VILNIUS UNIVERSITY

AIVARAS NOVIKAS

COMPOSITE NUMBERS IN THE SEQUENCES OF INTEGERS

Doctoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2012

The scientific work was carried out in 2008–2012 at Vilnius University.

Scientific supervisor:

prof. habil. dr. Artūras Dubickas (Vilnius University, physical sciences, mathematics – 01P)

Scientific adviser:

prof. dr. Ramūnas Garunkštis (Vilnius University, physical sciences, mathematics – 01P)

VILNIAUS UNIVERSITETAS

AIVARAS NOVIKAS

SUDĖTINIAI SKAIČIAI SVEIKŲJŲ SKAIČIŲ SEKOSE

Daktaro disertacija
Fiziniai mokslai, matematika (01P)

Vilnius, 2012 metai

Disertacija rengta 2008–2012 metais Vilniaus universitete.

Mokslinis vadovas:

prof. habil. dr. Artūras Dubickas (Vilniaus universitetas, fiziniai mokslai, matematika – 01P)

Konsultantas:

prof. dr. Ramūnas Garunkštis (Vilniaus universitetas, fiziniai mokslai, matematika – 01P)

Contents

Notation

$\mathbb{N}$	the set of all positive integers
$\mathbb{Z}$	the set of all integers
$\mathbb{Q}$	the set of all rational numbers
$\mathbb{R}$	the set of all real numbers
$\mathbb{C}$	the set of all complex numbers
$[x]$	an integer part of x
$\{x\}$	a fractional part of x
$\mathbb{N}^2$	the set of all non-zero perfect squares
$\mathbb{F}_q$	the Galois field of order q
$\left(\frac{a}{p}\right)$	the Jacobi symbol
$K(\alpha)$	the algebraic extension of the field K

Introduction

The topics examined in this thesis were the subject of my research as a PhD student at the Faculty of Mathematics and Informatics of Vilnius University. The presented investigation concerns the existence of composite numbers in some special sequences, such as the sequence of integer parts of powers of a fixed number and a linear recurrence sequence consisting of integer numbers.

Actuality. In number theory, the distinction between prime and composite numbers plays a crucial role. It was understood already in antiquity and the distinction grew in importance with number theory evolving as a separate large branch of mathematics in the new times. Prime and composite numbers were examined in the context of divisibility properties of integers (e.g., by Euclid in his "Elements" and much later by Fermat, Euler, etc.)

At the same time the interest of mathematicians shifted to examination of integer numbers of special form and determining whether they can be prime or composite. Fermat's conjecture that all numbers of the form $2^{2^n}+1$ are prime was soon disproved by Euler. However, many problems of this kind are very difficult and even remain unsolved to this day due to "irregular" pattern of the prime and composite numbers in the sequence of positive integers (e.g., the four Landau's problems). As such, they occupy a deserved position in contemporary number theory.

In this thesis we search for composite numbers in the sequence of integer parts of powers of a fixed number. Although questions related to these sequences and also to the similar sequences of fractional parts have been studied by many scientists some important problems remain out of reach: e.g., the distribution of fractional parts in even the seemingly most simple cases and existence of infinitely many prime numbers in the sequences of integer parts. The question of distribution of the fractional parts is, on the one hand, related to the behaviour of the integer parts, and, on the other hand, (in the case of the integer powers of the number 3/2) to such famous subjects as Waring's problem.

The actuality of particular problems is further discussed in detail in the section "Review and main results".

Aims and problems. The most general aim of this thesis is to determine the existence and properties of composite numbers in some special sequences of integers, also to construct sequences of some special form consisting of only composite numbers. To be precise, the following questions are considered:

- For which rational numbers $a > 1$ and real numbers $\xi > 0$, does the sequence
$$[\xi a^n], n = 1, 2, \dots,$$
of integer parts contain infinitely many composite numbers?
- If the sequence
$$[\xi a^n], n = 1, 2, \dots,$$
contains infinitely many composite numbers, then is it possible to indicate a finite set of prime numbers at least one of which divides infinitely many of those composite numbers?
- For which "shifted" sequences
$$[\xi a^n + \nu], n = 1, 2, \dots,$$
where $\nu \in \mathbb{R}$, can the first two questions be answered? Can one indicate inifinitely many values of ν for which such a sequence would contain infinitely many composite numbers for some certain a and any $\xi > 0$?
- For which binary linear recurrence equations
$$x_{n+1} = ax_n + bx_{n-1},$$
where $a, b \in \mathbb{Z}$, does there exist a corresponding binary linear recurrence sequence of integers whose two initial terms are positive and relatively prime and which consists of only composite numbers (the absolute values of the terms being taken)?
- Let t be a fixed positive integer. Which numbers belong to the set $E(t) = \{n \in \mathbb{N} : n = tM - d\}$, where M is a positive multiple of the product and d is a positive divisor of the sum of two positive integers a and b?

Methods. A variety of methods is applied in this thesis. In Section 1 we improve the achievements of Forman and Shapiro [14] not only reducing the length of their proofs, but also producing a series of new results, based on the examination of the behaviour and mutual relations between fractional parts of powers of rational numbers as well as their integer parts and avoiding initial assumption of the "proof by contradiction" method. This allows us to prove the most difficult case of the main Theorem 1.1 in Section 1.4 by using established divisibility properties of the terms of the sequence to determine combinatorial properties of the sequences of operations, interpreted as formal sequences of symbols. In Section 2 we apply the concept of covering systems introduced by Erdős to the linear recurrence sequences consisting of integer terms. In Section 3 we examine a special linear form whose relation to the Egyptian fractions and some minor facts about it established by us allows us to state a conjecture, which is tested by computer calculations. Throughout the thesis such classical number theory subjects as Chinese remainder theorem, Dirichlet's theorem on arithmetical progressions and Jacobi symbol are also occasionally used. See the introductory parts of Sections 1, 2 and 3 for more details.

Novelty and approbation. All research represented in this thesis is original. The main results have been published in the refereed journals (see "Principal publications"). They were also presented at the international conference "27th Journées Arithmétiques" (Vilnius, Lithuania, 2011), at the Conference of Lithuanian Mathematical Society and the seminar of the Department of Probability Theory and Number Theory of the Faculty of Mathematics and Informatics of Vilnius University.

Principal publications. The main results of the thesis are published in the following papers:

- A. Dubickas and A. Novikas, *Integer parts of powers of rational numbers,* Math. Zeitschrift, **251** (2005), 635–648.

- A. Dubickas, A. Novikas and J. Šiurys, *A binary linear recurrence sequence of composite numbers,* J. Number Theory, **130** (8) (2010), 1737–1749.
- A. Dubickas and A. Novikas, *On integers expressible by some special linear form,* Acta Math. Univ. Comen., New Ser., 9 p. (to appear).

Other publications. Preprints and conference abstracts:

- Integer parts of powers of rational numbers, *Preprint 2004–44,* Vilnius University, Faculty of Mathematics and Informatics 2004, 14 p. (with A. Dubickas)
- A binary linear recurrence sequence of composite numbers, *27th Journées Arithmétiques,* Vilnius, Lithuania, June 27 – July 1, 2010: Abstracts, http://atlas-conferences.com/c/b/b/v/22.htm (with J. Šiurys)
- Some remarks on the composition of competition problems, *The 9th International conference "Teaching mathematics: retrospective and perspectives",* Vilnius, Lithuania, May 16 – May 17, 2008: Abstracts

Acknowledgments. I would like to express my sincere gratitude to my supervisor Professor Artūras Dubickas. I am highly indebted to him for his valuable guidance, encouragement and advice.

I am also very thankful to my school teacher Antanas Skūpas and my university teacher Hamletas Markšaitis, whose enthusiastic instruction and friendly attitude was very inspiring and contributed much to my involvement in mathematical research.

Finally, I would like to thank everyone, whose constant support, fruitful collaboration or mere joyful moments of life accompanied me through the mathematical journey, notably Romualdas Kašuba, as well as Juozas Mačys, Paulius Šarka, Paulius Drungilas, Jonas Jankauskas, Jonas Šiurys and my other colleagues and co-workers at the Department of Probability Theory and Number Theory and the Department of Methodics of Mathematics and Informatics of the Faculty where this PhD thesis was written.

Review and main results. We start with some basic definitions. For any real number x, the biggest integer not exceeding x we will call *an integer part* of x and denote it by $[x]$. The number $\{x\} = x - [x]$ is called *a fractional part* of x. We define *a prime number* as a positive integer which has exactly two distinct positive integer divisors and *a composite number* as a positive integer which has at least three distinct positive integer divisors (i.e., it is not a prime number and is not equal to 1). Denote by $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ the sets of all integers, positive integers, rational numbers, real numbers and complex numbers, respectively.

Below, we present the research and our results related to

- the composite numbers in the sequences of integer parts of powers of rational numbers,
- the composite numbers in the binary linear recurrence sequences,
- the Egyptian fractions.

Integer parts of powers of rational numbers

There are many unsolved problems concerning the distribution of the fractional parts of powers of a rational number $a > 1$. The sequence $\{a^n\}$, $n = 1, 2, \dots,$ and, more generally, the sequence $\{\xi a^n\}$, $n = 1, 2, \dots,$ where ξ is a fixed positive number, was studied by Vijayaraghavan [34]. He proved the following:

The set of limit points of the sequence $\{(p/q)^n\}, n = 1, 2, \dots,$ *where* $p > q > 1$ *are integers satisfying* $\gcd(p, q) = 1$, *is infinite.*

The generalization of this proposition was proved by Pisot [27] (and later by Dubickas, in a different way [11]). Before stating it we recall what is *a Pisot-Vijayaraghavan number* (or *a PV number*). Firstly, a number $\alpha \in \mathbb{C}$ is called *an algebraic integer* if it is a root of an irreducible monic polynomial with integer coefficients. Other roots of that polynomial are called *conjugates* of α. The number $\alpha \in \mathbb{C}$ is called *a Pisot-Vijayaraghavan number* if it is a real algebraic integer greater than 1 such that all its conjugates are smaller than 1 in absolute value. Now we proceed with the generalized statement:

Let $\alpha > 1$ *be an algebraic number and let* $\xi > 0$ *be a real number. Then the set* $\{\xi\alpha^n\}, n \in \mathbb{N}$, *has only finitely many limit points if and only if* α *is a PV-number and* $\xi \in \mathbb{Q}(\alpha)$.

Despite these results, it remains unproved that the sequence $\{(3/2)^n\}, n = 1, 2, \dots,$ has infinitely many limit points in $[0, 1/2)$ or in $[1/2, 1]$. Flatto, Lagarias and Pollington [13] have made a step towards (see also [5] for other achievements in this direction) by proving the inequality

$$\limsup_{n\to\infty} \{(3/2)^n\} - \liminf_{n\to\infty} \{(3/2)^n\} \geqslant 1/3.$$

It would suffice to prove that $\limsup_{n\to\infty} \{(3/2)^n\} - \liminf_{n\to\infty} \{(3/2)^n\} > 1/2$. Let us consider a more general case of the sequence $\{(\xi/2)a^n\}$, $n \in \mathbb{N}$, where $\xi > 0$ and $a \in \mathbb{Q}, a > 1$, are some fixed numbers. Clearly, if one could prove that the distance between the largest limit point of $\{(\xi/2)a^n\}$, $n \in \mathbb{N}$, and the smallest one is greater than $1/2$, then the smallest limit point is smaller than $1/2$. This would imply that there are infinitely many even numbers among $[\xi a^n]$, $n \in \mathbb{N}$, which is the matter of our direct concern in this thesis. However, it is only known [13] that this distance is $\geqslant 1/b$, where b is the numerator of $a = b/c \in \mathbb{Q}$, $b > c > 1$, $(b, c) = 1$, which, although being a remarkable result itself, cannot be used to achieve our aims.

Hence, the question of distribution in even the simplest case of $a = 3/2$ is far from being understood; its importance is usually motivated by a remarkable connection between the distribution of $\{(3/2)^n\}$, $n = 1, 2, \dots$, and Waring's problem. (See, for instance, [33].) Essentially, Waring's problem has been solved by Hilbert who proved the following:

Every positive integer is the sum of a fixed number $g(n)$ of n^{th} powers of non-negative integers, where n is any given positive integer and $g(n)$ depends only on n.

However, the question of expressing the smallest possible $g(n)$ by a formula depends on the properties of $\{(3/2)^n\}$ which still remain to be determined.

Some metrical results on the distribution of the fractional parts are well-known. Koksma [21] proved that

The sequence $\{\xi a^n\}$, $n = 1, 2, \dots$, where $\xi > 0$, is uniformly distributed in $[0, 1]$ for almost all $a > 1$.

This implies that, for almost all $a > 1$, $[a^n]$ are composite for infinitely many n (see [14]). Baker and Harman [2] obtained other metrical results in this direction. Unfortunately, it is impossible to apply these results to rational numbers, because the set of rational numbers is of measure zero. To indicate certain values of a for which $[a^n]$ are composite for infinitely many n also presents a challenge.

In [22] Mahler asked the following question:

Is there a positive number α such that the numbers $\{\alpha(3/2)^n\}$, $n \in \mathbb{N}$, are all smaller than $1/2$?

This question is equivalent to another one: is there a positive number $\xi(= 2\alpha)$ such that the numbers $[\xi(3/2)^n]$, $n \in \mathbb{N}$, are *all* even? Mahler's question remains unsolved. Our Theorem 1.1 shows that, for *every* $\xi > 0$, the set $[\xi(3/2)^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by one of the numbers $2, 5, 7, 11$.

There is not too much information about $a > 1$ for which $[a^n]$ is prime for infinitely many integers n. See, for instance, [1], [2], [23], [37] for some existence results in this direction. In [2] Baker and Harman prove that

The sequence $[a^n], n = 1, 2, \dots,$ contains infinitely many primes for almost all $a > 1$.

However, no certain value of a is indicated by them. Mills [23] proved the existence of such a number A that an integer part $[A^{3^n}]$ is prime for any $n \in \mathbb{N}$. According to a conjecture of Whiteman (see Problem E19 in [17]) the sequence $[a^n]$, $n = 1, 2, \dots,$ where $a > 1$ is a rational noninteger number, contains infinitely many primes. However, no results are known to confirm this statement.

We are interested in a problem for which the cases $a = 3/2$ and $a = 4/3$ were successfully treated more than forty years ago by Forman and Shapiro [14], but no progress has been made since then for a long time. This at first glance simple problem can be stated as follows: prove that for every rational $a > 1$ the sequence of integer parts $[a^n]$ contains infinitely many composite numbers. (This problem is trivial for integer a.)

Very few explicit irrational $a > 1$ producing infinitely many composite numbers are known. Cass [7] proved that

The set $[a^n]$, $n \in \mathbb{N}$, contains infinitely many composite numbers if $a > 1$ is a unit in a real quadratic number field.

(By a unit in a real quadratic number field we mean a invertible element in the ring of algebraic integers of the real algebraic extension of $\mathbb{Q}$ of the second order.) This result was extended by Dubickas [8] to all Pisot-Vijayaraghavan and Salem numbers a :

The set $[a^n]$, $n \in \mathbb{N}$, *contains infinitely many composite numbers if* $a > 1$ *is a Pisot-Vijayaraghavan or a Salem number.*

(Every real quadratic unit is a Pisot number of degree 2. See also [10] for a generalization. By a Salem number we mean a real algebraic integer greater than 1 such that all its conjugates are not greater than 1 in absolute value and at least one of them is equal to 1 in absolute value.) Some explicit transcendental $a > 1$ for which $[a^n]$ are composite infinitely often were constructed in [1].

As for the rational numbers, our result below concerning composite numbers in the case of $a = 2$ has been recently improved by Dubickas [9]:

For any real numbers $\xi \neq 0$ *and* ν, *the sequence of integer parts* $[\xi 2^n + \nu], n = 1, 2, ...,$ *contains infinitely many composite numbers. Moreover, if the number* ξ *is irrational, then the above sequence contains infinitely many elements divisible by* 2 *or* 3*.*

We are able to extend the result of [14]. We begin with our main theorem. Set $\mathcal{P}(2) = \{2\}$, $\mathcal{P}(3) = \mathcal{P}(4) = \{2, 3\}$, $\mathcal{P}(6) = \mathcal{P}(4/3) = \{2, 3, 5\}$, $\mathcal{P}(3/2) = \{2, 5, 7, 11\}$, $\mathcal{P}(5/4) = \{2, 3, 7, 11, 13\}$.

Theorem 1.1. *Let* $\xi > 0$ *be a real number and let* $a \in \{2, 3, 4, 6, 3/2, 4/3, 5/4\}$. *Then the set* $[\xi a^n]$, $n \in \mathbb{N}$, *contains infinitely many elements divisible by at least one number of the set* $\mathcal{P}(a)$.

In the above mentioned paper [14] Forman and Shapiro proved that the sets $[(3/2)^n]$ and $[(4/3)^n]$, $n \in \mathbb{N}$, contain infinitely many composite numbers. Their proof extends without change to $[\xi(3/2)^n]$ and $[\xi(4/3)^n]$ with arbitrary $\xi > 0$. However, we will give a proof for $a = 4/3$ once again, because (after a small preparation) we will be able to do this in just few lines in contrast to eight lemmas used in [14]. This will serve as a warm-up for the proof of a corresponding result for $a = 5/4$. The proof of Theorem 1.1 for $a = 3/2$ is given by combining our Lemma 1.7 with the main result of [14].

A valuable difference between our approach and that of [14] is that we are seeking a contradiction with Lemma 1.7 below which is obtained using fractional parts rather than a similar lemma for the integer parts of powers as in [14]. The main advantage in doing this is that we are able to describe some explicit (unavoidable) finite sets for possible divisors. (We show, however, that such unavoidable sets do not exist for some rational a; see the Proposition below.)

Note that the number $a = 5$ is missing in Theorem 1.1. The only reason for this is that, for $a = 5$, such universal explicit (unavoidable) set for divisors of the elements of the set $[\xi 5^n]$, $n \in \mathbb{N}$, cannot be given. In fact, it cannot be given for any number $a = 4k + 1$, where $k \in \mathbb{N}$.

Proposition 1.2. *Let a be a positive integer of the form $4k + 1$, where $k \in \mathbb{N}$, and let $\mathcal{P}$ be an arbitrary finite set of prime numbers. Then there exists $\xi > 0$ such that every integer part $[\xi a^n]$, $n = 1, 2, \dots,$ is relatively prime with every prime number of the set $\mathcal{P}$.*

We prove Proposition 1.2 in Section 1.4. However, in the same section we prove that the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many composite numbers since a universal set of divisors does not work only for special values of ξ, which we are able to deal with separately. The fact is a direct consequence of the following theorem.

Theorem 1.3. *Let $\xi > 0$ be a real number. If $\xi \neq (4k + 3)/(2 \cdot 5^r)$, where k, r are nonnegative integers, then the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by $2, 3$ or 5. If $\xi = (4k+3)/(2 \cdot 5^r)$, where $(4k+3, 5^r) = 1$, then the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by $10k + 7$.*

It remains unproved that the integer parts $[\xi a^n]$, $n = 1, 2, \dots,$ where ξ is an arbitrary positive number and $a \geqslant 7$ is an integer, are composite for infinitely many $n \in \mathbb{N}$. Also, Theorem 1.1 has not been extended to any rational noninteger number other than $3/2, 4/3, 5/4$ even for $\xi = 1$, although at first glance the case $a = 6/5$ may seem simpler than the case $a = 5/4$. However, by slightly changing the problem, we can include some new rational numbers.

