VILNIUS UNIVERSITY

JONAS ŠIURYS

Linear recurrence sequences of composite numbers

Doctoral dissertation

Physical sciences, mathematics (01P)

Vilnius, 2013

The scientific work was carried out in 2009–2013 at Vilnius University.

Scientific supervisor:

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

Scientific adviser:

doc. dr. Paulius Drungilas (Vilnius University, physical sciences, mathematics – 01P)

VILNIAUS UNIVERSITETAS

JONAS ŠIURYS

Tiesinės rekurenčiosios sekos sudarytos iš sudėtinių skaičių

Daktaro disertacija

Fiziniai mokslai, matematika (01P)

Vilnius, 2013

Disertacija rengta 2009–2013 metais Vilniaus universitete.

Mokslinis vadovas:

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

Konsultantas:

doc. dr. Paulius Drungilas (Vilniaus Universitetas, fiziniai mokslai, matematika – 01P)

Contents

Notations

$\mathbb{Z}$ – the set of all positive integers

$\{x_n\}$, $n = 0, 1, \ldots$ – the sequence $x_0, x_1, x_2, \ldots$

(a, b) or $\gcd(a, b)$ – the greatest common divisor of a and b

$|z|$ – the absolute value of a complex number z

$\mathbb{F}_q$ – the Galois field of order q

$\left(\frac{a}{b}\right)$ – the Legendre symbol

$\mathscr{F}_k$ – the free abelian group of rank k

$S_k(x_0, x_1, \ldots, x_{k-1})$ – the k-step Fibonacci-like sequence

$\mathfrak{S}_k(N)$ – the set of triples (p_i, m_i, r_i)

1 Introduction

1.1 Linear recurrence sequence

The main objects studied in this thesis are linear recurrence sequences of composite numbers. The linear recurrence sequence $\{x_n\}$, $n = 0, 1, \ldots$ is defined by the linear recurrence equation

$$x_n = a_{d-1}x_{n-1} + a_{d-2}x_{n-2} + \cdots + a_0 x_{n-d}, \quad n \geqslant d,$$

where $a_{d-1}, a_{d-2}, \ldots, a_0$ are some constants and d is a positive integer. If the coefficient $a_0 \neq 0$, then the integer $d > 0$ is called *the order* of the sequence $\{x_n\}$, $n = 0, 1, \ldots$. The initial terms $x_0, x_1, \ldots, x_{d-1}$ can be taken to be any values, but then every successive term is determined uniquely. In this thesis we are interested in integer sequences, so the coefficients a_i and the initial values x_i are integers for $i = 0, 1, \ldots, d-1$.

To avoid confusion with zero and one, we call a non-negative integer n a composite number if $n \neq 0, 1$ and n is not a prime number.

1.2 Problems and results

This section contains a brief summary of problems examined in this doctoral dissertation.

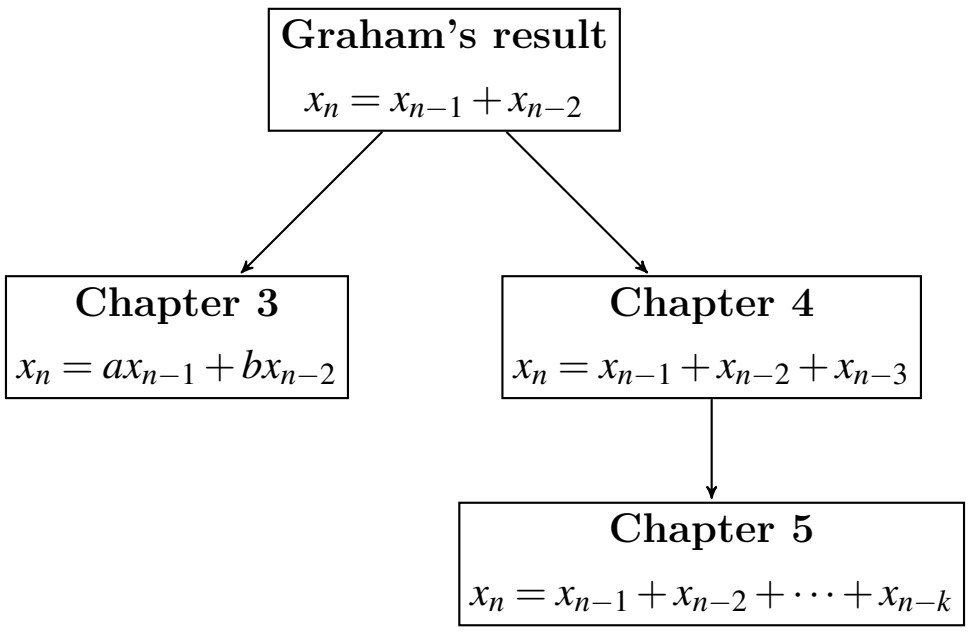
- In Chapter 3 we will study the second order (binary) linear recurrence sequences. Let $(a, b) \in \mathbb{Z}^2$, where $b \neq 0$ and $(a, b) \neq (\pm 2, -1)$. We will prove that then there exist two positive relatively prime composite integers x_0, x_1 such that the sequence given by $x_n = ax_{n-1} + bx_{n-2}$, $n = 2, 3, \ldots$, consists of composite terms only, i.e., $|x_n|$ is a composite integer for each $n \in \mathbb{N}$. In the proof of this result we will use certain covering systems, divisibility sequences and, for some special pairs

$(a, \pm 1)$, computer calculations. It extends the result of Graham [15] who proved this theorem in the special case of the Fibonacci-like sequence, where $(a,b) = (1,1)$.

- Chapter 4 is devoted for the special case of the third order linear recurrence sequences, i.e., tribonacci-like sequences. We find three positive integers x_0, x_1, x_2 satisfying $\gcd(x_0, x_1, x_2) = 1$ such that the sequence $\{x_n\}$, $n = 0, 1, \ldots$ given by the recurrence relation $x_n = x_{n-1} + x_{n-2} + x_{n-3}$ for $n \geqslant 3$ consists of composite numbers only. The initial values are $x_0 = 99202581681909167232$, $x_1 = 67600144946390082339$, $x_2 = 139344212815127987596$. This is also a natural extension of a similar result of Graham [15] for the Fibonacci-like sequence.

- In Chapter 5 we will generalize results of Chapter 4. We will prove that for each positive integer k in the range $2 \leqslant k \leqslant 10$ and for each positive integer $k \equiv 79 \pmod{120}$ there is a k-step Fibonacci-like sequence of composite numbers and will give some examples of such sequences.

The schematic diagram of the evolution of the results:



1.3 Methods

In this thesis one of the most often used and very powerful tool is a *covering system* invented by P. Erdős [11] in 1950. A covering system is a finite set of residue classes whose union covers all the integers, i.e., every integer n belongs to one of the residue classes.

Let $\{x_n\}, n = 0, 1, 2\ldots$ be a linear recurrence sequence of composite numbers. Our goal is to find a covering system with the following property:

- if m is the element of the residue class R then x_m is divisible by the prime number p_R which depends only on R.

If such covering system exists then we have that every term of the sequence $\{x_n\}$ is divisible by some prime.

The investigation of recurrence sequences using covering system requires computer algorithms. We first construct the appropriate covering system satisfying some properties. It is a difficult task if the number of residue classes is large. The second task is to solve the system of simultaneous congruences using Chinese Reminder Theorem (CRT). The solution usually is huge. These algorithms were implemented using a computer algebra system PARI/GP [37].

In order to establish the results on binary linear recurrence sequence, we will use the properties of *divisibility sequences*, some elements of the field theory, also Dirichlet's theorem on prime numbers in arithmetic progression.

1.4 Actuality and Applications

Prime and composite numbers play a very important role in modern cryptography. Many cryptographic methods are based on composite number problem, i.e., if for a given positive integer n there exists a nontrivial divisor. The security of the system depends on how much time we have used to factor the large composite number. Any research on prime and composite numbers can be useful in developing cryptographic methods.

The relation of the results of this doctoral dissertation and unsolved number theory problems is discussed in Literature review (Chapter 2).

1.5 Originality

The results presented in this doctoral dissertation are new and original. The main results have been published in the international journals (see Section 1.7). Since the results of Chapter 3 are based on the article [10], they were presented in my co-author's Novikas [26] doctoral dissertation in 2012.

The methods used in Chapter 4 and Chapter 5 for construction of composite number sequences are original and can be adapted in various cases.

1.6 Dissemination of results

The results of this thesis were presented in the following conferences:

- *27th Journées Arithmétiques*, June 27 – July 1, 2011, Vilnius;
- *Fifteenth International Conference on Fibonacci Numbers and Their Applications*, June 25 – 30, 2012, Eger, Hungary.

They were also presented in the number theory seminar of Department of Probability Theory and Number Theory on May 5, 2013.

1.7 Publications

1.7.1 Principal publications

The results of the doctoral dissertation can be found in three research papers. All of them were published in three foreign mathematical journals.

1. A. Dubickas, A. Novikas, and J. Šiurys, *A binary linear recurrence sequence of composite numbers*, Journal of Number Theory **130** (2010), 1737–1749.
2. J. Šiurys, *A tribonacci-like sequence of composite numbers*, Fibonacci Quarterly **49** (2011), no. 4, 298–302.
3. J. Šiurys, *A linear recurrence sequence of composite numbers*, LMS Journal of Computation and Mathematics **15** (2012), 360–373.

1.7.2 Conference abstracts

1. A. Novikas, and J. Šiurys, *A binary linear recurrence sequence of composite numbers*, 27th Journées Arithmétiques, June 27 – July 1, 2011, Vilnius, Lithuania: programme and abstract book. Vilnius, Vilniaus universitetas, 2011. Available online at http://atlas-conferences.com/cgi-bin/abstract/cbbv-22.

2. J. Šiurys, *A linear recurrence sequence of composite numbers*, Fifteenth International Conference on Fibonacci Numbers and Their Applications, June 25 – 30, 2012, Eger, Hungary: abstract book.

1.8 Acknowledgments

First of all, I would like to thank my advisor, Professor Artūras Dubickas, who proposed many interesting problems. Without his guidance this dissertation would not have been possible.

I wish to express my sincere gratitude to Dr. Paulius Drungilas for his constant encouragement and support on my scientific and teaching work.

I am grateful to Dr. Jonas Jankauskas, my friend and colleague. It is my great honor to know him. Jonas' devotion to his work is a perfect example of being a productive mathematician.

It is also my duty to record my thankfulness to Dr. Hamletas Markšaitis who gives the inspirational seminars.

I am grateful to Professor Ramūnas Garunkštis for his unexpected point of view to mathematical problems.

I would like to thank Dr. Romualdas Kašuba for his great sense of humor and many stories he told me.

I thank my friends and colleagues at Vilnius University: Mindaugas Skujus, Paulius Šarka, Gražvydas Šemetulskis, Albertas Zinevičius, Dr. Aivaras Novikas, Dr. Justas Kalpokas, Dr. Andrius Grigutis, Svajūnas Sajavičius, Edgaras Mielkaitis, Emilija Bernackaitė, Donata Puplinskaitė, Jurgita Markevičiūtė, Dr. Kristina Kaulakytė, Vytautė Pilipauskaitė and Ieva Grublytė. I really enjoy working with you.

I wish to express my sincere thanks to my parents for everything they did for me. Also I thank my brother Paulius and my sister Monika for the great time, my brother Andrius for many outstanding parties. Special

thanks to my sister Regina for her support and the positive influence. I am thankful to my good friend Robertas and my godson Jonas who never asked what my dissertation was about.

I am extremely grateful and indebted to my godfather Juozas Šiurys and my uncle Petras Šiurys for their persistent help.

I owe particular thanks to my mathematics teachers Kazys Šikšnius and Leonas Narkevičius. I am also grateful to Vytas Rutkauskas - intellectual and erudite - for his encouragement.

Finally, I thank to: Viktorija and Bernardas Prušinskai for the huge support in critical moments; Milda Prušinskaitė and Mantas Janušonis for the kind hospitality; Nerija Beniušytė and Steponas Kvietkauskas; Daiva Pliusnytė; Giedrė Rutkauskaitė; Mindaugas and Vaida Laganeckai; Laura Kinkaitė for valuable remarks about this dissertation; Barbora Drąsutytė for many advices on my teaching work; Julija Vasiliauskaitė; my former roommates Kęstutis Strazdauskas and Andrius Stankevičius; Vitalija Stepušaitytė and Inga Paškevičiūtė for the experience in the film production; Tomas Čerkasas for all his ideas and help in computations; all members of ultimate teams MIXtūra and KossMix (including Julija Grigorjevaitė).

2 Literature review

2.1 Primes and composite numbers in integer sequences

Many interesting questions about primes in integer sequences remain unsolved. For instance, it is not known if there are infinitely many primes of the form n^2+1, $n \in \mathbb{N}$. Although almost all positive integers are composite, for some quite natural sequences, for example, $[r^n]$, where $r > 1$ is a rational non-integer number and n runs through the set of positive integers $\mathbb{N}$, it is not even known if they contain infinitely many composite numbers or not (see Problem E19 in [16]). The latter question is only settled for $r = 3/2$, $r = 4/3$ in [13] and for $r = 5/4$ in [9]. See also [1], [2] for some related problems.

