Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 4, 58–68

Some results about linear recurrence relation homomorphisms

Alexandre Laugier[1] and Manjil P. Saikia[2]

[1] Lycée professionnel Tristan Corbière
16 rue de Kervéguen - BP 17149 - 29671 Morlaix Cedex, France
e-mail: `laugier.alexandre@orange.fr`

[2] Diploma Student (Mathematics), The Abdus Salam International Centre for Theoretical Physics
Strada Costiera-11, Miramare, I-34151, Trieste, Italy
e-mails: `manjil@gonitsora.com`, `msaikia@ictp.it`

Abstract: In this paper we propose a definition of a recurrence relation homomorphism and illustrate our definition with a few examples. We then define the period of a k-th order of linear recurrence relation and deduce certain preliminary results associated with them.
Keywords: k-th order of recurrence relations, Recurrence relation homomorphisms, Strong divisibility sequences, Periodic sequences.
AMS Classification: 11B37, 11B50.

1 Introduction and Motivation

This paper is divided into two sections, in the first section we give some introductory remarks and set the notation for the rest of the paper; whereas in the second section we discuss linear recurrence relation homomorphisms and discuss some preliminary properties of such homomorphisms.

We begin with the following definitions from [3] and a few notations to be used throughout this paper.

Definition 1.1. A k-th order of recurrence relation on some set X is a function $a : \mathbb{N} \to X$ with $a_1, \ldots, a_k$ defined for all $i \geq 0$, $k \geq 1$ and $a_{i+k+1} = f(a_{i+1}, \ldots, a_{i+k})$.

Definition 1.2. Let a_n be a k-th order recurrence relation on the set X defined by the map $f : X^k \to X$ with initial values. A map $\varphi : X \to Y$ is said to be a recurrence relation homomorphism on a, when there exists $f' : Y^k \to Y$ satisfying $\varphi \circ f = f \circ \varphi$.

Notation 1.3. (m, n) denotes the gcd of m and n for natural numbers m and n.

Notation 1.4. We denote the set $\{1, 2, \ldots, n\}$ by $[[1, n]]$ for $n \geq 2$.

Definition 1.5. A sequence (b_n) is called a strong divisibility sequence if $(b_n, b_m) = b_{(m,n)}$.

Definition 1.6. The Fibonacci sequence (F_n) is defined in the usual way as $F_0 = 0, F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

We see now that taking $k \geq 1$ and defining the maps $f : X^k \to X$, $\varphi : X \to Y$ and $\varphi^{(k)} : X^k \to Y^k$ such that $\varphi^{(k)}(a_i, \ldots, a_{i+k-1}) = (\varphi(a_i), \ldots, \varphi(a_{i+k-1}))$ for $i \geq 1$, and a be a k-th order of recurrence relation on X which is defined by the map f (with initial values $a_1, \ldots, a_k$), if there exists $f' : Y^k \to Y$ such that

$$\varphi \circ f(a_i, \ldots, a_{i+k-1}) = f' \circ \varphi^{(k)}(a_i, \ldots, a_{i+k-1})$$

for all $i \geq 1$ and for all $(a_i, \ldots, a_{i+k-1}) \in X^k$, then the diagram

$$\begin{array}{cccc} & X^k & \xrightarrow{f} & X & \\ \varphi^{(k)} & \downarrow & & \downarrow & \varphi \\ & Y^k & \xrightarrow{f'} & Y & \end{array}$$

commutes. That is $\varphi \circ f = f' \circ \varphi^{(k)}$.

So we propose the following alternative definition of a recurrence relation homomorphism as in Definition 1.2, which maps set X onto set Y.

Definition 1.7. Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on some set X such that $a_1, \ldots, a_k$ defined and for all $i, k \geq 1$, $a_{i+k} = f(a_i, \ldots, a_{i+k-1})$ with $f : X^k \to X$. A map $\varphi : X \to Y$ is said to be a recurrence relation homomorphism on a, when there exists $f' : Y^k \to Y$ satisfying the commutative relation $\varphi \circ f = f' \circ \varphi^{(k)}$.

