On the Fractional Parts of a^n/n

Javier Cilleruelo
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and
Universidad Autónoma de Madrid
28049-Madrid, Spain
franciscojavier.cilleruelo@uam.es

Angel Kumchev
Department of Mathematicss, Towson University
Towson, MD 21252, U.S.A.
akumchev@towson.edu

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, Mexico
fluca@matmor.unam.mx

Juanjo Rué
Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM)
C/ Nicolás Cabrera 13-15, 28049-Madrid, Spain
juanjo.rue@icmat.es

Igor E. Shparlinski
Deptartment of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor.shparlinski@mq.edu.au

Abstract

We give various results about the distribution of the sequence $\{a^n/n\}_{n \geq 1}$ modulo 1, where $a \geq 2$ is a fixed integer. In particular, we find an explicit infinite subsequence $\mathcal{A}$ such that $\{a^n/n\}_{n \in \mathcal{A}}$ is uniformly distributed modulo 1. Also we show that for any constant $c > 0$ and a sufficiently large N, the fractional parts of the first N terms of this sequence hit every interval $\mathcal{J} \subseteq [0,1]$ of length $|\mathcal{J}| \geq cN^{-0.475}$.

1 Introduction

1.1 Motivation

Let $a \geq 2$ be an integer. It has been asked [1] whether for every nonzero integer h, we have the estimate

$$\sum_{n \leq N} \mathbf{e}\left(h\frac{a^n}{n}\right) = o(N) \tag{1}$$

as $N \to \infty$, where, as usual, for a real number x we put $\mathbf{e}(x) = \exp(2\pi i x)$.

It is well-known that the bound (1) is equivalent to the uniform distribution modulo 1 of the sequence $\{a^n/n\}_{n \geq 1}$, where $\{\gamma\}$ denotes the fractional part of a real number γ.

While we certainly believe that (1) holds, we have not been able to confirm this conjecture.

1.2 Our results

Instead, here we settle for the somewhat more modest goal of showing that the sequence $\{a^n/n\}_{n \geq 1}$ is dense modulo 1. This statement is an immediate consequence of a stronger result which we obtain here, that asserts that the sequence $\{a^n/n\}$ is uniformly distributed when we restrict n to a certain subset of the positive integers.

We define the set

$$\mathcal{A} = \{pq : \ p, q \text{ primes}, \ q \leq (\log p)/(\log a)\}$$

and put $\mathcal{A}(N) = \mathcal{A} \cap [1, N]$. We recall that the *discrepancy* $\Delta(\Gamma)$ of a sequence Γ of M points

$$\Gamma = \left\{(\gamma_m)_{m=1}^{M}\right\} \tag{2}$$

2

in the unit interval $[0, 1]$ is defined as

$$\Delta(\Gamma) = \sup_{[\alpha,\beta] \subseteq [0,1]} \left| \frac{T_\Gamma([\alpha, \beta])}{M} - (\beta - \alpha) \right|,$$

where $T_\Gamma([\alpha, \beta])$ is the number of points of Γ inside the interval $[\alpha, \beta]$. Our first result provides bounds for the discrepancy of $\{a^n/n\}_{n \in \mathcal{A}(N)}$, showing that the sequence is dense in $[0, 1]$:

Theorem 1. *The discrepancy $D(N)$ of the sequence $\{a^n/n\}_{n \in \mathcal{A}(N)}$ is*

$$D(N) = O\left(\frac{\log \log \log \log N}{\log \log \log N} \right).$$

Since it is also interesting to derive strong explicit bounds on the density, we address this issue too. Our second result estimates the length of intervals in which we can assure the existence of points of the sequence for N sufficiently large:

Theorem 2. *For any constant $c > 0$ and a sufficiently large N, every interval $\mathcal{J} \subseteq [0, 1]$ of length $|\mathcal{J}| \geq cN^{-0.475}$ contains a number of the form $\{a^n/n\}$ for some $n \leq N$.*

If we assume some unproved hypothesis, say the Generalized Riemann Hypothesis or the Generalized Lindelöf Hypothesis, we can reduce the size of the intervals in Theorem 2 to $|\mathcal{J}| \geq N^{-1/2+\epsilon}$ for any fixed $\epsilon > 0$. Furthermore, by combining the argument of Theorem 2 with a slight generalization of a result of K. Matomäki [7] (to differences of primes in a progression with a small modulus), one can show that the total measure of gaps larger than $N^{-1/2}$ is $O\left(N^{-1/3} \right)$.

