A TRIBONACCI-LIKE SEQUENCE OF COMPOSITE NUMBERS

JONAS ŠIURYS

ABSTRACT. We find three positive integers x_0, x_1, x_2 satisfying $\gcd(x_0, x_1, x_2) = 1$ such that the tribonacci-like sequence $(x_n)_{n=0}^{\infty}$ given by $x_{n+1} = x_n + x_{n-1} + x_{n-2}$ for $n \geqslant 2$ consists of composite numbers only. The initial values are $x_0 = 99202581681909167232$, $x_1 = 67600144946390082339$, $x_2 = 139344212815127987596$. This is a natural extension of a similar result of Graham for the Fibonacci-like sequence.

1. Introduction

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

$$x_{n+1} = x_n + x_{n-1} + x_{n-2} \tag{1.1}$$

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, [5, 8, 11]. The aim of this paper 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.

In general, it is difficult to say whether a given integer sequence contains some prime (or composite) numbers or not. In 1960, Sierpiński [9] proved that there exist infinitely many odd integers k such that $k \cdot 2^n + 1$ is composite for every $n \in \mathbb{N}$. Two years later, Selfridge (unpublished) showed that 78557 is a Sierpiński number, i.e., $78557 \cdot 2^n + 1$ is composite for each $n \in \mathbb{N}$. However, after extensive computer calculation it has not yet been proven that 78557 is the smallest Sierpiński number (see, e.g., [3, Section B21], [14, 15]).

The main motivation of this paper is an old result of Graham [2]. He found a sequence given by some initial values x_0, x_1 with $\gcd(x_0, x_1) = 1$ and the binary recurrence

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

for $n = 1, 2, 3, \ldots$ that contains only composite numbers. Graham's pair (x_0, x_1) was

$$(331635635998274737472200656430763, 1510028911088401971189590305498785).$$

Several authors (see [6, 7, 12]) made some progress in finding smaller pairs. Currently, the smallest known such pair (in the sense that $\max(x_0, x_1)$ is the smallest positive integer) is due to Vsemirnov [10]

$$(x_0, x_1) = (106276436867, 35256392432).$$

The complete analysis of a binary linear recurrence sequence of composite numbers is given in [1]. The main result of [1] is the following: if $(a, b) \in \mathbb{Z}^2$, where $b \neq 0$ and $(a, b) \neq (\pm 2, -1)$, then there exist two positive relatively prime composite integers x_0, x_1 such that the sequence given by $x_{n+1} = ax_n + bx_{n-1}$, $n = 1, 2, \ldots$, consists of composite numbers only.

As pointed out in [1], all these results are 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 [4], 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 paper we shall overcome this difficulty and prove the following result.

Theorem 1.1. *If*

$$x_0 = 99202581681909167232,$$
$$x_1 = 67600144946390082339,$$
$$x_2 = 139344212815127987596,$$

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 2.2, we give a sufficient condition for the sequence $(y_n)_{n=0}^{\infty} \equiv S(0, a, b) \pmod{p}$ 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 $(y_n)_{n=0}^{\infty} \equiv S(0, a, b) \pmod{p}$ means "for every $n \geqslant 0$, $y_n \equiv S(0, a, b)_n \pmod{p}$". In Lemma 2.3 we discuss how to choose y_1 and y_2 so that the condition of Lemma 2.2 would be satisfied. In Section 3 our main result will be proved.

2. Auxiliary Lemmas

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

Lemma 2.1. *If* $(u_n)_{n=0}^{\infty} = S(a, b, c)$, $(v_n)_{n=0}^{\infty} = S(a', b', c')$, *and* $(z_n)_{n=0}^{\infty} = S(a+a', b+b', c+c')$, *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 $(s_n)_{n=0}^{\infty} = S(0, 1, 0)$ and $(t_n)_{n=0}^{\infty} = S(0, 0, 1)$. Let p be a prime number and let $(y_n)_{n=0}^{\infty} \equiv S(0, a, b) \pmod{p}$ for $a, b \in \mathbb{Z}$. Lemma 2.1 implies

$$y_n \equiv s_n a + t_n b \pmod{p}. \tag{2.1}$$

Lemma 2.2. *Let p be a prime number and let* $(y_n)_{n=0}^{\infty} \equiv S(0, a, b) \pmod{p}$ *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

$$Y_{km} = (y_{km+2}, y_{km+1}, y_{km}) = (y_2, y_1, y_0)(A^m)^k. \tag{2.2}$$

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 (2.2). 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 2.3. *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 2.2, 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:

$$\begin{cases} s_m a + t_m b \equiv 0 \pmod p, \\ s_{2m} a + t_{2m} b \equiv 0 \pmod p. \end{cases} \tag{2.3}$$