We shall now give an alternate proof of the following theorem that appears in [3].

Theorem 1.8. *Suppose we are given a recurrence relation homomorphism in the above notation, then $b_n = \varphi(a_n)$ is a k-th order of recurrence relation.*

Proof. It suffices to state that, according to our definition, defining the sequence $b : \mathbb{N} \to Y$ by $b_n = \varphi(a_n)$, we have for the given k initial values, with $i, k \geq 1$,

$$\begin{aligned} b_{i+k} = \varphi(a_{i+k}) &= \varphi(f(a_i, \ldots, a_{i+k-1})) = f'(\varphi^{(k)}(a_i, \ldots, a_{i+k-1})) \\ &= f'(\varphi(a_i), \ldots, \varphi(a_{i+k-1})) = f'(b_i, \ldots, b_{i+k-1}). \end{aligned}$$

This completes the proof. $\square$

We now illustrate our definition with the following examples.

Example 1.9. Let X be the ring of integers. Let a be a k-th order of recurrence relation on $\mathbb{Z}$ defined by the linear map $f : \mathbb{Z}^k \to \mathbb{Z}$ with $k \geq 1$ and initial values $a_1, \ldots, a_k$ given such that for $i \geq 1$ we have

$$a_{i+k} = f(a_i, \ldots, a_{i+k-1}) = \sum_{j=1}^{k} f_j \cdot a_{i+j-1},$$

with $(f_1, \ldots, f_k) \in \mathbb{Z}^k$. A particular case is when $f_j = a_j$ with $j = 1, \ldots, k$. It can be compared to the relation $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$ with $n \in \mathbb{N}$ and $m \in \mathbb{N}^\star$.

Example 1.10. In the following, we use the system of residue classes of integers modulo $m \geq 1$ given by $[0]_m, \ldots, [m-1]_m$ where the notation $[x]_m$ means the equivalence class of the integer $x \in [[0, m-1]]$ modulo $m \geq 1$

$$[x]_m = \{x + km \,:\, k \in \mathbb{Z}\}\,.$$

Let us consider the map $\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $m \in \mathbb{N}^\star$ defined for $x \in \mathbb{Z}$ by,

$$\pi_m(x) = [x]_m.$$

By our construction of π_m, it is a surjective morphism of rings. So, we will have for $i, k \geq 1$,

$$\pi_m(a_{i+k}) = \sum_{j=1}^{k} [f_j]_m \cdot [a_{i+j-1}]_m.$$

Therefore $(i, k \geq 1)$

$$[a_{i+k}]_m = \sum_{j=1}^{k} [f_j]_m \cdot [a_{i+j-1}]_m,$$

and so for $i, k \geq 1$ we have

$$[a_{i+k}]_m = \psi_f([a_i]_m, \ldots, [a_{i+k-1}]_m).$$

where $\psi_f : (\mathbb{Z}/m\mathbb{Z})^k \to \mathbb{Z}/m\mathbb{Z}$ is the linear map defined by $(i, k \geq 1)$:

$$\psi_f([a_i]_m, \ldots, [a_{i+k-1}]_m) = \sum_{j=1}^{k} [f_j]_m \cdot [a_{i+j-1}]_m.$$

So, as we can observe, $[a]_m$ is a k-th order of recurrence relation on the ring $\mathbb{Z}/m\mathbb{Z}$ such that all $[a_1]_m, \ldots, [a_k]_m$ are defined and for all $i, k \geq 1$, $[a_{i+k}]_m = \psi_f([a_i]_m, \ldots, [a_{i+k-1}]_m)$ with $\psi_f : (\mathbb{Z}/m\mathbb{Z})^k \to \mathbb{Z}/m\mathbb{Z}$.

