or simply $M(t)$) be the number of times the value t occurs in the sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$. We call the number $M_{\xi,\alpha}(t)$ the *multiplicity* of t in the sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$. In other words, $M_{\xi,\alpha}(t)$ is the number of positive integers n for which $\{\xi\alpha^n\} = t$. For example, $M_{1,3/2}(1/3) = 0$ and $M_{1,\sqrt{2}}(0) = \infty$.

Let us consider two progressions $\mathcal{G}$ and $\mathcal{A}$ as in (1), (2). We are interested in the upper bound for $|\mathcal{G} \cap \mathcal{A}|$, so assume, without loss of generality, that $0 \leqslant v < D$. Evidently, $uq^j = v + iD$ for some integers $i, j \geqslant 0$ if and only if

$$\frac{u}{qD} q^{j+1} = \frac{v}{D} + i. \tag{3}$$

Setting

$$\xi := u/qD, \quad \alpha := q, \quad n := j + 1, \quad t := v/D \tag{4}$$

in (3), we see that $\{\xi\alpha^n\} = t$. So each element of $\mathcal{G} \cap \mathcal{A}$ corresponds to the solution of the equation $\{\xi\alpha^n\} = t$ in positive integers n. In particular,

$$|\mathcal{G} \cap \mathcal{A}| = M_{\xi,\alpha}(t) \tag{5}$$

for $\mathcal{G} = \mathcal{G}(u, q)$, $\mathcal{A} = \mathcal{A}(v, D)$ with $u > 0, q > 1, D > 0, v \in [0, D)$ and ξ, α, t given in (4).

In [7], using a result of Boyd [5], the first named author proved that $M_{\xi,\alpha}(t) = \infty$ for $\xi > 0$, $\alpha > 1$ and $t \in [0, 1)$ if and only if $\alpha = m^{1/d}$ and $\xi = \frac{a}{b} m^{\ell/d}$ for some integers $m \geqslant 2$, $d, a, b \in \mathbb{N}$, $\ell \in \{0, 1, \dots, d-1\}$. By (5), this yields Theorem 1.

The problem of determining the multiplicity $M_{1,\alpha}(t)$, where $\alpha > 1$, has been studied by Supnick, Cohen and Keston [20] and also by Ehlich [9] and Posner [11]. They proved (independently) the following result which was conjectured by Vijayaraghavan (see p. 153 in [19]). If $\{\alpha^a\} = \{\alpha^b\} = \{\alpha^c\}$, where $a < b < c$ are positive integers, then $\alpha^a, \alpha^b, \alpha^c$ are integers. In other words, the multiplicity of the sequence $\{\alpha^n\}$, $n = 1, 2, 3, \dots,$ satisfies $M(t) \leqslant 2$, unless $\alpha > 1$ is a root of an integer in which case $M(0) = \infty$. The above bound 2 is attained. Indeed, the identity $\{\alpha^a\} = \{\alpha^b\}$ holds for any number $\alpha > 1$ which is a root of the trinomial

$$x^b - x^a - k,$$

where $k, a, b \in \mathbb{N}$, $a < b$. Thus, if this root α is not of the form $m^{1/d}$ with some integers $m \geqslant 2$ and $d \geqslant 1$, we have $M_{1,\alpha}(\{\alpha^a\}) = 2$. Clearly, $M_{1,\alpha}(0) = 0$ and $M_{1,\alpha}(\{\alpha\}) = 1$ for each transcendental number α. This shows that, for every $\alpha > 1$ and every $t \in [0, 1)$, we may have only the following multiplicities:

$$M_{1,\alpha}(t) \in \{0, 1, 2, \infty\}. \tag{6}$$

There are many more cases for general ξ. In contrast to (6), by Theorems 1, 2 and (5), we obtain

$$M_{\xi,\alpha}(t) \in \mathbb{N} \cup \{0, \infty\},$$

where each value in $\mathbb{N} \cup \{0, \infty\}$ occurs for some ξ, α, t.

There exists a direct correspondence between equal values of the fractional parts $\{\xi\alpha^n\}$ for different n's and equal values which appear in certain linear recurrent sequences. Indeed, let α be an algebraic number of degree d and $\xi \in \mathbb{Q}(\alpha)$. Then one can write $\xi\alpha^n$ as a linear combination

$$\xi\alpha^n = c_{d-1,n}\alpha^{d-1} + c_{d-2,n}\alpha^{d-2} + \dots + c_{1,n}\alpha + c_{0,n}$$

in the basis $1, \alpha, , \dots, \alpha^{d-1}$ with rational coefficients $c_{j,n}$, $j = 0, 1, \dots, d-1$. It is easy to see that the coefficients $c_{j,n}$ (for a fixed index j) satisfy a homogenous linear recurrence of order d whose characteristic polynomial is the minimal polynomial of α. Then $\{\xi\alpha^a\} = \{\xi\alpha^b\}$ holds precisely if

$$\xi\alpha^a - \xi\alpha^b = \sum_{j=0}^{d-1} \big(c_{j,a} - c_{j,b}\big)\alpha^j \in \mathbb{Z},$$

which implies the simultaneous $d-1$ equalities $c_{j,a} = c_{j,b}$ for $j = 1, 2, \dots, d-1$.