Theorem 1.4. *Let $\xi > 0$ be a real number. Then each of the sets $[\xi(5/2)^n] - 1$ and $[\xi(6/5)^n] - 1$, where $n \in \mathbb{N}$, contains infinitely many elements divisible by at least one number of the set $\{2, 3, 5\}$.*

The proof for $[\xi(5/2)^n] - 1$ presented in Section 1.6 can be applied without changes to all the sets of numbers the form $[\xi(5/2)^n] - 1 + 30k, n \in \mathbb{N}$, where k is any fixed integer.

One can also consider the nearest integers to powers instead of integer parts. We define the nearest integer to z as $[z+1/2]$. Some new numbers can be obtained again.

THEOREM 1.5. *Let $\xi > 0$ be a real number. Then*
(i) the set $[\xi 7^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many composite numbers,
(ii) the set $[\xi(5/3)^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by 2 or 3,
(iii) the set $[\xi(7/5)^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by at least one of the numbers $2, 3, 5, 11$.

Note that no definite divisors are indicated for the set $[\xi 7^n + 1/2]$, $n \in \mathbb{N}$. This case is different from all the other cases for the reason that it is not covered by Lemma 1.2 which holds only for non-integer rational numbers (as in the case $a = 5$) and, in contrast to the case $a = 5$, integer parts are used to finish the proof instead of fractional parts (which are instrumental in excluding most of the values of ξ in the proof of Theorem 1.3).

In Section 1.1 we define the sequences of operations which describe the behaviour of the sequences of integer parts, but which can also be viewed as infinite words, i.e. formal sequences of symbols belonging to some set, called an alphabet. We will study the patterns which could and could not occur in these words and the possible periodicity of these sequences of symbols, as well.

Binary linear recurrence sequences

A sequence of real numbers $x_n, n = 1, 2, \dots,$ is called *a linear recurrence sequence* if its terms satisfy the recurrence

$$x_{n+d} = a_1 x_{n+d-1} + a_2 x_{n+d-2} + \cdots + a_d x_n, \ \ n = 1, 2, 3, \dots,$$

for some fixed numbers $d \in \mathbb{N}$ and $a_1, a_2, \dots, a_d \in \mathbb{R}$. The number d is called an order of the linear recurrence sequence under the natural assumption that $a_d \neq 0$.

Our results concern the order 2 (or *binary*) linear recurrence sequences consisting of integers. The best-known example of a binary linear recurrence sequence is the Fibonacci sequence, given by $F_1 = F_2 = 1$ and the recurrence relation $F_{n+1} = F_n + F_{n-1}$ for $n \geqslant 2$.

The question of determining prime and composite numbers in a linear recurrence sequence is an old one. For instance, it is not known if there are infinitely many primes in the Fibonacci sequence.

The main motivation of our research is a result of Graham [15] who found two relatively prime positive integers x_1, x_2 such that the sequence

$$x_{n+1} = x_n + x_{n-1},$$

$n = 2, 3, 4, \dots,$ contains only composite numbers, i.e., x_n is composite for each $n \in \mathbb{N}$. Graham's pair (x_1, x_2) was

$$(331635635998274737472200656430763, 1510028911088401971189590305498785).$$

Knuth [20] found the smaller pair

$$(x_1, x_2) = (62638280004239857, 49463435743205655).$$

Wilf [36] slightly refined Knuth's computation and found the pair

$$(x_1, x_2) = (20615674205555510, 3794765361567513).$$

This was further reduced by Nicol [26] to

$$(x_1, x_2) = (407389224418, 76343678551).$$

Currently, the "smallest" known such pair (in the sense that $x_1 + x_2$ is the smallest positive integer or $\max(x_1, x_2)$ is the smallest positive integer) is due to Vsemirnov [35]

$$(x_1, x_2) = (106276436867, 35256392432).$$

We prove the generalized result of this kind for every binary linear recurrence sequence except two cases for which the impossibility to obtain such result will be proved by a short argument. To be precise, we prove the following:

Theorem 2.1. *Let $(a, b) \in \mathbb{Z}^2$ and let $(x_n)_{n=1}^{\infty}$ be a sequence given by some initial values x_1, x_2 and the binary linear recurrence*

$$x_{n+1} = ax_n + bx_{n-1}$$

for $n = 2, 3, 4, \dots$. Suppose that $b \neq 0$ and $(a, b) \neq (2, -1), (-2, -1)$. Then there exist two relatively prime positive integers x_1, x_2 such that $|x_n|$ is a composite integer for each $n \in \mathbb{N}$.

The exclusion of the two cases is explained in Section 2.1: the required pair of initial values does not exist, i.e. the sequence $(|x_n|)_{n=1}^{\infty}$, where x_1, x_2 are composite and $\gcd(x_1, x_2) = 1$, always contains infinitely many prime numbers. The proof (as well as a part of the proof of Theorem 2.1) uses Dirichlet's theorem on arithmetic progressions: an arithmetic progression whose initial term and common difference are coprime integers contains infinitely many prime numbers (we take absolute values of the terms).

Theorem 2.1 has been formulated and proved for non-degenerate sequences in [30], preceeded by a weaker result in that direction [19]. (Binary linear recurrence sequence given by the recurrence equation $x_{n+1} = ax_n + bx_{n-1}$ is called degenerate if either $a = 0$ or the roots α and β of the characteristic equation $x^2 - ax - b = 0$ satisfy $\alpha/\beta = u$, where u is some root of unity.) We present a full, independent and much more self-contained proof.

Like Graham [15], we shall use the concepts of *divisibility sequences* and *covering systems*, as well as his idea of finding an appropriate covering system for $|b| = 1$ and Vsemirnov's pair (7) in order to treat some special cases with $|b| = 1$, in our proof.

Definition 2.2. *A sequence of rational integers $(v_n)_{n=1}^{\infty}$ is called a divisibility sequence if v_r divides v_s whenever r divides s.*

The Fibonacci sequence is a *divisibility sequence.* A more general example of a divisibility sequence is called the *Lucas sequence of the first kind.* Assume that the roots α, β of the (characteristic) equation $x^2 - ax - b = 0$, where $a, b \in \mathbb{Z}, b \neq 0$, are distinct $\alpha \neq \beta$. Then

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z},$$

$n = 1, 2, 3, \ldots$, is a divisibility sequence. Indeed, if r divides s then, setting $l := s/r \in \mathbb{N}$, we see that

$$\frac{u_s}{u_r} = \frac{\alpha^{rl} - \beta^{rl}}{\alpha^r - \beta^r} = \alpha^{r(l-1)} + \alpha^{r(l-2)}\beta^r + \cdots + \beta^{r(l-1)}$$

is a symmetric function in α, β. Hence $u_s/u_r \in \mathbb{Z}$, giving $u_r | u_s$. If $(x_n)_{n=1}^{\infty}$ is a sequence given by the linear recurrence $x_{n+1} = ax_n + bx_{n-1}$ then one can consider a corresponding divisibility sequence, by selecting $u_1 := 1$, $u_2 := a$. This sequence is the *Lucas sequence of the first kind.*

Definition 2.3. *A collection of residue classes*

$$r_i \pmod{m_i} := \{r_i + m_i k \mid k \in \mathbb{Z}\},$$

where $m_i \in \mathbb{N}$, $r_i \in \mathbb{Z}$, $0 \leqslant r_i < m_i$, *and* $i = 1, \dots, t$, *is called a covering system if every integer* $n \in \mathbb{Z}$ *belongs to at least one residue class* $r_i \pmod{m_i}$, *where* $1 \leqslant i \leqslant t$.

For example, $0 \pmod 2$, $1 \pmod 2$ is a covering system. A more interesting example, used in our proof, is this covering system:

$$0 \pmod 2,\ 0 \pmod 3,\ 3 \pmod 4,\ 5 \pmod 8,\ 5 \pmod{12},\ 1 \pmod{24}.$$

It would be of interest to extend Theorem 2.1 to linear recurrence sequences of order d, where $d \geqslant 3$. For which $(a_1, \dots, a_d) \in \mathbb{Z}^d$, where $a_d \neq 0$, one can choose d integers $x_1, \dots, x_d$ satisfying $\gcd(x_1, \dots, x_d) = 1$ such that the sequence

$$x_{n+d} = a_1 x_{n+d-1} + a_2 x_{n+d-2} + \dots + a_d x_n, \ \ n = 1, 2, 3, \dots,$$

contains only composite numbers, i.e., $|x_n|$ is a composite integer for each $n \geqslant 1$?

It seems likely that the complete answer to this question is out of reach. Firstly, for most linear recurrences of order d, there are no divisibility sequences satisfying them. See, e.g., Theorem IV in the paper of Hall [18] for one of the first results of this kind for $d = 3$:

There is no regular divisibility (linear recurrence) sequence whose characteristic polynomial is an irreducible (in the ring of rational polynomials) cubic whose last two coefficients are relatively prime. (Here, divisibility sequence is called *regular* if its first term equals 0.)

So, using our methods, one will not be able to deal with the cases of regular divisibility sequences, where, e.g., $a_i \in \{-1, 0, 1\}$ for each $i = 1, \dots, d$ and the characteristic polynomial of the linear recurrence is irreducible. Secondly, and more importantly, there are no methods that would allow us to show that the cases, where the characteristic polynomial

$$x^d - a_1 x^{d-1} - a_2 x^{d-2} - \dots - a_d$$

is $(x+1)^d$ or $(x-1)^d$, are exceptional. Already for $d = 3$ and, say, $(a_1, a_2, a_3) = (3, -3, 1)$ one gets a problem on prime values of a quadratic polynomial $\mathbb{Z} \mapsto \mathbb{Z}$ at nonnegative integer points which is completely out of reach.

Recently, the case $x_{n+3} = x_{n+2} + x_{n+1} + x_n, n = 1, 2, 3, \ldots$, has been treated successfully in [31].

Egyptian fractions and numbers expressible by some special linear form

Let t be a fixed positive integer. We consider the set of positive integers

$$E(t) := \{n \, : \, n = tM - d\},$$

where M is a positive multiple of the product and d is a positive divisor of the sum of two positive integers, namely,

$$ab|M \quad \text{and} \quad d|(a+b)$$

for some $a, b \in \mathbb{N}$. Evidently,

$$E(t') \subseteq E(t) \quad \text{whenever} \quad t|t'.$$

It is easy to see that

$$E(1) = E(2) = \mathbb{N}.$$

Indeed, suppose first that $t = 1$. Then, for each $n \in \mathbb{N}$ selecting $a = 2n+1$, $b = 1$, $M = ab = 2n+1$ and $d = (a+b)/2 = n+1$, we find that

$$n = 2n + 1 - (n+1) = M - d,$$

giving $E(1) = \mathbb{N}$. In case $t = 2$, for each $n \in \mathbb{N}$ we may choose $a = n+1$, $b = 1$, $M = ab = n+1$ and $d = a+b = n+2$. Then $2M - d = 2(n+1) - (n+2) = n$, so that $E(2) = \mathbb{N}$.

Apart form the cases $t = 1$ and 2 the situation with $t \geqslant 3$ is not clear. In this context, the sets $E(4)$ and $E(5)$ are of special interest, because an integer n belongs to the set $E(t)$ if and only if

$$n = tM - d = tuab - (a+b)/v$$

with some $a, b, u, v \in \mathbb{N}$. Therefore, $n \in E(t)$ yields the representation

$$\frac{t}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

with positive integers

$$x := uab, \quad y := uvna, \quad z := uvnb.$$

Thus, this leads us to the subject of Egyptian fractions (the sums of distinct unit fractions) and the related famous conjectures. If $n \in E(t)$ then the fraction t/n is expressible by the sum of three unit fractions (i.e., three inverted positive integers). In particular, if every prime number p belongs to the set $E(4)$ then the Erdős-Straus conjecture (asserting that for each integer $n \geqslant 2$ the fraction $4/n$ is expressible by the sum $1/x + 1/y + 1/z$ with $x, y, z \in \mathbb{N}$) is true, whereas if every prime number p belongs to $E(5)$ then the corresponding conjecture of Sierpiński (asserting that for each $n \geqslant 4$ the fraction $5/n$ is expressible by the sum $1/x + 1/y + 1/z$) is true [29]. In this context the most general Schinzel's conjecture asserts that the fraction t/n for each $n \geqslant n(t)$ is expressible by the sum $1/x+1/y+1/z$. This clearly holds for $t \leqslant 3$ but is open for each fixed $t \geqslant 4$. Conjecture 3.5 given below implies that there is an integer $C(t)$ such that each prime number $p > C(t)$ belongs to $E(t)$. This would imply Schinzel's conjecture as well.

Yamamoto [38], [39] and Mordell [25] observed that it is sufficient to prove the Erdős-Straus conjecture for those prime numbers p which modulo 840 are $1, 121, 169, 289, 361$, or 529. Vaughan [32] showed that the Erdős-Straus conjecture is true for almost all positive integers n. See also the list of references in section D11 of [17] for the literature concerning the conjectures of Erdős-Straus, Sierpiński and Schinzel on Egyptian fractions. More references on the Erdős-Straus (including recent ones) can be found in a paper of Elsholtz and Tao [12] on the average number of solutions of the equation $4/p = 1/x + 1/y + 1/z$ with prime numbers p. At the computational side the calculations of Swett `http://math.uindy.edu/swett/esc.htm` show that the Erdős-Straus conjecture holds for integers n up to 10^{14}.

We observe that

Theorem 3.1. *The set $E(4)$ does not contain perfect squares and the numbers* 288*,* 336*,* 4545*.*

Suppose $k^2 \in E(4)$, i.e., there exist $u, v, a, b \in \mathbb{N}$ such that

$$v(4uab - k^2) = a + b.$$

To show that $k^2 \notin E(4)$ we shall use the fact, which was proved in [28], that

Lemma 3.2. *The equation above has no solutions in positive integers u, v, a, b, k.*

Lemma 3.2 implies that $-d$ is a quadratic nonresidue modulo $4ab$ if $d|(a+b)$. Note that the set of divisors of $a+b$, when $a < b$ both run through the set $\{1, 2, \dots, n\}$, contains the set $\{1, 2, \dots, 2n-1\}$. Thus, by Lemma 3.2, we find that

Corollary 3.3. *For each positive integer n the $2n-1$ consecutive integers*

$$4n! - 2n + 1, 4n! - 2n + 2, \dots, 4n! - 1$$

are quadratic nonresidues modulo $4n!$.

Corollary 3.3 gives the example of at least $(2-\varepsilon)\log m/\log\log m$ consecutive quadratic nonresidues modulo $m = 4n!$. In this direction, the most interesting problem is to determine how many consecutive quadratic residues and consecutive quadratic nonresidues modulo m may occur for prime numbers m. See, e.g., [6], [16], where it is shown that we have at least $c_1 \log m \log\log\log m$ consecutive quadratic residues modulo m for infinitely many primes m, and [24], where the factor $\log\log\log m$ is replaced by $\log\log m$ under assumption of the generalized Riemann hypothesis.

A set of positive integers which is a subset of $\cup_{q=0}^{\infty} E(4q+3)$ was recently considered in [3]. For $M = ab$ and $d = a+b$, where a, b are positive integers and $b \equiv 3 \pmod 4$, put

$$E^*(t) := \{n \ : \ n = tab - a - b\}.$$

Evidently, $E^*(t) \subseteq E(t)$. In [3] it was shown that the set $E := \cup_{q=0}^{\infty} E^*(4q+3)$ does not contain perfect squares and that all prime numbers of the form $4s+1$ less than 10^{10} belong to E.

As we already observed, the sets $\mathbb{N}\backslash E(1)$ and $\mathbb{N}\backslash E(2)$ are empty. By Lemma 3.2 the equation $v(4uab - k^2) = a + b$ has no solutions in positive integers u, v, a, b, k. In particular, if t is a positive integer divisible by 4 and $s \in \mathbb{N}$ is such that $4s|t$ then the equation $vs(4(t/4s)uab - k^2) = a + b$ has no solutions in positive integers u, v, a, b, k. The latter is equivalent to the equation $v(tuab - sk^2) = a + b$. Consequently, we obtain that

Corollary 3.4. *The set $E(t)$, where $4|t$, does not contain the numbers of the form sk^2, where $s \in \mathbb{N}$ satisfies $4s|t$ and $k \in \mathbb{N}$.*

In particular, this implies that the set $\mathbb{N}\backslash E(t)$ is infinite when $4|t$. We conjecture that all other sets, namely, $\mathbb{N} \setminus E(t)$ with $t \in \mathbb{N}$ which is not a multiple of 4 are finite. More precisely, we conjecture that

CONJECTURE 3.5. *There exists an integer $C(t) \in \mathbb{N} \cup \{0\}$ such that the set $E(t)$ contains all integers greater than or equal to $C(t) + 1$ if 4 does not divide t and all integers greater than or equal to $C(t) + 1$ except for sk^2, where $4s|t$ and $k \in \mathbb{N}$, if $4|t$.*

We have $C(1) = C(2) = 0$. It is known that the total number of representations of t/n by the sum $1/x + 1/y + 1/z$ does not exceed $c(\varepsilon)(n/t)^{2/3}n^{\varepsilon}$, where $\varepsilon > 0$ (see [4]). We know that if $n \in E(t)$ then t/n is expressible by the sum of three unit fractions, so this bound also holds for the number of representations of n in the form $tM - d$. On the other hand, by the result of Vaughan [32], almost all positive integers are expressible by the sum of three unit fractions. It is easy to see that for each fixed integer $t \geqslant 3$ almost all positive integers belong to the set $E(t)$.

In fact, one can easily show a much stronger statement:

PROPOSITION 3.6. *For any integer $t \geqslant 3$ almost all positive integers can be written in the form $pa - 1$ with some prime number $p \equiv -1 \pmod{t}$ and some $a \in \mathbb{N}$.*

If $n \in \mathbb{N}$ can be written in this way then

$$n = pa - 1 = (p + 1)a - a - 1 = tM - d \in E(t)$$

with $b = 1$, $d = a + 1$ and $M = (p + 1)a/t$. By the above, it suffices to show that the density of positive integers n that have no prime divisors of the form $p \equiv -1 \pmod{t}$ is zero. This can be easily done by a standard sieve argument (see Section 3.1).

1. Integer parts of powers of rational numbers

Let $a > 1$ be a rational number. In this section we will consider composite numbers in the sequence

$$[a^n], n = 1, 2, \ldots,$$

where the brackets denote an integer part of the number (i.e. $[a^n]$ is the biggest number that does not exceed a^n). We are interested in a problem for which the cases $a = 3/2$ and $a = 4/3$ were successfully treated forty-five years ago by Forman and Shapiro [14], but no progress had been made for a long time. This at first glance simple problem can be stated as follows: prove that for every rational $a > 1$ the sequence of integer parts $[a^n]$ contains infinitely many composite numbers. (This problem is trivial for integer a.)

The nature of the methods applied allows us to obtain the results for some sequences of a more general kind. Together with any sequence $[a^n]$, $n = 1, 2, \ldots$, all sequences of the form $[\xi a^n]$, $n = 1, 2, \ldots$, where ξ is any real positive number, are covered by the statements below (note that now the problem is not trivial even for integer values of a). The sequences of shifted powers of rational numbers $[\xi a^n + \nu]$, $n = 1, 2, \ldots$, are also considered.

