Some remarks regarding special elements in algebras obtained by the Cayley-Dickson process over $\mathbb{Z}_p$

Cristina Flaut, Andreea Baias

Abstract. In this paper we provide some properties of k-potent elements in algebras obtained by the Cayley-Dickson process over $\mathbb{Z}_p$. Moreover, we find a structure of nonunitary ring over Fibonacci quaternions over $\mathbb{Z}_3$ and we present a method to encrypt plain texts, by using invertible elements in such algebras.

1. Preliminaries

In [MS; 11], the authors provided some properties regarding quaternions over the field $\mathbb{Z}_p$. Since quaternions are special cases of algebras obtained by the Cayley-Dickson process, in this paper we extend the study of k-potent elements over quaternions to an arbitrary algebra obtained by the Cayley-Dickson process. These algebras, in general, are poor in properties: are not commutative, starting with dimension 4 (the quaternions), are not associative, strating with dimension 8 (the octonions) and lost alternativity, starting with dimension 16 (the sedionions).The good news is that all algebras obtained by the Cayley-Dickson process are power-associative and this is the property which will be used when we study the k-potent elements in these algebras. The paper is organized as follows: in Introduction, we present basic properties of algebras obtained by the Cayley-Dickson process, in section 3, we characterize the k-potent elements in these algebras, in section 4, we give a structure of non-unitary and noncommutative ring over the Fibonacci quaternions over $\mathbb{Z}_3$ and in the last section, we provide an encryption method by using invertible elements from these algebras.

2. Introduction

In the following, we consider A, a finite dimensional unitary algebra over a field K with $charK \neq 2$.

An algebra A is called *alternative* if $x^2y = x(xy)$ and $xy^2 = (xy)y$, for all $x, y \in A$, *flexible* if $x(yx) = (xy)x = xyx$, for all $x, y \in A$ and *power associative* if the subalgebra $< x >$ of A generated by any element $x \in A$ is associative. Each alternative algebra is a flexible algebra and a power associative algebra.

We consider the algebra $A \neq K$ such that for each element $x \in A$, the following relation is true

$$x^2 + t_x x + n_x = 0,$$

for all $x \in A$ and $t_x, n_x \in K$. This algebra is called a *quadratic algebra*.

It is well known that a finite-dimensional algebra A is *a division* algebra if and only if A does not contain zero divisors (See [Sc;66]).

A *composition algebra* A over the field K is an algebra, not necessarily associative, with a nondegenerate quadratic form n which satisfies the relation

$$n(xy) = n(x)n(y), \forall x, y \in A.$$

A unital composition algebras are called *Hurwitz algebras*.

Hurwitz's Theorem.[Ba; 01] $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ *and* $\mathbb{O}$ *are the only real alternative division algebras.*

Theorem 1. (Theorem 2.14, [McC,80]) *A is a composition algebra if and only if A is an alternative quadratic algebra.*

An element x in a ring R is called *nilpotent* if we can find a positive integer n such that $x^n = 0$. The number n, the smallest with this property, is called the *nilpotency index*. A power-associative algebra A is called a *nil algebra* if and only if each element of this algebra is nilpotent. An element x in a ring R is called *k-potent*, for $k > 1$, a positive integer, if k is the smallest number such that $x^k = x$. The number k is called the *k-potency index*. For $k = 2$, we have idempotent elements, for $k = 3$, we have tripotent elements, etc.

Let A be an algebra over the field K and a *scalar involution* over A,

$$\overline{} : A \to A, a \to \overline{a},$$

that means a linear map with the following properties

$$\overline{ab} = \overline{b}\overline{a}, \overline{\overline{a}} = a,$$

and

$$a + \overline{a}, a\overline{a} \in K \cdot 1, \text{ for all } a, b \in A.$$

For the element $a \in A$, the element $\overline{a}$ is called the *conjugate* of the element a. The linear form

$$\mathbf{t} : A \to K \ , \ \mathbf{t}\,(a) = a + \overline{a}$$

and the quadratic form

$$\mathbf{n} : A \to K, \ \mathbf{n}\,(a) = a\overline{a}$$

are called the *trace* and the *norm* of the element a, respectively. From here, it results that an algebra A with a scalar involution is a quadratic algebra. Indeed, if in the relation $\mathbf{n}\,(a) = a\overline{a}$, we replace $\overline{a} = \mathbf{t}\,(a) - a$, we obtain

$$a^2 - \mathbf{t}\,(a)\,a + \mathbf{n}\,(a) = 0. \tag{1.}$$

Let $\delta \in K$ be a fixed non-zero element. We define the following algebra multiplication on the vector space $A \oplus A$

$$(a_1, a_2)(b_1, b_2) = \left(a_1 b_1 + \delta \overline{b}_2 a_2, a_2 \overline{b_1} + b_2 a_1\right). \tag{2.}$$

The obtained algebra structure over $A \oplus A$, denoted by (A, δ) ,is called the *algebra obtained from A by the Cayley-Dickson process.* We have that $\dim(A, \delta) = 2 \dim A$.

