mathematics

Article

Density of Some Special Sequences Modulo 1

Artūras Dubickas

Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania; arturas.dubickas@mif.vu.lt

Abstract: In this paper, we explicitly describe all the elements of the sequence of fractional parts $\{a^{f(n)}/n\}$, $n = 1,2,3,\dots$, where $f(x) \in \mathbb{Z}[x]$ is a nonconstant polynomial with positive leading coefficient and $a \geq 2$ is an integer. We also show that each value $w = \{a^{f(n)}/n\}$, where $n \geq n_f$ and n_f is the least positive integer such that $f(n) \geq n/2$ for every $n \geq n_f$, is attained by infinitely many terms of this sequence. These results combined with some earlier estimates on the gaps between two elements of a subgroup of the multiplicative group $\mathbb{Z}_m^*$ of the residue ring $\mathbb{Z}_m$ imply that this sequence is everywhere dense in $[0,1]$. In the case when $f(x) = x$ this was first established by Cilleruelo et al. by a different method. More generally, we show that the sequence $\{a^{f(n)}/n^d\}$, $n = 1,2,3,\dots$, is everywhere dense in $[0,1]$ if $f \in \mathbb{Z}[x]$ is a nonconstant polynomial with positive leading coefficient and $a \geq 2$, $d \geq 1$ are integers such that d has no prime divisors other than those of a. In particular, this implies that for any integers $a \geq 2$ and $b \geq 1$ the sequence of fractional parts $\{a^n/\sqrt[b]{n}\}$, $n = 1,2,3,\dots$, is everywhere dense in $[0,1]$.

Keywords: fractional parts; density; powers modulo m; Euler's theorem

MSC: 11J71; 11B05; 11B50; 11B83

Citation: Dubickas, A. Density of Some Special Sequences Modulo 1. *Mathematics* **2023**, *11*, 1727. https://doi.org/10.3390/math11071727

Academic Editors: Diana Savin, Nicusor Minculete and Vincenzo Acciaro

Received: 23 March 2023
Revised: 3 April 2023
Accepted: 3 April 2023
Published: 4 April 2023

1. Introduction

Let $\xi \neq 0$ and $\alpha > 1$ be real numbers. The sequence of fractional parts of powers

$$\{\xi\alpha^n\}, \quad n = 1,2,3,\dots, \tag{1}$$

have been studied starting with the papers of Weyl [1] and Koksma [2], where some metrical results have been obtained. In particular, their results imply that if $\xi \neq 0$ (resp. $\alpha > 1$) is fixed then for almost all $\alpha > 1$ (resp. for almost all real ξ) the sequence (1) is uniformly distributed in $[0,1]$.

However, for most specific pairs, say for $(\xi, \alpha) = (1, a/b)$, where $a/b > 1$ is a rational number that is not an integer, the results obtained (see, e.g., [3,4]) are very far from establishing even the density of the sequence

$$\{(a/b)^n\}, \quad n = 1,2,3,\dots,$$

in $[0,1]$. (We say that a sequence S is *dense* or *everywhere dense* in an interval I if for any $c \in I$ and any $\varepsilon > 0$ the set $I \cap (c - \varepsilon, c + \varepsilon)$ contains infinitely many elements of the sequence S.) The most known conjecture concerning the fractional parts of powers of rational numbers is that of Mahler about the distribution of the sequence $\{\xi(3/2)^n\}$, $n = 1,2,3,\dots$ [5]. The situation with transcendental α is even less described. For example, any kind of result for $(\xi, \alpha) = (1, e)$ is completely out of reach: e.g., disprove that $\{e^n\} \to 0$ as $n \to \infty$.

A special kind of sequences for which the density modulo 1 is confirmed are those of the form $\{a^n b^m \xi\}$, $m, n = 1,2,3,\dots$, where $a, b \geq 2$ are two multiplicatively independent integers and ξ is irrational. See Furstenberg's theorem [6,7] and some more general results of this kind [8–14].

In [15], Cilleruelo, Kumchev, Luca, Rué and Shparlinski considered another interesting sequence

$$\{a^n/n\}, \ n = 1, 2, 3, \dots, \tag{2}$$

where $a \geq 2$ is an integer. They proved that the sequence (2) is everywhere dense in $[0, 1]$ and obtained some other results on its distribution. A more general sequence $\{Q(\alpha^n)/n\}$, $n = 1, 2, 3, \dots$, where $Q \in \mathbb{Z}[x]$ and α is a Pisot or a Salem number, has been considered by the author in [16].

In this paper, we will study some variations of the sequence (2) for a given integer $a \geq 2$. Specifically, we will investigate the sequence

$$\{a^{f(n)}/n^d\}, \ n = 1, 2, 3, \dots, \tag{3}$$

where $a \geq 2$, $d \geq 1$ are integers and $f \in \mathbb{Z}[x]$ is a nonconstant polynomial with a positive leading coefficient.