We begin with our main theorem. Set $\mathcal{P}(2) = \{2\}$, $\mathcal{P}(3) = \mathcal{P}(4) = \{2, 3\}$, $\mathcal{P}(6) = \mathcal{P}(4/3) = \{2, 3, 5\}$, $\mathcal{P}(3/2) = \{2, 5, 7, 11\}$, $\mathcal{P}(5/4) = \{2, 3, 7, 11, 13\}$.

Theorem 1.1. *Let $\xi > 0$ be a real number and let $a \in \{2, 3, 4, 6, 3/2, 4/3, 5/4\}$. Then the set $[\xi a^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by at least one number of the set $\mathcal{P}(a)$.*

In the above mentioned paper [14] Forman and Shapiro proved that the sets $[(3/2)^n]$ and $[(4/3)^n]$, $n \in \mathbb{N}$, contain infinitely many composite numbers. Their proof extends without change to $[\xi(3/2)^n]$ and $[\xi(4/3)^n]$ with arbitrary $\xi > 0$. However, we will give a proof for $a = 4/3$ once again, because (after a small preparation) we will be able to do this in just few lines in contrast to eight lemmas used in [14]. This will serve as a warm-up for the proof of a corresponding result for $a = 5/4$. The proof of Theorem 1.1 for $a = 3/2$ is given by combining our Lemma 1.7 with the main result of [14].

A valuable difference between our approach and that of [14] is that we are seeking a contradiction with Lemma 1.7 below which is obtained using fractional parts rather than a similar lemma for the integer parts of powers as in [14]. The main advantage in doing this is that we are able to describe some explicit (unavoidable) finite sets for possible divisors. (We show, however, that such unavoidable sets do not exist for some rational a; see the Proposition below.)

Note that the number $a = 5$ is missing in Theorem 1.1. The only reason for this is that, for $a = 5$, such universal explicit (unavoidable) set for divisors of the elements of the set $[\xi 5^n]$, $n \in \mathbb{N}$, cannot be given. In fact, it cannot be given for any number $a = 4k + 1$, where $k \in \mathbb{N}$.

Proposition 1.2. *Let a be a positive integer of the form $4k+1$, where $k \in \mathbb{N}$, and let $\mathcal{P}$ be an arbitrary finite set of prime numbers. Then there exists $\xi > 0$ such that every integer part $[\xi a^n]$, $n = 1, 2, \dots,$ is relatively prime with every prime number of the set $\mathcal{P}$.*

We prove Proposition 1.2 in Section 1.4. However, in the same section we prove that the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many composite numbers since a universal set of divisors does not work only for special values of ξ, which we are able to deal with separately. The fact is a direct consequence of the following theorem.

Theorem 1.3. *Let $\xi > 0$ be a real number. If $\xi \neq (4k+3)/(2 \cdot 5^r)$, where k, r are nonnegative integers, then the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by $2, 3$ or 5. If $\xi = (4k+3)/(2 \cdot 5^r)$, where $(4k+3, 5^r) = 1$, then the set $[\xi 5^n]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by $10k+7$.*

It remains unproved that the integer parts $[\xi a^n]$, $n = 1, 2, \dots,$ where ξ is an arbitrary positive number and $a \geqslant 7$ is an integer, are composite for infinitely many $n \in \mathbb{N}$. Also, Theorem 1.1 has not been extended to any rational noninteger number other than $3/2, 4/3, 5/4$ even for $\xi = 1$, although at first glance the case $a = 6/5$ may seem simpler than the case $a = 5/4$. However, by slightly changing the problem, we can include some new rational numbers.

Theorem 1.4. *Let $\xi > 0$ be a real number. Then each of the sets $[\xi(5/2)^n] - 1$ and $[\xi(6/5)^n] - 1$, where $n \in \mathbb{N}$, contains infinitely many elements divisible by at least one number of the set $\{2, 3, 5\}$.*

The proof for $[\xi(5/2)^n]-1$ presented in Section 1.6 can be applied without changes to all the sets of numbers the form $[\xi(5/2)^n]-1+30k, n \in \mathbb{N}$, where k is any fixed integer.

One can also consider the nearest integers to powers instead of integer parts. We define the nearest integer to z as $[z+1/2]$. Some new numbers can be obtained again.

Theorem 1.5. *Let $\xi > 0$ be a real number. Then*
(i) the set $[\xi 7^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many composite numbers,
(ii) the set $[\xi(5/3)^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by 2 or 3,
(iii) the set $[\xi(7/5)^n + 1/2]$, $n \in \mathbb{N}$, contains infinitely many elements divisible by at least one of the numbers $2, 3, 5, 11$.

Note that no definite divisors are indicated for the set $[\xi 7^n + 1/2]$, $n \in \mathbb{N}$. This case is different from all the other cases for the reason that it is not covered by Lemma 1.2 which holds only for non-integer rational numbers (as in the case $a=5$) and, in contrast to the case $a=5$, integer parts are used to finish the proof instead of fractional parts (which are instrumental in exluding most of the values of ξ in the proof of Theorem 1.3).

In Section 1.1 we define the sequences of operations which describe the behaviour of the sequences of integer parts, but which can also be viewed as infinite words, i.e. formal sequences of symbols belonging to some set, called an alphabet. We will study the patterns which could and could not occur in these words and the possible periodicity of these sequences of symbols, as well.

Proofs

1.1. **Preliminary considerations.**

Write $a = b/c$, where $b > c \geqslant 1$ are relatively prime integers. (Note that a is allowed to be an integer.) Setting $x_n = [\xi a^n + \nu]$ and $y_n = \{\xi a^n + \nu\}$, we obtain the equality $a(x_n + y_n - \nu) = x_{n+1} + y_{n+1} - \nu$. Consequently, $cx_{n+1} = bx_n + by_n - cy_{n+1} + (c-b)\nu$, so $s_n = by_n - cy_{n+1} + (c-b)\nu$ is an integer. It follows that

$$x_{n+1} = (bx_n + s_n)/c, \qquad y_{n+1} = (by_n + (c-b)\nu - s_n)/c.$$

Furthermore, since $0 \leqslant y_n, y_{n+1} < 1$, we deduce that $-c + (c-b)\nu < s_n < b + (c-b)\nu$. Let throughout $S(a, \nu)$ be the set of integers which belong to $(-c + (c-b)\nu, b + (c-b)\nu)$. Of course, $s_n \in S(a, \nu)$ can take only finitely many values $|S(a, \nu)|$.

Let $\mathcal{P}$ be a finite set of prime numbers . Assume that the numbers $x_n = [\xi a^n + \nu]$ are not divisible by a prime $p \in \mathcal{P}$ for every sufficiently large n. We know that $s_n \in S(a, \nu)$ for every $n \in \mathbb{N}$. If $p|bc$, then $p|b$ or $p|c$. Such p cannot divide s_n for n sufficiently large, since otherwise x_{n+1} or x_n is divisible by p. We will thus be able to exclude all numbers divisible by such primes from the set $S(a, \nu)$. Furthermore, the prime 2 lying in all sets $\mathcal{P}(a)$, by an easy parity argument, allows to exclude all odd numbers from $S(a, \nu)$ in case if b and c are both odd.

Throughout we will use the following notation. Instead of $s_1, s_2, s_3, \dots$ we will consider the sequence of operations denoted by $A, B, \dots$ corresponding to every $s \in S(a, \nu)$. If, say A corresponds to s, this means that A maps the integer x to the integer $(bx + s)/c$ (which corresponds to $[\xi a^n + \nu] \to [\xi a^{n+1} + \nu]$) and the fractional part y (of $\xi a^n + \nu$) to $(by - s + (c-b)\nu)/c$ (which is the fractional part of $\xi a^{n+1} + \nu$).

All this gives certain restrictions on the sequence of operations containing A's, B's etc. In particular, for every fixed prime p, every operation is a permutation of residues modulo p. (We will only use the primes $3, 5, 7, 11, 13$ in all our arguments below.) For instance, if say we seek for a contradiction modulo 7, then $2A1$ means that A maps the number of the form $7v + 2$, $v \in \mathbb{N}$, to the number of the form $7v' + 1$, $v' \in \mathbb{N}$, in the corresponding sequence of integer parts. In a more compact form we will write this in, say, the form $A = (12)(643|(5)$. This means that the only possible transformations modulo 7 are $1A2$, $2A1$, $6A4$, $4A3$ and $5A5$, whereas 3 maps to 0, i.e. the next integer part is divisible by 7, a contradiction. If, e.g., $B = (123)(4|(56)$, these two successive operations will 'multiply' as two permutations, namely, $AB = (413|(2)(56|$. Also, $AA = A^2 = (1)(2)(63|(4|(5)$. A pattern $AB \dots A$ is said to be impossible if $AB \dots A = (1|(2|(3|(4|(5|(6|$; this means that one of the corresponding integer parts, but not necessarily the last one, is divisible by 7. Because of this notation, it is convenient to write the residues 10 modulo 11 and 10,11,12 modulo 13 as a single digit numbers. Throughout we will use the notation $10 = \alpha, 11 = \beta$ and $12 = \gamma$. Note that A^∞ means the periodic sequence $AAAAA\dots$. (Similarly, $(AB)^\infty$ means $ABABAB\dots$.)

1.2. **Two lemmas: the periodicity of the sequences of operations.**

Lemma 1.6. *Suppose that $\xi > 0$ and ν are real numbers. If $a > 1$ is a rational noninteger number, then the sequence $\{\xi a^n + \nu\}$, $n = 1, 2, \dots,$ is not periodic.*

Proof of Lemma 1.6: Indeed, if the the sequence is periodic, then for infinitely many $m \in \mathbb{N}$ we have the equality $\{\xi a^n + \nu\} = \{\xi a^{n+m} + \nu\}$, where n is fixed. This implies that $\xi(a^{n+m} - a^n) = \xi a^n(a^m - 1)$ is an integer. This can only happen if ξ is a rational number. Writing $a = b/c$, where $b > c > 1$ are relatively prime integers, and multiplying the above number by c^n and by the denominator of ξ, we obtain that there is a fixed positive integer g such that $g(b^m - c^m)/c^m$ is an integer. For m sufficiently large, this can only happen if $b^m - c^m$ is divisible by c, which is impossible. This proves the lemma. □

Lemma 1.7. *Suppose that $a > 1$ is a rational noninteger number. Then the sequence $s_1, s_2, s_3, \dots$ is not periodic.*

Proof of Lemma 1.7: Assume it is periodic, of period ℓ. Then the sequence $((c-b)\nu - s_n)/c$, $n = 1, 2, \dots,$ is periodic too. So there is a positive integer n, and, for every $j = 0, 1, \dots, \ell-1$, there are two real numbers $\zeta = \zeta(j) > 1$ and $\omega = \omega(j)$ such that $y_{n+j+t\ell} = \zeta y_{n+j+(t-1)\ell} + \omega$ for every $t \in \mathbb{N}$. Fix j. Each fractional part in the subsequence $y_{n+j+t\ell}$, $t = 1, 2, \dots,$ is obtained from the preceding one by the formula $y \to \zeta y + \omega$. For $z = y + \omega/(\zeta - 1)$ this transformation can be written as $z \to \zeta z$. We claim that $y_{n+j} = -\omega/(\zeta - 1)$. Indeed, if $y_{n+j} > -\omega/(\zeta - 1)$ then $y_{n+j+t\ell} + \omega/(\zeta - 1) \to \infty$ as $t \to \infty$. This is impossible, because every fractional part is bounded above by 1. Similarly, if $y_{n+j} < -\omega/(\zeta - 1)$ then $y_{n+j+t\ell} + \omega/(\zeta - 1) \to -\infty$ as $t \to \infty$, which is also impossible. By the recurrent formula, it follows that $y_{n+j+t\ell} = -\omega/(\zeta - 1) = -\omega(j)/(\zeta(j) - 1)$ for every $t \in \mathbb{N}$. The same is true for every j in the range $0 \leqslant j \leqslant \ell - 1$. Hence the sequence

$y_n, y_{n+1}, y_{n+2}, \dots$ is purely periodic with period at most ℓ. This plainly implies that $y_1, y_2, y_3, \dots$ is periodic, contrary to Lemma 1. $\square$

The key difference between Lemma 1.7 and a respective result in [14] is that we claim that the sequence is not periodic without assumption that the sequence of integer parts contains only finitely many composite numbers. Note that the sequence can be periodic for integer a. For instance, we can take $\xi = 1/2$ and $a = 5$. Then $s_1 = s_2 = s_3 = \dots = 2$.

Hence, we obtain an important conclusion by Lemma 1.7 without making the above mentioned assumption: periodic sequences of operations (as defined in Section 1.1) for noninteger a cannot occur.

1.3. **Proof of Theorem 1.1: easy cases.**

Here we will prove Theorem 1.1 in all cases except the case $a = 5/4$.

For $a = 2$, the binary expansion of the number ξ contains infinitely many zeros. So the set $[\xi 2^n]$, $n \in \mathbb{N}$, contains infinitely many even numbers.

For $a = 3$, we have $S(3,0) = \{0,1,2\}$. Thus $x_{n+1} = 3x_n + s_n$ with $s_n \in \{0,1,2\}$. Since 3 and 1 are both odd, the sequence x_n, $n = 1, 2, \dots$, contains infinitely many even numbers or infinitely many numbers divisible by 3, unless $s_n = 2$ for all large n. Assume that it is so. But then $y_{n+1} = 3y_n - 2$ for all sufficiently large n. This implies that $y_n \to -\infty$ as $n \to \infty$, a contradiction.

For $a = 4$, $S(4,0) = \{0,1,2,3\}$. We either have infinitely many even integer parts or there are just two possibilities $x_{n+1} = 4x_n + 1$ and $x_{n+1} = 4x_n + 3$ starting with certain n. Assume that m is so large that $x_m, x_{m+1}, \dots$ are not divisible by 3. Then, by a simple argument modulo 3, we see that the possibility $x_{n+1} = 4x_n + 1$ cannot occur more than once. It follows that $x_{n+1} = 4x_n + 3$ for all sufficiently large n. Then $y_{n+1} = 4y_n - 3$ for all large n, so $y_n \to -\infty$ as $n \to \infty$, a contradiction.

For $a = 6$, $S(6,0) = \{0,1,2,3,4,5\}$. Now, either we have infinitely many integer parts divisible by 2 or 3 or there are just two possibilities $x_{n+1} = 6x_n + 1$ and $x_{n+1} = 6x_n + 5$ starting with certain n. Assume that m is so large that $x_m, x_{m+1}, \dots$ are not divisible by 5. Then, by a simple argument modulo 5, we see that the possibility $x_{n+1} = 6x_n + 1$ cannot occur more than three times. It follows that $x_{n+1} = 6x_n + 5$ for all sufficiently large n. Then $y_{n+1} = 6y_n - 5$ for all large n, so $y_n \to -\infty$ as $n \to \infty$, a contradiction.

For $a = 4/3$, $S(4/3, 0) = \{-2, -1, 0, 1, 2, 3\}$. Again, either there are infinitely many integer parts divisible by 2 or 3 or only two possibilities can occur $3x_{n+1} = 4x_n - 1$ (type A) and $3x_{n+1} = 4x_n + 1$ (type B) starting with certain n. Assume that there are only finitely many integer parts divisible by 5. Of course, $A = (1)(324|$ and $B = (231|(4)$ modulo 5. Since the sequence of A's and B's is not periodic, the pattern AB occurs infinitely often. More precisely, since $AB = (1|(3)(24|$, this pattern can only be $3AB3$ or $2AB4$. The second case is impossible, because we then must have B^∞, which is periodic, contrary to Lemma 1.7. Similarly, $3AB^21$ leads to A^∞, a contradiction again. So we can only have $3ABA2$. In order to avoid 1 and 4 in the sequence of residues modulo 5, we must have $(AB)^\infty$ which is also periodic, a contradiction.

For $a = 3/2$, $S(3/2) = \{-1, 0, 1, 2\}$. Now, either there are infinitely many even integer parts or there are two possibilities $2x_{n+1} = 3x_n - 1$ (type A) and $2x_{n+1} = 3x_n + 1$ (type B) starting with certain n. The arguments modulo $5, 7, 11$ of Forman and Shapiro [14] show however that this sequence must be periodic, unless there are infinitely many integer parts divisible by $5, 7$ or 11. This proves the result, by Lemma 1.7. The fact that they only consider the case $\xi = 1$ is not essential. We will not repeat their argument, although it can also be made much shorter than in [14].

1.4. The case $a = 5/4$.

Consider the case $a = 5/4$. Then $S(5/4, 0) = \{-3, -2, -1, 0, 1, 2, 3, 4\}$. At the expense of the prime 2, we can exclude $-2, 0, 2, 4$. The four remaining cases correspond to the recurrences $4x_{n+1} = 5x_n + s_n$ and $y_{n+1} = (5y_n - s_n)/4$. They are $s_n = -1$ (type A), $s_n = 3$ (type B), $s_n = 1$ (type C) and $s_n = -3$ (type D). Note that the operation A can only occur if $y_n \in [0, 3/5)$. On applying it, the fractional part y_{n+1} will be in the interval $[1/4, 1)$. So A acts on fractional parts as $[0, 3/5) \to [1/4, 1)$. Similarly, $B:\ [3/5, 1) \to [0, 1/2)$, $C:\ [1/5, 1) \to [0, 1)$ and

$D: \ [0,1/5) \to [3/4,1)$. We will write this in the form as below, where x, y refer to integer and fractional parts, respectively:

$$\begin{aligned}
&A: \ x \to (5x-1)/4, \ \ y \to (5y+1)/4, \ \ [0,3/5) \to [1/4,1);\\
&B: \ x \to (5x+3)/4, \ \ y \to (5y-3)/4, \ \ [3/5,1) \to [0,1/2);\\
&C: \ \ \ x \to (5x+1)/4, \ \ y \to (5y-1)/4, \ \ \ [1/5,1) \to [0,1);\\
&D: \ x \to (5x-3)/4, \ \ y \to (5y+3)/4, \ \ [0,1/5) \to [3/4,1).
\end{aligned}$$

In order to avoid confusion we must say that the composition of operations in the proof of Lemma 1.8 below is very unusual for a reader with an algebraic background. The composition of operations, say, BC is read from left to right giving $BC: y \to (25y-19)/16$. This of course contradicts to the usual rule of composition from right to left. However, in all our arguments following Lemma 1.8 we always use A, B, C and D, firstly, as elements of an infinite sequence and, secondly, as a kind of permutations. In both cases, it is much more convenient to write (and read), say, BC from left to right.

Lemma 1.8. *The patterns AD, DA, D^2, B^2, BC^kB, where $k \in \mathbb{N}$, BC^4, $(DB)^2D$, $BDCBDC^uBD$, $u \in \{0,1,2,3\}$, $(BD)^3$, $(DB)^2CD$, $(DB)^2C^2DBC^vD$, $v \in \{0,1\}$, cannot occur.*

Proof of Lemma 1.8: The result is evident for AD, DA, $D^2 = DD$ and $B^2 = BB$ from fractional parts. Also, $BC: \ y \to (25y-19)/16$ which is smaller than $3/8$. Since C maps every y to a smaller number, we deduce that BC^k maps y to a number smaller than $3/8$ for every $k \in \mathbb{N}$. Hence BC^kB cannot occur. Similarly, $C^4: \ y \to (625y-369)/256$, so C^4 can only be applied to $y \geqslant 369/625 > 1/2$. Hence BC^4 cannot occur. Also, $(DB)^2: \ y \to (625y+123)/256$ which is greater than $1/5$, so $(DB)^2D$ cannot occur.