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 (2.3) is satisfied. Then the second equation is equivalent to

$$-s_{2m} t_m + s_m t_{2m} \equiv 0 \pmod p. \tag{2.4}$$

Hence, by the condition of the lemma, (2.4) is true, which completes the proof of the lemma. □

3. Proof of Theorem 1.1

Consider the following table:

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 1

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

$$P_i = \{m_i k + r_i, k \in \mathbb{Z}\}, \quad i = 1, 2, \ldots 11. \tag{3.1}$$

In other words, the integers m_i, r_i are chosen so that $P_1, P_2, \ldots, P_{11}$ is a *covering system* of $\mathbb{Z}$, i.e.,

$$\mathbb{Z} = \bigcup_{i=1}^{11} P_i. \tag{3.2}$$

To prove (3.2) 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 (3.1).

We are interested in the differences $s_{m_i} t_{2m_i} - s_{2m_i} t_{m_i}$ $(i = 1, 2, \ldots, 11)$.
Let us fix $i \in \{1, 2, \ldots, 11\}$. As we can see from Table 2, each prime number p_i divides the corresponding difference $s_{m_i} t_{2m_i} - s_{2m_i} t_{m_i}$. By Lemma 2.3, 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

$$s_{km_i} a_i + t_{km_i} b_i \equiv 0 \pmod{p_i} \tag{3.3}$$

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

Next, we shall construct the sequence $(x_n)_{n=0}^{\infty} = S(x_0, x_1, x_2)$ satisfying

$$x_n \equiv s_{m_i - r_i + n}\, a_i + t_{m_i - r_i + n}\, b_i \pmod{p_i} \quad i = 1, 2, \ldots 11 \tag{3.4}$$

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

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

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 2

for $i = 1, 2, \ldots, 11$. Since the sequence $(x_n)_{n=0}^{\infty}$ is defined by its first three terms, it suffices to solve the following equations:

$$\begin{aligned} x_0 &\equiv A_i \pmod{p_i},\\ x_1 &\equiv B_i \pmod{p_i},\\ x_2 &\equiv C_i \pmod{p_i}, \end{aligned} \tag{3.5}$$

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 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 3

By the Chinese Reminder Theorem (see, e.g., in [13, Theorem 1.6.21]), we find that the system of congruences (3.5) 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 (3.3) and (3.4), 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 (2.3), then (ka, kb), where $k \in \mathbb{Z}$, is also a solution of (2.3). So we can vary (a_i, b_i) in Table 3. Also, we can choose a different covering system based on another set of primes.

4. Acknowledgement

I am very grateful to A. Dubickas and the referees for useful comments and corrections.

References

[1] A. Dubickas, A. Novikas, and J. Šiurys, *A binary linear recurrence sequence of composite numbers*, J. Number Theory, **130** (2010), 1737–1749.
[2] R. L. Graham, *A Fibonacci-like sequence of composite numbers*, Math. Mag., **37** (1964), 322–324.
[3] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer-Verlag, 2004.
[4] M. Hall, *Divisibility sequences of third order*, Am. J. Math., **58** (1936), 577–584.
[5] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav., **16** (2008), 15–20.
[6] D. E. Knuth, *A Fibonacci-like sequence of composite numbers*, Math. Mag., **63** (1990), 21–25.
[7] J. W. Nicol, *A Fibonacci-like sequence of composite numbers*, Electron. J. Comb., **6** (1999), #R44, 6p.
[8] T. D. Noe and J. V. Post, *Primes in Fibonacci n-step and Lucas n-step sequences*, J. Integer Seq., **8** (2005), Art. 05.4.4, 12p.
[9] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math., **15** (1960), 73–74.
[10] M. Vsemirnov, *A new Fibonacci-like sequence of composite numbers*, J. Integer Seq., **7** (2004), Art. 04.3.7, 3 p.
[11] M. E. Waddill, *Some properties of a generalized Fibonacci sequence modulo m*, The Fibonacci Quarterly, **16** (1978), 344–353.
[12] H. S. Wilf, *Letters to the editor*, Math. Mag., **63** (1990), 284.
[13] S. Y. Yan, *Number Theory for Computing*, 2nd ed., Springer, Berlin, 2002.
[14] `http://www.prothsearch.net/sierp.html`
[15] `http://www.seventeenorbust.com/stats/`

MSC2010: 11B37, 11A07, 11Y55

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, Vilnius, LT-03225, Lithuania
E-mail address: `jonas.siurys@gmail.com`