Integer, rational, algebraic and complex linear recurrences with repeating terms received considerable attention for a long time. See, for instance, [6, 18]. Effective upper bounds for the multiplicity of general linear recurrent sequences were obtained by Schlickewei [13, 14], Schmidt [15, 16] and then improved in some cases in [1, 2, 10]; see also a survey [17]. The complete classification of rational binary and ternary recurrences of highest multiplicity was accomplished by Beukers [3, 4]. These results provide additional tools and new motivation for the study of the multiplicity function $M_{\xi,\alpha}(t)$.

3 Lemmata

We shall derive Theorems 3 and 4 from the next theorem combined with Theorem 8 below and (5).

Theorem 5. *Let $\xi > 0$ and $\alpha > 1$ be arbitrary real numbers. Then the fractional parts $\{\xi\alpha^n\}$, $n = 1, 2, 3, \dots,$ take a fixed value $t \in [0, 1)$ at most 3 times, with two possible exceptions. The first exception occurs for $\alpha = r^{1/d}$, where $r \in \mathbb{Q}$, $r > 1$ and $d \in \mathbb{N}$. The other (possible) exception may occur for $\alpha = \beta^{1/d}$, where $\beta > 1$ is a real cubic algebraic number with two nonreal conjugates of moduli distinct from β. In the cubic case, the sequence of fractional parts can take the same value at most 6 times.*

We first give a simple lemma stating necessary and sufficient conditions for the sequence of fractional parts of powers to take some values two or three times. Firstly, the inequality $M(t) \geqslant 2$ implies that there exist two distinct positive integers, say, $a < b$ such that $t = \{\xi\alpha^b\} = \{\xi\alpha^a\}$. This is equivalent to the fact that the difference $k = \xi\alpha^b - \xi\alpha^a$ is a positive integer, thus $\xi = k/(\alpha^b - \alpha^a)$.

Secondly, assume that $M(t) \geqslant 3$ for some $t \in [0, 1)$. Now, there exist three positive integers $a < b < c$ such that the differences $k = \xi\alpha^b - \xi\alpha^a$ and $l = \xi\alpha^c - \xi\alpha^a$ belong to $\mathbb{N}$. This implies

$$\xi = \frac{k}{\alpha^b - \alpha^a} = \frac{l}{\alpha^c - \alpha^a}, \qquad k < l, \quad k, l \in \mathbb{N}. \tag{7}$$

These equations are *necessary and sufficient* for the sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \dots,$ to take values of multiplicity at least 3. The second equality in (7) can be rewritten as $k\alpha^c - l\alpha^b + (l-k)\alpha^a = 0$. Hence α must be a root of the trinomial (a polynomial with three nonzero coefficients) $kx^{c-a} - lx^{b-a} + l - k$.

In particular, α is an algebraic number over $\mathbb{Q}$. Summarizing, we have the following lemma:

Lemma 6. *The sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \dots,$ takes two equal values at $n = a, b$ if and only if $\xi = k/(\alpha^b - \alpha^a)$, where $a < b$, $a, b, k \in \mathbb{N}$. It takes three equal values at $n = a, b, c$ if and only if α is a root of the trinomial $T(x) = kx^{c-a} - lx^{b-a} + l - k \in \mathbb{Z}[x]$, $a, b, c, k, l \in \mathbb{N}$, $a < b < c$, $k < l$ and ξ is the form given by* (7).

Lemma 6 allows us to construct infinitely many examples of algebraic numbers α and ξ, such that the multiplicity of the sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \dots,$ is greater than or equal to 3. By Lemma 11 bellow, $T(x)$ has a root $\alpha > 1$ if and only if $l/k > (c-a)/(b-a)$. For instance, selecting in Lemma 6 $a = 1$, $b = 2$, $c = 4$, $k = 1$, $l \geqslant 4$ one has

$$T(x) = x^3 - lx + l - 1 = (x-1)(x^2 + x - l + 1).$$

Then $\alpha = (-1 + \sqrt{4l-3})/2 > 1$ is quadratic over $\mathbb{Q}$ provided that $4l - 3$ is not a perfect square. Set $\xi := 1/(\alpha^2 - \alpha)$. Then $t = \{\xi\alpha\} = \{\xi\alpha^2\} = \{\xi\alpha^4\}$. Hence $M(t) \geqslant 3$. In fact, we have $M(t) = 3$, by Theorem 5, because α is not of the form $\beta^{1/d}$ (see the proof of Theorem 7 below).

More generally, given any integer $s \geqslant 2$, let us take in Lemma 6 $k = 1$, $a = 1$, $b = s + 1$, $c = s + 2$, $l \geqslant 2$, $l \in \mathbb{N}$. Then $\alpha > 1$ is a root of the trinomial

$$T(x) = x^{s+1} - lx^s + l - 1 = (x-1)\big(x^s - (l-1)(x^{s-1} + \dots + x + 1)\big).$$

The polynomial

$$P(x) := x^s - (l-1)\big(x^{s-1} + \dots + x + 1\big), \tag{8}$$

where $l \geqslant 2$, divides T. Hence, by Rouché's theorem, it has a unique root outside the unit circle, and so is irreducible. This unique root must be α. By Lemma 6, for this α and for $\xi := 1/(\alpha^{s+1} - \alpha)$, $t := \{\xi\alpha\}$, we have

$$\big\{\xi\alpha\big\} = \big\{\xi\alpha^{s+1}\big\} = \big\{\xi\alpha^{s+2}\big\} = t. \tag{9}$$