A Mersenne prime is a prime number of the form $M_p = 2^p - 1$ (p must be a prime too). There are known only 48 Mersenne primes. The largest known Mersenne prime $M_{57,885,161}$ was found by Great Internet Mersenne Prime Search (GIMPS) [14] on January 25, 2013. It is also the largest known prime number. Lenstra [21], Pomerance [31], and Wagstaff [40] have conjectured that there is an infinite number of Mersenne primes. However, it is not even known whatever there are infinitely many composite numbers of the form $2^p - 1$ (with p a prime number).

2.2 Covering system

In 1934, Romanoff [32] proved that the set of positive odd integers which can be expressed in the form $2^n + p$, where p is a prime and n is nonnegative integer, has a positive asymptotic density. So, he asked Erdős if there are infinitely many odd integers not of the form $2^n + p$. This led Erdős to the

concept of the *covering system*. 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 $i = 1, \ldots, t$, 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 $1 \leqslant i \leqslant t$. In 1950, Erdős [11] constructed an arithmetic progression of odd integers not of the form $2^n + p$. Using similar methods many results were proven. Cohen and Selfridge [7] constructed a odd integer which is neither the sum nor the difference of two primes powers. Sun [36] extended their work and constructed an arithmetic progression or such numbers. Luca and Stănică [22] founded a infinite sequence of Fibonacci numbers that are not sums of two prime powers. See [4], [5], [8], [29], [42] for other related results.

Another term closely related to the covering system is *a covering set*. For the given sequence, a covering set is the finite set of prime numbers such that every member in the sequence is divisible by at least one prime of the set.

In 1960, Sierpiński [33] proved that there are infinitely many positive integers k (Sierpiński numbers) such that $k \cdot 2^n + 1$ is composite for each $n \in \mathbb{N}$. Sierpiński included in his paper the proof of Schinzel that a covering set of the sequence $k \cdot 2^n + 1$ must also be the covering set of the sequence $2^n + k$, where k is fixed positive integer. Two years later, Selfridge (unpublished) showed that 78557 is a Sierpiński number, i.e., $78557 \cdot 2^n + 1$ is composite for each $n \in \mathbb{N}$. The covering set for the sequence $78557 \cdot 2^n + 1$ is $\{3, 5, 7, 13, 19, 37, 73\}$. However, after extensive computer calculation it has not yet been proven that 78557 is the smallest Sierpiński number. There are six numbers which have not been eliminated as possible Sierpiński numbers: 10223, 21181, 22699, 24737, 55459, and 67607 (see, e.g., [16], Section B21, [27], [28]).

2.3 Fibonacci-like sequence

The sequence of Fibonacci numbers is a well known sequence defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}, \quad n = 2, 3, 4 \ldots,$$

with initial values $F_0 = 0$ and $F_1 = 1$.

If Fibonacci number F_k is a prime then k must also be a prime. Unfortunately, the converse is not always true. Moreover, it is not known if there are infinitely many Fibonacci primes.

Graham [15] investigated the sequence defined by the same recurrence relation as Fibonacci numbers but with different starting values, namely the sequence

$$x_n = x_{n-1} + x_{n-2}, \quad n = 2, 3, 4 \ldots,$$

with some initial values x_0 and x_1. This sequence is called *a Fibonacci-like sequence*. If there is a prime p which divides x_0 and x_1 then p divides every term of the Fibonacci-like sequence and in this case there are only finite number of primes in the sequence $\{x_n\}$, $n = 0, 1, 2 \ldots$. In 1964, Graham found two relatively prime positive integers x_0, x_1 such that the sequence

$$x_n = x_{n-1} + x_{n-2}, \quad n = 2, 3, 4 \ldots,$$

contains only composite numbers, i.e., x_n is composite for each $n \in \mathbb{N}$. Graham's pair (x_0, x_1) was

$$(331635635998274737472200656430763,$$
$$151002891108840197118959030549878 5).$$

Actually, he made a calculation mistake in the paper, but his reasoning was correct. The other results are based on changing the covering system.

Knuth [20] (1990) corrected Graham's mistake and found the smaller pair

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

Wilf [41] (1990) slightly refined Knuth's computation and found the pair

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

This was further reduced by Nicol [24] (1999) 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 [38] (2004)

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

All these results are based on the fact that the Fibonacci sequence is a *divisibility sequence,* i.e., $F_n | F_m$ whenever $n|m$, and on finding a covering system with the property that there exist distinct prime numbers p_i such that $p_i | F_{m_i}$ for $i = 1, \ldots, t$. However, for most linear recurrences of order $d \geqslant 3$, there are no divisibility sequences satisfying them (see, e.g., the paper of Hall [17]).

2.4 Binary linear recurrence sequences

Let k be a positive odd integer and $\{x_n\}$, $n = 0, 1, 2, \ldots$, be a sequence defined by a recurrence relation

$$x_n = 3x_{n-1} - 2x_{n-2}, \quad n = 2, 3, 4, \ldots,$$

with initial values $x_0 = k+1$, $x_1 = 2k+1$. If x_n is composite for all n, then k is a Sierpiński number.

The preceding observation and Graham's problem lead to a more general second order linear recurrence sequences.

Let a and b be two relatively prime integers and let $\{x_n\}$, $n = 0, 1, 2 \ldots$, be a sequence given by some initial values x_0, x_1 and the binary linear recurrence

$$x_n = ax_{n-1} + bx_{n-2}$$

for $n = 2, 3, 4, \ldots$. Izotov [18] proved what if a and b satisfy some conditions then there exist two relatively prime positive integers x_0, x_1 such that $|x_n|$ is a composite integer. Somer [35] completed Izitov's proof. He used deep results of Bilu et al. [3], Choi [6], and also the theorem of Parnami and Shorey [30] in his paper.

2.5 Tribonacci-like recurrence sequences

Let $S(x_0,x_1,x_2) = (x_n)_{n=0}^{\infty}$ be a sequence of integers satisfying the ternary recurrence relation

$$x_{n+1} = x_n + x_{n-1} + x_{n-2} \tag{2.1}$$

for $n = 2, 3, 4, \ldots$. The values of x_0, x_1 and x_2 determine the sequence $S(x_0,x_1,x_2)$. If $x_0 = 0$, $x_1 = 0$ and $x_2 = 1$, then $S(x_0,x_1,x_2)$ is a classical tribonacci sequence. This sequence has been examined by many authors. See, for example, [19], [25], [39].

2.6 k-step Fibonacci-like sequence

For each integer $k \geqslant 2$ one can define a k-step Fibonacci-like sequence, i.e., the sequence of integers x_n, $n = 0, 1, 2, \ldots$, satisfying the following relation

$$x_n = \sum_{i=1}^{k} x_{n-i}$$

for $n = k$, $k+1$, $k+2 \ldots$. Since the values of $x_0, x_1, \ldots, x_{k-1}$ determine the k-step Fibonacci-like sequence we denote it by $S_k(x_0, x_1, \ldots, x_{k-1})$. The terms of the sequence $S_k(0,0,\ldots,0,1)$ is well known Fibonacci k-step numbers.

Flores [12] developed the calculation of Fibonacci k-step numbers without recursion. Noe and Post [25] showed that Fibonacci k-step numbers are nearly devoid of primes in first 10000 terms for $k \leqslant 100$.

3 Binary linear recurrence sequences

3.1 Introduction

In this chapter our goal is to prove the following theorem:

Theorem 3.1. *Let $(a,b) \in \mathbb{Z}^2$ and let $\{x_n\}$, $n = 0, 1, 2 \ldots$, be a sequence given by some initial values x_0, x_1 and the binary linear recurrence*

$$x_n = ax_{n-1} + bx_{n-2} \tag{3.1}$$

for $n = 2,3,4,\ldots$. Suppose that $b \neq 0$ and $(a,b) \neq (2,-1),(-2,-1)$. Then there exist two relatively prime positive integers x_0, x_1 such that $|x_n|$ is a composite integer for $n = 0, 1, 2, \ldots$.

As it was mentioned in Section 2.4, the special case of Theorem 3.1 was proved by Izotov [18]. He added three conditions for the coefficients a and b of the sequence 3.1:

1) $a^2 + 4b > 0$;

2) $a > 2$;

3) a has an odd prime divisor p.

Izotov gave explicit initial values x_0 and x_1 such that $|x_n|$ is a composite integer for each $n \in \mathbb{N}$. For even n, x_n had an algebraic decomposition while, for odd n, x_n had a covering set $P = \{p\}$.

Somer [35] proved Theorem 3.1 in general case. However, he proved only the existence of such sequences. Our proof is more constructive. In some special cases we will give exact initial values.

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

$$x^2 - ax - b = (x-\alpha)(x-\beta) = 0 \tag{3.2}$$

with discriminant

$$D := (\alpha-\beta)^2 = a^2 + 4b. \tag{3.3}$$

By (3.2) and (3.3), we have $\alpha - \beta = \sqrt{D}$, $\alpha\beta = -b$ and $\alpha + \beta = a$. It is easily seen that the nth term of the sequence $\{x_n\}$, $n = 0, 1, 2, \ldots$, defined in (3.1) is given by

$$x_n = \frac{-x_0\beta + x_1}{\alpha-\beta}\alpha^n + \frac{x_0\alpha - x_1}{\alpha-\beta}\beta^n \tag{3.4}$$

provided that $\alpha \neq \beta$, i.e., $D \neq 0$. For $\alpha = \beta$, i.e., $D = 0$ we have

$$x_n = \alpha^n x_0 + (x_1 - \alpha x_0) n \alpha^{n-1} \tag{3.5}$$

for each nonnegative integer n (see for instance [23, Ch. 5] for more details).

Our plan of the proof of Theorem 3.1 can be described as follows. In Section 3.2 we shall examine the following three cases:

(i) $D = 0$;

(ii) $a = 0$;

(iii) $b = -1$, $|a| \leqslant 2$.

Also, in Section 3.2 we show that the condition of the theorem $(a,b) \neq (\pm 2, -1)$ is necessary.

In case $|b| \geqslant 2$ we shall take x_1 divisible by $|b|$. Then, by (3.1), x_2 and so, by induction, all x_n, where $n \geqslant 1$, are 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 $n \geqslant 2$, so that $|x_n|$ is composite. This case, $|b| \geqslant 2$, will be examined in Section 3.3. Finally, in Section 3.4 we shall describe the method of covering systems and prove the theorem for $|b| = 1$.

3.2 Several simple special cases

In this section we shall consider three special cases: (i) $D = 0$; (ii) $a = 0$; (iii) $b = -1$, $|a| \leqslant 2$.

Case (i). Since $D = a^2 + 4b = 0$, the solution of the linear recurrence (3.1) is given by (3.5). 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 and select $x_0 := p^2$, $x_1 := |\alpha| q^2$. Then x_1, x_2 are composite and $\gcd(x_0, x_1) = 1$. Furthermore, writing $|\alpha| = \alpha\varepsilon$, where $\varepsilon = \pm 1$, by (3.5), we obtain

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

for each $n \geqslant 0$. Clearly, $|x_n|$ is divisible by $|\alpha^2| = |b| \geqslant 4$ for $n \geqslant 2$, so $|x_n|$ is composite for each $n \in \mathbb{N}$, unless

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

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

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

is greater than 0 and smaller than 1, a contradiction. If $\varepsilon = 1$, then $nq^2 = (n-1)p^2$ implies $n = \ell p^2$ and $n - 1 = \ell q^2$ with $\ell \in \mathbb{Z}$. Hence $1 = n - (n-1) = \ell(p^2 - q^2)$, which is impossible, because $|p^2 - q^2| \geqslant |3^2 - 2^2| = 5 > 1$.

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. Moreover, it is easy to see that in this case the sequence $\{|x_n|\}$, $n = 0, 1, 2, \ldots$, where x_0, x_1 are composite and $\gcd(x_0, x_1) = 1$, contains infinitely many prime numbers. Indeed, by (3.5),

$$x_n = (\varepsilon x_0 + n(x_1 - \varepsilon x_0))\varepsilon^{n-1}$$

for each $n \geqslant 1$ and $\varepsilon = \pm 1$. Since x_0 and x_1 are relatively prime positive composite integers, we must have $u := \varepsilon x_0 \neq 0$ and $v := x_1 - \varepsilon x_0 \neq 0$. Moreover, $\gcd(x_0, x_1) = 1$ implies $\gcd(u, v) = 1$. So, by Dirichlet's theorem on prime numbers in arithmetic progressions, we conclude that $|x_n| = |u + nv|$ is a prime number for infinitely many $n \in \mathbb{N}$. This not only completes the

proof of Theorem 3.1 in the case $D = 0$, but also shows that the condition $(a,b) \neq (\pm 2, -1)$ is necessary.

Case (*ii*). For $a = 0$, we have $x_n = bx_{n-2}$ for $n \geqslant 2$. Let $p, q > |b|$ be two distinct primes. Selecting $x_0 := p^2$ and $x_1 := q^2$, we have $\gcd(x_0, x_1) = 1$. Furthermore, $x_{2k} = p^2 b^k$ and $x_{2k+1} = q^2 b^k$ for each $k \geqslant 0$, 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 $x_n = -x_{n-1} - x_{n-2}$ satisfying the condition of the theorem is, for example, the following periodic sequence:

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

For $(a,b) = (1,-1)$, we have the recurrence $x_n = x_{n-1} - x_{n-2}$. Now, the periodic sequence

$$16, 25, 9, -16, -25, -9, 16, 25, 9, -16, -25, -9, \ldots$$

satisfies the conditions of the theorem.