Since $BD: \ y \to (25y-3)/16$, it can only be applied if $3/5 \leqslant y < 19/25$. But $BDCBD: y \to (3125y-967)/1024$ which is greater than or equal to $227/256 = 0.88671\ldots$. On applying C at most three times to this number we will get a number greater than $0.77 > 0.76 = 19/25$, so the pattern $BDCBDC^uBD$, where $0 \leqslant u \leqslant 3$, cannot occur. Note that $(BD)^2: \ y \to (625y-123)/256$. For $y \geqslant 3/5$, this is greater than or equal to $63/64 > 19/25$, so $(BD)^2$ cannot be followed by one more BD, i. e. $(BD)^3$ cannot occur.

Similarly, $(DB)^2C : y \to (3125y + 359)/1024$ which is greater than $0.35 > 1/5$, so $(DB)^2CD$ is impossible. Furthermore, this implies that $(DB)^2C^2$ maps every y to a number $y' > 3/16$. But DB maps y' to $(25y' + 3)/16$ which is greater than 0.48, since $y' > 3/16$. Thus $(DB)^2C^2DBC^v$, $v \in \{0, 1\}$, is greater than 0.35 and cannot be followed by D. □

Lemma 1.9. *Suppose that the set of integer parts contains only finitely many elements divisible by* 2 *and* 3. *Then there are only finitely many* A*'s. Furthermore, starting from some place, the sequence of operations is either* $BDC^{k_1}BDC^{k_2}\dots$ *or* $DBC^{k_1}DBC^{k_2}\dots$, *where* $k_1, k_2, \dots \geqslant 0$.

Proof of Lemma 1.9: Note first that the patterns AC, CA, ABA, $ABDC$, CBC, CDC cannot occur. Indeed, modulo 3 we have $A = (1)(2|$, $B = (12)$, $C = (1|(2)$, $D = (12)$. This implies the above claim. We will frequently use it without referring to it. Sometimes we will combine it with Lemma 3 which gives other restrictions on patterns.

Assume that there are infinitely many A's. Then, since the sequence is not periodic and since the patterns AC, CA, AD and DA cannot occur, every pattern A^k, $k \in \mathbb{N}$, can only occur between two B's. Similarly, since BC^kB is impossible, every pattern C^k can only occur between B and D, giving BC^kD, D and B, giving DC^kB, or D and D, giving DC^kD. Fix a fragment BA^kB. Let's forget for a moment about A's and C's and consider the remaining subsequence of B's and D's (to the right of the fixed fragment BA^kB which can only be $2BA^kB2$). Next operation in this subsequence should be D, because neither B^2 nor ABA can occur, so the next operation cannot be B. Furthermore, this D should be of the form $2D1$. Now, the next operation in the subsequence should be B. Indeed, assume that it is D. Since the pattern D^2 is impossible, these two D's should be separated by C^k, $k \in \mathbb{N}$. Since CDC cannot occur, we must have the pattern $ABDC^kD$, but its subpattern $ABDC$ cannot occur, a contradiction. Furthermore, this B must be of the form $1B2$. Since BC^kB, where $k \geqslant 0$, is impossible, after D, B it should be $2D1$ again, etc. We thus deduce that the subsequence is $D, B, D, B, D, B, \dots$. These can only be separated by C^k, so there are no more A's, as claimed.

If there are only finitely many C's in the original sequence, we have $(DB)^\infty$, a contradiction. Assume that the first occurrence of C's is between D and B, i.

e. there is a pattern DC^kB with $k > 0$. Modulo 3 we must have $1DC^kB1$. This cannot be followed by C, so it must be followed by D and gives $1DC^kBD2$. This is clearly followed by $C^{k_1}B$, where $k_1 \geqslant 0$, and gives $1DC^kBDC^{k_1}B1$. Further, we must have D, then $C^{k_2}BD$, etc. Hence the sequence from certain place is $BDC^{k_1}BDC^{k_2}\dots$, $k_1, k_2, \dots \geqslant 0$. The argument when the first occurrence of C's is between B and D is precisely the same and gives the sequence $DBC^{k_1}DBC^{k_2}\dots$, where $k_1, k_2, \dots \geqslant 0$. $\square$

Lemma 1.10. *Suppose that the set of integer parts contains only finitely many elements divisible by* $2, 3, 7, 11$ *and* 13. *Then the sequence* $BDC^{k_1}BDC^{k_2}\dots$ *is impossible.*

Proof of Lemma 1.10: Modulo 7 we have $B = (63125|(4)$, $C = (21534|(6)$, $D = (14652|(3)$. Hence $BD = (1|(2)(346)(5|$.

We claim that there are infinitely many patterns $4BD6$. There are four possible cases $3BD4$, $6BD3$, $2BD2$ and $4BD6$. In the first case, we cannot have C next, so we must have $4BD6$ straight after $3BD4$. In the second case, $6BD3$, we have next either $3BD4$ (i.e. we are back to the first case), or $3C4$ which can only be followed by $4BD6$. Finally, in the third case, $2BD2$, since the sequence is not $(BD)^\infty$, we must have some C's later on. So next there is $2(BD)^u 2C^v$, where $u \geqslant 0$ and $v \in \{1, 2, 3, 4\}$, which ends with $1, 5, 3, 4$, respectively, and then BD again. But BD cannot begin with 1 or 5. So we either immediately get $4BD6$ or we are back to the case $3BD4$, which is already considered. This proves our claim.

Each pattern $4BD6$ is either followed immediately by $6BD3$ or it is followed by $6C^kBD3$. We thus have $4BDC^kBD3$, where $k \geqslant 0$. If next we would have $3BD4$ then this should be followed again by BD. But by Lemma 1.8 $(BD)^3$ cannot occur, so BD cannot be repeated more than twice, a contradiction. Thus we have the pattern $4BDC^kBDC4$ which must be followed by $4BD6$, etc. Hence our sequence is formed by the patterns $BDCBD$ which are separated by C^{u_i}, where $u_i \geqslant 0$. So the sequence is

$$BDCBDC^{u_1}BDCBDC^{u_2}\dots.$$

Furthermore, Lemma 1.8 implies that each u_i is greater than or equal to 4.

The number 10 modulo 11 occurs as one of the residues. Recall that throughout 10 will be denoted by α. We have that the operations $B: x \to 4x - 2$, $C: x \to 4x + 3$ and $D: x \to 4x + 2$ modulo 11, hence $B = (9126|(3\alpha574)(8)$, $C = (17965)(3482|(\alpha)$, $D = (16478)(2\alpha95|(3)$. Consequently, $BDCBDC^4 = (25|(79|(81|(3|(4|(6|(\alpha|$. Thus $BDCBDC^{u_i}$ can only end with one of the numbers $1, 7, 9, 6, 5$. However the next block $BDCBDC^{u_{i+1}}$ can only begin with 7. Thus each of the blocks $BDCBDC^{u_i}$ is of the form $7BDCBDC^{u_i}7$. This only happens if each u_i is of the form $8 + 5v_i$, where v_i is a nonnegative integer. Furthermore, there exist positive v_i, for otherwise we have $(BDCBDC^8)^\infty$. Hence $u_i \geqslant 13$ for some i.

We have no other choice modulo 13, but to continue with our curious notation $10 = \alpha$, $11 = \beta$ and $12 = \gamma$. Now, $B: x \to -2x + 4$, $C: x \to -2x + 10$, $D: x \to -2x + 9$. Hence $B = (49\gamma6573\beta812|(\alpha)$, $C = (\alpha3426\beta18795|(\gamma)$, $D = (941786\alpha25\gamma\beta|(3)$. Thus $BDCBD = (1|(2|(953|(8\beta6\alpha\gamma|(74|$. It follows that the block $BDCBDC^{u_i}$ with $u_i \geqslant 13$ can only be of the form $\alpha BDCBDC^{u_i}\gamma$, because $\gamma C^{u_i}\gamma$ is the only possibility if $u_i \geqslant 11$. However, the next block $BDCBDC^{u_{i+1}}$ cannot begin with γ, since the pattern $BDCBD$ cannot begin with γ, a contradiction. □

Lemma 1.11. *Suppose that the set of integer parts contains only finitely many elements divisible by* $2, 3, 7, 11$ *and* 13. *Then the sequence* $DBC^{k_1}DBC^{k_2}\ldots$ *is impossible.*

Proof of Lemma 1.11: We will first argue modulo 7 and claim that there are infinitely many patterns $3DB1$. Since $DB = (143)(5)(2|(6|$, other possibilities are $4DB3$, $1DB4$ and $5DB5$. Recall that $C = (21534|(6)$. The first possibility, $4DB3$, leads to $3DB1$ next or we must have $4DBC4$. So the only alternative to $4DB3$ to occur is $(DBC)^\infty$, a contradiction with Lemma 1.7. The pattern $1DB4$ leads to $4DB3$, so to the case which we just considered. After repeating $5DB5$ at most twice (Lemma 1.8), we should apply either C or C^2 and then DB again (modulo 7). This gives, respectively, $3DB1$ (as required) or $4DB3$ (which is the first possibility). The claim is proved.

If $3DB1$ is followed by DB again, we cannot have further DB, by Lemma 1.8, so it must be followed by C. But $(DB)^2C$ cannot begin with 3, a contradiction.

Hence $3DB1$ must be followed by C, i. e. we have infinitely many patterns $3DBC5$. What can happen between two successive $3DBC5$? Assume that the next operation after the first $3DBC5$ is C. Then either $3DBC^2 3$ is followed by $3DBC5$ or we have $3DBC^3 DB3$ and then further $(CDB)^k$ until the second $3DBC5$. Both cases can be written as $DBC^2(CDB)^u$, where $u \geqslant 0$. Alternatively, assume that after the first $3DBC5$ is DB. The whole pattern is $3DBCDB5$. We can have at most one DB until the next C, so the pattern can be written as $3DBC(DB)^v C3$, where $v \in \{1, 2\}$. We will show that the case $v = 2$ is impossible. Indeed, by Lemma 1.8, $(DB)^2 C$ should be followed by C which gives $3DBC(DB)^2 C^2 4$. This must be followed by $4DB3$ (modulo 7), so we get $(DB)^2 C^2 DB3$. Further, by Lemma 1.8, this cannot be followed by DB or by CDB. So it must be followed by C^2, which is impossible modulo 7. Hence $v = 1$, i. e. we have $3(DBC)^2 3$. The second $3DBC5$ begins either immediately or after inserting $(CDB)^k$, $k \in \mathbb{N}$. We conclude that the whole sequence consists of just two type blocks $DBC^2(CDB)^u$ and $(DBC)^2(CDB)^k$, where $k, u \geqslant 0$.

We now show that k and u can only take two values 0 and 1. Set $E = (DBC)^2$, $F = (DBC)^2(CDB)^k$, $G = DBC^2$, $H = DBC^2(CDB)^u$, where $k, u \in \mathbb{N}$. Note that the same letter F (and H) can denote different patterns. Modulo 11, we have $E = (371|(68|(\alpha 2|(9)(4|(5|$, $G = (427|(3\alpha 968|(1|(5|$, $CDB = (\alpha 185|(9342|(7)(6|$. (Here, we use the expressions for B, C, D from Lemma 1.10.) Assume that there is F with $k \geqslant 2$. By Lemma 1.8, $(DB)^2 CD$ is impossible, so F cannot be followed by another F (which can be different from the first F) or E. Thus it must be followed by G or H. Note that F with $k \geqslant 2$ can end up only with the residues $7, 5, 4, 2$. So FH can end up only with 7. FG can end up only with 2 or 7. In case it ends up with 2, FG must be followed by G or H which ends by 7. With 7 can only begin E or F; this ends with $1, 8$ or 5. But neither of E, F, G, H begins with $1, 8$ or 5, a contradiction. Similarly, assume that there is an H with $u \geqslant 2$. By Lemma 1.8, the patterns HE and HF cannot occur. H with $u \geqslant 2$ can end with $7, 8, 5, 4, 2$. This shows that HH, where both H can be different, can only end with 7, whereas HG can end with 2 or 7. In case it is 2, HG should be followed by G or H. This ends up with 7 and we get a contradiction as above. Hence $k = u = 1$ and F, H are uniquely determined. Thus the sequence can contain only four possible patterns $E = (DBC)^2$, $F = (DBC)^2CDB$, $G = DBC^2$ and $H = DBC^2CDB = DBC^3DB$.

Our next claim is that only the patterns of the form GH and G^2E^kF, where $k \geqslant 0$, can occur. We will still argue modulo 11. Recall that $E = (371|(68|(\alpha 2|(9)(4|(5|$, $G = (427|(3\alpha 968|(1|(5|$, $F = ECDB = (9378|(65|(1|(2|(4|(\alpha|$, and $H = GCDB = (27|(4|(\alpha 31|(9|(65|(8|$. None of the operations E, F, G, H begins with $1, 5, 8$, so they cannot end with $1, 5, 8$. With 7 can begin only E and F, but they end with 1 and 8, respectively. This is impossible, so no operation can begin or end with $1, 5, 7, 8$. All remaining possibilities are $\alpha E2$, $9E9$, $4G2$, $3G\alpha$, $\alpha G9$, $9G6$, $9F3$, $\alpha H3$. None of these begins with 2 or 6, so $\alpha E2$, $4G2$, $9G6$ cannot occur. Remaining are $9E9$, $3G\alpha$, $\alpha G9$, $9F3$, $\alpha H3$. It is easily seen that F and H must be followed by $3G\alpha$, so we have infinitely many $3G\alpha$, unless the sequence is E^∞. What can happen between two consecutive $3G\alpha$'s? If $3G\alpha$ is followed by $\alpha H3$, we immediately get the fragment GH, because the next $3G\alpha$ should follow. Otherwise, we have $3G^29$. If the next is $9F3$, we have $3G^2F3$ and the fragment is finished. The alternative is that we have several E's (which are all of the form $9E9$ inserted between G^2 and F). So another possible fragment is G^2E^kF, where $k \geqslant 0$.

We now derived that the sequence contains just two possible fragments GH and G^2E^kF. A contradiction will be obtained modulo 13. By a simple computation using the expressions for A, B, C, D from the previous lemma, we have modulo 13

$$G = DBC^2 = (125)(7)(64\beta|(38|(\gamma 9|(\alpha|,$$

$$H = DBC^3DB = (\gamma 679|(431\alpha|(5)(2|(8|(\beta|,$$

$$E = (DBC)^2 = (16)(34)(\gamma 8|(25|(9\beta|(7|(\alpha|,$$

$$F = (DBC)^2CDB = (937|(\gamma 1|(65|(42|(8|(\alpha|(\beta|.$$

Clearly, $G^2 = (152)(7)(6\beta|(3|(4|(8|(9|(\alpha|(\beta|(\gamma|$. In case if the sequence is not $(GH)^\infty$, we must have infinitely many fragments of the form G^2E^kF (with may be different $k \geqslant 0$). But G^2 can end only with $1, 2, 5, 7, \beta$, so G^2E^k can end with $1, 2, 5, 7, \beta, 6$. Among these numbers, F can only begin with 6 thus giving 5 at the end of each fragment G^2E^kF. If we have at least one fragment GH after certain G^2E^kF, then it must be $5GH\alpha$. However G cannot begin with α, a contradiction. So we only have the fragments of the form G^2E^kF with may be different k, but each ending (and so beginning) with 5. So we have $5G^22$. This cannot be followed neither by F nor by E^2, so it must be followed by E and then by F which is impossible modulo 13, a contradiction. This completes the proof of Lemma 6 □

By Lemma 1.9 there are no other possibilities for the sequence of operations under the conditions of Theorem 1.1 except the two eliminated by Lemma 1.10 and Lemma 1.11. This implies that Theorem 1.1 is correct for $a = 5/4$, as well as in all other cases explored in Section 1.3.

1.5. **The case $a = 5$ and Proposition 1.2.**

Proof of Proposition 1.2: Let P be the product of all odd primes of $\mathcal{P}$, and let $\delta = 1$ if P is of the form $4v + 3$, $v \geqslant 0$, and $\delta = 3$ if P is of the form $4v + 1$, $v \geqslant 0$. Put $\xi = \delta P/2$. Then $[\xi a^n] = (\delta P a^n - 1)/2$ is odd, so there are no numbers among integer parts divisible by 2. Also, if p is an odd prime which belongs to $\mathcal{P}$, then $(\delta P a^n - 1)/2$ is not divisible by p. □

Proof of Theorem 1.3: We have $x_{n+1} = 5x_n + s_n$ with $s_n \in S(5, 0) = \{0, 1, 2, 3, 4\}$. Assume that the sequence of integer parts contains only finitely many elements divisible by 2 and 5. Then, starting with some n, there are two possibilities $x_{n+1} = 5x_n + 2$ (type A) and $x_{n+1} = 5x_n + 4$ (type B). Suppose that there are also only finitely many elements divisible by 3. But $A = (1)(2|$ and $B = (1|(2)$ modulo 3, so the patterns AB and BA cannot occur. Thus we have either A^∞ or B^∞. In the second case, $y_{n+1} = 5y_n - 4$, hence $y_n \to -\infty$ as $n \to \infty$, a contradiction. So we must have A^∞, i. e. $x_{n+1} = 5x_n + 2$ and $y_{n+1} = 5y_n - 2$ for all sufficiently large n. In case if there is no n for which $y_n = 1/2$, we obtain a simple contradiction using fractional parts as in Lemma 1.7 and getting $y_n \to \infty$ or $y_n \to -\infty$ as $n \to \infty$. So $y_u = 1/2$ for some $u \in \mathbb{N}$. Setting $q = x_u$, we deduce that $\xi 5^u = q + 1/2$. Hence either we have infinitely many integer parts $[\xi 5^n]$ divisible by at least one number of the set $\{2, 3, 5\}$ or $\xi = (q + 1/2)5^{-u}$.

Let us choose the smallest nonnegative integers t and r for which we can write $\xi = (2q + 1)/(2 \cdot 5^u) = (2t + 1)/(2 \cdot 5^r)$. Then

$$x_{n+r} = [(t + 1/2)5^n] = t5^n + (5^n - 1)/2.$$

If t is even, then the numbers $t5^n + (5^n - 1)/2$, $n = 1, 2, 3, \ldots$, are all even. Hence the sequence $[\xi 5^n]$, $n = 1, 2, \ldots$, contains infinitely many even numbers, but this is already covered by the previous case, because $2 \in \{2, 3, 5\}$. So assume without loss of generality that t is odd: $t = 2k+1$, where $k \geqslant 0$. Then $\xi = (4k+3)/(2 \cdot 5^r)$, where $(4k + 3, 5^r) = 1$.