Below, using these α and ξ, we shall prove the following theorem:

Theorem 7. *For every integer $s \geqslant 2$, there is an algebraic number $\alpha > 1$ (which, for $s \neq 3$, is not of the form $\beta^{1/d}$ with $d \in \mathbb{N}$ and β either a rational or a cubic number with two nonreal conjugates) of degree s over $\mathbb{Q}$, a positive number $\xi \in \mathbb{Q}(\alpha)$ and $t \in [0, 1)$ such that $M_{\xi,\alpha}(t) = 3$.*

In order to prove Theorem 5, we shall use the following lemma.

Lemma 8. *Suppose that a real number $\beta > 1$ satisfies the equations*

$$\frac{k}{\beta^u - 1} = \frac{l}{\beta^v - 1} = \frac{m}{\beta^w - 1}, \tag{10}$$

where $k < l < m$ and $u < v < w$ are positive integers satisfying $\gcd(u, v, w) = 1$*. Then β is a rational number, a real quadratic number or a cubic number with two nonreal conjugates. Moreover, if β' is conjugate to β over $\mathbb{Q}$, $\beta' \neq \beta$, then $|\beta'| \neq \beta$.*

We shall also need two simple lemmas on the roots of trinomials. Lemmas 9 and 10 will be used in the proof of Lemma 8. The first one is essentially given on p. 248 in [20].

Lemma 9. *Suppose that the complex number $z = \rho e^{i\phi}$, where $\rho = |z| > 0$ and $\phi = \arg z \in [0, 2\pi)$, is a root of the trinomial $f(x) = Ax^r + Bx^s + C$, where A, B, C are nonzero real numbers and r, s are distinct positive integer exponents. Then*

$$\cos r\phi = -\big(A^2\rho^{2r} - B^2\rho^{2s} + C^2\big)/\big(2AC\rho^r\big).$$

Proof. The equation

$$f(\rho e^{i\phi}) = A\rho^r(\cos r\phi + i\sin r\phi) + B\rho^s(\cos s\phi + i\sin s\phi) + C = 0$$

implies

$$A\rho^r\cos r\phi + C = -B\rho^s\cos s\phi, \tag{11}$$

$$A\rho^r\sin r\phi = -B\rho^s\sin s\phi. \tag{12}$$

Squaring both sides of (11) and (12) and adding them we obtain

$$A^2\rho^{2r} + 2AC\rho^r\cos r\phi + C^2 = B^2\rho^{2s}.$$

The result now follows. □

The second Lemma was proved by Posner and Rumsey [12]. (We also give a short proof for the sake of completeness.)

Lemma 10. *Suppose that the complex numbers z_1 and z_2 are roots of the trinomial $f(x) = Ax^r + Bx^s + C \in \mathbb{R}[x]$. If $|z_1| = |z_2|$, then one has either $z_1^r = z_2^r$ or $z_1^r = \overline{z_2^r}$, where $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$.*

Proof. Let $\phi_1 = \arg z_1$, $\phi_2 = \arg z_2$. Set $|z_1| = |z_2| = \rho > 0$ in Lemma 9. The formulae of Lemma 9 then gives $\cos r\phi_1 = \cos r\phi_2$. This yields $\sin r\phi_1 = \pm \sin r\phi_2$. Hence $z_1^r = z_2^r$ or $z_1^r = \overline{z_2^r}$. □

Here is another useful observation.

Lemma 11. *The trinomial $f(x) = Ax^r - Bx^s + B - A \in \mathbb{R}[x]$, where $r > s > 0$, $A > 0$, $B > 0$ are integers, has a real root $y > 1$ if and only if $B/A > r/s$.*

Proof. Note that $f(1)$=0. The derivative $f'(x) = rAx^{r-1} - sBx^{s-1}$ has one positive real root $x_0 = (sB/rA)^{1/(r-s)} > 1$ if and only if $B/A > r/s > 1$. The necessity now follows from the theorem of Rolle. Conversely, $B/A > r/s > 1$ implies $f'(x) < 0$ for any positive $x < x_0$. Thus $f(x) < 0$ in $(1, x_0)$ and $f(+\infty) = +\infty$. Hence $f(y) = 0$ for some $y \geqslant x_0 > 1$. □

In addition, we make use of two classical results from the theory of linear recurrent sequences. Recall that a nonzero (which means that $u_n \neq 0$ for at least one $n \geqslant 0$) linear recurrence sequence u_n, $n = 0, 1, 2, \ldots$, satisfying

$$u_{n+d} = c_{d-1}u_{n+d-1} + \cdots + c_0 u_n$$

for $n = 0, 1, 2, \ldots$ is called *non-degenerate*, if the quotient α'/α'' is not a root of unity for any two distinct roots α', α'' of its characteristic polynomial $x^d - c_{d-1}x^{d-1} - \cdots - c_0$. The sequences corresponding to $d = 2$ and $d = 3$ are called *binary* and *ternary*, respectively.