Moreover, we have $(i, k \geq 1)$

$$\begin{aligned}
\psi_f(\pi_m^{(k)}(a_i, \ldots, a_{i+k-1})) &= \psi_f(\pi_m(a_i), \ldots, \pi_m(a_{i+k-1})) \\
&= \psi_f([a_i]_m, \ldots, [a_{i+k-1}]_m) \\
&= [a_{i+k}]_m = \pi_m(a_{i+k}) = \pi_m(f(a_i, \ldots, a_{i+k-1})).
\end{aligned}$$

Since f is any linear function, which maps the set $\mathbb{Z}^k$ onto the set $\mathbb{Z}$, the diagram

$$\begin{array}{ccccc}
 & \mathbb{Z}^k & \xrightarrow{f} & \mathbb{Z} & \\
\pi_m^{(k)} & \downarrow & & \downarrow & \pi_m \\
 & (\mathbb{Z}/m\mathbb{Z})^k & \xrightarrow{\psi_f} & \mathbb{Z}/m\mathbb{Z} &
\end{array}$$

commutes. That is $\pi_m \circ f = \psi_f \circ \pi_m^{(k)}$.

2 Some results on recurrence relation homomorphisms

We have seen that our definition of a recurrence relation homomorphism is more natural than Definition 1.2 given in [3] and in the remaining part of the paper we shall derive certain interesting results and consequences of this definition. We begin with the following definition.

Definition 2.1. Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by the map $f : X^k \to X$ with $k \geq 1$ and initial values $a_1, \dots, a_k$ given. a is periodic modulo a positive integer m if we can find at least a non-zero positive integer $\ell(m)$ such that for all $n \in \mathbb{N}$ $[a_n]_m = [a_{n+\ell(m)}]_m$.

Remark 2.2. The definition above implies that if a is periodic modulo a positive integer m, then we can find at least a non-zero positive integer $\ell(m)$ such that for all $j, n \in \mathbb{N}$ $[a_n]_m = [a_{n+j\ell(m)}]_m$.

Theorem 2.3. *Let X a (commutative) ring where an equivalence relation $\sim$ can be defined so that the canonical surjection $X \to X/\sim$ is a surjective morphism of rings. Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 1$ and initial values $a_1, \dots, a_k$ given. If*

$$[a_{1+\ell(m)}]_m = [a_1]_m,$$
$$\vdots$$
$$[a_{k+\ell(m)}]_m = [a_k]_m,$$

then a is a periodic sequence modulo m.

Proof. Let us prove the theorem by induction in the case where $X = \mathbb{Z}$. The generalization of that is trivial.

In the theorem, we consider a sequence a which is k-th order of recurrence relation on a set X defined by the linear map $f : X^k \to X$ with $k \geq 1$ such that $[a_{j+\ell(m)}]_m = [a_j]_m$ with $j = 1, \dots, k$. Let us assume that $[a_{j+\ell(m)}]_m = [a_j]_m$ with $j = k+1, \dots, n$ and $n > k$. We have

$$[a_{n+1+\ell(m)}]_m = \psi_f([a_{n-k+1+\ell(m)}]_m, \dots, [a_{n+\ell(m)}]_m).$$

Since the numbers $n - k + i$ with $i \in [[1, k]]$ are less than n we get

$$[a_{n+1+\ell(m)}]_m = \psi_f([a_{n-k+1}]_m, \dots, [a_n]_m) = [a_{n+1}]_m.$$

This completes the rest of the proof. □

Proposition 2.4. *Let i, j be two non-zero positive integers. If a is a strong divisibility sequence which is periodic modulo m, then a period $\ell(m)$ of the sequence a modulo m satisfies $[a_{(i+\ell(m),j)}]_m = [w]_m[a_{(i,j)}]_m$ with $w \in \mathbb{Z}$.*