Let $m \geq 2$ be an integer satisfying $\gcd(a, m) = 1$, and let $p_1, \dots, p_k$ be the set of all prime divisors of a. Consider the set

$$S_a = \{p_1^{\alpha_1} \dots p_k^{\alpha_k}, \text{ where } \alpha_1, \dots \alpha_k \geq 0 \text{ are integers}\}$$

generated by the prime divisors of a. By $R_m(a)$ we denote the set S_a modulo m. In other words, $R_m(a)$ is a subgroup of $\mathbb{Z}_m^*$ generated by the prime divisors of a. Since each element of $R_m(a)$ is coprime to m, we have

$$|R_m(a)| \leq \varphi(m),$$

where φ stands for the Euler totient function.

Our first result gives a complete description of all possible values attained by the sequence (3) with $d = 1$:

Theorem 1. *Let $a \geq 2$ be a positive integer, and let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial with positive leading coefficient. Suppose that n_f is the smallest positive integer such that $f(n) \geq n/2$ for each $n \geq n_f$, and $V_{a,f}$ is the set of values attained by the sequence of fractional parts*

$$\{a^{f(n)}/n\}, \quad n \geq n_f, \, n \in \mathbb{N}.$$

Then, $w \in V_{a,f}$ if and only if $w = 0$ or $w = r/m$, where $m \geq 2$ is an integer coprime to a and $r \in R_m(a)$. Furthermore, each value w of $V_{a,f}$ is attained for infinitely many indices n.

The last claim of the theorem is an unusual one. It does not hold either for the sequence of fractional parts of powers (in fact, for (1) an opposite situation holds by the results in [17]) or, for example, for the sequence $\{2^n/n^2\}$, $n = 1, 2, 3, \dots$, of type (3), where $a = d = 2$ and $f(x) = x$. In particular, by applying an old result of Hasse [18], we will show that infinitely many terms of the sequence $\{2^n/n^2\}$, $n = 1, 2, 3, \dots$, are attained by a unique $n \in \mathbb{N}$. (The proof is given at the end of Section 5).

Note that we have $n_f = 1$ in the case when the coefficients of $f \in \mathbb{Z}[x]$ are all non-negative. The condition $n \geq n_f$ in Theorem 1 cannot be removed. Indeed, take, for example, $f(x) = x - 1$ and $a = 2$. Then, the value $1/2$ of the sequence $\{2^{n-1}/n\}$, $n = 1, 2, 3, \dots$, is attained at $n = 1$ only. Since $x - 1 \geq x/2$ for $x \geq 2$, we have $n_f = 2$. Thus, Theorem 1 implies that each value of the sequence $\{2^{n-1}/n\}$, $n = 2, 3, 4, \dots$, is attained infinitely many times.

Recall that the radical $\mathrm{rad}(a)$ of an integer $a \geq 2$ is the product of its distinct prime divisors, and $\mathrm{rad}(1) = 1$. Theorem 1 implies the following:

Corollary 1. *For any nonconstant $f \in \mathbb{Z}[x]$ with positive leading coefficient and any integers $a, a' \geq 2$ satisfying $\mathrm{rad}(a) = \mathrm{rad}(a')$ we have $V_{a,f} = V_{a',f}$.*

On the other hand, if $\mathrm{rad}(a) \neq \mathrm{rad}(a')$ then there is an integer $m \geq 2$ which is coprime to one of the numbers a, a' but not to the other. If, say $\gcd(a, m) = 1$ and $\gcd(a', m) > 1$, then, by Theorem 1, we find that $1/m \in V_{a,f}$, but $1/m \notin V_{a',f}$.

Let $f, g \in \mathbb{Z}[x]$ be two nonconstant polynomials with positive leading coefficients. Assume that $n_f \geq n_g$. Then, by Theorem 1, for any integer $a \geq 2$ we have $V_{a,f} \cap V_{a,g} = V_{a,f}$ and $V_{a,f} \cup V_{a,g} = V_{a,g}$.

We will also prove the following:

Theorem 2. *Let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial with a positive leading coefficient, and let $a \geq 2$, $d \geq 1$ be integers satisfying $\mathrm{rad}(d) \mid \mathrm{rad}(a)$. Then, the sequence of fractional parts*

$$\{a^{f(n)}/n^d\}, \quad n = 1, 2, 3, \dots,$$

is everywhere dense in $[0, 1]$.

The condition $\mathrm{rad}(d) \mid \mathrm{rad}(a)$ trivially holds for $d = 1$, which implies the density of $\{a^{f(n)}/n\}$, $n = 1, 2, 3, \dots$. (Of course, Theorem 1 asserts much more than the density of this sequence in $[0, 1]$.)

Note that $\{a^{n^b}/n^d\}$, $n = 1, 2, 3, \dots$, is a subsequence of the sequence $\{a^n/n^{d/b}\}$, $n = 1, 2, 3, \dots$. So, Theorem 2 with $f(x) = x^b$, $b \in \mathbb{N}$, implies slightly more than what was proved in [15,16]:

Corollary 2. *For any integers $a \geq 2$, $b, d \geq 1$ satisfying $\mathrm{rad}(d) \mid \mathrm{rad}(a)$ the sequence of fractional parts*

$$\{a^n/n^{d/b}\} \quad n = 1, 2, 3, \dots,$$

is everywhere dense in $[0, 1]$.

