JOURNAL OF SCIENCE
SAKARYA UNIVERSITY

Sakarya University Journal of Science

ISSN 1301-4048 | e-ISSN 2147-835X | Period Bimonthly | Founded: 1997 | Publisher Sakarya University | http://www.saujs.sakarya.edu.tr/

Title: Some Notes on Odd or Even Indexed Fibonacci And Lucas Sequences

Authors: Alparslan Kargın, Emre Kişi, Halim Özdemir
Recieved: 2019-03-06 18:12:32

Accepted: 2019-05-11 17:49:56

Article Type: Research Article
Volume: 23
Issue: 5
Month: October
Year: 2019
Pages: 929-933

How to cite
Alparslan Kargın, Emre Kişi, Halim Özdemir; (2019), Some Notes on Odd or Even Indexed Fibonacci And Lucas Sequences. Sakarya University Journal of Science, 23(5), 929-933, DOI: 10.16984/saufenbilder.536642
Access link
http://www.saujs.sakarya.edu.tr/issue/44066/536642

Sakarya University Journal of Science 23(5), 929-933, 2019

Some Notes on Odd or Even Indexed Fibonacci and Lucas Sequences

Alparslan Kargın[1], Emre Kişi*[1] and Halim Özdemir[1]

Abstract

The uniqueness of the sum of the elements of finite subsets of the odd or even indexed Fibonacci and Lucas sequences are proved. Moreover, it is shown that the odd or even indexed Fibonacci and Lucas sequences are super-increasing sequences. By using the uniqueness properties established, a new cryptology method is presented and exemplified.

Keywords: Fibonacci numbers, Lucas numbers, odd index, even index, cryptology

1. INTRODUCTION

Fibonacci and Lucas sequences have been appearing not only in pure mathematics but also in many applied sciences such as cryptography and coding theory [6-11]. The odd indexed Fibonacci and Lucas sequences are the sequences which consist of odd indexed terms of the Fibonacci and Lucas sequences. Similarly, we can define even indexed Fibonacci and Lucas sequences. In this work, the odd and even indexed Fibonacci and Lucas sequences are mainly considered. The results related to the uniqueness of the sum of the elements of the finite subsets of the odd and even indexed Fibonacci and Lucas sequences are established. By utilizing the results obtained a new cryptology method is developed, and it is illustrated with an example. Moreover, it is shown that the odd or even indexed Fibonacci and Lucas sequences are super-increasing sequences. The super-increasing sequences are known to be used in the Merkle-Hellman cryptology system [1].

2. PRELIMINARIES

Definition 2.1. Let $F_0 = 0$ and $F_1 = 1$. The sequence $\{F_n\}(n = 1,2,3,...)$ with the recurrence relation $F_{n+1} = F_n + F_{n-1}$ is called *Fibonacci sequence* [2,3]. The elements of this sequence are called *Fibonacci numbers*.

From now on, the sets of Fibonacci numbers, the even indexed Fibonacci numbers, i.e. $\{F_0, F_2, F_4, ..., F_{2k}, ...\}$, and the odd indexed Fibonacci numbers, i.e. $\{F_1, F_3, F_5, ..., F_{2k+1}, ...\}$, will be denoted by F, F_E, and F_O, respectively.

* Corresponding Author
[1] Sakarya University, Department of Mathematics, 54100, Sakarya, Turkey akargin@gmail.com, ekisi@sakarya.edu.tr .ORCID: 0000-0001-7763-8932, hozdemir@sakarya.edu.tr .ORCID: 0000-0003-4624-437X

Definition 2.2. Let $L_0 = 1$ and $L_1 = 3$. The sequence $\{L_n\}(n = 1, 2, 3, ...)$ with the recurrence relation $L_{n+1} = L_n + L_{n-1}$ is called *Lucas sequence* [2,3]. The elements of this sequence are called *Lucas numbers*.

Hereafter, the sets of Lucas numbers, the even indexed Lucas numbers, and the odd indexed Lucas numbers will be denoted by L, L_E, and L_O, respectively.

Definition 2.3. Let (b_n) a sequence such that $b_n \in \mathbb{N}$ for every $n \in \mathbb{N}$. (b_n) is said to be a super-increasing sequence if it satisfies the property that $b_n > \sum_{j=1}^{n-1} b_j$ for each $n \geq 2$ [5].

Lemma 2.4. For each $n \in \mathbb{N}$, $\sum_{i=1}^{n} F_{2i-1} = F_{2n}$ [2].

Lemma 2.5. For each $n \in \mathbb{N}$, $\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$ [2].