Theorem 12. *Suppose that the non-degenerate rational binary linear recurrent sequence u_n, $n = 0, 1, 2, \ldots$, has a characteristic polynomial with two distinct real roots. Then the multiplicity of any rational value in the sequence u_n is at most* 3.

Theorem 12 was first proved by Chowla, Dunton and Lewis [6]. Their proof for integer sequences works for the rational (and real) sequences as well. An alternative proof of this result using an earlier result of Smiley [18] is also given on p. 837 in [6].

To settle the cubic case in Theorem 5, we use the following result of Beukers [4] on the multiplicity of rational ternary linear recurrent sequences.

Theorem 13. *Let u_n, $n = 0, 1, 2, \ldots$, be a non-degenerate ternary linear recurrent sequence of rational numbers. Then the zero multiplicity of u_n is at most* 6.

The proofs of Lemma 8 and of all our theorems will be given in the next section.

4 Proofs

Proof of Lemma 8. The equation $k/(\beta^u - 1) = l/(\beta^v - 1)$ yields $k\beta^v - l\beta^u + l - k = 0$. Similarly, using $l/(\beta^v - 1) = m/(\beta^w - 1)$ we obtain $l\beta^w - m\beta^v + m - l = 0$. Thus β is a common root of the trinomials

$$P(x) := kx^v - lx^u + l - k \quad \text{and} \quad Q(x) := -mx^v + lx^w + m - l.$$

Let $z \in \mathbb{C}$ be any common root of $P(x)$ and $Q(x)$. Set $\rho := |z|$, $\phi := \arg z$. Using Lemma 9 with $f(x) = P(x)$, $r = v$, one has

$$\cos v\phi = -\frac{k^2\rho^{2v} - l^2\rho^{2u} + (l-k)^2}{2k(l-k)\rho^v}.$$

Similarly, using Lemma 9 with $f(x) = Q(x)$, $r = v$, one obtains

$$\cos v\phi = -\frac{m^2\rho^{2v} - l^2\rho^{2w} + (m-l)^2}{2m(l-m)\rho^v}.$$

Hence

$$\frac{k^2\rho^{2v} - l^2\rho^{2u} + (l-k)^2}{k(l-k)} = \frac{m^2\rho^{2v} - l^2\rho^{2w} + (m-l)^2}{m(l-m)}.$$

This yields

$$kl(l-k)\rho^{2w} - mk(m-k)\rho^{2v} + ml(m-l)\rho^{2u} - (m-l)(m-k)(l-k) = 0.$$

By Descartes rule of signs, the quadrinomial

$$H(x) := kl(l-k)x^{2w} - mk(m-k)x^{2v} + ml(m-l)x^{2u} - (m-l)(m-k)(l-k)$$

has 1 or 3 positive real roots (counting with multiplicities), because $0 < u < v < w$ and $0 < k < l < m$. Observe that $H(1) = 0$ and, by (10), $H(\beta) = 0$. Hence $H(x)$ has three positive roots.

Let $\gamma > 0$ be a real number which is the third root of $H(x)$ (including the possible case of a multiple root $\gamma = 1$ or $\gamma = \beta$). Suppose that $\beta' \neq \beta$ is a conjugate of β over $\mathbb{Q}$. Since β' is a common root of P and Q, $|\beta'|$ is a root of H. Thus $H(|\beta'|) = 0$. Hence the number β and all its algebraic conjugates over $\mathbb{Q}$ must lie on three circles with the common center at $z = 0$ and the radii 1, β and γ.

If β has no other conjugates over $\mathbb{Q}$ then $\beta \in \mathbb{Q}$. Suppose β' is a conjugate of β over $\mathbb{Q}$ satisfying $\beta' \neq \beta$. We claim that β' cannot lie on either of the circles $|z| = 1$ or $|z| = \beta$. Suppose first that $|\beta'| = \beta$. Then, as β' and β lie on the same circle, by Lemma 10, one has either $\beta^r = \beta'^r$ or $\beta^r = \overline{\beta'^r}$ for every positive integer exponent r in $P(x)$ or $Q(x)$, namely, for $r = u, v, w$. Since β^r is a real number, we must have $\beta^r = \beta'^r$. Thus $\zeta^u = \zeta^v = \zeta^w = 1$, where $\zeta := \beta/\beta'$. This implies $\zeta = \zeta^{\gcd(u,v,w)} = 1$. So $\beta = \beta'$, a contradiction. Similarly, if β' lies on the circle $|z| = 1$, then $|\beta'| = 1$. Since $\beta' \neq \pm 1$, it must be a complex (nonreal) number. The number 1 is also the common root of $P(x)$ and $Q(x)$. Hence, as above, by Lemma 10, we obtain $\beta'^r = 1^r = 1$ for every positive integer exponent r in $P(x)$ or $Q(x)$, i.e., for $r = u, v, w$. So β' is a root of unity. However, its conjugate $\beta > 1$ over $\mathbb{Q}$ is not a root of unity, a contradiction.

Therefore, if $\beta \notin \mathbb{Q}$, then all its conjugates over $\mathbb{Q}$ (except for β itself but including β') must lie on the circle $|z| = \gamma$. In particular, $\gamma \neq 1$ and $\gamma \neq \beta$. Algebraic numbers lying with their conjugates on two circles were studied in [8]. However, as in [8] it is assumed that their norms are 1 (which is not the case here), we shall give an independent argument.