In particular, the sequence of fractional parts

$$\{a^n/\sqrt[b]{n}\} \quad n = 1, 2, 3, \dots,$$

is everywhere dense in $[0, 1]$.

An important auxiliary result that we will use several times is the following:

Lemma 1. *For any integers $t \geq 1$, $u \geq 0$, $v \geq 1$, $a \geq 2$ and any $f \in \mathbb{Z}[x]$ with positive leading coefficient there are infinitely many positive integers n for which*

$$f(va^n) - n \equiv u \pmod{t}. \tag{4}$$

In the Section 2 we will show how Theorem 1 implies the density of the set $V_{a,f}$ in $[0, 1]$ and give some examples of $R_m(a)$. In Section 3 we will prove Lemma 1 and its generalization. The proofs of Theorems 1 and 2 are given in Section 4. Finally, in Section 5 we will show that the sequence $\{2^n/n^2\}$, $n = 1, 2, 3, \dots$, contains infinitely many values that are attained only once and that it does not contain certain values r/m, where $m \geq 2$ is an integer coprime to a and $r \in R_m(a)$, at all.

2. Some Examples

Fix $a \geq 2$. Assume that $m = p$ is a prime number greater than $a + 1$. Clearly, $R_m(a)$ contains the multiplicative subgroup $\{1, a, a^2, \dots, a^{\delta-1}\}$ of $\mathbb{Z}_p^*$, where $\delta = \delta_p$ is the order of a modulo p.

An unsolved Artin's conjecture asserts that $\delta_p = p - 1$ for infinitely many primes p if a is not a square. In [19], Erdős and Murty obtained a nontrivial lower bound on δ_p, which implies

$$\delta_p > p^{1/2} \tag{5}$$

for almost all primes p. See also [20]. On the other hand, under assumption (5), the largest gap between any two consecutive δ_p powers of a modulo p is less than

$$p^{437/480+o(1)} \text{ as } p \to \infty$$

(see Theorem 6.8 of [21]); some earlier bounds with slightly worse exponents have been established in [22–25]). Thus, for almost all prime numbers p, every subinterval of length $p^{-0.0896}$ of $[0,1]$ contains the number r/p, with $r \in R_p(a)$. By Theorem 1, such r/p belongs to $V_{a,f}$, which implies the density of $V_{a,f}$ in $[0,1]$. For infinitely many prime numbers p, the exponent 0.0896 can be improved by combining [19] with a subsequent result of Baker and Harman [26] which yields the exponent 0.677 for p in (5).

By a result of Heath-Brown (Corolary 2 of [27]), there are at most three primes a for which Artin's conjecture fails to hold. Suppose a has at least three distinct prime divisors. Then, for infinitely many prime numbers p, at least one of the factors of a is a primitive root modulo p, that is, the order of this prime factor of a is $\delta_p = p-1$. This implies $R_p(a) = \{1,\dots,p-1\}$ for each p. Hence, by Theorem 1, each fraction r/p, where $r = 0,1,\dots,p-1$, belongs to the set $V_{a,f}$ provided that a has at least three distinct prime divisors. (For example, this is true if $30 \mid a$).

Let p be a Mersenne prime of the form $2^q - 1$, where $q \geq 2$ is a prime number. Then, for $a = 2$, the order δ_p of 2 modulo p is q. Hence, by Theorem 1, there are q positive rational numbers with denominator p that belong to V_2 (with, say $f(x) = x$ and $n_f = 1$), namely,

$$\frac{1}{p}, \frac{2}{p}, \frac{4}{p}, \frac{8}{p}, \dots, \frac{2^{q-1}}{p}.$$

Note that $q-1$ of them (all but the last one) belong to the interval $(0, 1/2)$.

Finally, assume that $A \geq 2$ and $d \geq 1$ are two fixed integers. Then, by the above-mentioned result [19], for almost all primes p the order of A modulo p is at least $p^{1/2}$. Thus, the order of the multiplicative group generated by A modulo p^d, where p is any of those almost all primes, is at least $p^{1/2}$ as well. The whole multiplicative group $\mathbb{Z}_{p^d}^*$ is of order $\varphi(p^d) = p^{d-1}(p-1)$. The distance between any two consecutive elements of the multiplicative group generated by A modulo p^d can be estimated using a corresponding exponential sum. (See, e.g., [28] (p. 12).) In our situation, using the main theorem in [29] or, more specifically, (Theorem 4.7 of [30]) we can record the following:

Lemma 2. *For any integers $A \geq 2$ and $d \geq 1$ there exist $\delta > 0$ and infinitely many prime numbers p such that the distance between any two consecutive elements of the multiplicative group generated by A modulo p^d is less than $p^{d-\delta}$.*

3. Proof of Lemma 1 and Its Generalization

Proof of Lemma 1. The claim is trivial if f is a constant, so assume that $\deg f \geq 1$. The proof is by induction on t. There is nothing to prove if $t = 1$. Assume that $t > 1$ and that the claim holds for all positive integers smaller than t. Suppose t_0 is the largest divisor of t which is coprime to a. Set

$$t' = t/t_0 \in \mathbb{N}.$$

Clearly, $1 \leq t_0 \leq t$, so $\varphi(t_0) < t$. By the induction hypothesis, there are infinitely many positive integers ℓ satisfying

$$f(va^\ell) - \ell \equiv u \pmod{\varphi(t_0)}. \tag{6}$$

Take any of those ℓ which is so large that

$$t' \mid va^\ell, \tag{7}$$

$f(va^\ell) > u + \ell$ and $f(x)$ is positive and increasing for $x \geq va^\ell$.