We need to show that the sequence of integer parts $(2k + 1)5^n + (5^n - 1)/2$, $n = 0, 1, 2, \ldots$, contains infinitely many elements divisible by $10k + 7$. Let us take n of the form $1 + \varphi(10k + 7)\ell$, where φ is Euler's function and $\ell \in \mathbb{N}$. Then

$$(2k + 1)5^n + (5^n - 1)/2 = (10k + 7)5^{\varphi(10k+7)\ell} + (5^{\varphi(10k+7)\ell} - 1)/2$$

is divisible by $10k+7$, by Euler's theorem, because $(5, 10k+7) = 1$. This completes the proof of Theorem 1.3. □

1.6. **Composite numbers in the sequences of shifted integer parts.**

Proof of Theorem 1.4: For $x_n = [\xi(5/2)^n - 1]$, $S(5/2, -1) = \{2, 3, 4, 5, 6, 7\}$. So we either have infinitely many shifted integer parts x_n divisible by 2 or 5 or two types of linear recurrences $2x_{n+1} = 5x_n + 3$ (type A) and $2x_{n+1} = 5x_n + 7$ (type B). Modulo 3, we have $A = (1)(2)$ and $B = (21|$. Hence, if only finitely many elements are divisible by 3, we cannot have more than one operation B which must be followed by A^∞, a contradiction with Lemma 2. (Note that the same proof applies without change to every set of the form $[\xi(5/2)^n] - 1 + 30k$, where k is a fixed integer and where n runs over every positive integer.)

Similarly, for $x_n = [\xi(6/5)^n - 1]$, $S(6/5, -1) = \{-3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$. All numbers in this set, except for -1 and 1, are divisible by $2, 3$ or 5. This, assuming that there are only finitely many shifted integer parts divisible by $2, 3, 5$, leaves just two possibilities. The corresponding formulas for fractional parts are $y_{n+1} = (6y_n + 2)/5$ and $y_{n+1} = 6y_n/5$. For n sufficiently large, $y_n > 0$, since we must have at least once the first operation. (Otherwise this contradicts to Lemma 2.) But, as in both cases $y_{n+1} \geqslant 6y_n/5$, we deduce that $y_n \to \infty$, a contradiction. □

Proof of Theorem 1.5: For 7, we have $S(7, 1/2) = \{-3, -2, -1, 0, 1, 2, 3\}$. Assume that we have only finitely many shifted integer parts x_n divisible by 2 and 7. Then, starting with certain n, we must have $x_{n+1} = 7x_n - 2$ (operation A) or $x_{n+1} = 7x_n + 2$ (operation B). Modulo 3 we have $A = (12|$ and $B = (21|$, so either there are infinitely many integer parts divisible by 3 or, starting with some place, we have $(AB)^\infty$. (There is no contradiction with Lemma 1.7, because for $a = 7$ it cannot be applied.) However, this means that there is an infinite subsequence of primes defined by the recurrent formula $x_{n+2} = 7(7x_n - 2) + 2 = 49x_n - 12$. Take one of these $x_n = p > 7$. Take q such that $4q + 1$ is divisible by p. Then, since $-12 \equiv 48q \pmod{p}$, we get $x_{m+2} + q \equiv 49(x_m + q) \pmod{p}$ for every $m = n, n+2, n+4, \ldots$. Choosing $e \in \mathbb{N}$ such that $p|(49^e - 1)$ and multiplying the first e congruences we get $x_{n+2e} + q \equiv (x_n + q) \pmod{p}$, hence $x_{n+2e} - x_n = x_{n+2e} - p$ is divisible by p. So $x_{n+2e} > p$ is divisible by p and thus cannot be prime, a contradiction. This proves part (i).

For 5/3, we have $S(5/3, 1/2) = \{-3, -2, -1, 0, 1, 2, 3\}$. Assume that there are only finitely many shifted integer parts divisible by 2 and 3. This leaves us two options -2 and 2 with two respective operations for fractional parts $A:\ y \to (5y+1)/3$ (which maps $[0, 2/5)$ to $[1/3, 1)$) and $B:\ y \to (5y-3)/3$ (which maps $[3/5, 1)$ to $[0, 2/3)$). If the sequence is not A^∞, B^∞ or $(AB)^\infty$ ($(BA)^\infty$ is the same), then we must have either A^2 or B^2. Since $A^2:\ y \to (25y+8)/9$ which is greater than or equal to 8/9, A^2 must be followed by B^2. Similarly, $B^2:\ y \to (25y-24)/9$ which is smaller than 1/9, so B^2 should be followed by A^2. We thus have $(A^2B^2)^\infty$, a contradiction with Lemma 1.7, which completes the proof of (ii).

Finally, $S(7/5, 1/2) = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. At the expense of prime numbers $2, 5$ we can exclude all numbers from $S(7/5, 1/2)$ except for -4, -2, 2, 4. The four remaining possibilities are

$$A:\ \ x \to (7x-4)/5,\ \ y \to (7y+3)/5,\ \ [0, 2/7) \to [3/5, 1);$$

$$B:\ \ x \to (7x-2)/5,\ \ y \to (7y+1)/5,\ \ [0, 4/7) \to [1/5, 1);$$

$$C:\ \ x \to (7x+2)/5,\ \ y \to (7y-3)/5,\ \ [3/7, 1) \to [0, 4/5);$$

$$D:\ \ x \to (7x+4)/5,\ \ y \to (7y-5)/5,\ \ [5/7, 1) \to [0, 2/5).$$

Modulo 3 we have $A = C = (1|(2)$ and $B = D = (1)(2|$. The sequence thus contains either the operations A and C only or the operations B and D only. (Otherwise there are infinitely many shifted integer parts divisible by 3.) We will consider the A, C case. Assume without loss of generality that the sequence is not C^∞. We then have infinite number of A's. Each A should be followed by a pattern of C's. But $C^4 : y \to (2401y - 2664)/625$, so it cannot occur. We thus can have the patterns AC, AC^2 and AC^3 only. Note that $AC : y \to (49y+6)/25$, $AC^2 : y \to f(y) = (343y - 33)/125$, $AC^3 : y \to g(y) = (2401y - 606)/625$. Since the functions $(49y + 6)/25$ and $f(y)$ at $6/25$ are greater than $2/7$, each AC should be followed by AC^3. By Lemma 1.7, the sequence is not $(AC^2)^\infty$, so this implies that there are infinitely many patterns AC^3. We claim that only the patterns AC^3AC and AC^3AC^2AC can occur. Indeed, since $g(2/7) = 16/125$ and $g(16/125) < 0$, AC^3 cannot be followed by AC^3, so it must be followed either by AC or by AC^2. In the first case we have AC^3 next after the pattern AC^3AC. In the second case, AC^3AC^2, since $f(16/125) < 0.09 < 16/125$ we cannot have AC^3 next. Also, since $f(0.09) < 0$, we cannot have AC^2 next, so AC^3AC^2 must be followed by AC which is always followed by AC^3. This proves that only the patterns $U = AC^3AC^2AC$ and $V = AC^3AC$ can occur.

We will now seek for a contradiction modulo 11. Assume that there are only finitely many elements divisible by 11. A acts as $x \to 8 - 3x$ and C acts as $x \to 7 - 3x$. This gives $A = (86154793\alpha|(2)$ and $C = (785392146|(\alpha)$. Thus $U = (18|(24|(76|(9)(3|(5|(\alpha|$ and $V = (1)(24\alpha|(93|(78|(5|(6|$. By Lemma 1.7, the sequence is not U^∞ or V^∞, so there are infinitely many patterns VU. But VU can only be of the form $1VU8$. This leads to a contradiction, because U and V cannot begin with 8, so neither VU^2 nor VUV can occur.

Finally, note that on replacing each pair x_n, y_n by $-x_n, 1 - y_n$, D becomes A and B becomes C. The endpoints of the intervals will be the only difference: e. g., instead of $[0, 2/7)$ the respective interval will be $(0, 2/7]$. This makes no difference in our argument, so we do not need to repeat it in the case when B and D are the only operations which occur. The proof of Theorem 1.5 is now completed. □

2. Binary linear recurrence sequences

Here, in Section 2, we will examine the occurrence of composite numbers in the sequences of integers of another kind.

A sequence of real numbers $x_n, n = 1, 2, \dots,$ is called *a linear recurrence sequence* if it's terms satisfy the recurrence

$$x_{n+d} = a_1 x_{n+d-1} + a_2 x_{n+d-2} + \cdots + a_d x_n, \;\; n = 1, 2, 3, \dots,$$

for some fixed numbers $d \in \mathbb{N}$ and $a_1, a_2, \dots, a_d \in \mathbb{R}$. The number d is called an order of the linear recurrence sequence under the natural assumption that $a_d \neq 0$.

Our results concern the order 2 (or *binary*) linear recurrence sequences consisting of integers. The best-known example of a binary linear recurrence sequence is the Fibonacci sequence, given by $F_1 = F_2 = 1$ and the recurrence relation $F_{n+1} = F_n + F_{n-1}$ for $n \geqslant 2$. Graham [15] found two relatively prime positive integers x_1, x_2 such that the sequence

$$x_{n+1} = x_n + x_{n-1},$$

$n = 2, 3, 4, \dots,$ contains only composite numbers, i.e., x_n is composite for each $n \in \mathbb{N}$. We will prove the generalized result of this kind for every binary linear recurrence sequence except two cases for which the impossibility to obtain such result will be proved by a short argument. To be precise, we prove the following:

Theorem 2.1. *Let $(a, b) \in \mathbb{Z}^2$ and let $(x_n)_{n=1}^{\infty}$ be a sequence given by some initial values x_1, x_2 and the binary linear recurrence*

$$x_{n+1} = ax_n + bx_{n-1} \tag{1}$$

for $n = 2, 3, 4, \dots$. Suppose that $b \neq 0$ and $(a, b) \neq (2, -1), (-2, -1)$. Then there exist two relatively prime positive integers x_1, x_2 such that $|x_n|$ is a composite integer for each $n \in \mathbb{N}$.

The exclusion of the two cases is explained in Section 2.1: the required pair of initial values does not exist, i.e. the sequence $(|x_n|)_{n=1}^{\infty}$, where x_1, x_2 are composite and $\gcd(x_1, x_2) = 1$, always contains infinitely many prime numbers. The proof (as well as a part of the proof of Theorem 2.1) uses Dirichlet's theorem on arithmetic progressions: an arithmetic progression whose initial term and common difference are coprime integers contains infinitely many prime numbers (we take absolute values of the terms).

In the proof of Theorem 2.1 we will use a well-known fact that the terms of linear recurrence sequence can be expressed by the roots of the characteristic equation. In our notation the characteristic equation is

$$x^2 - ax - b = 0. \tag{2}$$

Let $\alpha := (a + \sqrt{D})/2$ and $\beta := (a - \sqrt{D})/2$, where $\sqrt{D}$ is defined as $i\sqrt{-D}$ for $D < 0$, be two roots of the characteristic equation, i.e., $x^2 - ax - b = (x - \alpha)(x - \beta)$, and let discriminant of that equation be

$$D := (\alpha - \beta)^2 = a^2 + 4b. \tag{3}$$

By (2) and (3), we have $\alpha - \beta = \sqrt{D}$, $\alpha\beta = -b$ and $\alpha + \beta = a$. It is easily seen that, for each $n \in \mathbb{N}$, the nth term of the sequence $(x_n)_{n=1}^{\infty}$ defined in (1) is given by

$$x_n = \frac{-x_1\beta + x_2}{\alpha - \beta}\alpha^{n-1} + \frac{x_1\alpha - x_2}{\alpha - \beta}\beta^{n-1} \tag{4}$$

provided that $\alpha \neq \beta$, i.e., $D \neq 0$. Indeed, (4) is correct for $n = 1$ and 2. Since α^{n-1} and β^{n-1} satisfy the recurrence (1), so does the right side of the equality (4) for $n = 2, 3, \ldots$. Hence, both sequences, defined by the two sides of the equality (4), are given by the same two initial values and the same recurrence. Therefore, they coincide.

Similarly, for $\alpha = \beta$, i.e., $D = 0$ we have

$$x_n = (2x_1 - x_2\alpha^{-1} + n(x_2\alpha^{-1} - x_1))\alpha^{n-1} \tag{5}$$

for each $n \in \mathbb{N}$.

We deal with the cases $|b| > 1$ and $|b| = 1$ separately.

In the first case deal with in Section 2.2 the following observation is useful. Let b divide x_2. If $x_{n+1} = ax_n + bx_{n-1}, \quad n = 2, 3, 4, \ldots$, then b divides x_k, for $k = 2, 3, 4, \ldots$. If $|x_k| > b$, we have that $|x_k|$ is composite. In case $|b| \geqslant 2$ we shall take x_2 divisible by $|b|$. The main difficulty is to show that x_1 can be chosen so that $x_n \neq 0, b, -b$ for each $n \geqslant 3$, so that $|x_n|$ is composite. To see that the condition $|x_k| > b$ holds is not very difficult if the roots of the characteristic equation are real. However, for negative discriminant the argument is more sophisticated.

The second case dealt with in Section 2.3 will require the use of *divisibility sequences* and *covering systems.*

Definition 2.2. A sequence of rational integers $(v_n)_{n=1}^{\infty}$ is called a *divisibility sequence* if v_r divides v_s whenever r divides s.

The Fibonacci sequence is a *divisibility sequence.* A more general example of a divisibility sequence is called the *Lucas sequence of the first kind.* Assume that the roots α, β of the characteristic equation (2) are distinct $\alpha \neq \beta$. Then

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z}, \tag{6}$$

$n = 1, 2, 3, \ldots,$ is a divisibility sequence. Indeed, if r divides s then, setting $l := s/r \in \mathbb{N}$, we see that

$$\frac{u_s}{u_r} = \frac{\alpha^{rl} - \beta^{rl}}{\alpha^r - \beta^r} = \alpha^{r(l-1)} + \alpha^{r(l-2)}\beta^r + \cdots + \beta^{r(l-1)}$$

is a symmetric function in α, β. Hence $u_s/u_r \in \mathbb{Z}$, giving $u_r|u_s$. If $(x_n)_{n=1}^{\infty}$ is a sequence given by the linear recurrence (1) then one can consider a corresponding divisibility sequence, by selecting $u_1 := 1$, $u_2 := a$. This sequence is the *Lucas sequence of the first kind.*

From (1) and (6) one can calculate the terms of the Lucas sequence as follows:

$$u_3 = au_2 + bu_1 = a^2 + b,$$

$$u_4 = au_3 + bu_2 = a(a^2 + b) + ba = a(a^2 + 2b),$$

$$u_6 = u_3(\alpha^3 + \beta^3) = u_3((\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)) = a(a^2 + b)(a^2 + 3b),$$

$$u_{12} = u_6(\alpha^6 + \beta^6) = u_6((\alpha^3 + \beta^3)^2 - 2(\alpha\beta)^3) = a(a^2 + b)(a^2 + 2b)(a^2 + 3b)(a^4 + 4a^2b + b^2).$$

To obtain the last equality we used the identity

$$(a(a^2 + 3b))^2 + 2b^3 = (a^2 + 2b)(a^4 + 4a^2b + b^2).$$

Definition 2.3. A collection of residue classes

$$r_i \pmod{m_i} := \{r_i + m_ik \mid k \in \mathbb{Z}\},$$

where $m_i \in \mathbb{N}$, $r_i \in \mathbb{Z}$, $0 \leqslant r_i < m_i$, and $i = 1, \ldots, t$, is called a *covering system* if every integer $n \in \mathbb{Z}$ belongs to at least one residue class $r_i \pmod{m_i}$, where $1 \leqslant i \leqslant t$.

For example, 0 (mod 2), 1 (mod 2) is a covering system. A more interesting example, used in our proof, is this covering system:

$$0 \pmod 2,\ 0 \pmod 3,\ 3 \pmod 4,\ 5 \pmod 8,\ 5 \pmod{12},\ 1 \pmod{24}.$$

At the end of our proof we also consider the question of choosing the required pair of the smallest possible initial values x_1, x_2 ofr some certain recurrence sequences. The pair (x_1, x_2) found by Graham in [15] for the case $(a, b) = (1, 1)$ later has been reduced from

$$(331635635998274737472200656430763, 1510028911088401971189590305498785)$$

to

$$(x_1, x_2) = (106276436867, 35256392432). \tag{7}$$

We too indicate the pairs of initial values smaller than those given by our general method for certain sequences.

Proof of Theorem 2.1

2.1. Several exceptional cases.

In this section we prove that Theorem 2.1 does not hold for $(a, b) = (\pm 2, -1)$. Then we start the proof of Theorem 2.1 with three special cases: (*i*) $D = 0$; (*ii*) $a = 0$; (*iii*) $b = -1$, $|a| \leqslant 2$.

Let $(a, b) = (\pm 2, -1)$. It is easy to see that in this case the sequence $(|x_n|)_{n=1}^{\infty}$, where x_1, x_2 are composite and $\gcd(x_1, x_2) = 1$, contains infinitely many prime numbers. Indeed, by (5),

$$x_n = (2x_1 - x_2\varepsilon + n(x_2\varepsilon - x_1))\varepsilon^{n-1}$$

for each $n \geqslant 1$ and $\varepsilon = \pm 1$. Since x_1 and x_2 are relatively prime positive composite integers, we must have $u := 2x_1 - x_2\varepsilon \neq 0$ and $v := x_2\varepsilon - x_1 \neq 0$. Moreover, $\gcd(x_1, x_2) = 1$ implies $\gcd(u, v) = 1$. So, by Dirichlet's theorem on prime numbers in arithmetic progressions, we conclude that $|x_n| = |vn + u|$ is a prime number for infinitely many $n \in \mathbb{N}$. This not only completes the proof of Theorem 2.1 in the case $D = 0$, but also shows that the condition $(a, b) \neq (\pm 2, -1)$ is necessary. *Case* (*i*). Since $D = a^2 + 4b = 0$, the solution of the linear recurrence (2.1) is given by (5). Note that $a = 2\alpha$ and $b = -\alpha^2$. So α is a nonzero integer. We shall split the proof into two cases $|\alpha| \geqslant 2$ and $|\alpha| = 1$.

In the first case, $|\alpha| \geqslant 2$, let us take two distinct primes p, q satisfying $p, q > |\alpha|$ and select $x_1 := p^2$, $x_2 := |\alpha|q^2$. Then x_1, x_2 are composite and $\gcd(x_1, x_2) = 1$. Furthermore, writing $|\alpha| = \alpha\varepsilon$, where $\varepsilon = \pm 1$, by (5), we obtain

$$x_n = (2p^2 - q^2\varepsilon + n(q^2\varepsilon - p^2))\alpha^{n-1}$$

for each $n \geqslant 1$. Clearly, $|x_n|$ is divisible by $|\alpha^2| = |b| \geqslant 4$ for $n \geqslant 3$, so $|x_n|$ is composite for each $n \in \mathbb{N}$, unless

$$2p^2 - q^2\varepsilon + n(q^2\varepsilon - p^2) = 0$$

for some n. But this equality cannot hold for $n \in \mathbb{N}$. Indeed, if $\varepsilon = -1$, then

$$n = \frac{2p^2 + q^2}{p^2 + q^2} = 1 + \frac{p^2}{p^2 + q^2}$$

is greater than 1 and smaller than 2, a contradiction. If $\varepsilon = 1$, then $(n-1)q^2 = (n-2)p^2$ implies $n - 1 = \ell p^2$ and $n - 2 = \ell q^2$ with $\ell \in \mathbb{Z}$. Hence $1 = (n-1) - (n-2) = \ell(p^2 - q^2)$, which is impossible, because $p, q|\alpha| \geqslant 2$ yields $|p^2 - q^2| \geqslant |5^2 - 3^2| = 16 > 1$. Suppose next that $\alpha = \pm 1$. Then $b = -\alpha^2 = -1$ and $a = \pm 2$. This case is not allowed by the condition of the theorem.