Let $x \in (A, \delta)$, $x = (a_1, a_2)$. The map

$$^{-} : (A, \delta) \to (A, \delta)\ ,\ x \to \bar{x} = (\overline{a}_1, -a_2)\,,$$

is a scalar involution of the algebra (A, δ), extending the involution $^{-}$ of the algebra A. We consider the maps

$$\mathbf{t}(x) = \mathbf{t}(a_1)$$

and

$$\mathbf{n}(x) = \mathbf{n}(a_1) - \delta \mathbf{n}(a_2)$$

called the *trace* and the *norm* of the element $x \in (A, \delta)$, respectively.

If we consider $A = K$ and we apply this process t times, $t \geq 1$, we obtain an algebra over K,

$$A_t = \left(\frac{\delta_1, ..., \delta_t}{K}\right). \tag{3.}$$

Using induction in this algebra, the set $\{1, f_1, ..., f_{n-1}\}, n = 2^t$, generates a basis with the properties:

$$f_i^2 = \delta_i 1,\ {}_i \in K, \delta_i \neq 0,\ i = 1, ..., t \tag{4.}$$

and

$$f_i f_j = -f_j f_i = \alpha_{ij} f_k,\ \alpha_{ij} \in K,\ \alpha_{ij} \neq 0, i \neq j, i, j = \ 1, ...n-1, \tag{5.}$$

α_{ij} and f_k being uniquely determined by f_i and f_j.

From [Sc; 54], Lemma 4, it results that in any algebra A_t with the basis $\{1, f_1, ..., f_{n-1}\}$ satisfying relations (4) and (5) , we have:

$$f_i(f_i x) = \delta_i x = (x f_i) f_i, \tag{6.}$$

for all $i \in \{1, 2, ..., n-1\}$ and for every $x \in A$.

The field K is the center of the algebra A_t,for $t \geq 2$.(See [Sc; 54]). Algebras A_t of dimension 2^t obtained by the Cayley-Dickson process, described above, are flexible and power associative for all $t \geq 1$ and, in general, are not division algebras for all $t \geq 1$.

For $t = 2$, we obtain the generalized quaternion algebras over the field K. If we take $K = \mathbb{R}$ and $\delta_1 = \delta_2 = -1$, we obtain the real quaternion algebra over $\mathbb{R}$. This algebra is an associative and a noncommutative algebra and will be denoted with $\mathbb{H}$.

Let $\mathbb{H}$ be the real quaternion algebra with basis $\{1, i, j, k\}$, where

$$i^2 = j^2 = k^2 = -1, ij = -ji, ik = -ki, jk = -kj. \tag{7.}$$

Therefore, each element from $\mathbb{H}$ has the following form

$$q = a + bi + cj + dk, a, b, c, d \in \mathbb{R}.$$

We remark that $\mathbb{H}$ is a vector space of dimension 4 over $\mathbb{R}$ with the addition and scalar multiplication. Moreover, $\mathbb{H}$ has a ring structure with multiplication given by (7) and the usual distributivity law.

If we consider K a finite field with $charK \neq 2$, due to the Wedderburn's Theorem, a quaternion algebra over K is allways a non division algebra or a split algebra.

3. Characterization of k-potent elements in algebras obtained by the Cayley-Dickson process

In the paper [Mo; 15], the author gave several characterizations of k-potent elements in associative rings from an algebraic point of view. In [RPC; 22], the authors presented some properties of (m, k)-type elements over the ring of integers modulo n and in [Wu; 10], the author emphasize the applications of k-potent matrices to digital image encryption.

In the following, we will study the properties of k-potent elements in a special case of nonassociative structures, that means we characterize the k-potent elements in algebras obtained by the Cayley-Dickson process over the field of integers modulo p, p a prime number greater than 2, $K = \mathbb{Z}_p$.