3. RESULTS

In this section, the uniqueness of the sum of the elements of finite subsets of the odd or even indexed Fibonacci and Lucas sequences are proved. Moreover, it is shown that the odd and even indexed Fibonacci and Lucas sequences are super-increasing sequences. Since the proofs are similar, the proof will be given only for odd indexed Fibonacci sequence.

Theorem 3.1. .

a) Let A and B be any two finite subsets of F_O such that $A \neq B$. Then $\sum_{F_i \in A} F_i \neq \sum_{F_j \in B} F_j$.

b) Let A and B be any two finite subsets of L_O such that $A \neq B$. Then $\sum_{L_i \in A} L_i \neq \sum_{L_j \in B} L_j$.

Proof: Since the elements in the intersection of the sets A and B can be eliminated from both sides of the sum, without loss of generality it is assumed that $A \cap B = \varnothing$. Let k be a positive integer such that $F_{2k+1} = \max\{F_i \mid F_i \in A \cup B\}$. Then, either $F_{2k+1} \in A$ or $F_{2k+1} \in B$. If $F_{2k+1} \in A$, then $B \subset \{F_1, F_3, ..., F_{2k-1}\}$. Hence, we get the following inequality

$$\sum_{F_i \in B} F_i \leq \sum_{i=1}^{k} F_{2i-1} . \quad (1)$$

From the inequality (1) and Lemma 2.4, we get

$$\sum_{F_i \in B} F_i \leq \sum_{i=1}^{k} F_{2i-1} = F_{2k} < F_{2k+1} < \sum_{F_j \in A} F_j . \quad (2)$$

It is seen from the inequality (2) that $\sum_{F_i \in B} F_i \neq \sum_{F_j \in A} F_j$.

Hence, the proof is completed. ∎

Theorem 3.2.

a) Let A be a subset of F_O such that $A = \{a_i \in F_O \mid a_1 < a_2 < \cdots < a_n,\ n \in \mathbb{N}\}$. Then, A is a super-increasing sequence.

b) Let A be a subset of L_O such that $A = \{a_i \in L_O \mid a_1 < a_2 < \cdots < a_n,\ n \in \mathbb{N}\}$. Then, A is a super-increasing sequence.

Proof: Let $F_{2k+1} \in A$ and $F_i \in A$ such that $i < 2k+1$, where k is a positive integer and i is an odd positive integer. Then, we get the inequality

$$\sum_{F_i \in A} F_i \leq \sum_{j=1}^{k} F_{2j-1} . \quad (3)$$

From the inequality (3) and Lemma 2.4, we obtain

$$\sum_{F_i \in A} F_i \leq \sum_{j=1}^{k} F_{2j-1} = F_{2k} < F_{2k+1} .$$

Hence, the proof is completed. ∎

Corollary 3.3. Since $F_O \subset F_O$ and $L_O \subset L_O$, both F_O and L_O themselves are also super-increasing sequences.

Since the proofs of the Theorems 3.4 and 3.5 given in the following are quite similar with the proofs of the Theorems 3.1 and 3.2, respectively, they will be omitted.

Theorem 3.4.

a) Let A and B be any two finite subsets of F_E such that $A \neq B$. Then $\sum_{F_i \in A} F_i \neq \sum_{F_j \in B} F_j$.

b) Let A and B be any two finite subsets of L_E such that $A \neq B$. Then $\sum_{L_i \in A} L_i \neq \sum_{L_j \in B} L_j$.

Theorem 3.5.

a) Let A be a subset of F_E such that $A = \{a_i \in F_E \mid a_1 < a_2 < \cdots < a_n,\ n \in \mathbb{N}\}$. Then A is a super-increasing sequence.

b) Let A be a sorted subset of L_E such that $A = \{a_i \in F_E \mid a_1 < a_2 < \cdots < a_n,\ n \in \mathbb{N}\}$. Then A is a super-increasing sequence.

Corollary 3.6. Since $F_E \subset F_E$ and $L_E \subset L_E$, both F_E and L_E themselves are also super-increasing sequences.

4. APPLICATION

Fibonacci and Lucas sequences have been used in many applied sciences such as cryptography and coding theory [6-11]. In this section a new cryptology method, which is based on the uniqueness property of the sum of the elements of the subsets of the odd indexed Fibonacci sequences, is developed, and it is illustrated with an example. The method is presented for odd indexed Fibonacci sequence. Obviously, with a similar manner, it can be also developed for even indexed Fibonacci and odd and even indexed Lucas sequences.

Now we can explain the method. Firstly, each letter is matched with the numerical value of the odd indexed Fibonacci numbers. This match is listed in Table 1. Obviously, this table can be extended according to characters that are wanted to be used.