1.3   Notation

We use the Landau symbol O and o as well as the Vinogradov's symbols $\ll, \gg$ and $\asymp$. Recall that $A = O(B)$, $A \ll B$ and $B \gg A$ are all equivalent to the fact that the inequality $|A| \leq cB$ holds with some constant c. Furthermore, $A \asymp B$ means that both $A \ll B$ and $B \gg A$ hold.

Throughout the paper, p and q always denote prime numbers. For two integers u and v, their greatest common divisor is denoted by (u, v).

As usual, for relatively prime integers a and q we denote by $\mathrm{ord}_q\, a$ the multiplicative order of a in $\mathbb{Z}/q\mathbb{Z}$.

We use $\pi(x)$ for the number of primes $p \leq x$, and for coprime positive integers k and r we use $\pi(x; k, r)$ for the number of primes smaller than or equal to x in the arithmetic progression $r \pmod{k}$.

Finally, we denote by $\varphi(n)$ the Euler function and by $P(n)$ the largest prime divisor of an integer $n \geq 1$ (we set $P(1) = 1$).

2 Preliminaries

2.1 Some general facts

We use the asymptotic estimate that follows from the *Siegel–Walfisz Theorem*, see [4, Corollary 5.29],

$$\pi(x; k, r) = \frac{\pi(x)}{\varphi(k)} + O\left(\frac{x}{(\log x)^A}\right) \tag{3}$$

valid for any k with $(k, r) = 1$, and any constant $A > 0$. We also need the bound given by the *Brun-Titchmarsh Theorem*, see [4, Theorem 6.6]

$$\pi(x; k, r) \ll \frac{x}{\varphi(k) \log (x/k)} \qquad \text{valid for all} \qquad x > k. \tag{4}$$

We recall the *Mertens Formula* for the sum of reciprocals of the primes $p \leq x$ in the following crude form

$$\sum_{q \leq x} \frac{1}{x} = \log\log x + O(1). \tag{5}$$

We also use the following well–known lower bound

$$\varphi(n) \gg \frac{n}{\log\log n} \qquad \text{for } n \geq 3. \tag{6}$$

One of our main tools is the classical *Erdős-Turán Inequality* (see, for example, [2, Theorem 1.21]) that relates the uniformity of distribution to exponential sums.

Lemma 1. *For any integer $L \geq 1$, for the discrepancy $\Delta(\Gamma)$ of the sequence (2), we have*

$$\Delta(\Gamma) \ll \frac{1}{L} + \frac{1}{M} \sum_{0 < |h| \leq L} \frac{1}{|h|} \left| \sum_{m=1}^{M} \mathbf{e}\left(h\gamma_m\right) \right|.$$

To prove Theorem 2, we need the following slight modification of [3, Theorem 10.8].

Lemma 2. *There exists an absolute constant $\vartheta < 0.525$ with the following property: For any $A > 0$, if x is sufficiently large, $q \leq (\log x)^A$, $(l, q) = 1$ and $x^{\vartheta} \leq h \leq x$, then*

$$\pi(x; q, l) - \pi(x - h; q, l) \geq \frac{h}{20\phi(q) \log x}.$$

Proof. We recall that [3, Theorem 10.8] states such a result with $\vartheta = 0.525$ and the constant 0.09 in place of $1/20$ in the lower bound. In fact, the proof of [3, Theorem 10.8] yields a lower bound of the form

$$\pi(x; q, l) - \pi(x - h; q, l) \geq \frac{C(\theta)h}{\phi(q) \log x},$$

for $x^{\theta} \leq h \leq x$. Here, $C(\theta)$ is a continuous decreasing function of θ such that $C(0.525) \geq 0.09$. It is clear from the continuity of $C(\theta)$ (see also the comments in [3, §7.10]) that one also has $C(\theta_0) \geq 0.05$ for some $\theta_0 < 0.525$. Taking $\vartheta = \theta_0$, one obtains the lemma. $\square$