We will show that (4) holds for every n expressible as

$$n = f(va^{\ell}) - u.$$

Note that such n form an infinite set of positive integers, since so is the set of such ℓ.

Observe that for each n, we have

$$f(va^{n}) - n - u = f\left(va^{f(va^{\ell})-u}\right) - f(va^{\ell}),$$

which is divisible by

$$va^{f(va^{\ell})-u} - va^{\ell} = va^{\ell}(a^{f(va^{\ell})-\ell-u} - 1),$$

because $f \in \mathbb{Z}[x]$ and $A - B$ divides $f(A) - f(B)$ for any $A, B \in \mathbb{Z}$, $A \neq B$. Hence, (4) is true provided that

$$t \mid va^{\ell}(a^{f(va^{\ell})-\ell-u} - 1).$$

By (7) and $t = t't_0$, it remains to verify that

$$t_0 \mid a^{f(va^{\ell})-\ell-u} - 1.$$

However, this holds by Euler's theorem in view of $\gcd(a, t_0) = 1$ and (6). □

In the proof of Theorem 1, we will also need the following generalization of Lemma 1. (Of course, similarly to the case of Lemma 1, the nontrivial case is when f is non-constant.)

Lemma 3. *For any $f \in \mathbb{Z}[x]$ with positive leading coefficient, any integers $t \geq 1$, $k \geq 1$, $m \geq 1$, $u_1, \dots, u_k \geq 0$, $v_1, \dots, v_k \geq 1$, $K \geq 1$ and any k positive integers $P_1, \dots, P_k > 1$ there is a vector of positive integers $(n_1, \dots, n_k)$ such that*

$$v_i f(mP_1^{n_1} \dots P_k^{n_k}) - n_i \equiv u_i \pmod{t} \tag{8}$$

for $i = 1, \dots, k$ and $\min_{1 \leq i \leq k} n_i \geq K$.

Proof. We can clearly assume that $\deg f \geq 1$. As before the proof is by induction on t. Assume that $t > 1$ and that the claim holds for all positive integers smaller than t. Introduce t_0 and t' similarly as in the proof of Lemma 1, namely, let t_0 be the largest divisor of t which is coprime to $P_1 \dots P_k$, and $t' = t/t_0$.

This time, as $\varphi(t_0) < t$, by the induction hypothesis, there is a vector of positive integers $(\ell_1, \dots, \ell_k)$ satisfying

$$v_i f(mP_1^{\ell_1} \dots P_k^{\ell_k}) - \ell_i \equiv u_i \pmod{\varphi(t_0)} \tag{9}$$

for $i = 1, \dots, k$, which is so large that

$$t' \mid P_1^{\ell_1} \dots P_k^{\ell_k}, \tag{10}$$

$v_i f(mP_1^{\ell_1} \dots P_k^{\ell_k}) - u_i \geq \ell_i + K$ for $i = 1, \dots, k$, and $f(x)$ is increasing for $x \geq mP_1^{\ell_1} \dots P_k^{\ell_k}$.

Set

$$n_i = v_i f(mP_1^{\ell_1} \dots P_k^{\ell_k}) - u_i$$

for $i = 1, \dots, k$. Then, $n_i > \ell_i$ and $\min_{1 \leq i \leq k} n_i \geq K$. Furthermore, with this choice of n_i, for every $i = 1, \dots, k$ we obtain

$$v_i f(mP_1^{n_1} \dots P_k^{n_k}) - n_i - u_i = v_i f(mP_1^{n_1} \dots P_k^{n_k}) - v_i f(mP_1^{\ell_1} \dots P_k^{\ell_k}),$$

which is divisible by

$$v_i(mP_1^{n_1}\dots P_k^{n_k}-mP_1^{\ell_1}\dots P_k^{\ell_k})=v_imP_1^{\ell_1}\dots P_k^{\ell_k}(P_1^{n_1-\ell_1}\dots P_k^{n_k-\ell_k}-1).$$

By (10), t' divides $P_1^{\ell_1}\dots P_k^{\ell_k}$. So, in order to prove (8) it suffices to show that

$$t_0 \mid P_1^{n_1-\ell_1}\dots P_k^{n_k-\ell_k}-1.$$

As $n_i>\ell_i$, this is the case if, for instance, each factor

$$P_i^{n_i-\ell_i}=P_i^{v_if(mP_1^{\ell_1}\dots P_k^{\ell_k})-u_i-\ell_i},$$

where $i=1,\dots,k$, is 1 modulo t_0. However, the latter holds by Euler's theorem due to $\gcd(P_i,t_0)=1$ and (9). □

4. Proofs of Theorems 1 and 2

Proof of Theorem 1. Note that $\{a^{f(n)}/n\}=0$ for each $n=a^s$, where $s\in\mathbb{N}$ is large enough, so $0\in V_{a,f}$, and the value 0 is attained for infinitely many indices n.