Proof. Let i, j two non-zero positive integers. If a is a strong divisibility sequence which is periodic modulo m with period $\ell(m) > 0$, then we have

$$[a_{(i+\ell(m),j)}]_m = [(a_{i+\ell(m)}, a_j)]_m.$$

Moreover, there exist two integers x, y such that

$$(a_{i+\ell(m)}, a_j) = xa_{i+\ell(m)} + ya_j.$$

Since $[a_{i+\ell(m)}]_m = [a_i]_m$, we can find an integer k such that $a_{i+\ell(m)} = a_i + km$. It implies

$$\begin{aligned}(a_{i+\ell(m)}, a_j) &= xa_i + ya_j + xkm \\ &\equiv xa_i + ya_j \pmod{m}.\end{aligned}$$

Thus, $[(a_{i+\ell(m)}, a_j)]_m = [xa_i + ya_j]_m$. Since (a_i, a_j) divides any linear combination of a_i, a_j, there exists an integer w such that $xa_i + ya_j = w(a_i, a_j)$. We thus have

$$[(a_{i+\ell(m)}, a_j)]_m = [w]_m[(a_i, a_j)]_m = [w]_m[a_{(i,j)}]_m.$$

This completes the proof. □

Proposition 2.5. *Let i, j be two non-zero positive integers. If a is a strong divisibility sequence which is periodic modulo m, then for any given $n \in \mathbb{Z}$, there exists $w_n \in \mathbb{Z}$ such that*

$$[a_{n(i,j)}]_m = [w_n]_m[a_{(i,j)}]_m.$$

Proof. Let i, j two non-zero positive integers. Let a be a strong divisibility sequence which is periodic modulo m with period $\ell(m) > 0$. Then, there exist three integers x, y, z such that

$$\begin{aligned}(i + \ell(m), j) &= x(i + \ell(m)) + yj \\ &= xi + yj + x\ell(m) \\ &= z(i, j) + x\ell(m).\end{aligned}$$

Since $(i + \ell(m), j) > 0$, if $z > 0$, then it follows that

$$[a_{(i+\ell(m),j)}]_m = [a_{z(i,j)+x\ell(m)}]_m = [a_{z(i,j)}]_m.$$

Or, from Proposition 2.4, there exists an integer w_z such that $[(a_{i+\ell(m)}, a_j)]_m = [w_z]_m[a_{(i,j)}]_m$. Therefore, we deduce that ($z > 0$)

$$[a_{z(i,j)}]_m = [w_z]_m[a_{(i,j)}]_m.$$

The case for $z < 0$ can now be easily verified from the previous case. □

Remark 2.6. If i, j are two non-zero integers such that $(i + \ell(m), j) = (i, j) + \ell(m)$ with $\ell(m)$ a period of a sequence a modulo m, then (i, j) divides a multiple of $\ell(m)$. Moreover, in this case, we have $[a_{(i+\ell(m),j)}]_m = [a_{(i,j)+\ell(m)}]_m = [a_{(i,j)}]_m$.

We now find an algorithm to find a period of a sequence modulo a non-zero positive integer m.

Let i, j, h be three non-zero positive integers such that $(i, j) = g$ and $(h, j) = 1$ with $gh > i$. If a is a strong divisibility sequence, which is periodic modulo m, then the non-zero positive number $t = gh - i$ satisfies $[a_{(i+t,j)}]_m = [a_g]_m$. Since $gh > i$, then $t = gh - i > 0$. Thus, we can try numbers like t in order to find a period of a strong divisibility sequence a which is periodic modulo m.

For instance, let us consider the Fibonacci sequence $(F_n)_{n\in\mathbb{N}}$ (in this case, we have $k = 2$, which refers to a second order of recurrence relation on a set X defined by a (linear) map). Let $5q + 2$ be a prime with q an odd positive integer. We take $i = 5q + 2$ and $j = 5q + 3$. Since i, j are two consecutive integers, the numbers i, j are relatively prime $(i, j) = g = 1$. Moreover, taking $h = i + 2j = 15q + 8$, we can notice that $3j - h = 1$. So, from Bezout's identity, we have $(h, j) = 1$. We have $gh = 15q + 8 > i$. The number $t = gh - i$ is given by $t = 2(5q + 3)$. Or, $2(5q+3)$ is a period of the Fibonacci sequence modulo $5q+2$ with q an odd positive integer. Thus, the algorithm allows to get a period of the Fibonacci sequence modulo $5q+2$ with q an odd positive integer.