2.2 Some facts about $\mathcal{A}(N)$

Lemma 3. *We have*

$$\#\mathcal{A}(N) \sim \frac{N \log \log \log N}{\log N}.$$

Proof. We observe that if $pq \in \mathcal{A}(N)$ then

$$a^q \leq p \leq N/q.$$

Let Q be the largest prime q such that $a^q \leq N/q$ and notice that $Q \sim (\log N)/(\log a)$. We observe that

$$\sum_{q \leq Q} \pi(a^q) \ll \sum_{q \leq Q} \frac{a^q}{q} \ll \frac{a^Q}{Q} \ll \frac{N}{Q^2} \ll \frac{N}{\log^2 N}. \qquad (7)$$

Thus, we have

$$\#\mathcal{A}(N) = \sum_{q \leq Q} \left(\pi(N/q) - \pi(a^q) \right) = \sum_{q \leq Q} \pi(N/q) + O\left(\frac{N}{\log^2 N} \right).$$

On the other hand,

$$\sum_{q \leq Q} \pi(N/q) \sim \sum_{q \leq Q} \frac{N}{q \log(N/q)} \sim \frac{N}{\log N} \sum_{q \leq Q} \frac{1}{q} \sim \frac{N \log \log \log N}{\log N}$$

and the result follows. $\qquad \square$

For a pair of primes $p > q$ we define $u_q(p)$ by the condition

$$u_q(p)p \equiv 1 \pmod{q}, \qquad 1 \leq u_q(p) \leq q - 1. \qquad (8)$$

For real α and β, we also write $\alpha \equiv \beta \pmod 1$ if $\alpha - \beta \in \mathbb{Z}$.

Lemma 4. *For primes $p > q$, we have*

$$\frac{a^{pq}}{pq} \equiv \frac{(a^p - a)}{q} u_q(p) + \frac{a^q}{pq} \pmod 1.$$

Proof. By (8), we have

$$\frac{a^{p-1} - 1}{p} \equiv (a^{p-1} - 1)u_q(p) \pmod q,$$

and then

$$\frac{a^{pq}}{pq} = \frac{a^{(p-1)(q-1)}a^{p+q-1}}{pq} \equiv \frac{a^{p+q-1}}{pq} \equiv \frac{1}{q} \frac{a^q (a^{p-1} - 1)}{p} + \frac{a^q}{pq}$$

$$\equiv \frac{a (a^{p-1} - 1) u_q(p)}{q} + \frac{a^q}{pq} \equiv \frac{(a^p - a)}{q} u_q(p) + \frac{a^q}{pq} \pmod 1,$$

which concludes the proof. $\qquad \square$

3 Proofs of the Main Results

3.1 Proof of Theorem 1

The core of the proof is based on estimating the exponential sum

$$
\begin{aligned}
S(h, N) &= \sum_{pq \in \mathcal{A}(N)} \mathbf{e}\left(\frac{ha^{pq}}{pq}\right) \\
&= \sum_{pq \in \mathcal{A}(N)} \mathbf{e}\left(h\left(\frac{(a^p - a)}{q}u_q(p) + \frac{a^q}{pq}\right)\right) = \widetilde{S}(h, N) + E,
\end{aligned}
$$

where

$$
\widetilde{S}(h, N) = \sum_{n=pq \in \mathcal{A}(N)} \mathbf{e}\left(h\frac{(a^p - a)}{q}u_q(p)\right)
$$

and

$$
|E| \ll \sum_{pq \in \mathcal{A}(N)} \frac{|h|a^q}{pq}.
$$

Let Q be defined as in the proof of Lemma 3. We use (7) and Mertens formula (5) to get

$$
|E| \ll \sum_{q \leq Q} \frac{|h|a^q}{q} \sum_{p \leq N} \frac{1}{p} \ll \frac{|h|N \log \log N}{\log^2 N}. \tag{9}
$$