Table 1: Numerical correspondence of the letters

Letters	Corresponding Fibonacci Numbers	Numerical value
A	F_1	1
B	F_3	2
C	F_5	5
D	F_7	13
E	F_9	34
F	F_{11}	89
G	F_{13}	233
H	F_{15}	610
I	F_{17}	1.597
J	F_{19}	4.181
K	F_{21}	10.946
L	F_{23}	28.657
M	F_{25}	75.025
N	F_{27}	196.418
O	F_{29}	514.229
P	F_{31}	1.346.269
Q	F_{33}	3.524.578
R	F_{35}	9.227.465
S	F_{37}	24.157.817
T	F_{39}	63.245.986
U	F_{41}	165.580.141
V	F_{43}	433.494.437
W	F_{45}	1.134.903.170
X	F_{47}	2.971.215.073
Y	F_{49}	7.778.742.049
Z	F_{51}	20.365.011.074

Encryption Algorithm

Step 1: Determine the different letters in the plaintext.

Step 2: Sort them alphabetically and enumerate them.

Step 3: Sum the numerical values of the corresponding Fibonacci numbers of the letters.

Step 4: Set a sorting code by utilizing the corresponding enumeration of the letters.

Step 5: Set an ordered pair in which the first component is the sum and the second component is the sorting code. This ordered pair is the ciphertext.

Deciphering Algorithm

Step 1: Find the biggest Fibonacci number which is smaller than the sum (the first component of the ordered pair) and subtract it from the sum. Repeat this step until reaching zero.

Step 2: Determine the corresponding letters of the Fibonacci numbers used in step 1.

Step 3: Sort these letters alphabetically and enumerate them.

Step 4: Set the plaintext by utilizing the sorting code (the second component of the ordered pair)

Example 4.1: Let us encrypt the word "HELLO".

Encryption Algorithm:

Step 1: The different letters in the word are H, E, L, O.

Step 2: The enumeration of the alphabetically ordered letters is listed in Table 2.

Table 2: The enumeration of the alphabetically ordered letters

E	H	L	O
1	2	3	4

Step 3: The sum of the corresponding Fibonacci numbers of the letters is 34 + 610 + 28657 + 514229= 543530.

Step 4: The sorting code of the word is 21334.

Step 5: The ciphertext is (543530, 21334).

Deciphering Algorithm:

Step 1: The biggest Fibonacci number which is smaller than 543530 is 514229. The difference of these numbers is 543530 – **514229** = 29301. By continuing the process similarly, the numbers in the following are obtained: 29301 – **28657** = 644, 644 – **610** = 34, and 34 – **34** = 0.

Step 2: The corresponding letters of the Fibonacci numbers used in previous step are O, L, H, and E, respectively.

Step 3: The alphabetic order of the letters which are determined in step 2 and the corresponding enumeration of them are as in Table 2.

Step 4: By utilizing the sorting code 21334 the plaintext "HELLO" is obtained.

REFERENCES

[1] Merkle–Hellman knapsack cryptosystem, https://en.wikipedia.org/wiki/Merkle%E2%80%93Hellman_knapsack_cryptosystem.

[2] Koshy, T., 2001, Fibonacci and Lucas numbers with applications, John Wiley & Sons, New York-Toronto.

[3] Vajda, S., 1989, Fibonacci and Lucas Numbers and the Golden Section: Theory and Applications, Courier Corporation.

[4] Brannan, D.A., 2006, A First Course in Mathematical Analysis, Cambridge University Press.

[5] Mollin, R.A., 2007, An Introduction to Cryptography, Chapman&Hall/CRC, Boca Raton.

[6] Uçar, S., Taş, N., Özgür, N.Y., A new cryptography model via Fibonacci and Lucas numbers, arXiv: 1709.10355 [cs.CR].

[7] N Taş, S Uçar, N.Y. Özgür, Ö.Ö. Kaymak, 2018, A new coding/decoding algorithm using Fibonacci numbers, Discrete Mathematics, Algorithms and Applications 10 (02).

[8] M. Basu, B. Prasad, The generalized relations among the code elements for Fibonacci coding theory, Chaos Solitons Fractals 41 (2009), no. 5, 2517–2525.

[9] S. Prajapat, A. Jain, R. S. Thakur, A Novel Approach For Information Security With Automatic Variable Key Using Fibonacci Q-Matrix, IJCCT 3 (2012), no. 3, 54–57.

[10] A. Stakhov, V. Massingue, A. Sluchenkov, Introduction into Fibonacci Coding and Cryptography, Osnova, Kharkov (1999).

[11] A. P. Stakhov, Fibonacci matrices, a generalization of the Cassini formula and a new coding theory, Chaos Solitons Fractals 30 (2006), no. 1, 56–66.