3.3 The case $|b| \geqslant 2$

Lemma 3.2. *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. 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 $4kd + 1$, $k = 1, 2, \ldots$.) 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 3.3. *Let u_i, v_i, $i = 1, 2, \ldots, p-1$, 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 $i = 1, \ldots, p-1$.*

Proof. 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

$$uu_i + vv_i = s. \tag{3.6}$$

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 (3.6). By the same argument, (3.6) 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 (3.6) has a unique solution in v. This proves the claim.

As i runs through $1, \ldots, p-1$, we have $p-1$ equations (3.6) 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 $i = 1, \ldots, p-1$. □

Lemma 3.4. *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*

$$s_n := \frac{(a+\sqrt{D})^n - (a-\sqrt{D})^n}{2\sqrt{D}}, \tag{3.7}$$

$n = 0, 1, 2, \ldots$, is purely periodic modulo p with period $p-1$. Also, no two consecutive elements of the sequence $\{s_n\}$, $n = 0, 1, 2, \ldots$, can be zeros modulo p.

Proof. We set $s_0 = 0$. Now, let $n \geqslant 1$. By (3.7), 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

$$s_n \equiv \frac{(a+c)^n - (a-c)^n}{2c} \pmod{p}. \tag{3.8}$$

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

Lemma 3.5. *Let $\{x_n\}$, $n = 0, 1, 2, \ldots$, be a sequence of integers given by (3.1), $D = a^2 + 4b \neq 0$, $b \neq 0$, and let δ be a fixed real number. Then $x_n = \delta b$ for some $n \geqslant 1$ if and only if*

$$x_0 \frac{s_{n-1}}{2^{n-2}} + \frac{x_1}{b} \frac{s_n}{2^{n-1}} = \delta,$$

where s_n is given by (3.7).

Proof. The roots α and β of the characteristic equation (3.2) are distinct, so, by (3.4) and $\alpha-\beta=\sqrt{D}$, we have

$$x_n\sqrt{D}=(-x_0\beta+x_1)\alpha^n+(x_0\alpha-x_1)\beta^n \tag{3.9}$$

for each $n\geqslant 0$. Since $2\alpha=a+\sqrt{D}$ and $2\beta=a-\sqrt{D}$, using (3.7), we find that $\alpha^n-\beta^n=2^{1-n}\sqrt{D}s_n$. Since $\alpha\beta=-b$, equality (3.9) yields

$$x_n\sqrt{D}=x_1(\alpha^n-\beta^n)-x_0\alpha\beta(\alpha^{n-1}-\beta^{n-1})=x_1 2^{1-n}s_n\sqrt{D}+x_0 b2^{2-n}s_{n-1}\sqrt{D}.$$

Hence $x_n=x_0b2^{2-n}s_{n-1}+x_1 2^{1-n}s_n$, because $D\neq 0$. It follows that equality $x_n=\delta b$ is equivalent to

$$\delta=x_0\frac{s_{n-1}}{2^{n-2}}+\frac{x_1}{b}\frac{s_n}{2^{n-1}},$$

as claimed. □

Lemma 3.6. *Let* $\{x_n\}, n=0,1,2,\ldots,$ *be a sequence of integers given by* (3.1)*, where* $a\neq 0$ *and* $D>0$*. Then, for each* $K>0$ *and each* x_0*, there is a constant* $\lambda(K,\alpha,\beta,x_0)>0$ *such that by selecting the two first terms of the sequence* (3.1) *as* x_0 *and* $x_1>\lambda(K,\alpha,\beta,x_0)$ *we have* $|x_n|>K$ *for each* $n\geqslant 1$*.*

Proof. 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 (3.9), using several times the triangle inequality, for $n\geqslant 1$, we obtain

$$\begin{aligned}
|x_n|\sqrt{D} &\geqslant |(-x_0\beta+x_1)\alpha^n|-|(x_0\alpha-x_1)\beta^n| \\
&= |bx_0+x_1\alpha||\alpha|^{n-1}-|-bx_0-x_1\beta||\beta|^{n-1} \\
&\geqslant (|bx_0+x_1\alpha|-|bx_0+x_1\beta|)|\alpha|^{n-1} \\
&\geqslant (|x_1\alpha|-|bx_0|-|bx_0|-|x_1||\beta|)|\alpha|^{n-1} \\
&= (|x_1|(|\alpha|-|\beta|)-2|bx_0|)|\alpha|^{n-1}.
\end{aligned}$$

Since $|\alpha|^{n-1}\geqslant 1$ for $n\geqslant 1$, the last expression is greater than $K\sqrt{D}$ provided that $|x_1|(|\alpha|-|\beta|)>2|bx_0|+K\sqrt{D}$. So the lemma holds with

$$\lambda(K,\alpha,\beta,x_0):=\frac{2|bx_0|+K\sqrt{D}}{|\alpha|-|\beta|} \tag{3.10}$$

when $|\alpha| > |\beta|$. Evidently, the constants b, D appearing in the right hand side of (3.10) depend on α, β too, because $b = -\alpha\beta$ and $D = a^2 + 4b = (\alpha - \beta)^2$, by (3.2), (3.3). □

Lemma 3.7. *Let $a_0 \geqslant 0$ and $b_0, b_1 \geqslant 1$ be integers such that no prime number p divides the three numbers a_0, b_0, b_1. Then, for each $K > 0$, there exists an integer $k_0 > K$ such that $b_0 k_0 + a_0$ is a composite integer relatively prime to b_1.*

Proof. The lemma is trivial if $a_0 = 0$. Assume that $a_0 \geqslant 1$. Set $t := \gcd(b_0, a_0)$. By the condition of the lemma, t is relatively prime to b_1. By Dirichlet's theorem about prime numbers in arithmetic progressions, there is a $t_0 \in \mathbb{N}$ such that $(b_0/t)t_0 + a_0/t$ is a prime number greater than b_1. Then $b_0 t_0 + a_0 = t((b_0/t)t_0 + a_0/t)$ is relatively prime to b_1. This implies that, for any $s \in \mathbb{N}$, the number

$$b_0 b_1 s + b_0 t_0 + a_0 = b_0(b_1 s + t_0) + a_0$$

is relatively prime to b_1. Of course, there are infinitely many $s \in \mathbb{N}$ for which the number $b_0 b_1 s + b_0 t_0 + a_0$ is composite. It remains to take one of those $s \in \mathbb{N}$ for which $k_0 := b_1 s + t_0 > K$. □

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 3.2 to $d := -D$ and $\ell := |b|$. Then, by Lemma 3.2, there exist a positive integer c and three distinct odd primes p, q, r such that pqr divides $-D + c^2$ and

$$\gcd(pqr, |b|c) = 1. \tag{3.11}$$

Our aim is to choose two composite relatively prime positive integers x_0, x_1 so that $|b|$ divides x_1 and $x_n \notin \{0, b, -b\}$ for each $n \geqslant 1$. Then $|x_0| = x_0$ and $|x_1| = x_1$ are composite. Also, using (3.1), by induction on n we see that $|b|$ divides x_n for each $n \geqslant 2$. Since $x_n \notin \{0, b, -b\}$ for $n \geqslant 2$ and $|b|$ divides x_n for $n \geqslant 2$, we must have $|x_n| > |b|$ for each $n \geqslant 2$. Hence $|x_n|$ is a composite integer for every $n \geqslant 2$ too.

For a contradiction, assume that, for some $n \geqslant 1$, $x_n = \delta b$ with $\delta \in$

$\{0,1,-1\}$. Then, by Lemma 3.5, we have

$$x_0\frac{s_{n-1}}{2^{n-2}}+x_1'\frac{s_n}{2^{n-1}}=\delta, \tag{3.12}$$

where $x_1':=x_1/b$ and $n\in\mathbb{N}$. Firstly, let us choose x_0, x_1' modulo p so that

$$2x_0s_{n-1}+x_1's_n\neq 0, \quad n\in\mathbb{N}. \tag{3.13}$$

This is possible by combining Lemma 3.4 with Lemma 3.3. Indeed, by Lemma 3.4, the sequence $s_n \pmod p$, $n=0,1,2,\ldots$, is purely periodic with period $p-1$. So, by Lemma 3.3 applied to the pairs $(2s_0,s_1),(2s_1,s_2),\ldots,(2s_{p-2},s_{p-1})\in\mathbb{F}_p^2$ and $s=0$, we conclude that there are $x_0,x_1'\in\mathbb{F}_p$, not both zeros in $\mathbb{F}_p$, such that (3.13) holds.

Next, we shall choose $x_0,x_1'\in\mathbb{F}_q$ so that

$$2x_0s_{n-1}+x_1's_n\neq 2^n, \quad n\in\mathbb{N}, \tag{3.14}$$

in $\mathbb{F}_q$. As above, by Lemma 3.4, the sequence $s_n2^{-n} \pmod q$, $n=0,1,2,\ldots$, where 2^{-n} is the inverse of 2^n in $\mathbb{F}_q$, is purely periodic with period $q-1$. By Lemma 3.3 applied to $s=1$ and the pairs $(s_0,s_12^{-1}),(s_12^{-1},s_22^{-2}),\ldots,(s_{q-2}2^{-(q-2)},s_{q-1}2^{-(q-1)})\in\mathbb{F}_q^2$, we conclude that there are $x_0,x_1'\in\mathbb{F}_q$, not both zeros, such that (3.14) holds. By the same argument, there are $x_0,x_1'\in\mathbb{F}_r$, not both zeros, such that

$$2x_0s_{n-1}+x_1's_n\neq -2^n, \quad n\in\mathbb{N}, \tag{3.15}$$

in $\mathbb{F}_r$.

By the Chinese remainder theorem, combining (3.13), (3.14), (3.15), we see that there exist two congruence classes $a_0 \pmod{pqr}$ and $a_1 \pmod{pqr}$ such that for any integers x_0 and x_1' that belong to the first and the second class, respectively, equality (3.12) does not hold for $n\in\mathbb{N}$. Furthermore, by Lemma 3.3, each prime number p,q,r divides at most one of the integers a_0,a_1. It remains to select $k_0,k_1\in\mathbb{Z}$ so that $x_0=pqrk_0+a_0$ and $x_1=bx_1'=b(pqrk_1+a_1)$ are two composite relatively prime positive integers. Take $k_1\in\mathbb{Z}$ such that $|pqrk_1+a_1|>1$, $bk_1>0$. Then $x_1>0$ is a composite number. Furthermore, no prime number divides the three numbers pqr, a_0 and x_1, because the primes p,q,r do not divide $|b|$, by (3.11), and if, say,

$p|a_0$ then p does not divide $pqrk_1 + a_1$. Hence, by Lemma 3.7 applied to the triplet $b_0 := pqr$, a_0, $b_1 := x_1$, we may select $k_0 \in \mathbb{N}$ so that $x_0 = pqrk_0 + a_0$ is a composite integer relatively prime to x_1. 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_0, x_1 such that $|b|$ divides x_1 and show that this choice leads to $x_n \notin \{0, b, -b\}$ for each $n \geqslant 2$. If $|\alpha| = |\beta|$, then $\alpha = -\beta$, so $a = \alpha + \beta = 0$. This case is already settled in Section 3.2. Assume next that $|\alpha| \neq |\beta|$. Take $x_0 := p^2$ and $x_1 := b^2 q$, 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 (3.10). Then, by Lemma 3.6, $|x_n| > |b|$ for $n \geqslant 2$. This completes the proof of Theorem 3.1 in case $|b| \geqslant 2$.

3.4 Divisibility sequences, covering systems and the case $|b| = 1$

We remind the reader once again that a sequence of rational integers $\{v_n\}$, $n = 0, 1, 2, \ldots$, is called a *divisibility sequence* if v_r divides v_s whenever r divides s. Assume that the roots α, β of the characteristic equation (3.2) are distinct $\alpha \neq \beta$. Then

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta} \in \mathbb{Z}, \tag{3.16}$$

$n = 0, 1, 2, \ldots$, is a divisibility sequence. Indeed, if $r|s$ 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 $\{x_n\}$, $n = 0, 1, 2, \ldots$, is a sequence given by the linear recurrence (3.1) then one can consider a corresponding divisibility sequence, by selecting $u_0 := 0$, $u_1 := 1$. This sequence is called the *Lucas sequence of the first kind*.

From (3.1) and (3.16) one can calculate the terms of the Lucas sequence

as follows:

$$\begin{aligned}
u_2 &= au_1 + bu_0 = a,\\
u_3 &= au_2 + bu_1 = a^2 + b,\\
u_4 &= au_3 + bu_2 = a(a^2+b) + ba = a(a^2+2b),\\
u_6 &= u_3(\alpha^3+\beta^3) = u_3((\alpha+\beta)^3 - 3\alpha\beta(\alpha+\beta)) = a(a^2+b)(a^2+3b),\\
u_{12} &= u_6(\alpha^6+\beta^6) = u_6((\alpha^3+\beta^3)^2 - 2(\alpha\beta)^3)\\
&= a(a^2+b)(a^2+2b)(a^2+3b)(a^4+4a^2b+b^2).
\end{aligned}$$

To obtain the last equality we used the identity

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

Lemma 3.8. *If $b=-1$ and $|a| \geqslant 4$ then there exist five distinct prime numbers p_i, $i=1,\ldots,5$, such that $p_1|u_2$, $p_2|u_3$, $p_3|u_4$, $p_4|u_6$ and $p_5|u_{12}$.*

Proof. 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, $i=1,\ldots,4$. 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 $p_5 \neq p_3$. □

One can easily check that Lemma 3.8 does not hold for $|a| = 3$. The next lemma is very similar to that above.