We first claim that β may have at most two such conjugates, so β is of degree 2 or 3 over $\mathbb{Q}$. Indeed, assume that β has at least three distinct conjugates on $|z| = \gamma$, namely, β', $\overline{\beta'}$ and, say, $\beta'' \notin \{\beta', \overline{\beta'}\}$. Then

$$\beta'\overline{\beta'} = \beta''\overline{\beta''},$$

where $\overline{\beta''}$ is a conjugate of β which is equal to β'' if $\beta'' \in \mathbb{R}$. Taking an automorphism σ of the Galois group of $\mathbb{Q}(\beta)/\mathbb{Q}$ which maps β' to β we obtain

$$\beta\sigma(\overline{\beta'}) = \sigma(\beta'')\sigma(\overline{\beta''}). \tag{13}$$

However, the modulus of the left hand side of (13) is equal to $\beta\gamma$, whereas the modulus of its right hand side is equal to γ^2, because all conjugates of β except for β itself lie on the circle $|z| = \gamma$. This is a contradiction, because $\beta\gamma \neq \gamma^2$. Hence β is of degree at most 3 over $\mathbb{Q}$ and, in case $\deg \beta = 3$, β has two nonreal conjugates on $|z| = \gamma$, where $\gamma \neq \beta$. □

Proof of Theorem 5. Suppose that the multiplicity $M(t)$ of some sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$, where $\xi > 0$, $\alpha > 1$, is greater than or equal to 4. Then there exist positive integers $a < b < c < e$ such that $\{\xi\alpha^a\} = \{\xi\alpha^b\} = \{\xi\alpha^c\} = \{\xi\alpha^e\}$. This occurs precisely if and only if the differences $k = \xi\alpha^b - \xi\alpha^a$, $l = \xi\alpha^c - \xi\alpha^a$, $m = \xi\alpha^e - \xi\alpha^a$ are positive integers $k < l < m$. Then

$$\xi\alpha^a = \frac{k}{\alpha^{b-a} - 1} = \frac{l}{\alpha^{c-a} - 1} = \frac{m}{\alpha^{e-a} - 1}. \tag{14}$$

Let $d := \gcd(b-a, c-a, e-a)$. Then $b-a = du$, $c-a = dv$, $e-a = dw$, where $u < v < w$, $d, u, v, w \in \mathbb{N}$ and $\gcd(u, v, w) = 1$. Set $\beta := \alpha^d$. Then, by (14), we find that

$$\frac{k}{\beta^u - 1} = \frac{l}{\beta^v - 1} = \frac{m}{\beta^w - 1}.$$

Hence, Lemma 8 implies that $\beta > 1$ is a rational number, a real quadratic number or a cubic number with two nonreal conjugates. In the first case, $\alpha = r^{1/d}$, $r \in \mathbb{Q}$, which is an exceptional case in the statement of the theorem. The third, cubic, case is also exceptional and will be considered below. Before this, let us examine the quadratic case.

Quadratic case. Set $\nu := k/(\beta^u - 1)$. Obviously, $\nu \in \mathbb{Q}(\beta)$. Observe that the fractional parts $\{\nu\}$, $\{\nu\beta^u\}$, $\{\nu\beta^v\}$ and $\{\nu\beta^w\}$ are equal, by (7). Write

$$\nu\beta^n = a_n\beta + b_n, \quad n = 0, 1, 2, \dots,$$

where $a_n, b_n \in \mathbb{Q}$. The sequences a_n, $n = 0, 1, 2, \dots$, and b_n, $n = 0, 1, 2, \dots$, satisfy a linear homogeneous recurrence of order two with characteristic polynomial which is the minimal polynomial of β over $\mathbb{Q}$. Then $\nu\beta^u - \nu = k$, $\nu\beta^v - \nu = l$, $\nu\beta^w - \nu = m$ leads to $a_0 = a_u = a_v = a_w$, because all differences are positive integers. So the multiplicity of the value a_0 in the sequence a_n, $n = 0, 1, 2, \dots$ at a_0 is at least 4.

By Theorem 12, the sequence a_n, $n = 0, 1, 2, \dots$, must be degenerate. This means that either a_n, $n = 0, 1, 2, \dots$, is the zero sequence or β/β' is a root of unity. In the first case, $a_1 = a_0 = 0$ implies $\beta = \nu\beta/\nu = b_1/b_0 \in \mathbb{Q}$, a contradiction. Also, by Lemma 8, β has one real conjugate $\beta' \neq \pm\beta$. Thus β/β' is not a root of unity. This is also a contradiction which shows that β (which is a power of α) cannot be a quadratic number with two real conjugates β, β' satisfying $|\beta'| \neq \beta$ in case $M_{\xi,\alpha}(t) \geqslant 4$.

Cubic case (with two nonreal conjugates). Now, we will show that $M(t) \leqslant 6$. Suppose that $M_{\xi,\alpha}(t) > 6$ for some $\xi > 0$, $\alpha > 1$, $t \in [0, 1)$, where $\beta = \alpha^d > 1$ is a cubic number with two nonreal conjugates and $d \in \mathbb{N}$. Assume that d is the smallest positive number for which α^d is a cubic number.