Case (ii). For $a = 0$, we have $x_{n+1} = bx_{n-1}$ for $n \geqslant 2$. Let $p, q > |b|$ be two distinct primes. Selecting $x_1 := p^2$ and $x_2 := q^2$, we have $\gcd(x_1, x_2) = 1$. Furthermore, $x_{2k-1} = p^2 b^{k-1}$ and $x_{2k} = q^2 b^{k-1}$ for each $k \geqslant 1$, so $|x_n|$ is composite for every $n \in \mathbb{N}$.

Case (iii). The cases $(a, b) = (\pm 2, -1)$ and $(a, b) = (0, -1)$ are already covered by Case (i) and Case (ii), respectively. If $(a, b) = (-1, -1)$ the recurrence sequence $x_{n+1} = -x_n - x_{n-1}$ satisfying the condition of the theorem is, for example, the following periodic sequence:

$$9, 16, -25, 9, 16, -25, 9, 16, -25, \dots.$$

For $(a, b) = (1, -1)$, we have the recurrence $x_{n+1} = x_n - x_{n-1}$. Now, the periodic sequence

$$16, 25, 9, -16, -25, -9, 16, 25, 9, -16, -25, -9, \dots$$

satisfies the conditions of the theorem.

2.2. The case $|b| \geqslant 2$.

In this Section we prove the lemmas below and, afterwards, Theorem 2.1 in the case $|b| \geqslant 2$.

Lemma 2.4. *Let d and ℓ be two positive integers. Then there is a positive integer c and three distinct odd prime numbers p, q, r such that pqr divides $d + c^2$ and* $\gcd(pqr, \ell c) = 1$.

Proof of Lemma 2.4: Given $h \in \mathbb{Z}$ and a prime number p, let $\left(\frac{h}{p}\right)$ be the Legendre symbol. Take three distinct prime numbers p, q, r greater than $\max(d, \ell)$ such that

$$\left(\frac{-d}{p}\right) = \left(\frac{-d}{q}\right) = \left(\frac{-d}{r}\right) = 1.$$

(For example, one can take the prime numbers p, q, r in the arithmetic progression $4kd + 1$, $k = 1, 2, \dots$.) Then there are three positive integers c_1, c_2, c_3 such that $c_1^2 \equiv -d \pmod{p}$, $c_2^2 \equiv -d \pmod{q}$, $c_3^2 \equiv -d \pmod{r}$. By the Chinese remainder theorem, there is a positive integer c such that $c \equiv c_1 \pmod{p}$, $c \equiv c_2 \pmod{q}$, $c \equiv c_3 \pmod{r}$. Then $c^2 \equiv -d \pmod{pqr}$. This proves that pqr divides $d + c^2$.

Since $p, q, r > \ell$, none of the primes p, q, r divides ℓ. Assume that $p|c$. Then $p|(d + c^2)$ implies $p|d$, which is impossible, because $p > d$. By the same argument, q and r do not divide c. This completes the proof of $\gcd(pqr, \ell c) = 1$. □

Lemma 2.5. *Let u_i, v_i, $i = 1, 2, \dots, p-1$, and s be the elements of the field $\mathbb{F}_p$, where p is a prime number. Assume that for each i at least one of u_i, v_i is nonzero. Then there exist $u, v \in \mathbb{F}_p$ such that at least one of u, v is nonzero and $uu_i + vv_i \neq s$ for each $i = 1, \dots, p-1$.*

Proof of Lemma 2.5: Fix an index i in the range $1 \leqslant i \leqslant p-1$. We claim that there are exactly p pairs $(u, v) \in \mathbb{F}_p^2$ for which

$$uu_i + vv_i = s. \tag{8}$$

Indeed, if $u_i = 0$, then $v_i \neq 0$ and (u, sv_i^*), where $u \in \mathbb{F}_p$ and v_i^* is the inverse element of v_i in $\mathbb{F}_p$, are the solutions of (8). By the same argument, (8) has p solutions if $v_i = 0$. Finally, if $u_i \neq 0$ and $v_i \neq 0$, then we can take any $u \in \mathbb{F}_p$ and the linear equation (8) has a unique solution in v. This proves the claim.

As i runs through $1, \dots, p-1$, we have $p-1$ equations (8) which all together have at most $p(p-1)$ distinct solutions $(u,v) \in \mathbb{F}_p^2$. But $\mathbb{F}_p^2$ consists of the pair $(0,0)$ and p^2-1 pairs (u,v) with at least one u,v nonzero. Since $p^2-1 > p(p-1)$, there exists a pair $(u,v) \in \mathbb{F}_p^2$ as required, namely, $u \neq 0$ or $v \neq 0$ and $uu_i + vv_i \neq s$ for each $i = 1, \dots, p-1$. □

LEMMA 2.6. *Let $c > 0$, $D < 0$ and a be three integers. Suppose that p is an odd prime number which divides $-D + c^2$ but does not divide c. Then the sequence of rational integers*

$$s_n := \frac{(a+\sqrt{D})^n - (a-\sqrt{D})^n}{2\sqrt{D}}, \tag{9}$$

$n = 1, 2, 3, \dots,$ is purely periodic modulo p with period $p-1$. Also, no two consecutive elements of the sequence $(s_n)_{n=1}^{\infty}$ can be zeros modulo p.

PROOF OF LEMMA 2.6: By (9), we have

$$s_n = \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1} D^k,$$

where 0^0 is defined as 1. Since $D \equiv c^2 \pmod{p}$ and

$$\sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1} c^{2k} = \frac{(a+c)^n - (a-c)^n}{2c},$$

we find that

$$s_n \equiv \frac{(a+c)^n - (a-c)^n}{2c} \pmod{p}. \tag{10}$$

Since p and $2c$ are relatively prime, it remains to show that, for each $n \geqslant 1$, we have

$$(a+c)^{n+p-1} - (a-c)^{n+p-1} \equiv (a+c)^n - (a-c)^n \pmod{p}.$$

Indeed, by Fermat's little theorem, p divides both the numbers $(a+c)^{n+p-1} - (a+c)^n = (a+c)^n((a+c)^{p-1} - 1)$ and $(a-c)^{n+p-1} - (a-c)^n$, so p also divides their difference. This proves the periodicity.

For the second statement of the lemma, assume that $s_n \equiv 0 \pmod{p}$ and $s_{n+1} \equiv 0 \pmod{p}$ for some $n \in \mathbb{N}$. Then, by (10), $(a+c)^n \equiv (a-c)^n \pmod{p}$ and $(a+c)^{n+1} \equiv (a-c)^{n+1} \pmod{p}$. If $a \equiv c \pmod{p}$ then $a \equiv -c \pmod{p}$, so p divides $2c$, which is not the case by the condition of the lemma. Similarly, a and $-c$ modulo p are distinct. Hence, from

$$(a-c)^{n+1} \equiv (a+c)^{n+1} \equiv (a+c)^n(a+c) \equiv (a-c)^n(a+c) \pmod{p},$$

we find that $a + c \equiv a - c \pmod{p}$. Once again this yields $p|2c$, a contradiction. $\square$

Lemma 2.7. *Let $(x_n)_{n=1}^{\infty}$ be a sequence of integers given by* (1), $D = a^2+4b \neq 0$, $b \neq 0$, *and let δ be a fixed real number. Then $x_{n+1} = \delta b$ for some $n \geqslant 2$ if and only if*

$$x_1 \frac{s_{n-1}}{2^{n-2}} + \frac{x_2}{b} \frac{s_n}{2^{n-1}} = \delta,$$

where s_n is given by (9).

Proof of Lemma 2.7: The roots α and β of the characteristic equation (2) are distinct, so, by (4) and $\alpha - \beta = \sqrt{D}$, we have

$$x_{n+1}\sqrt{D} = (-x_1\beta + x_2)\alpha^n + (x_1\alpha - x_2)\beta^n \tag{11}$$

for each $n \geqslant 0$. Since $2\alpha = a + \sqrt{D}$ and $2\beta = a - \sqrt{D}$, using (9), we find that $\alpha^n - \beta^n = 2^{1-n}\sqrt{D}s_n$. Since $\alpha\beta = -b$, equality (11) yields

$$x_{n+1}\sqrt{D} = x_2(\alpha^n - \beta^n) - x_1\alpha\beta(\alpha^{n-1} - \beta^{n-1}) = x_2 2^{1-n} s_n\sqrt{D} + x_1 b 2^{2-n} s_{n-1}\sqrt{D}.$$

Hence $x_{n+1} = x_1 b 2^{2-n} s_{n-1} + x_2 2^{1-n} s_n$, because $D \neq 0$. It follows that equality $x_{n+1} = \delta b$ is equivalent to

$$\delta = x_1 \frac{s_{n-1}}{2^{n-2}} + \frac{x_2}{b} \frac{s_n}{2^{n-1}},$$

as claimed. $\square$

Lemma 2.8. *Let $(x_n)_{n=1}^{\infty}$ be a sequence of integers given by* (1), *where $a \neq 0$ and $D > 0$. Then, for each $K > 0$ and each x_1, there is a constant $\lambda(K, \alpha, \beta, x_1) > 0$ such that by selecting the two first terms of the sequence* (1) *as x_1 and $x_2 > \lambda(K, \alpha, \beta, x_1)$ we have $|x_n| > K$ for each $n \geqslant 2$.*

Proof of Lemma 2.8: Since $D > 0$ and $a = \alpha + \beta \neq 0$, we have $|\alpha| \neq |\beta|$. Suppose that $|\alpha| > |\beta|$. (The proof in the case $|\alpha| < |\beta|$ is the same.) From $\alpha\beta = -b$, we obtain $|\alpha| > \sqrt{|b|} \geqslant 1$. Hence, by (11), using several times the triangle inequality, for $n \geqslant 1$, we obtain

$$|x_{n+1}|\sqrt{D} \geqslant |(-x_1\beta+x_2)\alpha^n| - |(x_1\alpha-x_2)\beta^n| = |bx_1+x_2\alpha||\alpha|^{n-1} - |-bx_1-x_2\beta||\beta|^{n-1}$$

$$\geqslant (|bx_1 + x_2\alpha| - |bx_1 + x_2\beta|)|\alpha|^{n-1} \geqslant (|bx_1 + x_2\alpha| - |bx_1 + x_2\beta|)|\alpha|^{n-1}$$

$$\geqslant (|x_2\alpha| - |bx_1| - |bx_1| - |x_2||\beta|)|\alpha|^{n-1} = (|x_2|(|\alpha| - |\beta|) - 2|bx_1|)|\alpha|^{n-1}.$$

Since $|\alpha|^{n-1} \geqslant 1$ for $n \geqslant 1$, the last expression is greater than $K\sqrt{D}$ provided that $|x_2|(|\alpha| - |\beta|) > 2|bx_1| + K\sqrt{D}$. So the lemma holds with

$$\lambda(K, \alpha, \beta, x_1) := \frac{2|bx_1| + K\sqrt{D}}{|\alpha| - |\beta|} \tag{12}$$

when $|\alpha| > |\beta|$. Evidently, the constants b, D appearing in the right hand side of (12) depend on α, β too, because $b = -\alpha\beta$ and $D = a^2 + 4b = (\alpha - \beta)^2$, by (2), (3). □

Lemma 2.9. *Let $a_1 \geqslant 0$ and $b_1, b_2 \geqslant 1$ be integers such that no prime number p divides the three numbers a_1, b_1, b_2. Then, for each $K > 0$, there exists an integer k_1K such that $b_1k_1 + a_1$ is a composite integer relatively prime to b_2.*

Proof of Lemma 2.9: The lemma is trivial if $a_1 = 0$. Assume that $a_1 \geqslant 1$. Set $t := \gcd(b_1, a_1)$. By the condition of the lemma, t is relatively prime to b_2. By Dirichlet's theorem about prime numbers in arithmetic progressions, there is a $t_1 \in \mathbb{N}$ such that $(b_1/t)t_1 + a_1/t$ is a prime number greater than b_2. Then $b_1t_1 + a_1 = t((b_1/t)t_1 + a_1/t)$ is relatively prime to b_2. This implies that, for any $s \in \mathbb{N}$, the number

$$b_1b_2s + b_1t_1 + a_1 = b_1(b_2s + t_1) + a_1$$

is relatively prime to b_2. Of course, there are infinitely many $s \in \mathbb{N}$ for which the number $b_1b_2s + b_1t_1 + a_1$ is composite. It remains to take one of those $s \in \mathbb{N}$ for which $k_1 := b_2s + t_1 > K$. □

We begin the proof of the theorem for $|b| \geqslant 2$ from the more difficult case when the discriminant $D = a^2 + 4b$ is negative. Let us apply Lemma 2.4 to $d := -D$ and $\ell := |b|$. Then, by Lemma 2.4, there exist a positive integer c and three distinct odd primes p, q, r such that pqr divides $-D + c^2$ and

$$\gcd(pqr, |b|c) = 1. \tag{13}$$

Our aim is to choose two composite relatively prime positive integers x_1, x_2 so that $|b|$ divides x_2 and $x_{n+1} \notin \{0, b, -b\}$ for each $n \geqslant 2$. Then $|x_1| = x_1$ and $|x_2| = x_2$ are composite. Also, using (1), by induction on n we see that $|b|$ divides x_{n+1} for each $n \geqslant 1$. Since $x_n \notin \{0, b, -b\}$ for $n \geqslant 3$ and $|b|$ divides x_n for $n \geqslant 2$, we must have $|x_n| > |b|$ for each $n \geqslant 3$. Hence $|x_n|$ is a composite integer for every $n \geqslant 3$ too.

For a contradiction, assume that, for some $n \geqslant 1$, $x_{n+2} = \delta b$ with $\delta \in \{0, 1, -1\}$. Then, by Lemma 2.7, we have

$$x_1 \frac{s_n}{2^{n-1}} + x_2' \frac{s_{n+1}}{2^n} = \delta, \tag{14}$$

where $x_2' := x_2/b$ and $n \in \mathbb{N}$. Firstly, let us choose x_1, x_2' modulo p so that

$$2x_1 s_n + x_2' s_{n+1} \neq 0, \ \ n \in \mathbb{N}. \tag{15}$$

This is possible by combining Lemma 2.6 with Lemma 2.5. Indeed, by Lemma 2.6, the sequence $s_n \pmod{p}$, $n = 1, 2, 3, \dots$, is purely periodic with period $p - 1$. So, by Lemma 2.5 applied to the pairs $(2s_1, s_2), (2s_2, s_3), \dots, (2s_{p-1}, s_p) \in \mathbb{F}_p^2$ and $s = 0$, we conclude that there are $x_1, x_2' \in \mathbb{F}_p$, not both zeros in $\mathbb{F}_p$, such that (15) holds.

Next, we shall choose $x_1, x_2' \in \mathbb{F}_q$ so that

$$2x_1 s_n + x_2' s_{n+1} \neq 2^n, \ \ n \in \mathbb{N}, \tag{16}$$

in $\mathbb{F}_q$. As above, by Lemma 2.6, the sequence $s_n 2^{1-n} \pmod{q}$, $n = 1, 2, 3, \dots$, where 2^{1-n} is the inverse of 2^{n-1} in $\mathbb{F}_q$, is purely periodic with period $q - 1$. By Lemma 2.5 applied to the pairs $(s_1, 2^{-1}s_2), (s_2 2^{-1}, s_3 2^{-2}), \dots, (s_{q-1} 2^{-(q-2)}, s_q 2^{-(q-1)}) \in \mathbb{F}_q^2$ and $s = 1$, we conclude that there are $x_1, x_2' \in \mathbb{F}_q$, not both zeros, such that (16) holds. By the same argument, there are $x_1, x_2' \in \mathbb{F}_r$, not both zeros, such that

$$2x_1 s_n + x_2' s_{n+1} \neq -2^n, \ \ n \in \mathbb{N}, \tag{17}$$

in $\mathbb{F}_r$.

By the Chinese remainder theorem, combining (15), (16), (17), we see that there exist two congruence classes $a_1 \pmod{pqr}$ and $a_2 \pmod{pqr}$ such that for any integers x_1 and x_2' that belong to the first and the second class, respectively, equality (14) does not hold for $n \in \mathbb{N}$. Furthermore, by Lemma 2.5, each prime number p, q, r divides at most one of the integers a_1, a_2. It remains to select $k_1, k_2 \in \mathbb{Z}$ so that $x_1 = pqrk_1 + a_1$ and $x_2 = bx_2' = b(pqrk_2 + a_2)$ are two composite relatively prime positive integers. Take $k_2 \in \mathbb{Z}$ such that $|pqrk_2 + a_2| > 1$, $bk_2 > 0$. Then $x_2 > 0$ is a composite number. Furthermore, no prime number divides the three numbers pqr, a_1 and x_2, because the primes p, q, r do not divide $|b|$, by (13), and if, say, $p | a_1$ then p does not divide $pqrk_2 + a_2$. Hence, by Lemma 2.9 applied to the triplet $b_1 := pqr$, a_1, $b_2 := x_2$, we may select $k_1 \in \mathbb{N}$ so that $x_1 = pqrk_1 + a_1$

is a composite integer relatively prime to x_2. This proves the theorem for $|b| \geqslant 2$, $D < 0$.

The case when $D = a^2 + 4b > 0$ is easier. As above, we need to choose two composite relatively prime positive integers x_1, x_2 such that $|b|$ divides x_2 and show that this choice leads to $x_{n+1} \notin \{0, b, -b\}$ for each $n \geqslant 2$. If $|\alpha| = |\beta|$, then $\alpha = -\beta$, so $a = \alpha + \beta = 0$. This case is already settled in Section 2. Assume next that $|\alpha| \neq |\beta|$. Take $x_1 := p^2$ and $x_2 := b^2 q$, where $p, q > |b|$ are prime numbers and q is so large that $b^2 q$ is greater than the constant $\lambda(|b|, \alpha, \beta, p^2)$ given in (12). Then, by Lemma 2.8, $|x_{n+1}| > |b|$ for $n \geqslant 2$. This completes the proof of Theorem 2.1 in case $|b| \geqslant 2$.

2.3. **Divisibility sequences, covering systems and the case $|b| = 1$.**

In this Section we use divisibility sequences and covering systems to prove the lemmas below and, afterwards, Theorem 2.1 in the case $|b| = 1$.

LEMMA 2.10. *If $b = -1$ and $|a| \geqslant 4$ then there exist five distinct prime numbers p_i, $i = 1, \dots, 5$, such that $p_1 | u_2$, $p_2 | u_3$, $p_3 | u_4$, $p_4 | u_6$ and $p_5 | u_{12}$.*

PROOF OF LEMMA 2.10: Let p_1 be any prime divisor of $u_2 = a$, and let $p_2 \neq 2$ be any prime divisor of $u_3 = a^2 - 1 = (a-1)(a+1)$. Such p_2 exists, because $|a| \geqslant 4$. Clearly, $p_2 \neq p_1$. Since $a^2 - 2$ is either 2 or 3 modulo 4, it is not divisible by 4. So $a^2 - 2$ must have an odd prime divisor p_3. Clearly, $p_3 \neq p_1$. Furthermore, $p_3 \neq p_2$, because $\gcd(a^2 - 1, a^2 - 2) = 1$. We select this p_3 as a divisor of u_4. Observing that 9 does not divide $a^2 - 3$, we get that there is prime number $p_4 \neq 3$ that divides $a^2 - 3$. Since $\gcd(a, a^2 - 3)$ is either 1 or 3, this yields $p_4 \neq p_1$. Also, since $\gcd(a^2 - 1, a^2 - 3)$ is either 1 or 2, we may have $p_4 = p_2$ only if $p_2 = 2$, which is not the case. So $p_4 \neq p_2$. The fact that $p_4 \neq p_3$ follows from $\gcd(a^2 - 2, a^2 - 3) = 1$. We select this p_4 as a divisor of u_6.