Lemma 3.9. *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. 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 $p_5\neq p_3$. □

To illustrate Lemma 3.9, 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 3.9 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

$$\begin{array}{llllll} 0 & (\mathrm{mod}\ 2), & 0 & (\mathrm{mod}\ 3), & 1 & (\mathrm{mod}\ 4), \\ 5 & (\mathrm{mod}\ 6), & 7 & (\mathrm{mod}\ 12). & & \end{array} \tag{3.17}$$

Lemma 3.10. *Let $r_i \pmod{m_i}$, $i=1,\dots,t$, be a covering system, and let $\{u_n\}$,*
$n=0,1,2,\dots$, be a divisibility sequence given by $u_0:=0$, $u_1:=1$ and $u_n=au_{n-1}+bu_{n-2}$ 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_0,x_1 such that each $|x_n|$, $n=0,1,2,\dots$, where x_n is a sequence defined in (3.1)*, is a composite number.*

Proof. By the Chinese remainder theorem, there exist $s,l\in\mathbb{Z}$ satisfying

$$\begin{aligned} s &\equiv u_{m_i-r_i} \pmod{p_i},\\ l &\equiv u_{m_i-r_i+1} \pmod{p_i} \end{aligned}$$

for $i=1,\dots,t$. Note that two consecutive terms of the sequence $\{u_n\}, n=0,1,2,\dots$, cannot be divisible by the same prime number p. Indeed, if $p|u_{n-1}$ and $p|u_n$ then using $b=\pm1$ from $u_n=au_{n-1}+bu_{n-2}$ we find that $p|u_{n-2}$. By the same argument, $p|u_{n-3}$ and so on. Hence $p|u_1$, a contradiction.

So, for every x_0 in the residue class $s \pmod P$, where $P=p_1\dots p_t$, and for every x_1 in the residue class $l \pmod P$, we have $x_0\equiv u_{m_i-r_i} \pmod{p_i}$ and $x_1\equiv u_{m_i-r_i+1} \pmod{p_i}$ for $i=1,\dots,t$. By induction on n, this implies

$$x_n \equiv u_{m_i-r_i+n} \pmod{p_i} \tag{3.18}$$

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 (3.18) yields

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

giving $p_i|x_n$.

It remains to choose two composite relatively prime positive integers $x_0\equiv s \pmod P$ and $x_1\equiv l \pmod P$ so that $|x_n|>\max(p_1,\dots,p_t)$ for every non-negative integer 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 $x_0>\max(p_1,\dots,p_t)$ satisfying $x_0\equiv s \pmod P$. Then we can select $x_1\equiv l \pmod P$ as required, by Lemma 3.6 and Lemma 3.7, where $a_0:=l$, $b_0:=P$, $b_1:=x_0$, 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 3.8, there are five distinct primes $p_1, \ldots, p_5$ dividing $u_2, u_3, u_4, u_6, u_{12}$, respectively. Since $D = a^2 - 4 > 0$, the theorem follows from Lemma 3.10 applied to the covering system (3.17). 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 3.9 and 3.10.

Recall that the cases $b = -1$, $|a| \leqslant 2$ and $b = 1$, $a = 0$ have been considered in Section 3.2. In Section 2.3 we already described the literature concerning the case $(a,b) = (1,1)$ (Graham's result). 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 of two composite relatively prime integers

$$V_0 := 106276436867, \quad V_1 := 35256392432$$

shows that the numbers

$$V_n = V_{n-1} + V_{n-2} = F_n V_1 + F_{n-1} V_0, \quad n \geqslant 2, \tag{3.19}$$

are all composite. Here, F_n is the nth Fibonacci number. For the sequence $x_n = -x_{n-1} + x_{n-2}$, we clearly have

$$x_n = (-1)^{n+1} F_n x_1 + (-1)^n F_{n-1} x_0, \quad n \geqslant 2. \tag{3.20}$$

Selecting $x_0 := -V_1 + V_0 = 71020044435$ and $x_1 := V_0 = 106276436867$, one can easily check that x_0 and x_1 are relatively prime composite integers. Moreover, by (3.19) and (3.20),

$$\begin{aligned} x_n &= (-1)^{n+1} F_n V_0 + (-1)^n F_{n-1}(-V_1 + V_0) = (-1)^{n+1} F_{n-1} V_1 + (-1)^{n+1} F_{n-2} V_0 \\ &= (-1)^{n+1}(F_{n-1} V_1 + F_{n-2} V_0) = (-1)^{n+1} V_{n-1} \end{aligned}$$

for $n \geqslant 2$. Thus $|x_n| = V_{n-1}$ is also composite integer for each $n \geqslant 2$.

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

$$\begin{array}{llllll} 1 & (\mathrm{mod}\ 2), & 1 & (\mathrm{mod}\ 3) & 0 & (\mathrm{mod}\ 4), \\ 6 & (\mathrm{mod}\ 8), & 6 & (\mathrm{mod}\ 12) & 2 & (\mathrm{mod}\ 24). \end{array}$$

The divisibility sequence $\{u_n\}$, $n = 0, 1, 2, \ldots$, is given by $u_0 := 0$, $u_1 := 1$

and $u_n = -3u_{n-1} - u_{n-2}$, $n = 2, 3, \ldots$. 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 3.10, we calculated the pair

$$(x_0, x_1) = (13271293, 219498)$$

satisfying the conditions of the theorem.

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

$$\begin{array}{llllll} 0 & (\mathrm{mod}\ 2), & 0 & (\mathrm{mod}\ 3), & 3 & (\mathrm{mod}\ 4), \\ 5 & (\mathrm{mod}\ 8), & 5 & (\mathrm{mod}\ 12), & 1 & (\mathrm{mod}\ 24). \end{array}$$

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 3.10, we found the pair

$$(x_0, x_1) = (7373556, 2006357)$$

satisfying the conditions of the theorem. The proof of Theorem 3.1 is thus completed. □

3.5 Other examples

Below, we shall find smaller solutions for $(a, b) = (\pm 3, -1)$. Instead of using Lemma 3.10, we may directly search for a pair of relatively prime positive integers x_0, x_1 such that each of the first 24 elements of the sequence (3.1) 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 $i = 1, \ldots, 6$, such that, for each n in the range $0 \leqslant n \leqslant 23$ and each i in the range $1 \leqslant i \leqslant 6$, $n \equiv r_i \pmod{m_i}$ implies $p_i | x_n$. This would be enough for $p_i | x_n$ to hold for any n, $n \geqslant 0$, belonging to the residue class $r_i \pmod{m_i}$. Using this direct method, we found smaller pairs (x_0, x_1) 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_0 divisible by 7 and x_1 divisible by 2 and 3, we found

the pair

$$(x_0, x_1) = (35, 3294).$$

One can easily check that

$$\begin{array}{llllll} 1 & (\text{mod } 2), & 1 & (\text{mod } 3), & 0 & (\text{mod } 4), \\ 2 & (\text{mod } 8), & 6 & (\text{mod } 12), & 14 & (\text{mod } 24) \end{array}$$

is indeed a covering system. Also, if n, where $n \geqslant 0$, belongs to the residue class $r_i \pmod{m_i}$ we use the fact that $p_i | x_n$. This explains why we take x_0 divisible by 7 and x_1 divisible by 6. It is clear that $\gcd(x_0, x_1) = \gcd(35, 3294) = 1$. Also, $|x_n| > \max(p_1, \ldots, p_6) = 1103$ for $n \geqslant 2$, so $|x_n|$ is composite for each non-negative integer 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 $(x_0, x_1) = (3294, 35)$. Similarly, taking $(r_1, r_2, r_3, r_4, r_5, r_6) = (0, 2, 1, 3, 3, 7)$, we established that

$$(x_0, x_1) = (2367, 3031)$$

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 $(x_0, x_1) = (3031, 2367)$.

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

$$(x_0, x_1) = (3399, 35).$$

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 $(x_0, x_1) = (35, 3399)$.

4 A tribonacci-like sequence

4.1 Introduction

In this chapter we will study tribonacci-like sequences. Let $\{x_n\}$ be an infinite sequence of integers satisfying the ternary recurrence relation

$$x_n = x_{n-1} + x_{n-2} + x_{n-3}, \tag{4.1}$$

for $n = 3, 4, \ldots$ Since values of x_0, x_1 and x_2 determine the sequence $\{x_n\}$ we denote $S(x_0, x_1, x_2) := \{x_n\}$, where $S(x_0, x_1, x_2)_n := x_n$, $n = 0, 1, 2, \ldots$. If $x_0 = 0$, $x_1 = 0$ and $x_2 = 1$, then $S(x_0, x_1, x_2)$ is a classical tribonacci sequence.

The aim of this chapter is to find three positive integers A, B and C satisfying $\gcd(A, B, C) = 1$ such that the sequence $S(A, B, C)$ contains no prime numbers.

As it was pointed out in Section 2.3, Graham's result is based on the fact that the Fibonacci sequence is a *regular divisibility sequence*, i.e., $F_0 = 0$ and $F_n \mid F_m$ if $n \mid m$. However, by a result of Hall [17], there are no regular divisibility sequences in case $S(0, x_1, x_2)$ for any $x_1, x_2 \in \mathbb{Z}$.

In this chapter we shall overcome this difficulty and prove the following result:

Theorem 4.1. *If*

$$\begin{aligned} x_0 &= 99202581681909167232, \\ x_1 &= 67600144946390082339, \\ x_2 &= 139344212815127987596, \end{aligned}$$

then $\gcd(x_0, x_1, x_2) = 1$ *and the sequence* $S(x_0, x_1, x_2)$ *contains no prime numbers.*

As the proof of this theorem is quite long, we will first prove two auxiliary lemmas. In Lemma 4.3, we give a sufficient condition for the sequence

$\{y_n\} \equiv S(0,a,b) \pmod{p}$ under which $y_{km} \equiv 0 \pmod{p}$, where p is a prime number, $m \geqslant 2$ and $a,b \in \mathbb{Z}$. The notation $\{y_n\} \equiv S(0,a,b) \pmod{p}$ means "for every integer $n \geqslant 0$, $y_n \equiv S(0,a,b)_n \pmod{p}$". In Lemma 4.4 we discuss how to choose y_1 and y_2 so that the condition of Lemma 4.3 would be satisfied. In Section 4.3 our main result will be proved.

4.2 Auxiliary lemmas

We first observe one elementary property of the tribonacci-like sequence.

Lemma 4.2. *If $\{u_n\} = S(a,b,c)$, $\{v_n\} = S(a',b',c')$, and $\{z_n\} = S(a+a', b+b', c+c')$, then $z_n = u_n + v_n$ for all $n \geqslant 0$.*

The proof of this fact is by a trivial induction.

Define two sequences $\{s_n\} = S(0,1,0)$ and $\{t_n\} = S(0,0,1)$. Let p be a prime number and let $\{y_n\} \equiv S(0,a,b) \pmod{p}$ for $a,b \in \mathbb{Z}$. Lemma 4.2 implies

$$y_n \equiv s_n a + t_n b \pmod{p}. \tag{4.2}$$

Lemma 4.3. *Let p be a prime number and let $\{y_n\} \equiv S(0,a,b) \pmod{p}$ with some $a,b \in \mathbb{Z}$. Suppose that $m \geqslant 2$ is an integer. If $y_m \equiv y_{2m} \equiv 0 \pmod{p}$ then $y_{km} \equiv 0 \pmod{p}$ for $k = 0,1,2,\ldots$.*

Proof. Let

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad Y_n = (y_{n+2}, y_{n+1}, y_n).$$

Then the recurrence relation $y_{n+3} = y_{n+2} + y_{n+1} + y_n$ can be rewritten in the matrix form $Y_{n+1} = Y_n A$, for $n = 0,1,2\ldots$. In particular, $Y_n = Y_0 A^n$ and

$$Y_{km} = (y_{km+2}, y_{km+1}, y_{km}) = (y_2, y_1, y_0)(A^m)^k. \tag{4.3}$$

Assume, that $y_0 \equiv y_m \equiv y_{2m} \equiv 0 \pmod{p}$. If the vector $Y_0 \pmod{p}$ is an eigenvector of $A^m \pmod{p}$, then $y_{km} \equiv 0 \pmod{p}$ by (4.3). If not, then $Y_m \pmod{p}$ and $Y_0 \pmod{p}$ (considered as vectors over the finite field $\mathbb{Z}/p\mathbb{Z}$) are linearly independent, hence form a basis for the vector space $V =$

$\{(u,v,0)\} \subset (\mathbb{Z}/p\mathbb{Z})^3$. Since $Y_{2m} = Y_m A^m$ modulo p is also in V by assumption, we have that $VA^m \subset V$. Therefore, by induction, $Y_{km} \pmod p$ is in V for $k = 0,1,2,\ldots$. Hence $y_{km} \equiv 0 \pmod p$. □

Lemma 4.4. *Let p be a prime number. Suppose that $m \geqslant 2$ and $s_m t_{2m} - s_{2m} t_m \equiv 0 \pmod p$. Then there exist a, $b \in \mathbb{Z}$ such that at least one of a, b is not divisible by p and*

$$s_{km} a + t_{km} b \equiv 0 \pmod p$$

for $k = 0,1,2,\ldots$.