We claim that the number α^m is cubic if and only if $d|m$. There is nothing to prove for $d = 1$. Assume that $d > 1$. Clearly, $\alpha = \beta^{1/d}$ has conjugates on two circles $|z| = \beta^{1/d}$ and $|z| = \gamma^{1/d}$, where β' and $\beta'' = \overline{\beta'}$ are two conjugates of β lying on $|z| = \gamma$, $\gamma \neq \beta$. Moreover, the conjugates of $\alpha = \alpha_1$ lying on the circle $|z| = \beta^{1/d}$ must be of the form $\alpha_j = \zeta_j\beta^{1/d}$, $j = 2, \dots, s$, where ζ_j is a root of unity satisfying $\zeta_j^d = 1$. Since α is not a root of a rational number or a quadratic number, $\deg(\alpha^m) = 3$ if and only if

$$\alpha_1^m = \alpha_2^m = \cdots = \alpha_s^m. \tag{15}$$

Write $m \in \mathbb{N}$ in the form $m = dk + l$, where $0 \leqslant l < d$. Assume that $l > 0$. Then $\alpha_1^{dk} = \alpha_2^{dk} = \cdots = \alpha_s^{dk}$ combined with (15) yields $\alpha_1^l = \alpha_2^l = \cdots = \alpha_s^l$ Thus $\deg(\alpha^l) = 3$, a contradiction with the minimality of d.

Since $M(t) > 6$, there exist some positive integers $e_0 < e_1 < \cdots < e_6$ such that $\{\xi\alpha^{e_0}\} = \cdots = \{\xi\alpha^{e_6}\}$. In particular, the differences $k_i = \xi\alpha^{e_i} - \xi\alpha^{e_0}$, $i = 1, \dots, 6$, must be positive integers. Hence

$$\xi\alpha^{e_0} = \frac{k_i}{\alpha^{e_i - e_0} - 1}$$

for $i = 1, \dots, 6$. Set $g := \gcd(e_1 - e_0, \dots, e_6 - e_0)$ and $w_i := (e_i - e_0)/g \in \mathbb{N}$ for $i = 1, \dots, 6$. Then $\gcd(w_1, \dots, w_6) = 1$ and

$$\frac{k_1}{\alpha^{gw_1} - 1} = \cdots = \frac{k_6}{\alpha^{gw_6} - 1}. \tag{16}$$

Put $g_1 := \gcd(w_1, w_2, w_3)$ and $v_i := w_i/g_1 \in \mathbb{N}$ for $i = 1, 2, 3$. By Lemma 8 applied to the first two equalities of (16), we deduce that α^{gg_1} is a rational, a quadratic or a cubic number. Since α^d is cubic and no positive integer power of α is of degree smaller than 3, the number α^{gg_1} must be cubic. Hence d divides gg_1, by the above claim. It follows that d divides $gg_1v_1 = gw_1$, and gw_2, gw_3. By the same argument applied to the last two equalities of (16), d divides gw_4, gw_5, gw_6. Since $\alpha^d = \beta$, equalities (16) can be written in the form

$$\frac{k_1}{\beta^{u_1} - 1} = \cdots = \frac{k_6}{\beta^{u_6} - 1} \tag{17}$$

with positive integers $u_1 < \cdots < u_6$.

Set $\nu := k_1/(\beta^{u_1} - 1) \in \mathbb{Q}(\beta)$. Note that the fractional parts $\{\nu\}, \{\nu\beta^{u_1}\}, \dots, \{\nu\beta^{u_6}\}$ are equal, by (17). Thus the sequence $\{\nu\beta^n\}$, $n = 0, 1, 2, \dots$, takes the value $t = \{\nu\}$ at least seven times. Let

$$H(x) = x^3 - Ax^2 - Bx - C, \qquad A, B, C \in \mathbb{Q}, \tag{18}$$

be the minimal polynomial of β over $\mathbb{Q}$. Write

$$\nu\beta^n = a_n\beta^2 + b_n\beta + c_n, \qquad n = 0, 1, 2, \dots, \qquad a_n, b_n, c_n \in \mathbb{Q}. \tag{19}$$

Note that the sequences a_n, $n = 0, 1, 2, \ldots$, and b_n, $n = 0, 1, 2, \ldots$, satisfy a homogeneous linear recurrence of order 3 with characteristic polynomial $H(x)$. The relation $\nu\beta^m - \nu\beta^s \in \mathbb{Z}$ implies $a_m = a_s$, $b_m = b_s$. Hence, there exist $a, b \in \mathbb{Q}$ such that $(a_n, b_n) = (a, b)$ for seven distinct nonnegative integers n.

Consider the sequence $d_n := ba_n - ab_n$, $n = 0, 1, 2, \ldots$. Then

$$d_{n+3} = Ad_{n+2} + Bd_{n+1} + Cd_n$$

for $n = 0, 1, 2, \ldots$. Note that $d_n = 0$ for seven distinct non-negative indices n. We shall prove that $d_n = 0$ for each $n \geqslant 0$. By Theorem 13, it suffices to show that the quotient of two distinct conjugates of β is not a root of unity. Indeed, by Lemma 8, the conjugates β' and $\beta'' = \overline{\beta'}$ are of modulus $|\beta'| \neq \beta$. So only β'/β'' can be a root of unity. But then $\beta'^m = \beta''^m$ for some $m \in \mathbb{N}$. Mapping β' to β, we get $\beta^m = \sigma(\beta'')^m$, where $\sigma(\beta'') \in \{\beta', \beta''\}$, which is a contradiction, by modulus consideration. This proves that $d_n = 0$ for each $n \geqslant 0$.