The above result was also found in [4] by independent methods.

We are now ready to prove and discuss a few more general results in the remainder of this section.

Theorem 2.7. *Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 1$ and initial values $a_1, \ldots, a_k$ given. The sequence a is periodic modulo m with period $\ell(m) > k - 1$ if for all $i \in [[1, k]]$*

$$[f_i]_m = [a_i]_m,$$

$$[a_{2i+\ell(m)-k-1}]_m = [1]_m,$$

and

$$\sum_{j\in[[1,k]]-\{i\}} [f_j]_m \cdot [a_{i+\ell(m)-k+j-1}]_m = [0]_m.$$

Proof. We can notice that since $\ell(m) > k - 1$, we have $\ell(m) > k - i$ for all $i \in [[1, k]]$. Thus

$$a_{i+\ell(m)} = f(a_{i+\ell(m)-k}, \ldots, a_{i+\ell(m)-1}) = \sum_{j=1}^{k} f_j \cdot a_{i+\ell(m)-k+j-1}.$$

So,

$$\begin{aligned}
[a_{i+\ell(m)}]_m &= \sum_{j=1}^{k} [f_j]_m \cdot [a_{i+\ell(m)-k+j-1}]_m \\
&= [f_i]_m \cdot [a_{2i+\ell(m)-k-1}]_m + \sum_{j\in[[1,k]]-\{i\}} [f_j]_m \cdot [a_{i+\ell(m)-k+j-1}]_m \\
&= [a_i]_m.
\end{aligned}$$

Since i is any number of the set $[[1, k]]$, from Theorem 2.3, we conclude that $\ell(m)$ is a period of the sequence a. $\square$

Theorem 2.8. *Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 2$ and initial values $a_1, a_2, \ldots, a_k$ given. If a is a periodic sequence modulo m with period $\ell(m)$, then*

$$[a_k]_m = [f_1]_m[a_{\ell(m)}]_m + \sum_{i=2}^{k}[f_i]_m[a_{i-1}]_m.$$

The proof is an easy application of Theorem 2.3, so for the sake of brevity we shall omit it here.

Remark 2.9. Theorem 2.8 allows us to find in an algorithmic way, a period of sequence a modulo some positive integer $m \geq 1$. Indeed, the residue class $[r_{\ell(m)}]_m$ of $a_{\ell(m)}$ modulo a positive integer $m \geq 1$ such that $r_{\ell(m)}$ belongs to $[[0, m-1]]$, can be found by solving in the ring $\mathbb{Z}/m\mathbb{Z}$, the diophantine equation

$$[a_k]_m = [f_1]_m[a_{\ell(m)}]_m + \sum_{i=2}^{k}[f_i]_m[a_{i-1}]_m$$

where the unknown is $[a_{\ell(m)}]_m$ and $[a_i]_m$ with $i = 1, 2, \ldots, k$ such that $k \geq 2$ as well as m are given.

Theorem 2.10. *Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 1$ and initial values $a_1, \ldots, a_k$ given. Then, we have ($k \geq i \geq 1$)*

$$a_{k+i} = \sum_{m=1}^{i} C_{k,i-m+1} \sum_{j=m}^{k} f_{j-m+1} a_j,$$

with the sequence $(C_{k,n})$ defined by ($k \geq 1$)

$$C_{k,1} = 1,$$

and ($n \in [[2, k]]$ with $k \geq 2$)

$$C_{k,n} = \sum_{j=1}^{n-1} f_{k-j+1} C_{k,n-j}.$$

Proof. We can notice that for $i \geq 1$,

$$a_{k+i} = \sum_{j=1}^{k} f_j a_{i+j-1} = \sum_{j=1}^{k-i+1} f_j a_{i+j-1} + f_{k-i+2}a_{k+1} + \ldots + f_k a_{k+i-1}$$