Proof. Set $y_n = s_n a + t_n b$. Since $y_0 = s_0 a + t_0 b = 0$, by Lemma 4.3, it suffices to show that there exist a, b such that $y_m \equiv 0 \pmod p$ and $y_{2m} \equiv 0 \pmod p$. Our aim is to solve the following system of linear equations:

$$\begin{cases} s_m a + t_m b \equiv 0 \pmod p, \\ s_{2m} a + t_{2m} b \equiv 0 \pmod p. \end{cases} \tag{4.4}$$

If $s_m \equiv t_m \equiv s_{2m} \equiv t_{2m} \equiv 0 \pmod p$, then we can choose $a = b = 1$. Suppose that $t_m \not\equiv 0 \pmod p$ (the proof in the other cases, when p does not divide s_m, s_{2m} or t_{2m}, is the same). Set $a = 1$, $b = -t_m^{-1} s_m$ where t_m^{-1} denote an integer for which $t_m t_m^{-1} \equiv 1 \pmod p$. It follows easily that the first equation of (4.4) is satisfied. Then the second equation is equivalent to

$$-s_{2m} t_m + s_m t_{2m} \equiv 0 \pmod p. \tag{4.5}$$

Hence, by the condition of the lemma, (4.5) is true, which completes the proof of the lemma. □

4.3 Proof of Theorem 4.1

Consider the following table:

One can verify that every integer belongs to at least one of the arithmetic progressions

$$P_i = \{m_i k + r_i, k \in \mathbb{Z}\}, \quad i = 1,2,\ldots 11. \tag{4.6}$$

In other words, the integers m_i, r_i are chosen so that $P_1, P_2, \ldots, P_{11}$ is a *cov-*

i	1	2	3	4	5	6	7	8	9	10	11
m_i	2	5	6	8	10	12	15	20	24	30	40
r_i	0	0	5	7	9	9	13	17	3	1	27

Table 4.1: Covering system

ering system of $\mathbb{Z}$, i.e.,

$$\mathbb{Z} = \bigcup_{i=1}^{11} P_i. \tag{4.7}$$

To prove (4.7) it is enough to check that any number between 1 and $\gcd(m_1, m_2, \ldots, m_{11}) = 120$ is covered by at least one progression (4.6).

We are interested in the differences $s_{m_i}t_{2m_i} - s_{2m_i}t_{m_i}$ $(i = 1, 2, \ldots, 11)$.

i	p_i	m_i	$\lvert s_{m_i}t_{2m_i} - s_{2m_i}t_{m_i}\rvert$
1	2	2	2
2	29	5	29
3	17	6	$2 \cdot 17$
4	7	8	$2^6 \cdot 7$
5	11	10	$2 \cdot 11 \cdot 29$
6	107	12	$2^3 \cdot 17 \cdot 107$
7	8819	15	$29 \cdot 8819$
8	19	20	$2^3 \cdot 11 \cdot 19 \cdot 29 \cdot 239$
9	1151	24	$2^6 \cdot 7 \cdot 17 \cdot 107 \cdot 1151$
10	1621	30	$2 \cdot 11 \cdot 17 \cdot 29 \cdot 1621 \cdot 8819$
11	79	40	$2^6 \cdot 7 \cdot 11 \cdot 19 \cdot 29 \cdot 79 \cdot 239 \cdot 35281$

Table 4.2: Primes and modulus

Let us fix $i \in \{1, 2, \ldots, 11\}$. As we can see from Table 4.2, each prime number p_i divides the corresponding difference $s_{m_i}t_{2m_i} - s_{2m_i}t_{m_i}$. By Lemma 4.4, for every pair (p_i, m_i) we can choose $a_i, b_i \in \mathbb{Z}$ so that at least one of a_i, b_i is not divisible by p_i and

$$s_{km_i}a_i + t_{km_i}b_i \equiv 0 \pmod{p_i} \tag{4.8}$$

for $k = 0, 1, 2, \ldots$.

Next, we shall construct the sequence $\{x_n\} = S(x_0, x_1, x_2)$ satisfying

$$x_n \equiv s_{m_i - r_i + n}\, a_i + t_{m_i - r_i + n}\, b_i \pmod{p_i} \quad i = 1, 2, \ldots 11 \tag{4.9}$$

for $n = 0, 1, 2, \ldots$. Set

$$\begin{aligned} A_i &= s_{m_i - r_i}\, a_i + t_{m_i - r_i}\, b_i, \\ B_i &= s_{m_i - r_i + 1}\, a_i + t_{m_i - r_i + 1}\, b_i, \\ C_i &= s_{m_i - r_i + 2}\, a_i + t_{m_i - r_i + 2}\, b_i, \end{aligned}$$

for $i = 1, 2, \ldots, 11$. Since the sequence $\{x_n\}$ is defined by its first three terms, it suffices to solve the following equations:

$$\begin{aligned} x_0 &\equiv A_i \pmod{p_i}, \\ x_1 &\equiv B_i \pmod{p_i}, \\ x_2 &\equiv C_i \pmod{p_i}, \end{aligned} \tag{4.10}$$

for $i = 1, 2, \ldots, 11$. The values of a_i, b_i, and $A_i \pmod{p_i}, B_i \pmod{p_i}$, $C_i \pmod{p_i}$ for $i = 1, 2, \ldots 11$ are given in Table 4.3.

i	1	2	3	4	5	6	7	8	9	10	11
a_i	1	1	1	1	1	1	1	1	1	1	1
b_i	0	21	4	5	5	14	2994	7	858	623	61
A_i	0	0	1	1	1	15	2994	8	43	95	41
B_i	1	8	4	5	5	30	2995	16	1127	0	50
C_i	0	23	5	6	6	59	5990	12	1132	1556	50

Table 4.3: Coefficients

By the Chinese reminder theorem (see, e.g., Theorem 1.6.21 in [43]), we find that the system of congruences (4.10) has the following solution

$$\begin{aligned} x_0 &= 99202581681909167232, \\ x_1 &= 67600144946390082339, \\ x_2 &= 139344212815127987596. \end{aligned}$$

Moreover, we have $\gcd(x_0, x_1, x_2) = 1$.

By (4.8) and (4.9), p_i divides x_n if $n \equiv r_i \pmod{m_i}$, where $i \in \{1, 2, \ldots, 11\}$. Since $\{P_i, i = 1, 2, \ldots, 11\}$ cover the integers, we see that for every nonnegative integer n there is some i, $1 \leqslant i \leqslant 11$, such that p_i divides x_n. All prime divisors p_i are relatively small (smaller than $\min_{i \geqslant 0} x_i = x_1$), so $p_i \mid x_n$, where $i = 1, 2, \ldots 11$, implies that x_n is composite for each $n = 0, 1, 2, \ldots$. This completes the proof of the theorem.

Another interesting problem is to determine how far from the optimal (i.e., the smallest) solution we are. If (a, b) is a solution of (4.4), then (ka, kb), where $k \in \mathbb{Z}$, is also a solution of (4.4). So we can vary (a_i, b_i) in Table 4.3. Also, we can choose a different covering system based on another set of primes.

5 Linear higher-order recurrences

5.1 Introduction

In this chapter we will extend the methods used in Chapter 4. For each integer $k \geqslant 2$ one can define a k-step Fibonacci-like sequence, i.e., the sequence of integers $\{x_n\}$, $n = 0, 1, 2, \ldots$, satisfying the following relation

$$x_n = \sum_{i=1}^{k} x_{n-i}$$

for $n = k, k+1, k+2 \ldots$. Since the values of $x_0, x_1, \ldots, x_{k-1}$ determine the k-step Fibonacci-like sequence we denote it by $S_k(x_0, x_1, \ldots, x_{k-1})$. The terms of the sequence $S_k(0, 0, \ldots, 0, 1)$ is well known Fibonacci k-step numbers.

The aim of this chapter is to prove the following theorem:

Theorem 5.1. *For each positive integer k in the range $2 \leqslant k \leqslant 10$ and for each positive integer $k \equiv 79 \pmod{120}$ there are positive integers $a_0, a_1, \ldots, a_{k-1}$ such that $\gcd(a_0, a_1, \ldots, a_{k-1}) = 1$ and the sequence $S_k(a_0, a_1, \ldots, a_{k-1})$ consists of composite numbers only.*

Section 5.3 is devoted to the generalisation of the proof developed in Chapter 4. We will describe the set of triples of positive integers and show how to prove Theorem 5.1 if this set is given. In Section 5.4 we will prove Theorem 5.1 for all $k \equiv 79 \pmod{120}$ and construct corresponding sequences for these cases. Finally, we will give an algorithm for the construction of the set of positive integer triples and list examples of k-step Fibonacci-like sequences for k in the range $4 \leqslant k \leqslant 10$.

5.2 Auxiliary lemmas

We start with the following elementary property of the k-step Fibonacci-like sequence.

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{Z}^k$. Define $S_k(\mathbf{a}) = S_k(a_0, a_1, \ldots, a_{k-1})$. We will denote by $\mathscr{F}_k$ the set of all k-step Fibonacci-like sequences.

Lemma 5.2. *$\mathscr{F}_k$ is a free abelian group of rank k, and the map*

$$\mathbb{Z}^k \to \mathscr{F}_k, \quad \mathbf{a} \to S_k(\mathbf{a})$$

is an isomorphism of abelian groups.

The proof of this fact is straightforward.

Define

$$\{s_n^{(i)}\} = S_k\left(\delta_0^i, \delta_1^i, \ldots, \delta_{k-1}^i\right)$$

for $i = 1, 2, \ldots, k-1$, where δ_j^i is Kronecker's delta symbol. Let p be a prime number and let $\{y_n\} \equiv S_k(0, a_1, a_2, \ldots, a_{k-1}) \pmod{p}$ for $a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}$. Lemma 5.2 implies

$$y_n \equiv \sum_{i=1}^{k-1} a_i s_n^{(i)} \pmod{p}. \tag{5.1}$$

Lemma 5.3. *Fix $k \geqslant 3$. Let p be a prime number and let $\{y_n\} \equiv S_k(0, a_1, a_2, \ldots, a_{k-1}) \pmod{p}$ with some $a_i \in \mathbb{Z}$ for i in the range $1 \leqslant i \leqslant k-1$. Suppose that $m \geqslant 2$ is an integer. If $y_{im} \equiv 0 \pmod{p}$ for i satisfying $1 \leqslant i \leqslant k-1$, then $y_{lm} \equiv 0 \pmod{p}$ for $l = 0, 1, 2, \ldots$.*

Proof. Let

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 1 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}$$

be a $k \times k$ matrix and

$$Y_n = (y_{n+k-1}, y_{n+k-2}, \ldots, y_{n+1}, y_n).$$

Then the recurrence relation $y_{n+k} = y_{n+k-1} + y_{n+k-2} + \cdots + y_{n+1} + y_n$ can be rewritten in the matrix form $Y_{n+1} = Y_n A$, for $n = 0, 1, 2 \ldots$. In particular, $Y_n = Y_0 A^n$ and

$$Y_{lm} = (y_{lm+k-1}, y_{lm+k-2}, \ldots, y_{lm+1}, y_{lm}) = (y_{k-1}, y_{k-2}, \ldots, y_1, y_0)(A^m)^l. \quad (5.2)$$

Let $B = A^m$. This is a $k \times k$ matrix with integer coefficients. By the Cayley-Hamilton Theorem,

$$B^k = b_0 I + b_1 B + b_2 B^2 + \cdots + b_{k-1} B^{k-1},$$

for some integers $b_0, b_1, \ldots, b_{k-1}$. Since $Y_{lm} = Y_0 B^l$ we find that

$$Y_{lm} = b_0 Y_{(l-k)m} + b_1 Y_{(l-k+1)m} + \cdots + b_{k-1} Y_{(l-1)m}$$

for $l \geqslant k$. Considering the last entries for these vectors,

$$y_{lm} = b_0 y_{(l-k)m} + b_1 y_{(l-k+1)m} + \cdots + b_{k-1} y_{(l-1)m}.$$

The lemma follows by induction. □

Define the matrix

$$B_{k,m} = \begin{pmatrix} s_m^{(1)} & s_{2m}^{(1)} & \cdots & s_{(k-1)m}^{(1)} \\ s_m^{(2)} & s_{2m}^{(2)} & \cdots & s_{(k-1)m}^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ s_m^{(k-1)} & s_{2m}^{(k-1)} & \cdots & s_{(k-1)m}^{(k-1)} \end{pmatrix} \quad (5.3)$$

for each positive integer m. Let $\left|B_{k,m}\right|$ be the determinant of the matrix (5.3).

Lemma 5.4. *Let $m \geqslant 2$ be an integer. If p is prime number and*

$$\left|B_{k,m}\right| \equiv 0 \pmod{p}.$$

then there exist $a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}$ such that a_i is not divisible by p for at

least one $i = 1, 2, \ldots k-1$, *and*

$$\sum_{i=1}^{k-1} a_i s_{lm}^{(i)} \equiv 0 \pmod{p}$$

for $l = 0, 1, 2, \ldots$.