Now, assume that $w\neq 0$ is in $V_{a,f}$. Evidently, w must be a rational number lying in the interval $(0,1)$. Suppose that $w=\{a^{f(s)}/s\}$ for some $s\in\mathbb{N}$ satisfying $s\geq n_f$. We claim that $w=\{a^{f(n)}/n\}$ for infinitely many n of the form $n=sa^\ell$, where ℓ runs through an infinite set of positive integers. In order to prove this it suffices to show that the difference

$$\frac{a^{f(n)}}{n}-\frac{a^{f(s)}}{s}=\frac{a^{f(sa^\ell)}}{sa^\ell}-\frac{a^{f(s)}}{s}=\frac{a^{f(sa^\ell)-\ell}-a^{f(s)}}{s}=\frac{a^{f(s)}}{s}(a^{f(sa^\ell)-f(s)-\ell}-1)$$

is an integer. Let s_0 be the largest divisor of s which is coprime to a. Set $s'=s/s_0\in\mathbb{N}$. We will prove that

$$s' \mid a^{f(s)} \tag{11}$$

and

$$s_0 \mid a^{f(sa^\ell)-f(s)-\ell}-1 \tag{12}$$

for infinitely many $\ell\in\mathbb{N}$.

Fix any prime p that divides s' (if any) and assume that the order of p in s' is $l\geq 1$. Then, $p^{2l}\mid a^s$, since the order of p in a^s is at least

$$s\geq s'\geq p^l\geq 2^l\geq 2l.$$

Applying this argument to each prime divisor p of s' we deduce $s'^2\mid a^s$. Since $s\leq 2f(s)$ for $s\geq n_f$, this yields $s'^2\mid a^{2f(s)}$, and (11) follows. (There is nothing to prove if $s'=1$.)

To prove (12), by $\gcd(s_0,a)=1$, $f(sa^\ell)-f(s)-\ell>0$ and Euler's theorem, it suffices to show that

$$\varphi(s_0)\mid f(sa^\ell)-f(s)-\ell$$

for infinitely many $\ell\in\mathbb{N}$. This clearly follows by Lemma 1 with parameters $(t,u,v)=(\varphi(s_0),f(s),s)$. Consequently, each value $w=\{a^s/s\}$ of $V_{a,f}$ is attained for infinitely many indices $n=sa^\ell$ with certain $\ell\in\mathbb{N}$.

Next, assume that $w=r/m\in V_{a,f}$, where $m\geq 2$, $1\leq r<m$, and $\gcd(r,m)=1$. Then, for some $s\geq n_f$, we must have $r/m=\{a^{f(s)}/s\}$. Write s in the form $s's_0$, where s_0 is the largest divisor of s coprime to a. We claim that $s_0=m$.

Indeed, by (11), we have $s'\mid a^{f(s)}$. So, setting $L=[a^{f(s)}/s]$, we find that $\{a^{f(s)}/s\}$ equals

$$\frac{r}{m}=\frac{a^{f(s)}}{s}-L=\frac{a^{f(s)}}{s's_0}-L=\frac{a^{f(s)}/s'-Ls_0}{s_0}.$$

Here, the numerator $a^{f(s)}/s' - Ls_0$ is coprime to s_0, which implies

$$r = a^{f(s)}/s' - Ls_0 \quad \text{and} \quad m = s_0.$$

In order to complete the proof of Theorem 1 it remains to show that only $r \in R_m(a)$ occur as numerators of the rational numbers $w = r/m \in V_{a,f}$ and that all $r \in R_m(a)$ indeed occur as numerators. The first assertion is clear, because $1 \leq r < m$ and $a^{f(s)}/s'$ is an integer in S_a, so that

$$r = a^{f(s)}/s' - Ls_0 = a^{f(s)}/s' - Lm \in R_m(a).$$

To prove the second assertion assume that $r \in R_m(a)$. Then, for some integers $u_1, \dots, u_k, T \geq 0$, we have

$$r = p_1^{u_1} \dots p_k^{u_k} - Tm. \tag{13}$$

(Recall that $p_1, \dots, p_k$ are the prime divisors of a.)