It remains to show that there is a prime divisor p_5 of $a^4 - 4a^2 + 1$ distinct from p_i, $i = 1, \dots, 4$. Note that $a^4 - 4a^2 + 1$ is not zero modulo 4 and modulo 3. Hence there is a prime number $p_5 \neq 2, 3$ that divides $a^4 - 4a^2 + 1 \geqslant 4^4 - 4^3 + 1 = 193$. Evidently, $p_5 \neq p_1$. Writing

$$a^4 - 4a^2 + 1 = (a^2 - 1)(a^2 - 3) - 2$$

and using $p_5 \neq 2$, we may conclude that $p_5 \neq p_2, p_4$. Similarly, from $a^4 - 4a^2 + 1 = (a^2 - 2)^2 - 3$ and $p_5 \neq 3$, we see that $p_5 \neq p_3$. $\square$

One can easily check that Lemma 2.10 does not hold for $|a| = 3$. The next lemma is very similar to that above.

Lemma 2.11. *If $b = 1$ and $|a| \geqslant 2$ then there exist five distinct prime numbers p_i, $i = 1, \dots, 5$, such that $p_1 | u_2$, $p_2 | u_3$, $p_3 | u_4$, $p_4 | u_6$ and $p_5 | u_{12}$.*

Proof of Lemma 2.11: Take any prime divisor p_1 of $u_2 = a$. Let $p_2 \neq 2$ be any prime divisor of $u_3 = a^2 + 1$. Such p_2 exists, because $a^2 + 1$ is not divisible by 4. Evidently, $p_2 \neq p_1$. Similarly, let $p_3 \neq 2$ be any prime divisor of $a^2 + 2$. Clearly, $p_3 \neq p_2$. Since $\gcd(a, a^2 + 2)$ is either 1 or 2, $p_3 = p_1$ only if they both are equal to 2, which is not the case. So we may select this p_3 as a divisor of u_4. Observing next that 9 does not divide $a^2 + 3$, we deduce that there is prime number $p_4 \neq 3$ that divides $a^2 + 3$. Since $\gcd(a, a^2 + 3)$ is either 1 or 3, this yields $p_4 \neq p_1$. Also, since $\gcd(a^2 + 1, a^2 + 3)$ is either 1 or 2, we may have $p_4 = p_2$ only if $p_2 = 2$, which is not the case. Hence $p_4 \neq p_2$. As above, the fact that $p_4 \neq p_3$ follows from $\gcd(a^2 + 2, a^2 + 3) = 1$. We select this p_4 as a divisor of u_6.

It remains to show that there is a prime divisor p_5 of $a^4 + 4a^2 + 1$ which is distinct from p_i, $i = 1, \dots, 4$. Note that $a^4 + 4a^2 + 1 > 6$ is not zero modulo 4 and modulo 9. Hence there is a prime $p_5 \neq 2, 3$ that divides $a^4 + 4a^2 + 1$. Evidently, $p_5 \neq p_1$. Writing

$$a^4 + 4a^2 + 1 = (a^2 + 1)(a^2 + 3) - 2$$

and using $p_5 \neq 2$, we may conclude that $p_5 \neq p_2, p_4$. Finally, from $a^4 + 4a^2 + 1 = (a^2 + 2)^2 - 3$ and $p_5 \neq 3$, it follows that $p_5 \neq p_3$. $\square$

To illustrate Lemma 2.11, let us take $(a, b) = (\pm 2, 1)$. Then $u_2 = \pm 2$, $u_3 = 5$, $u_4 = \pm 2^2 \cdot 3$, $u_6 = \pm 2 \cdot 5 \cdot 7$ and $u_{12} = \pm 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. Hence Lemma 2.11 holds with $p_1 = 2$, $p_2 = 5$, $p_3 = 3$, $p_4 = 7$, $p_5 = 11$.

The next lemma uses the concept of covering systems introduced by Erdős. In the proof of the theorem for $|b| = 1$ we shall use the following well-known covering system

$$0 \pmod 2,\ 0 \pmod 3,\ 1 \pmod 4,\ 5 \pmod 6,\ 7 \pmod{12}. \tag{18}$$

Lemma 2.12. *Let $r_i \pmod{m_i}$, $i = 1, \dots, t$, be a covering system, and let $(u_n)_{n=1}^{\infty}$ be a divisibility sequence given by $u_1 := 1$, $u_2 := a$ and $u_{n+1} = au_n + bu_{n-1}$*

for $n = 2, 3, \dots,$ where $a \in \mathbb{Z}$, $b = \pm 1$ and $D = a^2 + 4b > 0$. Suppose that there exist t distinct prime numbers $p_1, \dots, p_t$ such that $p_i | u_{m_i}$ for each $i = 1, \dots, t$. Then there are two relatively prime composite positive integers x_1, x_2 such that each $|x_n|$, $n \in \mathbb{N}$, where x_n is a sequence defined in (1)*, is a composite number.*

Proof of Lemma 2.12: By the Chinese remainder theorem, there exist $s, l \in \mathbb{Z}$ satisfying

$$s \equiv u_{m_i - r_i} \pmod{p_i},$$

$$l \equiv u_{m_i - r_i + 1} \pmod{p_i}$$

for $i = 1, \dots, t$. Note that two consecutive terms of the sequence $(u_n)_{n=1}^{\infty}$ cannot be divisible by the same prime number p. Indeed, if $p|u_n$ and $p|u_{n+1}$ then using $b = \pm 1$ from $u_{n+1} = au_n + bu_{n-1}$ we find that $p|u_{n-1}$. By the same argument, $p|u_{n-2}$ and so on. Hence $p|u_1$, a contradiction.

So, for every x_1 in the residue class $s \pmod{P}$, where $P = p_1 \dots p_t$, and for every x_2 in the residue class $l \pmod{P}$, we have $x_1 \equiv u_{m_i - r_i} \pmod{p_i}$ and $x_2 \equiv u_{m_i - r_i + 1} \pmod{p_i}$ for $i = 1, \dots, t$. By induction on n, this implies

$$x_{n+1} \equiv u_{m_i - r_i + n} \pmod{p_i} \tag{19}$$

for each $n \geqslant 0$ and each $i = 1, \dots, t$. Since $r_i \pmod{m_i}$, $i = 1, \dots, t$, is a covering system, every non-negative integer n belongs to certain residue class $r_i \pmod{m_i}$, where i is some of the numbers $1, \dots, t$. Fix one of those i and write $n = r_i + km_i$, where $k \geqslant 0$. Note that $p_i | u_{m_i(k+1)}$, because $p_i | u_{m_i}$ and $u_{m_i} | u_{m_i(k+1)}$. Thus (19) yields

$$x_{n+1} \equiv u_{m_i(k+1)} \pmod{p_i} \equiv 0 \pmod{p_i},$$

giving $p_i | x_{n+1}$.

It remains to choose two composite relatively prime positive integers $x_1 \equiv s \pmod{P}$ and $x_2 \equiv l \pmod{P}$ so that $|x_n| > \max(p_1, \dots, p_t)$ for every $n \in \mathbb{N}$. Then each $|x_n|$ is divisible by some p_i and greater than p_i, so it is a composite number. To do this let us choose a composite integer $x_1 > \max(p_1, \dots, p_t)$ satisfying $x_1 \equiv s \pmod{P}$. Then we can select $x_2 \equiv l \pmod{P}$ as required, by Lemma 2.8 and Lemma 2.9, where $a_1 := l$, $b_1 := P$, $b_2 := x_1$, because no prime number $p_1, \dots, p_t$ divides both s and l. □

Now, we shall prove the theorem for $|b| = 1$. Suppose first that $b = -1$ and $|a| \geqslant 4$. Then, by Lemma 2.10, there are five distinct primes $p_1, \dots, p_5$ dividing $u_2, u_3, u_4, u_6, u_{12}$, respectively. Since $D = a^2 - 4 > 0$, the theorem follows from Lemma 2.12 applied to the covering system (18). Similarly, if $b = 1$ and $|a| \geqslant 2$ we also have $D = a^2 + 4b = a^2 + 4 > 0$, so the theorem follows by Lemmas 2.11 and 2.12.

Recall that the cases $b = -1$, $|a| \leqslant 2$ and $b = 1$, $a = 0$ have been considered in Section 2. In Section 1 we already described the literature concerning the case $(a, b) = (1, 1)$. So three cases that remain to be considered are $(a, b) = (-1, 1)$, $(a, b) = (-3, -1)$, $(a, b) = (3, -1)$.

We begin with the case $(a, b) = (-1, 1)$. Vsemirnov's pair (7) of two composite relatively prime integers

$$V_1 := 106276436867, \quad V_2 := 35256392432$$

shows that the numbers

$$V_n = V_{n-1} + V_{n-2} = F_{n-1}V_2 + F_{n-2}V_1, \quad n \geqslant 2, \tag{20}$$

are all composite. Here, F_n is the nth Fibonacci number, $F_0 := 0$. For the sequence $x_{n+1} = -x_n + x_{n-1}$, we clearly have

$$x_n = (-1)^n F_{n-1}x_2 + (-1)^{n-1}F_{n-2}x_1, \quad n \geqslant 3. \tag{21}$$

Selecting $x_1 := -V_2 + V_1 = 71020044435$ and $x_2 := V_1 = 106276436867$, one can easily check that x_1 and x_2 are relatively prime composite integers. Moreover, by (20) and (21),

$$x_n = (-1)^n F_{n-1}V_1 + (-1)^{n-1}F_{n-2}(-V_2 + V_1) = (-1)^n F_{n-2}V_2 + (-1)^n F_{n-3}V_1$$

$$= (-1)^n (F_{n-2}V_2 + F_{n-3}V_1) = (-1)^n V_{n-1}$$

for $n \geqslant 3$. Thus $|x_n| = V_{n-1}$ is also composite integer for each $n \geqslant 3$.

For $(a, b) = (-3, -1)$, we use the covering system

$$1 \pmod 2, \ 1 \pmod 3, \ 0 \pmod 4, \ 6 \pmod 8, \ 6 \pmod{12}, \ 2 \pmod{24}.$$

The divisibility sequence $(u_n)_{n=1}^{\infty}$ is given by $u_1 := 1$, $u_2 := -3$ and $u_{n+1} = -3u_n - u_{n-1}$, $n = 2, 3, \dots$. We select the following primes dividing $u_2, u_3, u_4, u_8, u_{12}, u_{24}$, respectively: $3, 2, 7, 47, 23, 1103$. By the method described in Lemma 2.12, we calculated the pair

$$(x_1, x_2) = (13271293, 219498)$$

satisfying the conditions of the theorem.

For $(a, b) = (3, -1)$, we use the covering system

$$0 \pmod 2,\ 0 \pmod 3,\ 3 \pmod 4,\ 5 \pmod 8,\ 5 \pmod{12},\ 1 \pmod{24}.$$

As above, the primes dividing $u_2, u_3, u_4, u_8, u_{12}, u_{24}$ are $3, 2, 7, 47, 23, 1103$, respectively. This time, using the method described in Lemma 2.12, we found the pair

$$(x_1, x_2) = (7373556, 2006357)$$

satisfying the conditions of the theorem. The proof of Theorem 2.1 is thus completed. □

Below, we shall find smaller solutions for $(a, b) = (\pm 3, -1)$. Instead of using Lemma 2.12, we may directly search for a pair of relatively prime positive integers x_1, x_2 such that each of the first 24 elements of the sequence (1) is divisible by at least one of the primes $3, 2, 7, 47, 23, 1103$. Then we may choose a covering system $r_i \pmod{m_i}$, where $m_1 = 2$, $m_2 = 3$, $m_3 = 4$, $m_4 = 8$, $m_5 = 12$, $m_6 = 24$, and $i = 1, \dots, 6$, such that, for each n in the range $0 \leqslant n \leqslant 23$ and each i in the range $1 \leqslant i \leqslant 6$, $n+1 \equiv r_i \pmod{m_i}$ implies $p_i | x_{n+1}$. This would be enough for $p_i | x_{n+1}$ to hold for any $n+1$, $n \geqslant 0$, belonging to the residue class $r_i \pmod{m_i}$. Using this direct method, we found smaller pairs (x_1, x_2) producing sequences consisting of composite numbers.

For $(a, b) = (-3, -1)$, by selecting the residues of the covering system as

$$(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 1, 0, 2, 6, 14)$$

and searching over x_1 divisible by 7 and x_2 divisible by 2 and 3, we found the pair

$$(x_1, x_2) = (35, 3294).$$

One can easily check that

$$1 \pmod 2,\ 1 \pmod 3,\ 0 \pmod 4,\ 2 \pmod 8,\ 6 \pmod{12},\ 14 \pmod{24}$$

is indeed a covering system. Also, if $n+1$, where $n \geqslant 0$, belongs to the residue class $r_i \pmod{m_i}$ we use the fact that $p_i | x_{n+1}$. This explains why we take x_1 divisible by 7 and x_2 divisible by 6. It is clear that $\gcd(x_1, x_2) = \gcd(35, 3294) = 1$. Also, $|x_n| > \max(p_1, \dots, p_6) = 1103$ for $n \geqslant 2$, so $|x_n|$ is composite for each $n \in \mathbb{N}$.

Selecting $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 0, 1, 7, 7, 11)$, we found the symmetric pair $(x_1, x_2) = (3294, 35)$. Similarly, taking $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 2, 1, 3, 3, 7)$, we established that

$$(x_1, x_2) = (2367, 3031)$$

is also such a pair. Note that $3294 + 35 < 2367 + 3031$. On the other hand, $\max(3294, 35) > \max(2367, 3031)$. In the same way, using $(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 2, 0, 6, 10, 18)$, we found the symmetric pair $(x_1, x_2) = (3031, 2367)$.

For $(a, b) = (3, -1)$, selecting $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 2, 1, 3, 7, 15)$, we found the pair

$$(x_1, x_2) = (3399, 35).$$

Choosing the residues $(r_1, r_2, r_3, r_4, r_5, r_6) = (1, 2, 0, 6, 6, 10)$, we arrived to the symmetric pair $(x_1, x_2) = (35, 3399)$.

3. Egyptian fractions and numbers expressible by a special linear form

Let t be a fixed positive integer. In this Section we consider the set of positive integers

$$E(t) := \{n \in \mathbb{N} \,:\, n = tM - d\},$$

where M is a positive multiple of the product and d is a positive divisor of the sum of two positive integers, namely,

$$ab|M \quad \text{and} \quad d|(a+b)$$

for some $a, b \in \mathbb{N}$. Evidently,

$$E(t') \subseteq E(t) \quad \text{whenever} \quad t|t'.$$

It is easy to see that

$$E(1) = E(2) = \mathbb{N}. \tag{22}$$

Indeed, suppose first that $t = 1$. Then, for each $n \in \mathbb{N}$ selecting $a = 2n+1$, $b = 1$, $M = ab = 2n+1$ and $d = (a+b)/2 = n+1$, we find that

$$n = 2n + 1 - (n+1) = M - d,$$

giving $E(1) = \mathbb{N}$. In case $t = 2$, for each $n \in \mathbb{N}$ we may choose $a = n+1$, $b = 1$, $M = ab = n+1$ and $d = a + b = n+2$. Then $2M - d = 2(n+1) - (n+2) = n$, so that $E(2) = \mathbb{N}$.

Apart from (22) the situation with $t \geqslant 3$ is not clear. In this context, the sets $E(4)$ and $E(5)$ are of special interest, because an integer n belongs to the set $E(t)$ if and only if

$$n = tM - d = tuab - (a+b)/v$$

with some $a, b, u, v \in \mathbb{N}$. Therefore, $n \in E(t)$ yields the representation

$$\frac{t}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

with positive integers

$$x := uab, \quad y := uvna, \quad z := uvnb.$$

Thus this leads us to the subject of Egyptian fractions (the sums of distinct unit fractions) and the related famous conjectures. If $n \in E(t)$ then t/n is expressible as the sum of three unit fractions. In particular, if every prime number p belongs to the set $E(4)$ then the Erdős-Straus conjecture (asserting that for each integer $n \geqslant 2$ the fraction $4/n$ is expressible by the sum $1/x + 1/y + 1/z$ with $x, y, z \in \mathbb{N}$) is true, whereas if every prime number p belongs to $E(5)$ then the corresponding conjecture of Sierpiński (asserting that for each $n \geqslant 4$ the fraction $5/n$ is expressible by the sum $1/x + 1/y + 1/z$) is true [29]. In this context the most general Schinzel's conjecture asserts that the fraction t/n for each $n \geqslant n(t)$ is expressible by the sum $1/x + 1/y + 1/z$. This clearly holds for $t \leqslant 3$ but is open for each fixed $t \geqslant 4$. Conjecture 3.5 below implies that there is an integer $C(t)$ such that each prime number $p > C(t)$ belongs to $E(t)$. This would imply Schinzel's conjecture as well.

In this note we observe that

Theorem 3.1. *The set $E(4)$ does not contain perfect squares and the numbers* 288, 336, 4545.

Suppose $k^2 \in E(4)$, i.e., there exist $u, v, a, b \in \mathbb{N}$ such that

$$v(4uab - k^2) = a + b. \tag{23}$$

To show that $k^2 \notin E(4)$ we shall use the fact that

Lemma 3.2. *The equation (23) has no solutions in positive integers u, v, a, b, k.*

Lemma 3.2 implies that $-d$ is a quadratic nonresidue modulo $4ab$ if $d|(a + b)$. Indeed, if the number $-d$ were a quadratic residue modulo $4ab$ then selecting the positive integer $v := (a+b)/d$ we see that the equation $k^2 = -d+4uab$ with some $u \in \mathbb{N}$ has a solution $k \in \mathbb{N}$, which is impossible in view of Lemma 3.2. Note that the set of divisors of $a + b$, when $a < b$ both run through the set $\{1, 2, \dots, n\}$, contains the set $\{1, 2, \dots, 2n - 1\}$. Thus, by Lemma 3.2, we find that

Corollary 3.3. *For each positive integer n the $2n - 1$ consecutive integers*

$$4n! - 2n + 1, 4n! - 2n + 2, \dots, 4n! - 1$$

are quadratic nonresidues modulo $4n!$.

Corollary 3.3 gives the example of at least $(2-\varepsilon)\log m/\log\log m$ consecutive quadratic nonresidues modulo $m = 4n!$ (by using Stirling's approximation $n! \sim \sqrt{2\pi n}\frac{n^n}{e^n}$).