Now we fix a prime q and a pair of integers (u, v) with $1 \leq u, v \leq q - 1$ and $(u, q) = (v, q - 1) = 1$. By the Chinese Remainder Theorem, we see that the primes p which satisfy

$$
up \equiv 1 \pmod{q}, \qquad p \equiv v \pmod{q - 1},
$$

belong to a certain arithmetic progression $z_q(u, v) \pmod{q(q - 1)}$. Thus,

$$
\begin{aligned}
\widetilde{S}(h, N) &= \sum_{q \leq Q} \sum_{u=1}^{q-1} \sum_{\substack{v=1 \\ (v, q-1)=1}}^{q-2} \mathbf{e}\left(h\frac{(a^v - a)}{q}u\right) \\
&\quad \times \left(\pi\left(\frac{N}{q}; q(q-1), z_q(u, v)\right) - \pi\left(a^q; q(q-1), z_q(u, v)\right)\right).
\end{aligned}
$$

7

Using (3) (with $A = 2$) and (4) and noticing that the sum over u and v contains $\varphi(q(q-1))$ terms, we obtain

$$\widetilde{S}(h, N) = \Sigma_0 + O(\Sigma_1 + \Sigma_2), \qquad (10)$$

where

$$\Sigma_0 \;=\; \sum_{q \leq Q} \frac{\pi(N/q)}{\varphi(q(q-1))} \sum_{u=1}^{q-1} \sum_{\substack{v=1 \\ (v,q-1)=1}}^{q-2} \mathbf{e}\left(h\frac{(a^v - a)}{q}u\right), \qquad (11)$$

$$\Sigma_1 \;=\; \sum_{q \leq Q} \frac{a^q}{q} \ll \frac{N}{\log^2 N}, \qquad (12)$$

$$\Sigma_2 \;=\; \sum_{q \leq Q} \frac{N}{q\,(\log(N/q))^2} \ll \frac{N \log \log \log N}{\log^2 N}. \qquad (13)$$

We continue getting estimates for Σ_0. Write

$$s(h, q) = \sum_{u=1}^{q-1} \sum_{\substack{v=1 \\ (v,q-1)=1}}^{q-2} \mathbf{e}\left(h\frac{(a^v - a)}{q}u\right).$$

We observe that for q with $(q, ah) = 1$ we have

$$\sum_{u=1}^{q-1} \mathbf{e}\left(h\frac{a^v - a}{q}u\right) = \begin{cases} -1 & \text{if } a^{v-1} \not\equiv 1 \pmod q, \\ q - 1 & \text{if } a^{v-1} \equiv 1 \pmod q. \end{cases}$$

From this observation, for a prime q such that $(q, ah) = 1$ we have the exact value

$$s(h, q) = -\varphi(q-1) + q\#\{v : \ (v, q-1) = 1, \ a^{v-1} \equiv 1 \pmod q\}.$$

Thus,

$$|s(h, q)| \leq \varphi(q-1) + \frac{q(q-1)}{\operatorname{ord}_q a} \leq 2\frac{q(q-1)}{\operatorname{ord}_q a}. \qquad (14)$$

8

We also have the trivial bound $|s(h, q)| \leq \varphi(q(q-1))$ if $(q, ah) > 1$. Therefore,

$$
\begin{aligned}
|\Sigma_0| &\leq 2N \sum_{\substack{q \leq Q \\ q \nmid ah}} \frac{q(q-1)}{q\varphi(q(q-1)) \log(N/q) \operatorname{ord}_q a} \\
&\quad + N \sum_{\substack{q \leq Q \\ q \mid ah}} \frac{\varphi(q(q-1))}{q\varphi(q(q-1)) \log(N/q)} \\
&\ll \frac{N}{\log N} \sum_{q \leq Q} \frac{1}{\varphi(q-1) \operatorname{ord}_q a} + \frac{N}{\log N} \sum_{\substack{q \leq Q \\ q \mid ah}} \frac{1}{q}.
\end{aligned}
$$

Using the trivial bound $\operatorname{ord}_q a \geq \log q / \log a$ and the bound (6), we obtain

$$
\sum_{q \leq Q} \frac{1}{\varphi(q-1) \operatorname{ord}_q a} \ll \sum_q \frac{\log \log q}{q \log q} = O(1).
$$

where in the last sum the summation is taken over all prime numbers. Hence,

$$
\Sigma_0 \ll \frac{N}{\log N} \left(1 + \sum_{q \mid h} \frac{1}{q} \right). \tag{15}
$$