So for $2 \leq i \leq k$, it gives

$$\begin{aligned} a_{k+i} &= \sum_{j=1}^{k-i+1} f_j a_{i+j-1} + \sum_{j=1}^{i-1} f_{k-i+j+1} a_{k+j} = \sum_{j=1}^{i-1} f_{k-i+j+1} a_{k+j} + \sum_{j=1}^{k-i+1} f_j a_{i+j-1} \\ &= \sum_{j=1}^{i-1} f_{k-i+j+1} a_{k+j} + \sum_{j=i}^{k} f_{j-i+1} a_j \end{aligned}$$

where we make the change of label $j \to l = i - 1 + j$ and afterwards we renamed l by j in the discrete sum $\sum_{j=1}^{k-i+1} f_j a_{i+j-1}$.

Let us prove the theorem by finite induction on the integer i (see [2] p.146, exercise 27). We have

$$a_{k+1} = \sum_{j=1}^{k} f_j a_j = C_{k,1} \sum_{j=1}^{k} f_j a_j = \sum_{m=1}^{1} C_{k,2-m} \sum_{j=m}^{k} f_{j-m+1} a_j.$$

Let us assume that for an integer $1 \leq i < k$, we have $a_{k+i} = \sum_{m=1}^{i} C_{k,i-m+1} \sum_{j=m}^{k} f_{j-m+1} a_j$. Using the formula of a_{k+i} above and the assumption, we have

$$\begin{aligned} a_{k+i+1} &= \sum_{j=1}^{i} f_{k-i+j} a_{k+j} + \sum_{j=i+1}^{k} f_{j-i} a_j \\ &= \sum_{j=1}^{i} f_{k-i+j} \sum_{m=1}^{j} C_{k,j-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l + \sum_{j=i+1}^{k} f_{j-i} a_j. \end{aligned}$$

Or,

$$\sum_{j=1}^{i} f_{k-i+j} \sum_{m=1}^{j} C_{k,j-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l = \sum_{j=1}^{i} f_{k-j+1} \sum_{m=1}^{i-j+1} C_{k,i+1-m+1-j} \sum_{l=m}^{k} f_{l-m+1} a_l$$

where we made the change of label $j \to t = i - j + 1$ and afterwards we renamed t by j.

We can notice that for fixed m, j runs from 1 to $i - m + 1$ since from the definition of the sequence $(C_{i,n})$, the label $i + 1 - m + 1 - j$ should be greater than 1. Since the minimum value of m is 1 and the maximum value of m is i, permuting the discrete sums over j, m, it results that

$$\begin{aligned} \sum_{j=1}^{i} f_{k-i+j} \sum_{m=1}^{j} C_{k,j-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l &= \sum_{m=1}^{i} \sum_{j=1}^{i-m+1} f_{k-j+1} C_{k,i+1-m+1-j} \sum_{l=m}^{k} f_{l-m+1} a_l \\ &= \sum_{m=1}^{i} C_{k,i+1-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l. \end{aligned}$$

So, we have

$$\begin{aligned} a_{k+i+1} &= \sum_{m=1}^{i} C_{k,i+1-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l + \sum_{j=i+1}^{k} f_{j-i} a_j \\ &= \sum_{m=1}^{i} C_{k,i+1-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l + C_{k,1} \sum_{j=i+1}^{k} f_{j-(i+1)+1} a_j \\ &= \sum_{m=1}^{i+1} C_{k,i+1-m+1} \sum_{l=m}^{k} f_{l-m+1} a_l. \end{aligned}$$

Thus the proof of the theorem is complete by induction. $\square$

Corollary 2.11. *Let $a : \mathbb{N} \to X$ be a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 2$ and initial values $a_1, a_2, \ldots, a_k$ given. Then, we have ($k > i \geq 1$)*

$$a_{k+i} = \sum_{m=1}^{i} a_m \sum_{j=1}^{m} f_j C_{k,i-m+j} + \sum_{m=i+1}^{k} a_m \sum_{j=1}^{i} f_{m-i+j} C_{k,j}.$$