Remark 2. Since algebras obtained by the Cayley-Dickson process are power associative, we can define the power of an element. In this paper, we consider A_t such an algebra, given by the relation (3), with $\delta_i = -1$, for all i, $i \in \{1, ..., t\}$. We consider $x \in A_t$, a k-potent element, that means k is the smallest positive integer with this property. Since A_t is a quadratic algebra, from relation (1), we have that $x^2 - \mathbf{t}(x)\, x + \mathbf{n}(x) = 0$, with $\mathbf{t}(x) \in K$ the trace and $\mathbf{n}(x) \in K$ the norm of the element x. To make calculations easier, we will denote $\mathbf{t}(x) = t_x$ and $\mathbf{n}(x) = n_x$.

Remark 3. In general, algebras obtained by the Cayley-Dickson process are not composition algebras, but the following relation

$$\mathbf{n}(x^m) = (\mathbf{n}(x))^m$$

is true, for m a positive integer. Indeed, we have $\mathbf{n}(x^m) = x^m \overline{x^m}$ and $(\mathbf{n}(x))^m = (x\overline{x})^m = x\overline{x} \cdot ... \cdot x\overline{x}$, m-times with $\overline{x} = t_x - x, t_x \in K$. Since x and $\overline{x}$ are in the algebra generated by x, they associate and comute, due to the power associativity property. If $x \in A_t$ is an invertible element, that means $n_x \neq 0$, then the same remark is also true for $x^{-1} = \frac{\overline{x}}{n_x}$, the inverse of the element x. The element x^{-1} is in the algebra generated by x, therefore associate and comute with x.

ii) We know that $x^2 - t_x x + n_x = 0$. If $x \in A_t$ is a nonzero k-potent element, then, from the above, we have $n_x = 0$ or $n_x \neq 0$ and $n_x^{k-1} = 1$.

iii) Let $x \in A_t$ be a nonzero k-potent element such that $n_x \neq 0$. Then, the element x is an invertible element in A_t such that $x^{k-1} = 1$. Indeed, if $x^k = x$, multiplying with x^{-1} we have $x^{k-1} = 1$.

iv) For a nilpotent element $x \in A_t$ there is a positive integer $k \geq 2$ such that $x^k = 0, k$ the smallest with this property. From here, we have that $n_x = 0$, therefore $x^2 = t_x x$. It results that $x^k = t_x x^{k-1}$, then $t_x x^{k-1} = 0$ with $x^{k-1} \neq 0$. We get that $t_x = 0$ and $x^2 = 0$. Therefore, we can say that in an algebra A_t, if exist, we have only nilpotent elements of index two.

In the following, we will characterize the k-potent elements in the case when $n_x = 0$.

Proposition 4. *The element $x \in A_t$, $x \neq 0$, with $n_x = 0$ and $t_x \neq 0$ is a k-potent element in A_t if and only if t_x is a k-potent element in $\mathbb{Z}_p^*, 2 \leq k \leq p$ (t_x has $k-1$ as multiplicative order in $\mathbb{Z}_p^*$).*

Proof. We must prove that if k is the smallest positive integer such that $x^k = x$, then $t_x^k = t_x$, therefore $t_x^{k-1} = 1$, with k the smallest positive integer with this property.

We have $x^k = x^{k-2}x^2 = x^{k-2}t_x x = t_x x^{k-1} = t_x x^{k-3}x^2 = t_x^2 x^{k-2} = ... = t_x^{k-1}x$. If $t_x^{k-1} = 1$, we have $x^k = x$ and if $x^k = x$, we have $x = t_x^{k-1}x$, therefore $t_x^{k-1} = 1$.

Now, we must prove that $k \leq p$. We know that in $\mathbb{Z}_p$ the multiplicative order of a nonzero element is a divisor of $p-1$. If the order is $p-1$, the element is called a primitive element. If $t_x \neq 0$ in $\mathbb{Z}_p$ and $t_x^{k-1} = 1$, it results that $(k-1) \mid (p-1)$, then $k-1 \leq p-1$ and $k \leq p$.

Remark 5. For elements x with $n_x = 0$ and $t_x \neq 0$, from the above theorem, we remark that in an algebra A_t over $\mathbb{Z}_p$ we have $k \leq p$, where k is the potency index. That means the k-potency index in these conditions does not exceed the prime number p. Since $a^{p-1} \equiv 1 \ mod \ p$, for all nonzero $a \in \mathbb{Z}_p$, allways it results that $x^p = x$. It is not necessary for p to be the smallest with this property.