Substituting the bound (15) together with the bound (12) and (13) in (10), taking into account (9) and recalling the bound for $\#\mathcal{A}(N)$ obtained in Lemma 3 we get

$$
S(h, N) \ll \frac{|h| N \log \log N}{\log^2 N} + \frac{N}{\log N} \left(1 + \sum_{q \mid h} \frac{1}{q} \right).
$$

We now take

$$
L = \frac{\log \log \log N}{\log \log \log \log N}
$$

and apply Lemma 1 (with $M = \#\mathcal{A}(N)$) to derive that the discrepancy

$D(N)$ of the sequence $\mathcal{A}(N)$ satisfies the bound

$$
\begin{aligned}
D(N) \quad \ll \quad & \frac{1}{L} + \frac{1}{M} \sum_{0<|h|\leq L} \frac{|S(h;N)|}{|h|} \\
\ll \quad & \frac{1}{L} + \frac{L}{M} \frac{N \log\log N}{\log^2 N} + \frac{N \log L}{M \log N} + \frac{N}{M \log N} \sum_{0<|h|\leq L} \frac{1}{|h|} \sum_{q|h} \frac{1}{q} \\
\ll \quad & \frac{\log\log\log\log N}{\log\log\log N} + \frac{1}{\log\log\log N} \sum_{q} \frac{1}{q} \sum_{0<|l|\leq L/q} \frac{1}{|ql|} \\
\ll \quad & \frac{\log\log\log\log N}{\log\log\log N} + \frac{\log L}{\log\log\log N} \ll \frac{\log\log\log\log N}{\log\log\log N},
\end{aligned}
$$

which concludes the proof.

3.2 Proof of Theorem 2

Let N be large. We consider the largest prime $q \leq (\log N)/(\log a)$ and write $T = a^q/q$. We fix some $c > 0$ and prove that any interval $\mathcal{J}$ of length $|\mathcal{J}| \geq cN^{-0.475}$ contains some element of the form $\{a^{pq}/(pq)\}$ for some prime p in the set

$$
\mathcal{P} = \{p, \ p \equiv 1 \pmod{q-1}, \quad T/2 \leq p \leq T\}.
$$

Lemma 2 implies that consecutive primes in this set satisfy $p_{n+1} - p_n \ll T^\vartheta$, with some constant $\vartheta < 0.525$. We observe also that if $p \equiv 1 \pmod{q-1}$ then $a^{p-1} \equiv 1 \pmod{q}$. Thus $a^{p-1} \equiv 1 \pmod{pq}$. Then we have that

$$
\frac{a^{pq}}{pq} \equiv \frac{a^{(p-1)q}a^q}{pq} \equiv \frac{a^q}{pq} \equiv \frac{T}{p} \pmod 1.
$$

Finally, we observe that if p runs in $\mathcal{P}$, then $T/p \in [1,2]$ and that consecutive fractional parts, corresponding to consecutive primes $p_n, p_{n+1} \in \mathcal{P}$ satisfy

$$
\begin{aligned}
0 < \left\{\frac{T}{p_n}\right\} - \left\{\frac{T}{p_{n+1}}\right\} &= \left(\frac{T}{p_n} - 1\right) - \left(\frac{T}{p_{n+1}} - 1\right) \\
&= \frac{T}{p_n} - \frac{T}{p_{n+1}} = \frac{T(p_{n+1} - p_n)}{p_n p_{n+1}} \ll T^{\vartheta-1} = o(N^{-0.475}),
\end{aligned}
$$

which concludes the proof.

Acknowledgments

References

[1] W. D. Banks, M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Uniform distribution of fractional parts related to pseudoprimes', *Canadian J. Math.* **61** (2009), 481–502.

[2] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[3] G. Harman, *Prime-Detecting Sieves*, LMS Monographs **33**, Princeton University Press, 2007.

[4] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[5] P. Kurlberg and C. Pomerance, 'On the period of the linear congruential and power generators', *Acta Arith.*, **119** (2005), 149–169.

[6] F. Luca and I. E. Shparlinski, 'Quadratic fields generated by the Shanks sequence', *Proc. Edinb. Math. Soc.*, **52** (2009), 719–729.

[7] K. Matomäki, 'Large differences between consecutive primes', *Quart. J. Math. (Oxford)*, **58** (2007), 489–518.