Write

$$a = p_1^{v_1} \dots p_k^{v_k},$$

with $v_1, \dots, v_k \in \mathbb{N}$. Then, by Lemma 3 with $t = \varphi(m)$ and $P_i = p_i$, there is a vector of positive integers $(n_1, \dots, n_k)$ satisfying

$$v_i f(mp_1^{n_1} \dots p_k^{n_k}) - n_i \equiv u_i \pmod{\varphi(m)} \tag{14}$$

for $i = 1, \dots, k$. Therefore, for

$$n = mp_1^{n_1} \dots p_k^{n_k}, \tag{15}$$

we find that

$$\frac{a^{f(n)}}{n} = \frac{p_1^{v_1 f(n)} \dots p_k^{v_k f(n)}}{mp_1^{n_1} \dots p_k^{n_k}} = \frac{p_1^{v_1 f(mp_1^{n_1} \dots p_k^{n_k}) - n_1} \dots p_k^{v_k f(mp_1^{n_1} \dots p_k^{n_k}) - n_k}}{m}.$$

In view of (14) and $\gcd(p_i, m) = 1$, $i = 1, 2, \dots, k$, the numerator of the last fraction equals $p_1^{u_1} \dots p_k^{u_k}$ modulo m, which is r modulo m by (13). Thus, $a^{f(n)}/n = r/m + B$ with some $B \in \mathbb{Z}$. Consequently, for every n as in (15), we obtain $\{a^{f(n)}/n\} = r/m$, which completes the proof of the theorem. □

Proof of Theorem 2. Write

$$f(x) = a_m x^m + \dots + a_1 x + a_0 \in \mathbb{Z}[x], \quad m, a_m \in \mathbb{N},$$

and select a nonnegative integer c such that

$$d \mid a_0 - c.$$

In all what follows we will show that the sequence $\{a^{f(n)-c}/n^d\}$, $n \geq 1$, is everywhere dense in $[0,1]$. In particular, it is everywhere dense in $[0, a^{-c}]$. Since

$$\{a^{f(n)}/n^d\} - a^c\{a^{f(n)-c}/n^d\} \in \mathbb{Z},$$

this clearly implies that the original sequence $\{a^{f(n)}/n^d\}$, $n = 1, 2, 3, \dots$, is everywhere dense in $[0,1]$.

Let $p > a$ be a prime number. Consider the value of $a^{f(n)-c}/n^d$ at $n = pa^s$, where $s \geq 0$ is an integer:

$$\frac{a^{f(n)-c}}{n^d} = \frac{a^{f(pa^s)-c}}{(pa^s)^d} = \frac{a^{f(pa^s)-c-ds}}{p^d}. \tag{16}$$

We claim that for each $u \geq 0$ there are infinitely many positive integers s for which

$$p^d \mid a^{f(pa^s)-c-ds} - a^{du} = a^{du}(a^{f(pa^s)-c-ds-du} - 1). \tag{17}$$

If this is the case, then, by (16), each value

$$\frac{A^u \pmod{p^d}}{p^d},$$

where $A = a^d$ and $u \geq 0$ is an integer, is attained for infinitely many indices n of the sequence $\{a^{f(n)-c}/n^d\}$, $n = 1, 2, 3, \ldots$. Thus, this sequence is everywhere dense by Lemma 2.

In order to prove (17) we will apply Lemma 1 to the polynomial

$$g(x) = \frac{f(a^l x) - c}{d} = \frac{a_m(a^l x)^m + \cdots + a_1 a^l x}{d} + \frac{a_0 - c}{d} \in \mathbb{Z}[x]$$

with $v = p$, $t = \varphi(p^d)$ and $u + l$ in place of u, where $l \geq 0$ is a fixed integer satisfying $d \mid a^l$. (Here, we use the condition $\mathrm{rad}(d) \mid \mathrm{rad}(a)$.) Then, by (4) applied to the polynomial g, there are infinitely many integers $s > l$ satisfying

$$g(pa^{s-l}) - (s - l) \equiv u + l \pmod{\varphi(p^d)},$$

and hence

$$\varphi(p^d) \mid g(pa^{s-l}) - s - u.$$

Thus, from $dg(pa^{s-l}) = f(pa^s) - c$ it follows that

$$\varphi(p^d) \mid f(pa^s) - c - ds - du.$$

Also, $f(pa^s) - c - ds - du > 0$ for s sufficiently large. Since $\gcd(a, p^d) = 1$, this implies (17) by Euler's theorem, which completes the proof of Theorem 2. □

5. Fractional Parts of $2^n/n^2$ Behave Differently

First, we will show that the sequence $\{2^n/n^2\}$, $n = 1, 2, 3, \ldots$, attains the value $7/25$ for $n = 5$ only and does not attain the value, e.g., $2/25$ at all, although $2 \in R_{25}(2)$. This indicates that the behaviour of $\{2^n/n^2\}$, $n = 1, 2, 3, \ldots$, is different from that of $\{2^n/n\}$, $n = 1, 2, 3, \ldots$, as described in Theorem 1. (Note that $\{2^n/n^2\}$, $n = 1, 2, 3, \ldots$, is everywere dense in $[0, 1]$ by Corollary 2).