Example 6. If we take $p = 5$ and we have $x \in A_t$ such that $x^{38} = x$, since we known that $x^5 = x$, we obtain $x^{38} = x^{35}x^3 = \left(x^5\right)^7 x^3 = x^7x^3 = x^{10} = x^5x^5 = x^2$. Therefore, $x^2 = x$ and the k-potency index is 2.

In the following, we will characterize the k-potent elements when $n_x \neq 0$ and $n_x^{k-1} = 1$. We suppose that $k \geq 3$. Indeed, if $k = 2$, we have $x^2 = x$, then $x = 1$.

The following result it is well known from literature. We reproduce here the proof.

Proposition 7. *Each element of a finite field K can be expressed as a sum of two squares from K.*

Proof. If $charK = 2$, we have that the map $f : K \rightarrow K, f(x) = x^2$ is an injective map, therefore is bijective and each element from K is a square. Indeed, if $f(x) = f(y)$, we have that $x^2 = y^2$ and $x = y$ or $x = -y = y$,since $-1 = 1$ in $charK = 2$.

Assuming that $charK = p \neq 2$. We suppose that K has $q = p^n$ elements, then K^* has $q-1$ elements. Since $(K^*, \cdot)$ is a cyclic group with $q-1$ elements, $K^* = \{1, v, v^2, ..., v^{q-2}\}$, half of them, namely the even powers are squares. The zero element is also a square, then we have $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ square elements from K which are squares. We known that from a finite group $(G, *)$ if S and T are two subsents of G and $|S| + |T| > |G|$, we have that each $x \in G$ can be expresses as $x = s * t$, $s \in S, t \in T$. For $g \in G$, we consider the set $gS^{-1} = \{g * s^{-1}, s \in S\}$ wich has the same cardinal as the set T. Since $|S| + |T| > |G|$, it results that $|T| + \left|gS^{-1}\right| > |G|$, therefore $T \cap gS^{-1} \neq \emptyset$. Then, there are the elements $s \in S$ and $t \in T$ such that $t = g * s^{-1}$ and $g = s * t$. Now, if we consider S and T two sets equal with the multiplicative. In the group $(K, +)$, we have that $|S| + |T| = q + 1 > |K|$, therefore each $x \in K$ can be writen as $x = s^2 + t^2$, with $s \in S, t \in T$.

Remark 8. i) We can find an element $w \in A_t$, different from elements of the base, such that $w^2 = -1$. Indeed, such an element has $n_w = 1$ and $t_x = 0$. With the above notations and from the above proposition, since $1 = a^2 + b^2$, we can take $w_{ij} = af_i + bf_j$, $a, b \in \mathbb{Z}_p$ and f_i, f_j elements from the basis in A_t, given by (4). Therefore, $w_{ij}^2 = -1$.

ii) The group $\left(\mathbb{Z}_p^*, \cdot\right)$ is cyclic and has $p-1$ elements. Elements of order $p-1$ are primitive elements. The rest of the elements have orders divisors of $p-1$.

Now, we consider the equation in A_t

$$x^n = 1, n \text{ a positive integer.} \qquad (8.)$$

In the following, we will find some conditions such that this equation has solutions different from 1.

Remark 9. i) With the above notations, we consider $w \in A_t$ a nilpotent element (it has the norm and the trace zero). Therefore, the element $z = 1 + w$ has the property that $z^n = 1 + nw$, therefore if $n = pr, r$ a positive integer, the equation (8) has solutions of the form $z = 1 + w$, for all nilpotent elements $w \in A_t$. It is clear that z has the norm equal with 1 and $z^p = 1$, therefore $z^{p+1} = z$, is a p-potent element.

ii) If we consider $\eta \in \mathbb{Z}_p^*$ with the multiplicative order θ and $z = \eta + w$, w nilpotent, we have that $(\eta + w)^p = \eta^p + pw = \eta^p$ and $(\eta + w)^{p\theta} = 1$. Therefore, if $n = pr, r$ a positive integer, the equation (8) has solutions of the form $z = 1+w$, for all nilpotent elements $w \in A_t$. If r is a multiplicative order of an element from $\mathbb{Z}_p^*$ and $n = pr, r$ a positive integer, then the equation (8) has solutions of the form $z = \eta + w$, for all $\eta \in A_t$, η of order r, w a nilpotent element in A_t.