Therefore, $ba_n = ab_n$ for each $n \geqslant 0$. Obviously, by (19), $a \neq 0$ or $b \neq 0$, since otherwise $a_n = b_n = 0$ for each $n \geqslant 0$, by Theorem 13. Assume, without loss of generality, that $a \neq 0$. By (18), $\beta^3 = A\beta^2 + B\beta + C$. So (19) yields

$$\nu\beta^{n+1} = a_n\beta^3 + b_n\beta^2 + c_n\beta = \big(b_n + Aa_n\big)\beta^2 + \big(c_n + Ba_n\big)\beta + Ca_n. \quad (20)$$

It follows that $a_{n+1} = (b_n + Aa_n) = (b/a + A)a_n$. Hence $a_n = (b/a + A)^n a_0$ for each integer $n \geqslant 0$. Since $a_0 \neq 0$, two terms of the sequence a_n, $n = 0, 1, 2, \ldots$, are equal only if $b/a + A = \pm 1$. Then $a_n = a_{n+2}$ for each $n \geqslant 0$. This implies $c_n = c_{n+2}$ for each $n \geqslant 1$, since $c_{n+1} = Ca_n$, by (20). In the same way, $b_{n+2} = b_n$, because $b_{n+1} = c_n + Ba_n$, by (20). In view of (19), we obtain $\nu\beta^{n+2} = \nu\beta^n$. This leads to $\beta^2 = 1$ and gives the desired contradiction. □

Proof of Theorem 7. Suppose first that $s \neq 3$. We will show that α defined in (8) is not of the form $\beta^{1/d}$ with rational or cubic β. Then, applying Theorem 5 and (9), we will immediately obtain $M_{\xi,\alpha}(t) = 3$.

Assume that α^d is a rational or a cubic number for some $d \in \mathbb{N}$. Since the minimal polynomial (8) of α is irreducible, α is of degree s. Since $s \geqslant 2$, every positive integral power of α is of degree s too, because α is an algebraic integer having a unique conjugate outside the unit circle α itself, hence no two powers of distinct conjugates of α can be equal. This proves the theorem for $s \neq 3$.

For $s = 3$, we select in (8) $l = 2$, so that $\alpha = 1.839286\ldots$ is the root of $x^3 - x^2 - x - 1 = 0$. This time, we take

$$\xi := \frac{1}{\alpha^4 - \alpha} = \frac{3}{2} + 2\alpha - \frac{3}{2}\alpha^2.$$

By (9),

$$\{\xi\alpha\} = \{\xi\alpha^4\} = \{\xi\alpha^5\} = \xi\alpha = \frac{1}{\alpha^3 - 1} = \frac{1}{2}\alpha^2 - \frac{3}{2}.$$

Hence $M_{\xi,\alpha}(t_0) \geqslant 3$ for $t_0 := \alpha^2/2 - 3/2 = 0.191487\ldots$.

We will show that

$$M_{\xi,\alpha}(t) \leqslant 3 \tag{21}$$

for each $t \in [0, 1)$. In particular, combining (21) with the reverse inequality for $t = t_0$, we find that $M_{\xi,\alpha}(t_0) = 3$.

Indeed, for α and ξ as above, let us write $\xi\alpha^n = a_n\alpha^2 + b_n\alpha + c_n$ with rational a_n, b_n, c_n. Then the sequences a_n, b_n, c_n, where $n = 1, 2, 3, \ldots$, satisfy the same linear recurrence

$$x_{n+3} = x_{n+2} + x_{n+1} + x_n$$

for $n = 1, 2, 3, \ldots$. The first terms of those recurrence sequences are given in the following table:

n	a_n	b_n	c_n
1	$1/2$	0	$-3/2$
2	$1/2$	-1	$1/2$
3	$-1/2$	1	$1/2$
4	$1/2$	0	$-1/2$
5	$1/2$	0	$1/2$
6	$1/2$	1	$1/2$
7	$3/2$	1	$1/2$

It is easy to see that $a_{n+1} > \max(a_1, \ldots, a_n)$ for each $n \geqslant 6$, because the numbers a_n are positive for $n \geqslant 4$. So the equality $a_u = a_v$ can only hold for integers $u, v \in \mathbb{N}$ in the range $1 \leqslant u, v \leqslant 6$. As above, the sequence $\{\xi\alpha^n\} = \{a_n\alpha^2 + b_n\alpha + c_n\}$, $n = 1, 2, 3, \ldots$, may take equal values at $n = u$ and $n = v$ only if $(a_u, b_u) = (a_v, b_v)$. (In fact, they are equal if, in addition, $c_v - c_u \in \mathbb{Z}$.) Note that there are only three equal vectors among (a_n, b_n), $n = 1, \ldots, 6$, namely, $(a_1, b_1) = (a_4, b_4) = (a_5, b_5) = (1/2, 0)$. So at most 3 values of the sequence $\{\xi\alpha^n\}$, $n = 1, 2, 3, \ldots$, can be equal. This proves inequality (21). □