Proof. Set $y_n = \sum_{i=1}^{k-1} a_i s_n^{(i)}$. Since $y_0 = \sum_{i=1}^{k-1} a_i s_0^{(i)} = 0$, by Lemma 5.3, it suffices to show that there exist suitable $a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}$ such that $y_{lm} \equiv 0 \pmod{p}$ for $l = 1, 2, \ldots, k-1$. Our aim is to solve the following system of linear equations:

$$(a_1, a_2, \ldots, a_{k-1}) B_{k,m} \equiv (0, 0, \ldots, 0) \pmod{p}. \tag{5.4}$$

Let us consider system (5.4) as a homogeneous linear system over the finite field $\mathbb{Z}/p\mathbb{Z}$. The assumption $|B_{k,m}| \equiv 0 \pmod{p}$ implies that the rank of the system (5.4) is at most $k-2$. Therefore, the system has non-trivial solution in $\mathbb{Z}/p\mathbb{Z}$. In other words, there exist $a_1, a_2, \ldots, a_{k-1} \in \mathbb{Z}$ such that a_i is not divisible by p for at least one $i = 1, 2, \ldots k-1$. □

5.3 General case

Let I be a positive integer (to be defined later). Our goal is to find a finite set $\mathfrak{S}_k(N)$ of positive integer triples (p_i, m_i, r_i) $(i = 1, 2, \ldots, I)$ with the following properties:

1. each p_i is a prime number and $p_i \neq p_j$ if $i \neq j$;
2. p_i divides the determinant $|B_{k,m_i}|$, where B_{k,m_i} is the matrix (5.3);
3. the congruences
$$x \equiv r_i \pmod{m_i} \tag{5.5}$$
cover the integers, i.e., for any integer x there is some index i, $1 \leqslant i \leqslant I$, such that $x \equiv r_i \pmod{m_i}$.

Now, suppose that we already found the set $\mathfrak{S}_k(N)$ and I is a fixed positive integer. Choose i, where $1 \leqslant i \leqslant I$. Since $B_{k,m_i} \equiv 0 \pmod{p_i}$, by Lemma 5.4, there exist $a_{i,1}, a_{i,2}, \ldots, a_{i,k-1} \in \mathbb{Z}$ such that $a_{i,j}$ is not divisible by p_i for at

least one $j = 1,2,\ldots k-1$, and

$$\sum_{j=1}^{k-1} a_{i,j} s_{lm_i}^{(j)} \equiv 0 \pmod{p_i} \tag{5.6}$$

for $l = 0,1,2,\ldots$.

We shall construct the sequence $\{x_n\} = S_k(x_0, x_1, \ldots, x_{k-1})$ satisfying

$$x_n \equiv \sum_{j=1}^{k-1} s_{m_i - r_i + n}^{(j)} a_{i,j} \pmod{p_i} \quad i = 1,2,\ldots I \tag{5.7}$$

for $n = 0,1,2,\ldots$. Set

$$\begin{aligned} A_{i,0} &= \sum_{j=1}^{k-1} s_{m_i - r_i}^{(j)} a_{i,j}, \\ A_{i,1} &= \sum_{j=1}^{k-1} s_{m_i - r_i + 1}^{(j)} a_{i,j}, \\ &\vdots \\ A_{i,k-1} &= \sum_{j=1}^{k-1} s_{m_i - r_i + k - 1}^{(j)} a_{i,j} \end{aligned} \tag{5.8}$$

for $i = 1,2,\ldots,I$. Since the sequence $\{x_n\}$ is defined by its first k terms, it suffices to solve the following equations:

$$\begin{aligned} x_0 &\equiv A_{i,0} \pmod{p_i}, \\ x_1 &\equiv A_{i,1} \pmod{p_i}, \\ &\vdots \\ x_{k-1} &\equiv A_{i,k-1} \pmod{p_i} \end{aligned} \tag{5.9}$$

for $i = 1,2,\ldots,I$. By the Chinese reminder theorem, the system of congruences (5.9) has the positive integer solution $x_0 = X_0$, $x_1 = X_1, \ldots, x_{k-1} = X_{k-1}$. It is assumed that $\gcd(X_0, X_1, \ldots, X_{k-1}) = 1$.

By (5.6) and (5.7), p_i divides x_n if $n \equiv r_i \pmod{m_i}$, where $i \in \{1,2,\ldots,I\}$. Since congruences (5.5) cover the integers, we see that for every nonnegative integer n there is some i, $1 \leqslant i \leqslant I$, such that p_i divides x_n. The sequence $\{x_n\}$, $n = I, I+1, \ldots$, is strictly increasing, so x_n must be composite for $n \geqslant I$. In this way, we can construct the k-step Fibonacci-like sequence of composite

numbers $\{x_n\}$, $n = I, I+1, \ldots$, if the set $\mathfrak{S}_k(N)$ is given.

Note that the assumption $\gcd(X_0, X_1, \ldots, X_{k-1}) = 1$ is unnecessarily restrictive. We can always construct the solution of (5.9) with this property. Indeed, let $\gcd(X_1, \ldots, X_{k-1}) = d_1$, $\gcd(X_0, d_1) = d_0 > 1$, and $P = \prod_{i=1}^{I} p_i$. Suppose that p is a prime number and $p \mid d_0$. If $p \mid P$, then, by (5.9),

$$\begin{aligned} A_{i,0} &\equiv 0 \pmod{p}, \\ A_{i,1} &\equiv 0 \pmod{p}, \\ &\vdots \\ A_{i,k-1} &\equiv 0 \pmod{p}. \end{aligned} \tag{5.10}$$

Let

$$C = \begin{pmatrix} s^{(1)}_{m_i - r_i} & s^{(1)}_{m_i - r_i + 1} & \cdots & s^{(1)}_{m_i - r_i + k - 1} \\ s^{(2)}_{m_i - r_i} & s^{(2)}_{m_i - r_i + 1} & \cdots & s^{(2)}_{m_i - r_i + k - 1} \\ \vdots & \vdots & \ddots & \vdots \\ s^{(k-1)}_{m_i - r_i} & s^{(k-1)}_{m_i - r_i + 1} & \cdots & s^{(k-1)}_{m_i - r_i + k - 1} \end{pmatrix}$$

be a $(k-1) \times k$ matrix over the finite field $\mathbb{Z}/p\mathbb{Z}$. By (5.8) and (5.10), we get

$$(a_{i,1}, a_{i,2}, \ldots, a_{i,k-1})C \equiv (0, 0, \ldots, 0) \pmod{p}. \tag{5.11}$$

The system of equations (5.11) has nontrivial solution if $\operatorname{rank}(C) \leqslant k-2$. But

$$\operatorname{rank}(C) = \operatorname{rank} \begin{pmatrix} s^{(1)}_{m_i - r_i - 1} & s^{(1)}_{m_i - r_i} & \cdots & s^{(1)}_{m_i - r_i + k - 2} \\ s^{(2)}_{m_i - r_i - 1} & s^{(2)}_{m_i - r_i} & \cdots & s^{(2)}_{m_i - r_i + k - 2} \\ \vdots & \vdots & \ddots & \vdots \\ s^{(k-1)}_{m_i - r_i - 1} & s^{(k-1)}_{m_i - r_i} & \cdots & s^{(k-1)}_{m_i - r_i + k - 2} \end{pmatrix} =$$

$$\operatorname{rank} \begin{pmatrix} s^{(1)}_0 & s^{(1)}_1 & \cdots & s^{(1)}_{k-1} \\ s^{(2)}_0 & s^{(2)}_1 & \cdots & s^{(2)}_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ s^{(k-1)}_0 & s^{(k-1)}_1 & \cdots & s^{(k-1)}_{k-1} \end{pmatrix} = \operatorname{rank} \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix} = k-1,$$

a contradiction. From this if follows that

$$\gcd(X_0, d_1, P) = 1. \tag{5.12}$$

It is easy to check that if $(X_0, X_1, \ldots, X_{k-1})$ is a solution of (5.9) then $(X_0 + lP, X_1, \ldots, X_{k-1})$ is also a solution for all integers l. Let $\gcd(X_0, P) = d$, then, by Dirichlet's theorem on prime numbers in arithmetic progression, we conclude that $X_0/d + lP/d$ is a prime number for infinitely many integers l. So, $\gcd(X_0/d + lP/d, d_1) = 1$ for some l. It follows from (5.12) that $\gcd(X_0 + lP, d_1) = 1$ for some l, which is the desired conclusion.

5.4 Proof of Theorem 5.1 for $k \equiv 79 \pmod{120}$

In this section we will show that if $k \equiv 79 \pmod{120}$, then there exist a k-step Fibonacci-like sequence of composite numbers. We will need the following lemma:

Lemma 5.5. *Suppose that the numbers k, p and the sequence $\{y_n\}$ are defined as in Lemma 5.3. If there is a positive integer l such that*

$$\sum_{n=0}^{l-1} y_n \equiv 0 \pmod{p} \tag{5.13}$$

and

$$y_n \equiv y_{n-l} \pmod{p} \qquad \text{for } n = l,\ l+1,\ l+2, \ldots, \tag{5.14}$$

then for every nonnegative integer t the sequence

$$\{y_n^{(t)}\} \equiv S_{tl+k}(y_0, y_1, \ldots, y_{tl+k-1}) \pmod{p}$$

has the following property:

$$y_n^{(t)} \equiv y_n \pmod{p} \tag{5.15}$$

for $n = 0, 1, 2, \ldots$.

Proof. If $t = 0$, then the statement of the lemma is trivial. Let $t \geqslant 1$. By the definition of the sequence $y_n^{(t)}$, $n = 0, 1, 2, \ldots$, (5.15) is true for $n = 0, 1, \ldots, tl + k - 1$. Let $r \geqslant k$ be an integer and suppose (5.15) is true for $n = 0, 1, \ldots tl +$

$r-1$. By (5.13) and (5.14), $\sum_{n=r}^{r+l-1} y_n \equiv 0 \pmod{p}$ for any positive integer r. Thus we have

$$y_{tl+r}^{(t)} \equiv \sum_{i=r-k}^{tl+r-1} y_i \equiv \sum_{i=r-k}^{r-1} y_i \equiv y_r \equiv y_{tl+r} \pmod{p}.$$

By a induction, (5.15) is true for $n = 0, 1, 2, \ldots$. □

Assume that $k = 4$ and $B_{4,3}$ is the matrix defined in (5.3). It is easy to check that

$$|B_{4,3}| = \begin{vmatrix} 0 & 3 & 23 \\ 0 & 4 & 27 \\ 1 & 4 & 29 \end{vmatrix} = -11,$$

and

$$(1,\ 2,\ 0)B_{4,3} = (0,\ 0,\ 0) \pmod{11}.$$

By Lemma 5.4, the sequence $\{y_n\} \equiv S_4(0,1,2,0) \pmod{11}$ has the following property:

$$11 \mid y_{3n} \tag{5.16}$$

for $n = 0, 1, 2, \ldots$. We calculate the first elements of sequence $\{y_n\} \pmod{11}$:

$$0,\ 1,\ 2,\ 0,\ 3,\ 6,\ 0,\ 9,\ 7,\ 0,\ 5,\ 10,\ 0,\ 4,\ 8,\ 0,\ 1,\ 2,\ 0, \ldots$$

By a simple induction, one can prove that the sequence $\{y_n\} \pmod{11}$ is periodic. The length of the period is 15 and $\sum_{i=0}^{14} y_i \equiv 0 \pmod{11}$. By Lemma 5.5 applied to $k = 4$, $l = 15$, $p = 11$ and to the sequence $\{y_n\}$, we conclude that the sequence

$$\{y_n^{(t)}\} \equiv S_{15t+4}(y_0, y_1, \ldots, y_{15t+3}) \pmod{11}$$

satisfies the property (5.15) for $t = 0, 1, 2, \ldots$. It follows that $\{y_n^{(t)}\}$ satisfies the property (5.16) for $t = 0, 1, 2, \ldots$.

Now, let $k = 7$. It is easy to check that

$$|B_{7,3}| = \begin{vmatrix} 0 & 0 & 3 & 24 & 191 & 1508 \\ 0 & 0 & 4 & 28 & 223 & 1761 \\ 1 & 0 & 4 & 30 & 239 & 1888 \\ 0 & 0 & 4 & 31 & 247 & 1952 \\ 0 & 0 & 4 & 32 & 251 & 1984 \\ 0 & 1 & 4 & 32 & 253 & 2000 \end{vmatrix} = -5 \cdot 17$$

and

$$\begin{aligned} (1,2,0,2,4,0)B_{7,3} &= (0,0,0,0,0,0) \pmod 5, \\ (1,2,0,9,1,0)B_{7,3} &= (0,0,0,0,0,0) \pmod{17}. \end{aligned}$$

Lemma 5.4 implies that the sequence

$$\{u_n\} \equiv S_7(0,1,2,0,2,4,0) \pmod 5$$

has the property

$$5 \mid u_{3n} \tag{5.17}$$

for $n = 0,1,2,\ldots$ and the sequence

$$\{v_n\} \equiv S_7(0,1,2,0,9,1,0) \pmod{17}$$

has the property

$$17 \mid v_{3n} \tag{5.18}$$

for $n = 0,1,2,\ldots$. The first members of the sequence $\{u_n\} \pmod 5$ are

$$0,\ 1,\ 2,\ 0,\ 2,\ 4,\ 0,\ 4,\ 3,\ 0,\ 3,\ 1,\ 0,\ 1,\ 2,\ 0,\ 2,\ 4,\ 0,\ldots,$$

and those of the sequence $\{v_n\} \pmod{17}$ are

$$\begin{aligned} &0,\ 1,\ 2,\ 0,\ 9,\ 1,\ 0,\ 13,\ 9,\ 0,\ 15,\ 13,\ 0,\ 16,\ 15,\ 0,\ 8,\ 16,\ 0,\ 4,\ 8,\ 0,\ 2,\ 4, \\ &0,\ 1,\ 2,\ 0,\ 9,\ 1,\ 0\ldots. \end{aligned}$$

By induction, one can prove that the sequences $\{u_n\}$ and $\{v_n\}$ are periodic with the length of the period 12 and 24, respectively. Since $\sum_{i=0}^{11} u_i \equiv 0$

(mod 5) and $\sum_{i=0}^{23} v_i \equiv 0 \pmod{17}$, by Lemma 5.5 applied to $\{u_n\}$ and $\{v_n\}$, we derive that the sequences

$$\{u_n^{(t)}\} \equiv S_{12t+7}(u_0, u_1, \ldots, u_{12t+6})$$

and

$$\{v_n^{(t)}\} \equiv S_{24t+7}(v_0, v_1, \ldots, v_{24t+6})$$

satisfy the property (5.15) for $t = 0, 1, 2, \ldots$. Hence, the sequence $u_n^{(t)}$ for $n = 0, 1, 2, \ldots$ satisfies the property (5.17) and the sequence $v_n^{(t)}$ for $n = 0, 1, 2, \ldots$ - the property (5.18) for $t = 0, 1, 2, \ldots$.