Proof. From the theorem above, we have for $k > i \geq 1$,

$$\begin{aligned}
a_{k+i} &= \sum_{m=1}^{i} C_{k,i-m+1} \sum_{j=m}^{k} f_{j-m+1} a_j \\
&= C_{k,i} \sum_{j=1}^{k} f_j a_j + C_{k,i-1} \sum_{j=2}^{k} f_{j-1} a_j + \ldots + C_{k,1} \sum_{j=i}^{k} f_{j-i+1} a_j \\
&= \sum_{m=1}^{i} a_m \left[C_{k,i} f_m + \ldots + C_{k,i-m+1} f_1\right] + \sum_{m=i+1}^{k} a_m \left[C_{k,i} f_m + \ldots + C_{k,1} f_{m-i+1}\right] \\
&= \sum_{m=1}^{i} a_m \sum_{j=1}^{m} f_j C_{k,i-m+j} + \sum_{m=i+1}^{k} a_m \sum_{j=1}^{i} f_{m-i+j} C_{k,j}.
\end{aligned}$$

This completes the proof. □

Thus, a generic term a_{k+i} with $k > i \geq 1$ of a sequence a which is a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 2$ and initial values $a_1, a_2, \ldots, a_k$ given, can be rewritten as

$$a_{k+i} = \sum_{m=1}^{k} (M_k)_{i,m} a_m,$$

with M_k defined by

$$(M_k)_{i,m} = \begin{cases} \sum_{j=1}^{m} f_j C_{k,i-m+j} & 1 \leq m \leq i, \\ \sum_{j=1}^{i} f_{m-i+j} C_{k,j} & i < m \leq k. \end{cases}$$

This formula implies that for $1 \leq l(m) < k$ we have

$$[a_{k+\ell(m)}]_m = \sum_{i=1}^{k} [(M_k)_{\ell(m),i}]_m [a_i]_m = [a_k]_m.$$

Thus, we obtain a diophantine equation in the ring $\mathbb{Z}/m\mathbb{Z}$ where the residue class $[(r_k)_{\ell(m),i}]_m$ of $(M_k)_{\ell(m),i}$ modulo a (non-zero) positive integer m such that the numbers $(r_k)_{\ell(m),i}$ belong to $[[0, m-1]]$, are the unknowns and $[a_i]_m$ with $i = 1, \ldots, k$ as well as m are given. Solving this equation, it allows to determine a period $\ell(m)$ of the sequence a modulo m. Indeed, since all the coefficients of matrix M_k can be computed by the formula above, it suffices to compare numbers $(r_k)_{\ell(m),i} + tm$ with t an integer with the numbers $(M_k)_{l,i}$ with l a non-zero positive integer. A value of label l for which $(r_k)_{\ell(m),i} + tm = (M_k)_{l,i}$ whatever $i \in [[1, k]]$ corresponds to a value of a period $\ell(m)$ of sequence a modulo m.

We can notice that if a sequence a which is a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 1$ and initial values $a_1, \ldots, a_k$ given, is a strong divisibility sequence, then from the associative property of the GCD operation, we have ($n \geq 1$ and $s_l \geq 1$ with $l \in [[1, n]]$)

$$(a_{s_1}, \ldots, a_{s_n}) = a_{(s_1, \ldots, s_n)}.$$

We recall the following easy exercise from [1] without proof.