Suppose that $\{2^n/n^2\} = r/25$, where r is a positive integer smaller than 25 and coprime to 5. Set $L = [2^n/n^2]$. Then,

$$\frac{rn^2}{25} = 2^n - n^2 L \in \mathbb{N}, \tag{18}$$

so $25 \mid n^2$. Hence, $n = 5^l m$ with $l, m \in \mathbb{N}$, $\gcd(m, 5) = 1$. Inserting this into (18) we obtain

$$5^{2l-2} rm^2 = 2^{5^l m} - 5^{2l} m^2 L.$$

The argument modulo 5 shows that $l = 1$ is the only possibility, and hence $rm^2 = 2^{5m} - 25m^2 L$. Now, the argument modulo m shows that $m = 2^\ell$, where ℓ is a nonnegative integer. It follows that

$$r + 25L = \frac{2^{5m}}{m^2} = 2^{5 \cdot 2^\ell - 2\ell},$$

and so

$$r \equiv 2^{5 \cdot 2^\ell - 2\ell} \pmod{25}.$$

Therefore, $r/25$, where $1 \le r < 25$ and $\gcd(r,5) = 1$, occurs as the value of $\{2^n/n^2\}$ if and only if $r = r_\ell$, where

$$r_\ell = 2^{5\cdot 2^\ell - 2\ell} \pmod{25}$$

for some integer $\ell \ge 0$.

Note that $2^{20} \equiv 1 \pmod{25}$. Hence, the sequence $r_2, r_3, r_4, \dots$ is purely periodic with period 10, because for each $\ell \ge 2$ the difference

$$5 \cdot 2^{\ell+10} - 2(\ell+10) - 5\cdot 2^\ell + 2\ell = 5 \cdot 1023 \cdot 2^\ell - 20$$

is divisible by 20.

For $\ell = 0, 1, \dots, 11$ we have the following table.

ℓ	0	1	2	3	4	5	6	7	8	9	10	11
$5\cdot 2^\ell - 2\ell$	5	8	16	34	72	150	308	626	1264	2542	5100	10,218
r_ℓ	7	6	11	9	21	24	6	14	16	4	1	19

Therefore, the fractional parts $\{2^n/n^2\}$, $n = 1, 2, 3, \dots$, attain any value from the set

$$\left\{\frac{1}{25}, \frac{4}{25}, \frac{6}{25}, \frac{9}{25}, \frac{11}{25}, \frac{14}{25}, \frac{16}{25}, \frac{19}{25}, \frac{21}{25}, \frac{24}{25}\right\}$$

for infinitely many $n \in \mathbb{N}$. The value $7/25$ is taken for $n = 5$ only, since $r_\ell = 7$ for $\ell = 0$ only, while the values

$$\frac{2}{25}, \frac{3}{25}, \frac{8}{25}, \frac{12}{25}, \frac{13}{25}, \frac{17}{25}, \frac{18}{25}, \frac{22}{25}, \frac{23}{25} \tag{19}$$

are not attained.

The reason behind this is that, in general, for integers $t \ge 1$, $u \ge 0$, $v \ge 1$ we cannot claim that there are nonnegative integers n for which

$$v2^n - 2n \equiv u \pmod{t}. \tag{20}$$

(Compare to (4) in Lemma 1.) For $v = 5$ and $t = 20$ all possible u that can be obtained in (20) are either 5 (which happens for $n = 0$) or even. The values $u = 1, 3, 7, 9, 11, 13, 15, 17, 19$ are never attained in (20), which gives the corresponding numerators

$$2^u \pmod{25} = 2, 8, 3, 12, 23, 17, 18, 22, 13$$

in (19).

Finally, take any odd prime p such that the order δ_p of 2 modulo p is even. There are infinitely many of such p, and, by [18], the density of such primes is $17/24$. Consider the value $w = \{2^p/p^2\}$. We claim that the value w is unique, namely, attained by $n = p$ only.

Assume that $w = \{2^n/n^2\}$ for some $n \ne p$. Then, it is easy to see that n must be of the form $n = p2^k$ with some $k \in \mathbb{N}$. This happens if and only if

$$\frac{2^n}{n^2} - \frac{2^p}{p^2} = \frac{2^{p2^k}}{p^2 2^{2k}} - \frac{2^p}{p^2} = \frac{2^p}{p^2}(2^{p2^k - 2k - p} - 1)$$

is an integer. This is only possible if p divides $2^{p2^k-2k-p} - 1$. Since the order δ_p of 2 modulo p is even, and δ_p divides the exponent $p2^k - 2k - p$, the latter integer must be even, which is not the case. This completes the proof of the fact that for each of those infinitely many primes p the value $w = \{2^p/p^2\}$ in the sequence $\{2^n/n^2\}$, $n = 1, 2, 3, \dots$, is attained at $n = p$ only.

Funding: This research received no external funding.