Proof of Theorem 2. Write $r^{1/d}$ in the form r_1^{1/d_1} with $r_1 \in \mathbb{Q}$ and the smallest possible $d_1 \in \mathbb{N}$. By abuse of notation, we shall keep the same notation

r, d for r_1, d_1. Write $r = a/b$, where $a > b > 1$ are integers satisfying $\gcd(a, b) = 1$. Take $u := b^{s-1}$. We claim that the geometric progression

$$\mathcal{G}(u, q) = b^{s-1}, b^{s-1}(a/b)^{1/d}, b^{s-1}(a/b)^{2/d}, b^{s-1}(a/b)^{3/d}, \dots \quad (22)$$

contains exactly s positive integers.

Indeed, the number $(a/b)^{n/d}$ is rational if and only if $n = 0, d, 2d, 3d, \dots$. Hence $b^{s-1}(a/b)^{n/d} \in \mathbb{N}$ implies $n = md$, where $m \geqslant 0$ is an integer. It is clear that $b^{s-1}(a/b)^{md/d} = b^{s-1-m}a^m$ is an integer for $m = 0, \dots, s-1$. Thus the sequence $b^{s-1-m}a^m$, $m = 0, 1, 2, \dots$, (and so $\mathcal{G}$ defined in (22)) contains exactly s positive integers. □

Proof of Theorem 3. By Theorem 5 and (5), we have $|\mathcal{G} \cap \mathcal{A}| \leqslant 3$. On the other hand, Theorem 7 combined with (5) implies the existence of $\mathcal{A}$ with parameters given in (4) for which $|\mathcal{G} \cap \mathcal{A}| = 3$.

Finally, it is easy to see that Theorem 4 follows from the last statement of Theorem 5 combined with (5).

References

[1] P. Allen. *On the multiplicity of linear recurrence sequences.* J. Number Theory, **126** (2007), 212–216.

[2] F. Amoroso and E. Viada. *On the zeros of linear recurrent sequences*, (submitted).

[3] F. Beukers. *The multiplicity of binary recurrences.* Compositio Math., **80** (1980), 251–267.

[4] F. Beukers. *The zero-multiplicity of ternary recurrences.* Compositio Math., **77** (1991), 165–177.

[5] D.W. Boyd. *Irreducible polynomials with many roots of maximal modulus.* Acta Arith., **68** (1994), 85–88.

[6] S. Chowla, M. Dunton and D.J. Lewis. *Linear recurrences of order two.* Pacific J. Math., **11** (1961), 833–845.

[7] A. Dubickas. *On the fractional parts of natural powers of a fixed number.* Siberian Math. J., **47** (2006), 879–882.

[8] A. Dubickas and C.J. Smyth. *On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles.* Proc. Edinburgh Math. Soc., **44** (2001), 1–17.

[9] H. Ehlich. *Die positiven Lösungen der Gleichung* $y^a - [y^a] = y^b - [y^b] = y^c - [y^c]$. Math. Zeitschr., **76** (1960), 1–4.

[10] J.-H. Evertse, H.-P. Schlickewei and W. Schmidt. *Linear equations in variables which lie in a finitely generated group.* Annals of Math., **155** (2002), 807–836.

[11] E.C. Posner. *Diophantine problems involving powers modulo one.* Illinois J. Math., **6** (1962), 251–263.

[12] E.C. Posner and H.R. Rumsey. *Polynomials that divide infinitely many trinomials.* Michigan Math. J., **12** (1965), 339–348.

[13] H.-P. Schlickewei. *Multiplicities of recurrence sequences.* Acta Math., **176** (1996), 171–243.

[14] H.-P. Schlickewei. *The multiplicity of binary recurrences.* Invent. Math., **129** (1997), 11–36.

[15] W.M. Schmidt. *The zero multiplicity of linear recurrence sequences.* Acta Math., **182** (1999), 243–282.

[16] W.M. Schmidt. *Zeros of linear recurrence sequences.* Publ. Math. Debrecen, **56** (2000), 609–630.

[17] W.M. Schmidt. *Linear recurrence sequences*, in: Diophantine Approximation, Lectures given at the C.I.M.E. summer school, Cetraro, Italy, June 28–July 6, 2000, (Amoroso, F. (ed.) et al.), Berlin, Springer, Lect. Notes Math. 1819 (2003), pp. 171–247.

[18] M.F. Smiley. *On the zeros of a cubic recurrence.* Amer. Math. Monthly, **63** (1956), 171–172.

[19] O. Strauch and Š. Porubský. *Distribution of sequences: A sampler.* Schriftenreihe der Slowakischen Akademie der Wissenschaften 1, Peter Lang, Frankfurt (2005).

[20] F. Supnick, H.J. Cohen and J.F. Keston. *On the powers of a real number reduced modulo one.* Trans. Amer. Math. Soc., **94**(2) (1960), 244–257.

Artūras Dubickas and **Jonas Jankauskas**
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24, Vilnius LT-03225
LITHUANIA

E-mails: arturas.dubickas@mif.vu.lt / jonas.jankauskas@gmail.com