As we already observed in (22), the sets $\mathbb{N} \setminus E(1)$ and $\mathbb{N} \setminus E(2)$ are empty. By Lemma 3.2 the equation $v(4uab - k^2) = a + b$ has no solutions in positive integers u, v, a, b, k. In particular, if t is a positive integer divisible by 4 and $s \in \mathbb{N}$ is such that $4s|t$ then the equation $vs(4(t/4s)uab - k^2) = a + b$ has no solutions in positive integers u, v, a, b, k. The latter is equivalent to the equation $v(tuab - sk^2) = a + b$. Consequently, we obtain that

Corollary 3.4. *The set $E(t)$, where $4|t$, does not contain the numbers of the form sk^2, where $s \in \mathbb{N}$ satisfies $4s|t$ and $k \in \mathbb{N}$.*

In particular, this implies that the set $\mathbb{N}\setminus E(t)$ is infinite when $4|t$. We conjecture that all other sets, namely, $\mathbb{N} \setminus E(t)$ with $t \in \mathbb{N}$ which is not a multiple of 4 are finite. More precisely, we conjecture that

Conjecture 3.5. *There exists an integer $C(t) \in \mathbb{N} \cup \{0\}$ such that the set $E(t)$ contains all integers greater than or equal to $C(t) + 1$ if 4 does not divide t and all integers greater than or equal to $C(t) + 1$ except for sk^2, where $4s|t$ and $k \in \mathbb{N}$, if $4|t$.*

By (22), we have $C(1) = C(2) = 0$. It is known that the total number of representations of t/n by the sum $1/x + 1/y + 1/z$ does not exceed $c(\varepsilon)(n/t)^{2/3}n^{\varepsilon}$, where $\varepsilon > 0$ (see [4]). We know that if $n \in E(t)$ then t/n is expressible by the sum of three unit fractions, so this bound also holds for the number of representations of n in the form $tM - d$. On the other hand, by the result of Vaughan [32], almost all positive integers are expressible by the sum of three unit fractions. It is easy to see that for each fixed integer $t \geqslant 3$ almost all positive integers belong to the set $E(t)$.

In fact, one can easily show a much stronger statement:

Proposition 3.6. *For any integer $t \geqslant 3$ almost all positive integers can be written in the form $pa - 1$ with some prime number $p \equiv -1 \pmod{t}$ and some $a \in \mathbb{N}$.*

If $n \in \mathbb{N}$ can be written in this way then

$$n = pa - 1 = (p+1)a - a - 1 = tM - d \in E(t)$$

with $b = 1$, $d = a + 1$ and $M = (p+1)a/t$. By the above, it suffices to show that the density of positive integers n that have no prime divisors of the form $p \equiv -1 \pmod{t}$ is zero. This can be easily done by a standard sieve argument (see Section 3.1).

In the proof of Theorem 3.1 we describe an algorithm how to check if any particular number belongs to the set $E(t)$ or not and present the corresponding Maple program. We applied this algorithm to make also other calculations with C++ (with a better performance than that of Maple) below.

Coming back to Conjecture 3.5, by calculation with C++, in the range $[1, 2\cdot 10^9]$ we found only three exceptional integers $6, 36, 3600$ which do not belong to the set $E(3)$. So we conjecture that

$$E(3) = \mathbb{N} \setminus \{6, 36, 3600\} \quad \text{and} \quad C(3) = 3600.$$

For $t = 4$ we have

$$288, 336, 4545, \mathbb{N}^2 \in \mathbb{N} \setminus E(4),$$

and we conjecture that $C(4) = 4545$.

There are much more integers which do not lie in $E(5)$. In the range $[1, 2 \cdot 10^9]$ there are 48 such integers:

$$1, 2, 5, 6, 10, 12, 20, 21, 30, 32, 45, 46, 50, 60, 92, 102, 105, 126, 141, 182, 192,$$

$$210, 282, 320, 330, 366, 406, 600, 650, 726, 732, 842, 846, 920, 992, 1020, 1446,$$

$$1452, 1905, 1920, 2100, 2250, 2262, 3962, 7320, 9050, 11520, 40500.$$

We conjecture that this list is full, i.e., $C(5) = 40500$. The list of integers in $[1, 2 \cdot 10^9]$ which do not lie in $E(6)$ contains 108 numbers, the largest one being 684450. We are more cautious to claim that $C(6) = 684450$, since this number is quite large compared to the computation bound $2 \cdot 10^9$. Here is a result of our calculations with C++ for $3 \leqslant t \leqslant 9$.

t	computation bound	number of exceptions	largest exception
3	$2 \cdot 10^9$	3	3600
4	$2 \cdot 10^9$	3	4545
5	$2 \cdot 10^9$	48	40500
6	$2 \cdot 10^9$	108	684450
7	10^9	270	9673776
8	10^9	335	3701376
9	10^9	932	18481050

In the above table, for $t = 4$ all squares k^2 are excluded, whereas for $t = 8$ all squares k^2 and all numbers of the form $2k^2$ are excluded (see Corollary 3.4 and Conjecture 3.5).

3.1. **Proofs.**

Proof of Lemma 3.2: Lemma 3.2 was apparently first proved by Yamamoto [39]. See also Lemma 2 in [28] and Proposition 1.6 in [12]. Here is a short proof.

Since $a = vd - b$, equality (23) yields

$$k^2 = 4u(vd - b)b - d = (4buv - 1)d - 4b^2u.$$

So if (23) has a solution in positive integers then the Jacobi symbol $\left(\frac{-4b^2u}{4buv-1}\right) = \left(\frac{k^2}{4buv-1}\right)$ must be equal to 1. Indeed, since $-4b^2u$ and $4buv - 1$ are relatively prime, we have $\left(\frac{-4b^2u}{4buv-1}\right) \neq 0$ and so $\left(\frac{k^2}{4buv-1}\right) = 1$. We will show, however, that it is equal to -1. Indeed, writing $u = 2^r u_0$, where $r \geqslant 0$ is an integer and $u_0 \geqslant 1$ is an odd integer and using $\left(\frac{-1}{4buv-1}\right) = -1$ and also $\left(\frac{2}{4buv-1}\right) = 1$ in case u is even, i.e., $r \geqslant 1$, we find that

$$\left(\frac{-4b^2u}{4buv-1}\right) = \left(\frac{-2^{r+2}b^2u_0}{4buv-1}\right) = -\left(\frac{2^r u_0}{4buv-1}\right) = -\left(\frac{u_0}{4buv-1}\right).$$

Further, by the quadratic reciprocity law, in view of $u_0|u$ we conclude that

$$-\left(\frac{u_0}{4buv-1}\right) = -(-1)^{(u_0-1)/2}\left(\frac{4buv-1}{u_0}\right) = -(-1)^{(u_0-1)/2}\left(\frac{-1}{u_0}\right) = -1.$$

□

Proof of Theorem 3.1: Lemma 3.2 implies that $k^2 \notin E(4)$. To complete the proof of Theorem 3.1 we need to show that $288, 336, 4545 \notin E(4)$.

The case $n = 288$ can be easily checked 'by hand'. Observe that $288 = 4M - d$ implies that $d = 4s$ and $M = (288 + 4s)/4 = 72 + s$. Furthermore, from

$$72 + s = M \geqslant ab \geqslant a + b - 1 \geqslant d - 1 = 4s - 1$$

we find that $1 \leqslant s \leqslant 24$. So for each $s = 1, 2, \ldots, 24$ it remains to check that there are no positive integers a, b for which $4s|(a + b)$ and $ab|(72 + s)$.

Note first that for $s \geqslant 11$ we must have $a + b = 4s$ and $ab = 72 + s$. Indeed, if $a + b > 4s$ then $a + b \geqslant 8s$ and so

$$72 + s = M \geqslant ab \geqslant a + b - 1 \geqslant 8s - 1,$$

which is impossible, because $s \geqslant 11$. If $ab < 72 + s$ then $2ab \leqslant 72 + s$, so that $72+s \geqslant 2ab \geqslant 2(a+b-1) \geqslant 2(d-1) = 2(4s-1) = 8s-2$, which is a contradiction again. However, from $a + b = 4s$ and $ab = 72 + s$ it follows that

$$(4s)^2 - 4(72 + s) = 4(4s^2 - s - 72)$$

is a perfect square. So $4s^2 - s - 72$ must be a perfect square. It remains to check the values of s between 11 and 24 which modulo 4 are 0 or 3, namely, $s = 11, 12, 15, 16, 19, 20, 23, 24$. For none of these values $4s^2 - s - 72$ is a perfect square.

The values of s between 1 and 10 can also be excluded, because there are no a, b, with $ab|(72 + s)$, for which $4s$ divides $a + b$; see the table below.

s	1	2	3	4	5	6	7	8	9	10
$4s$	4	8	12	16	20	24	28	32	36	40
$72 + s$	73	$2 \cdot 37$	$3 \cdot 5^2$	$2^2 \cdot 19$	$7 \cdot 11$	$2 \cdot 3 \cdot 13$	79	$2^4 \cdot 5$	3^4	$2 \cdot 41$

To complete the proof of the theorem observe that if $n = tM - d$ then

$$n \geqslant tab - a - b \geqslant ta^2 - 2a$$

in case $a \leqslant b$. Hence $(at - 1)^2 \leqslant nt + 1$ and $b \leqslant (a + n)/(ta - 1)$. Therefore, all values from 1 to 10000 which do not belong to $E(4)$ can be found with Maple as follows.

For every particular value of n from 1 to 10000 we check all the pairs (a, b) which satisfy the above inequalities for the existence of an appropriate value of d, i.e., for the divisibility of $a + b$ by some positive integer of the form $d = tuab - n$. However, $d \leqslant a + b \leqslant tab$ which means that there is only one possible such integer *d*. Take a unique integer in the interval $[1, tab]$ which equals $-n$ modulo tab. It can be expressed as $tab - n \pmod{tab}$, as in the Maple code describing our algorithm below.

```
$t := 4$: $k := 0$:
for $n$ from 1 to 10000 do $s := true$;
for $a$ from 1 by 1 while ($s$ and $(at-1)^2 \leqslant tn+1$) do $B := (a+n)/(ta-1)$;
for $b$ from $a$ by 1 while ($s$ and $b \leqslant B$) do
if $a+b \pmod{(tab - n \pmod{tab})} = 0$ then $s := false$
end; end; end;
if $s$ then $k := k+1$;
print($n$);
end; end:
print($k$):
```

As a result (in less than three seconds) we got that only 100 perfect squares and three exceptional numbers $288, 336, 4545$ less than 10000 do not lie in $E(4)$. This completes the proof of Theorem 3.1. □

Proof of Proposition 3.6: Let $p_1 < p_2 < p_3 < \ldots$ denote consecutive primes in the arithmetic progression $kt - 1$, $k = 1, 2, 3, \ldots$. By Dirichlet's theorem, the sum $\sum_{j=1}^{\infty} 1/p_j$ diverges. Thus for each $\varepsilon > 0$ we can pick $s \in \mathbb{N}$ for which $\prod_{j=1}^{s}(1 - 1/p_j) < \varepsilon/2$. Further, for each $N \geqslant P := p_1 p_2 \ldots p_s$ select a unique $k \in \mathbb{N}$ for which $kP \leqslant N < (k+1)P$. The number of positive integers $n \leqslant N$ without prime divisors in the set $\{p_1, \ldots, p_s\}$ does not exceed the number of such positive integers in the interval $[1, (k+1)P]$. The latter, by the inclusion-exclusion principle, is equal to

$$(k+1)P \prod_{j=1}^{s} \Big(1 - \frac{1}{p_j}\Big) \leqslant \frac{(k+1)P\varepsilon}{2} \leqslant \frac{(1+1/k)N\varepsilon}{2} \leqslant \frac{2N\varepsilon}{2} = N\varepsilon.$$

This implies the claim. □

Conclusions

Throughout this thesis, we have established the following results corresponding to the raised questions (see the subsection "Aims and problems"):

- The sequence
$$[\xi a^n], n = 1, 2, \dots,$$
contains infinitely many composite numbers for any $\xi > 0$ and any $a \in \{2, 3, 4, 5, 6, 3/2, 4/3, 5/4\}$.

- There exist finite sets of prime numbers of which at least one divides infinitely many numbers in the sequence
$$[\xi a^n], n = 1, 2, \dots,$$
for $a \in \{2, 3, 4, 6, 3/2, 4/3, 5/4\}$, and these sets do not depend on the number $\xi > 0$. For example, for $a = 5/4$, such a set is $\mathcal{P}(5/4) = \{2, 3, 7, 11, 13\}$. For $a = 5$, there are such sets corresponding to any particular $\xi > 0$. However, one such finite set for all $\xi > 0$ does not exist in this case.

- The sequence
$$[\xi a^n + \nu], n = 1, 2, \dots,$$
contains infinitely many composite numbers for any $\xi > 0$ and any $a \in \{7, 5/3, 7/5\}$ if $\nu = 1/2$. The same holds for $\nu = -1$, any $\xi > 0$ and $a = 6/5$. The sequence $[\xi(5/2)^n - 1 + 30k], n = 1, 2, \dots,$ contains infinitely many composite numbers for any $\xi > 0$ and any integer k . The sets of prime divisors are explicitly indicated, except for the case $a = 7$.

- For every binary linear recurrence equation
$$x_{n+1} = ax_n + bx_{n-1},$$
where $a, b \in \mathbb{Z}, (a, b) \neq (\pm 2, -1)$, there exists a corresponding binary linear recurrence sequence of integers whose two initial terms are positive and relatively prime and which consists of only composite numbers (the

absolute values of the terms are taken). For $(a, b) = (\pm 2, -1)$ such a sequence does not exist.

- Almost all positive integers belong to each of the sets $E(t)$ (and $E(1) = E(2) = \mathbb{N}$). The set $E(t)$, where $4|t$, does not contain the numbers of the form sk^2, where $s \in \mathbb{N}$ satisfies $4s|t$ and $k \in \mathbb{N}$.

References

[1] G. Alkauskas and A. Dubickas, *Prime and composite numbers as integer parts of powers,* Acta Math. Hungar., **105** (2004), 249–256.

[2] R.C. Baker and G. Harman, *Primes of the form $[c^p]$,* Math. Zeitschrift, **221** (1996), 73–81.

[3] M. Bello-Hernández, M. Benito and E. Fernández, *On Egyptian fractions,* preprint at `arXiv:1010.2035v1`, 2010.

[4] T.D. Browning and C. Elsholtz, *The number of representations of rationals as a sum of unit fractions,* Illinois J. Math. (to appear).

[5] Y. Bugeaud, *Linear mod one transformations and the distribution of fractional parts* $\{\xi(p/q)^n\}$, Acta Arith. **114** (2004), 301–311.

[6] D.A. Buell and R.H. Hudson, *On runs of consecutive quadratic residues and quadratic nonresidues,* BIT **24** (1984), 243–247.

[7] D. Cass, *Integer parts of powers of quadratic units,* Proc. Amer. Math. Soc., **101** (1987), 610–612.

[8] A. Dubickas, *Integer parts of powers of Pisot and Salem numbers,* Archiv der Math., **79** (2002), 252–257.

[9] A. Dubickas, *Prime and composite integers close to powers of a number,* Monatsh. Math., **156** (3) (2009), 271–284.

[10] A. Dubickas, *Sequences with infinitely many composite numbers,* Analytic and Probabilistic Methods in Number Theory, Palanga, 2001 (eds. A. Dubickas, A. Laurinčikas and E. Manstavičius), TEV, Vilnius (2002), 57–60.

[11] A. Dubickas, *There are infinitely many limit points of the fractional parts of powers,* Proc. Indian Acad. of Sciences (Math. Sc.), **115** (4) (2005), 391–397.

[12] C. Elsholtz and T. Tao, *Counting the number of solutions to the Erdős-Straus equation on unit fractions,* preprint at `arXiv:1107.1010v3`, 2011.

[13] L. Flatto, J.C. Lagarias, A.D. Pollington, *On the range of fractional parts* $\{\xi(p/q)^n\}$, Acta Arith., **70** (1995), 125–147.

[14] W. Forman and H.N. Shapiro, *An arithmetic property of certain rational powers,* Comm. Pure Appl. Math., **20** (1967), 561–573.

[15] R.L. Graham, *A Fibonacci-like sequence of composite numbers,* Math. Mag., **37** (1964), 322–324.

[16] S.W. Graham and C.J. Ringrose, *Lower bounds for least quadratic non-residues,* in: Analytic number theory, Proc. Conf. in Honor of Paul T. Bateman, Urbana, IL, USA, 1989, Prog Math. 85, 1990, pp.269–309.

[17] R.K. Guy, *Unsolved problems in number theory,* 3rd. ed, Springer, New-York, 2004.

[18] M. Hall, *Divisibility sequences of third order,* American J. Math., **58** (1936), 577–584.

[19] A.S. Izotov, *Second-order linear recurrences of composite numbers,* Fibonacci Quart. **40** (3) (2002), 266–268.

[20] D.E. Knuth, *A Fibonacci-like sequence of composite numbers,* Math. Mag., **63** (1990), 21–25.

[21] J.F. Koksma, *Ein mengen-theoretischer Satz über Gleichverteilung modulo eins,* Compositio Math., **2** (1935), 250–258.

[22] K. Mahler, *An unsolved problem on the powers of 3/2, J. Austral. Math. Soc.,* **8** (1968), 313–321.

[23] H.W. Mills, *A prime representing function,* Bull. Amer. Math. Soc., **53** (1947), 604.

[24] H.L. Montgomery, *Topics in multiplicative number theory,* Lecture Notes in Mathematics 227, Springer, New York, 1971.

[25] L.J. Mordell, *Diophantine equations,* Academic Press, London, New-York, 1969.

[26] J.W. Nicol, *A Fibonacci-like sequence of composite numbers,* Electronic J. Combin., **6** (1999), #R44, 6 p.

[27] C. Pisot, *Répartition (mod 1) des puissances successives des nombres rèels,* Comment. Math. Helv., **19** (1946) 153–160.

[28] A. Schinzel, *On sums of three unit fractions with polynomial denominators,* Funct. Approx. Comment. Math. **28** (2000), 187–194.

[29] W. Sierpiński, *Sur les décompositions de nombres rationale en fractions primaires,* Mathesis **65** (1956), 16–32.

[30] L. Somer, *Second-order linear recurrences of composite numbers,* Fibonacci Quart. **44** (4) (2006), 358–361.

[31] J. Šiurys, *A tribonacci-like sequence of composite numbers,* Fibonacci Quart. **49** (4) (2011), 298–302.

[32] R.C. Vaughan, *On a problem of Erdős, Straus and Schinzel,* Mathematika **65** (1970), 193–198.

[33] R.C. Vaughan, T.D. Wooley, *Waring's problem: a survey,* Number theory for the millennium, III (Urbana, IL, 2000), A. K. Peters, Natick, MA (2002), 301–340.

[34] T. Vijayaraghavan, *On the fractional parts of the powers of a number,* J. London Math. Soc., **15** (1940), 159–160.

[35] M. Vsemirnov, *A new Fibonacci-like sequence of composite numbers,* Journal of Integer Sequences, **7** (2004), Article 04.3.7, 3 p.

[36] H.S. Wilf, *Letters to the editor,* Math. Mag., **63** (1990), 284.

[37] E.M. Wright, *A prime representing function,* Amer. Math. Monthly, **58** (1951), 616–618.

[38] K. Yamamoto, *On a conjecture of Erdős,* Mem. Fac. Sci. Kyuchu Univ. Ser. A **18** (1964), 166–167.

[39] K. Yamamoto, *On the Diophantine equation* $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, Mem. Fac. Sci. Kyuchu Univ. Ser. A **19** (1965), 37–47.