Set $t_1 = 8t + 5$, $t_2 = 10t + 6$, $t_3 = 5t + 3$ for some positive integer t. Our goal is to find a sequence $x_n^{(t)}$ for $n = 0, 1, 2, \ldots$ satisfying the following conditions for every positive integer n:

$$\begin{aligned} x_n^{(t)} &\equiv y_n^{(t_1)} \pmod{11}, \\ x_n^{(t)} &\equiv u_{n+1}^{(t_2)} \pmod{5}, \\ x_n^{(t)} &\equiv v_{n+2}^{(t_3)} \pmod{17}. \end{aligned} \tag{5.19}$$

Using the definition of the sequences $y_n^{(t)}$, $u_n^{(t)}$, and $v_n^{(t)}$ for $n = 0, 1, 2, \ldots$ we can rewrite (5.19) as

$$\begin{aligned} \{x_n^{(t)}\} &\equiv S_{120t+79}(y_0, y_1, \ldots, y_{120t+78}) \pmod{11}, \\ \{x_n^{(t)}\} &\equiv S_{120t+79}(u_1, u_2, \ldots, u_{120t+78}, u_7) \pmod{5}, \\ \{x_n^{(t)}\} &\equiv S_{120t+79}(v_2, v_3, \ldots, v_{120t+78}, v_7, v_8) \pmod{17}. \end{aligned}$$

By the Chinese Reminder Theorem, the system of equations (5.19) has a solution for every nonnegative integer t. For $t = 0$ we find that

$$\begin{aligned} \{x_n^{(0)}\} = S_{79}(&121, 782, 145, 902, 289, 710, 264, 493, 865, 693, 731, 560, 66, 697, 195, \\ &407, 34, 310, 484, 663, 325, 803, 306, 205, 121, 357, 230, 902, 884, 30, \\ &264, 408, 695, 693, 476, 50, 66, 867, 535, 407, 544, 395, 484, 323, 580, \\ &803, 221, 35, 121, 102, 655, 902, 119, 370, 264, 918, 780, 693, 136, 305, \\ &66, 782, 365, 407, 289, 820, 484, 493, 920, 803, 731, 120, 121, 697, \\ &910, 902, 34, 200, 264), \end{aligned}$$

and for $t > 0$ define

$$\{x_n^{(t)}\} = S_{120t+79}(x_0^{(0)}, x_1^{(0)}, \ldots, x_{120t+78}^{(0)}).$$

By (5.15), (5.19) and by the properties (5.16), (5.17), (5.18), it follows immediately that

- if $n \equiv 0 \pmod 3$ then $x_n^{(t)} \equiv 0 \pmod{11}$,
- if $n \equiv 1 \pmod 3$ then $x_n^{(t)} \equiv 0 \pmod{17}$,
- if $n \equiv 2 \pmod 3$ then $x_n^{(t)} \equiv 0 \pmod 5$.

Since $x_n^{(0)} > 17$ for $n = 0, 1, 2, \ldots$, we conclude that $x_n^{(t)}$ for $n = 0, 1, 2, \ldots$ is a k-step Fibonacci-like sequence of composite numbers for $k = 120t + 79$ and $t = 0, 1, 2, \ldots$.

5.5 An algorithm for the construction of the set $\mathfrak{S}_k(N)$

The construction of the set $\mathfrak{S}_k(N)$ splits into two parts. We first generate the finite set $\mathfrak{s}_k(N) = \{(p_1, m_1), (p_2, m_2), \ldots, (p_I, m_I), \}$, where p_i is a prime number and m_i is a positive integer (Algorithm 1). Then we try to construct the covering system $\{r_1 \pmod{m_1}, r_2 \pmod{m_2}, \ldots, r_{I'} \pmod{m_{I'}}\}$ for $I' \leqslant I$. Algorithm 2 gives the answer "I can't construct a covering system" or returns a covering system. In the second case, we construct the set $\mathfrak{S}_k(N) = \{(p_i, m_i, r_i)\}$. These algorithms were implemented using a computer algebra system PARI/GP [37].

The only thing we can control in the construction of the set $\mathfrak{S}_k(N)$ is the integer N. If Algorithm 2 gives an answer "I can't construct a covering system" then we can choose different N and try again. We can have different sets $\mathfrak{S}_k(N)$ for different values of N. The implementation of these algorithms takes less than one minute to give an answer on a modestly powered computer (Athlon XP 2100+) for $3 \leqslant k \leqslant 10$ and for good choice of N.

Algorithm 1 Construct the set $\mathfrak{s}_k(N)$

Require: $k \geqslant 2$, $N \geqslant 2$.
Ensure: The set $\mathfrak{s}_k(N)$.

```
primes_list ← {}
𝔰_k(N) ← {}
divisors_list ← list of N divisors
for d ∈ divisors_list do
    Construct the matrix B_{k,d} {see Section 5.2}
    determinant ← |B_{k,d}|
    factors_list ← prime factors of determinant
    for factor ∈ factors_list do
        if factor ∉ primes_list then
            Put factor in primes_list
            Put (factor, divisor) in 𝔰_k(N)
        end if
    end for
end for
return 𝔰_k(N)
```

Define $A_N = \{1, 2, \ldots, N\}$ for some positive integer N and let $A_N(m, r) = \{a | a \in A_N, a \equiv r \pmod{m}\}$.

Empirical results suggest that we can choose suitable N for any positive integer $k \geqslant 2$ so we state a following conjecture:

Conjecture 1. *Let $k \geqslant 2$ be some fixed positive integer. Then there exist positive integers $a_0, a_1, \ldots, a_{k-1}$ such that $\gcd(a_0, a_1, \ldots, a_{k-1}) = 1$ and the sequence $S_k(a_0, a_1, \ldots, a_{k-1})$ contains no prime numbers.*

5.6 Examples of sequences for $k = 4, 5, \ldots, 10$

Since the case $k = 2$ is proved in [15] and the case $k = 3$ in [34], in this section we will prove Theorem 5.1 for $k = 4, 5, \ldots, 10$. As it was noticed in Section 5.3, we only need to construct the set $\mathfrak{S}_k(N)$. Below we list some examples of sequences $\{x_n\}$, $n = 0, 1, 2 \ldots$ for each k in the range $4 \leqslant k \leqslant 10$.

$$\begin{aligned}\{x_n\} = S_4(&69653411979972166034413452555549082199598,\\ &10958188570324452297588339728720332112233,\\ &33385065960431566962335079967849088541 02,\\ &11794350400878505028751078386520701499400).\end{aligned}$$

Algorithm 2 Construct a covering system

Require: A finite set of positive integers $\{m_1, m_2, \ldots, m_I\}$.

Ensure: The covering system $\{r_1 \pmod{m_1}, r_2 \pmod{m_2}, \ldots, r_{I'} \pmod{m_{I'}}\}$.

$N \leftarrow \text{lcm}(m_1, m_2, \ldots, m_I)$
Covering_set $\leftarrow \{\}$
$B \leftarrow A_N$
for i from 1 to I **do**
  MAX $\leftarrow 0$
  for r from 0 to $m_i - 1$ **do**
    if MAX $< |A_N(m_i, r) \cap B|$ **then**
      $r_i \leftarrow r$
    end if
    Put $r_i \pmod{m_i}$ in Covering_set
    $B \leftarrow B \backslash A_N(m_i, r_i)$
    if $B = \{\}$ **then**
      return Covering_set
    end if
  end for
end for
print "I can't construct a covering system"

$$\{x_n\} = S_5(1670030, 2329659, 907322, 2009158, 580558).$$

$$\{x_n\} = S_6(146468256594419699081616456 20, 175283236549590294825071678 66,$$
$$348909702963579545828827375 64, 268733381450210620447735786 13,$$
$$515502315341834259100334992 05, 426284491559997601974226015 56).$$

$$\{x_n\} = S_7(49540, 32691, 13932, 18650, 9962, 31004, 21990).$$

$$\{x_n\} = S_8(45401808216635955486 72, 46980788627273312337 61,$$
$$61551037975894065620 86, 63722830451034530089 50,$$
$$22798260853249471505 46, 19970116230841081657 56,$$
$$25580829254880232019 96, 15745290204660716415 36).$$

$$\{x_n\} = S_9(56233156963124, 2686035354591, 59483968596828,$$
$$9266206975260, 5763383142928, 2968317519550,$$
$$56580150371822, 38270799500006, 16687306893378).$$

$$\{x_n\} = S_{10}(2757357, 684913, 197119, 5440883, 4628571,$$
$$6208094, 871487, 2421952, 1064430, 5329024).$$

Since the set $\mathfrak{S}_k(N)$ is essential in the construction of k-step Fibonacci-like sequence $S_k(x_0, x_1, \ldots, x_{k-1})$ we give this set for each k in the range $4 \leqslant k \leqslant 10$.

Table 5.1: The set $\mathfrak{S}_4(360)$

i	p_i	m_i	r_i	$\lvert B_{4,m_i}\rvert$
1	11	3	0	11
2	2	5	0	2^6
3	41	6	1	$11\cdot 41$
4	1511	8	0	1511
5	521	9	2	$11\cdot 521$
6	29	10	2	$2^{12}\cdot 29$
7	167	12	10	$11^2\cdot 41\cdot 167$
8	33391	15	8	$2^6\cdot 11\cdot 33391$
9	73	18	5	$11\cdot 41\cdot 73\cdot 251\cdot 521$
10	251	18	17	$11\cdot 41\cdot 73\cdot 251\cdot 521$
11	10399	20	4	$2^{18}\cdot 29\cdot 10399$
12	13177	24	4	$11^2\cdot 41\cdot 167\cdot 1511\cdot 13177$
13	6781	30	26	$2^{12}\cdot 11\cdot 29\cdot 41\cdot 6781\cdot 33391$
14	37	36	14	$11^2\cdot 37\cdot 41\cdot 73\cdot 167\cdot 251\cdot 521\cdot 195407$
15	195407	36	26	$11^2\cdot 37\cdot 41\cdot 73\cdot 167\cdot 251\cdot 521\cdot 195407$

Table 5.2: The set $\mathfrak{S}_5(16)$

i	p_i	m_i	r_i	$\lvert B_{5,m_i}\rvert$
1	2	2	0	2^2
2	3	4	1	$2^4\cdot 3^2$
3	71	8	3	$2^6\cdot 3^2\cdot 71$
4	47	16	7	$2^8\cdot 3^2\cdot 47\cdot 71\cdot 193$
5	193	16	15	$2^8\cdot 3^2\cdot 47\cdot 71\cdot 193$

Table 5.3: The set $\mathfrak{S}_6(32)$

i	p_i	m_i	r_i	$\lvert B_{6,m_i}\rvert$
1	5	4	0	$5\cdot 41$
2	41	4	1	$5\cdot 41$
3	31	8	2	$5\cdot 31\cdot 41\cdot 239$
4	239	8	3	$5\cdot 31\cdot 41\cdot 239$
5	79	16	6	$5\cdot 31\cdot 41\cdot 79\cdot 239\cdot 271\cdot 1777$
6	271	16	7	$5\cdot 31\cdot 41\cdot 79\cdot 239\cdot 271\cdot 1777$
7	1777	16	14	$5\cdot 31\cdot 41\cdot 79\cdot 239\cdot 271\cdot 1777$
8	257	32	15	$B_{6,m_{16}}\cdot 257\cdot 3827975948383$
9	3827975948383	32	31	$B_{6,m_{16}}\cdot 257\cdot 3827975948383$

Table 5.4: The set $\mathfrak{S}_7(6)$

i	p_i	m_i	r_i	$\lvert B_{7,m_i}\rvert$
1	2	2	0	2^3
2	5	3	0	$5 \cdot 17$
3	17	3	1	$5 \cdot 17$
4	337	6	5	$2^3 \cdot 5 \cdot 17 \cdot 337$