Acknowledgments: The author thanks Igor Shparlinski, who explained the current state-of-the-art approaches related to the estimates for the gaps between elements of a multiplicative subgroup in a residue ring and supplied with corresponding references.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Weyl, H. Über die Gleichverteilung von Zahlen modulo Eins. *Math. Ann.* **1916**, *77*, 313–352. [CrossRef]
2. Koksma, J.F. Ein mengen-theoretischer Satz über Gleichverteilung modulo eins. *Compos. Math.* **1935**, *2*, 250–258.
3. Dubickas, A. Arithmetical properties of powers of algebraic numbers. *Bull. Lond. Math. Soc.* **2006**, *38*, 70–80. [CrossRef]
4. Dubickas, A. On the distance from a rational power to the nearest integer. *J. Number Theory* **2006**, *117*, 222–239. [CrossRef]
5. Mahler, K. An unsolved problem on the powers of 3/2. *J. Aust. Math. Soc.* **1968**, *8*, 313–321. [CrossRef]
6. Boshernitzan, M.D. Elementary proof of Furstenberg's Diophantine result. *Proc. Am. Math. Soc.* **1994**, *122*, 67–70.
7. Furstenberg, H. Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation. *Math. Syst. Theory* **1967**, *1*, 1–49. [CrossRef]
8. Abramoff, M.; Berend, D. A polynomial-exponential variation of Furstenberg's $\times 2 \times 3$ theorem. *Ergod. Theory Dyn. Syst.* **2020**, *40*, 1729–1737. [CrossRef]
9. Bourgain, J.; Lindenstrauss, E.; Michel, P.; Venkatesh, A. Some effective results for $\times a \times b$. *Ergod. Theory Dyn. Syst.* **2009**, *29*, 1705–1722. [CrossRef]
10. Gorodnik, A.; Kadyrov, S. Algebraic numbers, hyperbolicity, and density modulo one. *J. Number Theory* **2012**, *132*, 2499–2509. [CrossRef]
11. Katz, A. Generalizations of Furstenberg's Diophantine result. *Ergod. Theory Dyn. Syst.* **2018**, *38*, 1012–1024. [CrossRef]
12. Kra, B. A generalization of Furstenberg's diophantine theorem. *Proc. Am. Math. Soc.* **1999**, *127*, 1951–1956. [CrossRef]
13. Urban, R. Sequences of algebraic integers and density modulo 1. *J. Théor. Nombres Bordx.* **2007**, *19*, 755–762. [CrossRef]
14. Urban, R. Algebraic numbers and density modulo 1. *J. Number Theory* **2008**, *128*, 645–661. [CrossRef]
15. Cilleruelo, J.; Kumchev, A.; Luca, F.; Rué, J.; Shparlinski, I.E. On the fractional parts of a^n/n. *Bull. Lond. Math. Soc.* **2013**, *45*, 249–256. [CrossRef]
16. Dubickas, A. Density of some sequences modulo 1. *Colloq. Math.* **2012** *128*, 237–244. [CrossRef]
17. Dubickas, A. On the fractional parts of natural powers of a fixed number. *Sib. Math. J.* **2006**, *47*, 879–882. [CrossRef]
18. Hasse, H. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod.p ist. *Math. Ann.* **1966**, *166*, 19–23. [CrossRef]
19. Erdős, P.; Murty, M.R. On the order of $a \pmod p$. In *Number Theory*; CRM Proc. Lecture Notes; Ottawa, ON, Canada, 1996; pp. 87–97.
20. Pappalardi, F. On the order of finitely generated subgroups of $\mathbb{Q}^* \pmod p$ and divisors of $p-1$. *J. Number Theory* **1996**, *57*, 207–222. [CrossRef]
21. Murphy, B.; Rudnev, M.; Shkredov, I.; Shteinikov, Y. On the few products, many sums problem. *J. Théor. Nombres Bordx.* **2019**, *31*, 573–602. [CrossRef]
22. Bourgain, J.; Konyagin, S.V.; Shparlinski, I.E. Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm. *Int. Math. Res. Not.* **2008**, *2008*, rnn090.
23. Konyagin, S.V.; Shparlinski, I.E. *Character Sums with Exponential Functions and Their Applications;* Cambridge Tracts in Mathematics; Cambridge University Press: Cambridge, UK, 1999; Volume 136.
24. Shparlinski, I.E. Estimates for Gaussian sums. *Math. Notes* **1991**, *50*, 740–746. [CrossRef]
25. Shteinikov, Y. Estimates of trigonometric sums over subgroups and some of their applications. *Math. Notes* **2015**, *98*, 667–684. [CrossRef]
26. Baker, R.C.; Harman, G. Shifted primes without large prime factors. *Acta Arith.* **1998**, *83*, 331–361. [CrossRef]
27. Heath-Brown, D.R. Artin's conjecture for primitive roots. *Quart. J. Math. Oxf. Ser.* **1986**, *37*, 27–38. [CrossRef]
28. Konyagin, S.V.; Shparlinski, I.E. On the consecutive powers of a primitive root: Gaps and exponential sums. *Mathematika* **2012**, *58*, 11–20. [CrossRef]
29. Bourgain, J. Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary. *J. Anal. Math.* **2005**, *97*, 317–355. [CrossRef]
30. Bourgain, J.; Chang, M.-C. Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors. *Geom. Funct. Anal.* **2006**, *16*, 327–366. [CrossRef]