Proposition 2.12. *Given two positive integers x and y, let m, n two positive integers such that $m = ax + by$ and $n = cx + dy$ with $ad - bc = \pm 1$. Then we have $(m, n) = (x, y)$.*

We generalize the above as follows

Proposition 2.13. *Let n be a positive integer which is greater than 2. Given n positive integers $x_1, x_2, \ldots, x_n$, let $y_1, y_2, \ldots, y_n$ be n positive integers such that ($i = 1, 2, \ldots, n$)*

$$y_i = \sum_{j=1}^{n} A_{i,j} x_j,$$

with $\det(A) = \pm 1$. Then we have

$$(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n).$$

Proof. Let $g = (x_1, x_2, \ldots, x_n)$ and $G = (y_1, y_2, \ldots, y_n)$. So, there exist $2n$ integers, say

$$u_1, u_2, \ldots, u_n, U_1, U_2, \ldots, U_n$$

such that

$$g = u_1 x_1 + u_2 x_2 + \ldots + u_n x_n$$

and

$$G = U_1 y_1 + U_2 y_2 + \ldots + U_n y_n.$$

Let d a common divisor of $x_1, x_2, \ldots, x_n$. From the linearity property of divisibility, since $d | x_i$ with $i = 1, 2, \ldots, n$, $d | y_i$ with $i = 1, 2, \ldots, n$ and so $d | G$. In particular, $g | G$. Let D be a common divisor of $y_1, y_2, \ldots, y_n$.

If A is a $n \times n$ square matrix whose determinant is non-zero ($\det(A) = \pm 1$ and so $rank(A) = n$), then the linear system of equations $y_i = \displaystyle\sum_{j=1}^{n} A_{i,j} x_j$ with $i = 1, 2, \ldots, n$ is a Cramer linear system of n equations, which has a unique solution given by the n-tuple $(x_1, x_2, \ldots, x_n)$ such that ($i = 1, 2, \ldots, n$)

$$x_i = \frac{\Delta_i(A)}{\det(A)} = \pm \Delta_i(A),$$

where $\Delta_i(A)$ is the determinant of the $n \times n$ square matrix which is obtained from the matrix A by replacing the i^{th} column of A by the column $\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$.

From the linearity property of divisibility, since $D|y_i$ with $i = 1, 2, \ldots, n$, $D|x_i$ with $i = 1, 2, \ldots, n$ and so $D|g$. In particular, $G|g$.

From $g|G$ and $G|g$, since g and G are positives, it results that $g = G$. $\square$

Remark 2.14. This property can be extended to the case where the determinant of the matrix A is a common divisor of the numbers $\Delta_1(A), \Delta_2(A), \ldots, \Delta_n(A)$.

Remark 2.15. If a sequence a which is a k-th order of recurrence relation on X defined by a linear map $f : X^k \to X$ with $k \geq 2$ and initial values $a_1, a_2, \ldots, a_k$ given, is a strong divisibility sequence, since a_{k+i} with $i \geq 1$ is a linear combination of $a_1, a_2, \ldots, a_k$, if the determinant of the $k \times k$ square matrix $((M_k)_{i,m})$ with $1 \leq i \leq k$ and $1 \leq m \leq k$ which we denote simply by M_k when there is no ambiguity (the matrix elements $(M_k)_{i,m}$ was defined previously for $1 \leq i < k$ and the matrix elements $(M_k)_{k,m}$ can be determined from the definition of sequence a), is either ± 1 or a common divisor of the numbers $\Delta_1(M_k), \Delta_2(M_k), \ldots, \Delta_k(M_k)$, then we have

$$(a_{k+1}, a_{k+2}, \ldots, a_{2k}) = (a_1, a_2, \ldots, a_k) = a_{(1,2,\ldots,k)} = a_1.$$

Acknowledgments

The authors would like to thank the annonymous referees and the editor for helpful comments. The second author was supported by DST INSPIRE Scholarship 422/2009 from Department of Science and Technology, Government of India.

References

[1] Apostol, T. M., *An Introduction to the Analytic Theory of Numbers*, Springer–Verlag, 1975.

[2] Chartrand, G., P. Zhang, *Discrete Mathematics*, Waveland Press, 2011.

[3] Gandhi, K. R., Divisibility properties of Fibonacci numbers, *South Asian J. Math.*, Vol. 1, 2011, No. 3, 140–144.

[4] Laugier, A., M. P. Saikia, *Some properties of Fibonacci numbers*, submitted for publication.