Table 5.5: The set $\mathfrak{S}_8(30)$

i	p_i	m_i	r_i	$\lvert B_{8,m_i}\rvert$
1	2	3	0	2^7
2	3	5	0	$3^2 \cdot 7^2 \cdot 59$
3	7	5	1	$3^2 \cdot 7^2 \cdot 59$
4	59	5	2	$3^2 \cdot 7^2 \cdot 59$
5	41	6	1	$2^{15} \cdot 41$
6	586919	10	4	$3^4 \cdot 7^2 \cdot 59 \cdot 586919$
7	151	15	8	$2^7 \cdot 3^4 \cdot 7^2 \cdot 59 \cdot 151 \cdot 25025941$
8	25025941	15	13	$2^7 \cdot 3^4 \cdot 7^2 \cdot 59 \cdot 151 \cdot 25025941$
9	31	30	29	$B_{8,m_{15}} \cdot 2^8 \cdot 3^4 \cdot 31 \cdot 41 \cdot 586919 \cdot 38457989$

Table 5.6: The set $\mathfrak{S}_9(12)$

i	p_i	m_i	r_i	$\lvert B_{9,m_i}\rvert$
1	2	2	0	2^4
2	31	4	1	$2^8 \cdot 31$
3	74933	6	1	$2^4 \cdot 74933$
4	2927	12	3	$2^8 \cdot 31 \cdot 2927 \cdot 4957 \cdot 74933$
5	4957	12	11	$2^8 \cdot 31 \cdot 2927 \cdot 4957 \cdot 74933$

Table 5.7: The set $\mathfrak{S}_{10}(8)$

i	p_i	m_i	r_i	$\lvert B_{10,m_i}\rvert$
1	3	4	0	$3 \cdot 17 \cdot 257$
2	17	4	1	$3 \cdot 17 \cdot 257$
3	257	4	2	$3 \cdot 17 \cdot 257$
4	7	8	3	$3^3 \cdot 7 \cdot 17 \cdot 71 \cdot 257 \cdot 3391$
5	71	8	7	$3^3 \cdot 7 \cdot 17 \cdot 71 \cdot 257 \cdot 3391$

Finally, we give the coefficients of the system of equations (5.9). It is necessary because in Lemma 5.4 we prove only existence of these coefficients, i.e., with the same set $\mathfrak{S}_k(N)$ we can find the different k-step Fibonacci-like sequence $S_k(x_0, x_1, \ldots, x_{k-1})$.

Table 5.8: Coefficients of (5.9) for $k = 4$

i	1	2	3	4	5	6	7
$A_{i,0}$	0	0	21	0	421	7	124
$A_{i,1}$	1	1	0	1	128	7	64
$A_{i,2}$	2	0	35	4	0	0	22
$A_{i,3}$	0	0	5	1305	9	2	44

Table 5.9: Coefficients of (5.9) for $k = 4$

i	8	9	10	11	12	13	14	15
$A_{i,0}$	19247	1	1	10164	12571	151	22	75748
$A_{i,1}$	25767	46	11	752	7342	302	5	105421
$A_{i,2}$	2901	66	52	3340	5671	603	25	65611
$A_{i,3}$	8709	70	64	6542	770	5420	11	100766

Table 5.10: Coefficients of (5.9) for $k = 5$

i	1	2	3	4	5
$A_{i,0}$	0	2	39	26	1
$A_{i,1}$	1	0	7	10	149
$A_{i,2}$	0	2	13	34	29
$A_{i,3}$	0	1	0	2	28
$A_{i,4}$	0	1	62	14	14

Table 5.11: Coefficients of (5.9) for $k = 6$

i	1	2	3	4	5	6	7	8	9
$A_{i,0}$	0	8	8	51	25	3	1147	44	1
$A_{i,1}$	1	0	16	60	43	62	1159	123	1671520683283
$A_{i,2}$	4	18	0	120	35	126	353	123	1187982745969
$A_{i,3}$	3	31	11	0	49	93	940	187	2373684950413
$A_{i,4}$	0	21	3	37	56	45	46	116	1575934864371
$A_{i,5}$	1	0	23	65	29	79	92	206	2981147295654

Table 5.12: Coefficients of (5.9) for $k = 7$

i	1	2	3	4
$A_{i,0}$	0	0	2	1
$A_{i,1}$	1	1	0	2
$A_{i,2}$	0	2	9	115
$A_{i,3}$	0	0	1	115
$A_{i,4}$	0	2	0	189
$A_{i,5}$	0	4	13	0
$A_{i,6}$	0	0	9	85

Table 5.13: Coefficients of (5.9) for $k = 8$

i	1	2	3	4	5	6	7	8	9
$A_{i,0}$	0	0	1	35	9	506111	92	14176025	1
$A_{i,1}$	1	1	0	11	0	249334	80	6652214	12
$A_{i,2}$	0	1	2	0	14	146730	9	1932056	17
$A_{i,3}$	0	0	6	51	1	293460	17	15861862	13
$A_{i,4}$	0	0	2	40	2	0	18	16528118	12
$A_{i,5}$	0	0	4	15	3	8526	127	23725749	12
$A_{i,6}$	0	2	0	30	3	85280	14	3798202	15
$A_{i,7}$	0	0	5	0	0	511720	96	7596404	20

Table 5.14: Coefficients of (5.9) for $k = 9$

i	1	2	3	4	5
$A_{i,0}$	0	2	33332	143	1
$A_{i,1}$	1	0	0	286	1095
$A_{i,2}$	0	27	72006	571	4380
$A_{i,3}$	0	23	63225	0	3835
$A_{i,4}$	0	23	18734	1286	405
$A_{i,5}$	0	0	37468	2185	1364
$A_{i,6}$	0	16	2	2886	3240
$A_{i,7}$	0	1	0	92	2547
$A_{i,8}$	0	1	24967	20	1996

Table 5.15: Coefficients of (5.9) for $k = 10$

i	1	2	3	4	5
$A_{i,0}$	0	8	4	1	1
$A_{i,1}$	1	0	8	5	47
$A_{i,2}$	1	4	0	6	23
$A_{i,3}$	2	16	193	0	11
$A_{i,4}$	0	15	1	3	10
$A_{i,5}$	2	0	2	4	67
$A_{i,6}$	2	16	0	1	33
$A_{i,7}$	1	13	241	1	0
$A_{i,8}$	0	9	193	3	69
$A_{i,9}$	1	0	129	1	48

6 Conclusions

All the results of this thesis were achieved during the doctoral studies in Vilnius University. The main attention was devoted to linear recurrence sequences of composite numbers. We will briefly overview the results presented in the previous chapters.

- We studied the second order linear recurrence sequences of composite numbers. Let $(a,b) \in \mathbb{Z}^2$, where $b \neq 0$ and $(a,b) \neq (\pm 2, -1)$. We proved that then there exist two positive relatively prime composite integers x_0, x_1 such that the sequence given by $x_n = ax_{n-1} + bx_{n-2}$, $n = 2, 3, \ldots$, consists of composite terms only, i.e., $|x_n|$ is a composite integer for each $n \in \mathbb{N}$. In the exceptional case $(a,b) = (\pm 2, -1)$ we showed that such initial values x_0, x_1 do not exist. It extends a result of Graham [15] who proved this statement in the special case of the Fibonacci-like sequence, where $(a,b) = (1,1)$.

- We investigated the special case of the third order linear recurrence sequences, i.e., tribonacci-like sequences. We found three positive integers x_0, x_1, x_2 satisfying $\gcd(x_0, x_1, x_2) = 1$ such that the sequence $\{x_n\}$, $n = 0, 1, \ldots$ given by $x_n = x_{n-1} + x_{n-2} + x_{n-3}$ for $n \geqslant 3$ consists of composite numbers only. The initial values are
  $x_0 = 99202581681909167232$, $x_1 = 67600144946390082339$,
  $x_2 = 139344212815127987596$. This is also a natural extension of a similar result of Graham [15] for the Fibonacci-like sequence.

- Finally, we generalized the previous result. We proved that for each positive integer k in the range $2 \leqslant k \leqslant 10$ and for each positive integer $k \equiv 79 \pmod{120}$ there is a k-step Fibonacci-like sequence of composite numbers and gave examples of such sequences.

The thesis has raised significant questions, which have been left unanswered and could be analyzed in further research. It would be of great

interest to extend our results to linear recurrence sequences of order d, where $d \geqslant 3$. For which $(a_0, \ldots, a_{d-1}) \in \mathbb{Z}^d$, where $a_d \neq 0$, one can choose d integers $x_0, \ldots, x_{d-1}$ satisfying $\gcd(x_0, \ldots, x_{d-1}) = 1$ such that the sequence

$$x_{n+d} = a_{d-1}x_{n+d-1} + a_{d-2}x_{n+d-2} + \cdots + a_0 x_n, \ n = 0, 1, 2, \ldots,$$

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. There are no methods that would allow us to show that the cases, where the characteristic polynomial

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

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 non-negative integer points which is completely out of reach.

We hope that the results of this thesis will be useful for further research.

Bibliography

[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] Y. Bilu, G. Hanrot, P.M. Voutier, and M. Mignotte, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122.

[4] Y.G. Chen, *On integers of the form* $2^n \pm p_1^{\alpha_1} \dots p_r^{\alpha_r}$, Proc. Amer. Math. Soc. **128** (2000), 1613 – 1616.

[5] Y.G. Chen, R. Feng, and N. Templier, *Fermat numbers and integers of the form* $a^k + a^l + p^a$, Acta Arith. **135** (2008), 51–61.

[6] S.L.G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comp. **25** (1971), 885–895.

[7] F. Cohen and J.L. Selfridge, *Not every number is the sum or difference of two prime powers*, Math. Comp. **29** (1975), 79 – 81.

[8] R. Crocker, *On the sum of the prime and two powers of two*, Pacific J. Math. **36** (1971), 103 – 107.

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

[10] A. Dubickas, A. Novikas, and J. Šiurys, *A binary linear recurrence sequence of composite numbers*, J. Number Theory **130** (2010), 1737–1749.

[11] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. **36** (1950), 113–123.

[12] I. Flores, *Direct calculation of k-generalized Fibonacci numbers*, Fibonacci Quart. **5** (1967), 259–266.

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

[14] Great Internet Mersenne Prime Search (GIMPS), `http://mersenne.org/`.

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

[16] R. Guy, *Unsolved problems in number theory*, Springer, New York, 2004.

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

[18] A.S. Izotov, *Second-order linear recurrences of composite numbers*, Fibonacci Quart. **40** (2001), no. 3, 266 – 268.

[19] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav. **16** (2008), 15–20.

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

[21] H.W. Lenstra, *Primality testing*, Studieweek Getaltheorie en Computers, Amsterdam, Sept. 1-5 1980.

[22] F. Luca and P. Stănică, *Fibonacci numbers that are not sums of two prime powers*, Proc. Amer. Math. Soc. **133** (2005), 1887 – 1890.

[23] E. Manstavičius, *Analizinė ir tikimybinė kombinatorika*, TEV, Vilnius, 2007.

[24] J.W. Nicol, *A Fibonacci-like sequence of composite numbers*, Electron. J. Comb. **6** (1999), no. #R44, 6p.

[25] T.D. Noe and J.V. Post, *Primes in Fibonacci n-step and Lucas n-step sequences*, J. Integer Seq. **8** (2005), no. Art. 05.4.4, 12p.

[26] A. Novikas, *Composite numbers in the sequences of integers*, Ph.D. thesis, Vilnius University, 2012.

[27] The Seventeen or Bust, `http://www.seventeenorbust.com/stats/`.

[28] Proth Search Page, `http://www.prothsearch.net/sierp.html`.

[29] H. Pan and W. Zhang, *On the integers of the form* $p^2+b^2+2^n$ *and* $b_1^2+b_2^2+2^{n^2}$, Math. Comp. **80** (2011), 1849 – 1864.

[30] J.C. Parnami and T.N. Shorey, *Subsequences of binary recursive sequences*, Acta Arith. **40** (1982), 193–196.

[31] C. Pomerance, *Recent developments in primality testing*, Math. Intelligencer **3** (1981), no. 3, 97 – 105.

[32] N.P. Romanoff, *Über einige sätze der additiven zahlentheorie*, Math. Ann. **57** (1934), 668 – 678.

[33] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. **15** (1960), 73–74.

[34] J. Šiurys, *A tribonacci-like sequence of composite numbers*, Fibonacci Quart. **49** (2011), no. 4, 298–302.

[35] L. Somer, *Second-order linear recurrences of composite numbers*, Fibonacci Quart. **44** (2006), no. 4, 358–361.

[36] Z.W. Sun, *On integers not of the form* $\pm p^a \pm q^b$, Proc. Amer. Math. Soc. **128** (2000), 997–1002.

[37] The PARI Group, *PARI/GP, version* 2.5.3, 2012, Available online at
`http://pari.math.u-bordeaux.fr/`.

[38] M. Vsemirnov, *A new Fibonacci-like sequence of composite numbers*, J. Integer Seq. **7** (2004), no. Art. 04.3.7, 3 p.

[39] M.E. Waddill, *Some properties of a generalized Fibonacci sequence modulo* m, Fibonacci Quart. **16** (1978), 344–353.

[40] S.S. Wagstaff, *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), 385–397.

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

[42] K.J. Wu and Z.W. Sun, *Covers of the integers with odd moduli and their applications to the forms* $x^m - 2^n$ *and* $x^2 - F_{3n}/2$, Math. Comp. **78** (2009), no. 267, 1853 – 1866.

[43] S.Y. Yan, *Number theory for computing*, 2nd ed., Springer, Berlin, 2002.