iii)With the above notations, we consider the element $w \in A_t$ sucht that $w^2 = -1$ and $z = 1 + w$. We have that $z^2 = (1+w)^2 = 2w, z^3 = (1+w)^3 = 2w - 2$ and $z^4 = \left(z^2\right)^2 = -4$ *modulo* p. Let $\eta = -4 \in \mathbb{Z}_p^*$ with the multiplicative order θ, θ is allways an even number. We have that $z^{4\theta} = 1$.

iv) Let $z = a + w \in A_t$, where $a \in \mathbb{Z}_p$ and $w \in A_t$, with $t_w = 0$ and $n_w \neq 0$. We have that $w^2 = \alpha \in \mathbb{Z}_p^2$, therefore, $z^r = C_r + D_r w$. If $z^s = 1$, then there is a positive integer $m \leq s$ such that $C_m = 0$ or $D_m = 0$. Indeed, if $m = s$, we have $D_s = 0$ and $C_s = 1$.

Proposition 10. *By using the above notations, we consider the element $z = a + w$, where $a \in \mathbb{Z}_p$ and $w \in A_t$ with the trace zero. Assuming that there is a nonegative integer m such that C_m or D_m is zero, then there is a positive integer k such that $z^k = 1$ and z is $(k+1)$-potent element.*

Proof. Since w has the trace zero, let $w^2 = \beta$, with τ the multiplicative order of β. We have that $z^m = C_m + D_m w, C_m, D_m \in \mathbb{Z}_p$. Supposing that C_m is zero, then we have $z^m = D_m w$, with θ the multiplicative order of D_m. Therefore $z^{mM} = 1$, where $M =$*lcm* $\{2\tau, \theta\}$. If D_m is zero, then we have $z^m = C_m$ with υ the multiplicative order of C_m. It results that $z^{\upsilon m} = 1$.

Now, we can say that we proved the following theorem.

Theorem 11. *With the above notations, an element $z \in A_t$ is a k-potent element, if z is of one of the forms:*

Case 1. $n_z \neq 0$.

i) $z = 1 + w$, with $w \in A_t$, w is a nilpotent element. In this case, z is $(p+1)$-potent;

ii) $z = 1 + w$, with $w \in A_t$ sucht that $w^2 = -1$. Since $z^4 = -4$ modulo p and θ is the multiplicative order of -4 in $\mathbb{Z}_p^*$, we have that z is $(4\theta + 1)$-potent.

iii) $z = a + w$, where $a \in \mathbb{Z}_p$, $w \in A_t$ with $t_w = 0$, $w^2 = \beta \in \mathbb{Z}_p^*$, with τ the multiplicative order of β, and $z^r = C_r + D_r w$. Assuming that there is a nonegative integer m such that C_m or D_m is zero, then there is a positive integer k such that $z^k = 1$ and z is $(k+1)$-potent element. If $C_m = 0$, then $k = mM$, where $M =$lcm $\{2\tau, \theta\}$ and θ is the multiplicative order of D_m. If $D_m = 0$, then we have $k = \upsilon m$, with υ the multiplicative order of C_m.

Case 2. $n_z = 0$. The element $z \in A_t$ is k-potent if and only if t_z is k-potent element in $\mathbb{Z}_p^*$, that means $k - 1$ is a divisor of $p - 1$.

Example 14. In the following, we will give some examples of values of the potency index k.

i) Case $p = 5$ and $t = 2$, therefore we work on quaternions. We consider $z = 2 + i + j + k$ with the norm $n_x = 2 \neq 0$. We have $w = i + j + k$ and $z = 2 + w$. We have $z^2 = 1 + 4w, z^3 = 4w$, therefore $m = 3$ and $D_m = 4$, with $\theta = 4$. Since $w^2 = 2$, it results that $\tau = 4$ and $M = 4$. We have that $z^{24} = 1$, then $z^{25} = z$ and z is 25-potent element, $k = 25$.

ii) Case $p = 7$, $t = 2$ and $z = 2 + i + j + k$. The norm is zero and the trace is 4. Since 4 has multiplicative order equal with 3, from Proposition 4, we have $z^4 = z$. Indeed, $z^2 = 1 + 4w, z^3 = 4 + 2w, z^4 = 2 + w = z$ and $k = 4$.

iii) Case $p = 5$ and $t = 2$. The element $z = 1+3i+4j$ has $n_z = 1, w = 3i+4j$, with $n_w = t_w = 0$, therefore w is a nilpotent element. We have $z^5 = 1$, $z^6 = z$ and $k = 6$.

iv) Case $p = 3$ and $t = 2$. The element $z = 1 + i + j + k$ has $n_z = 1$ and $w = i + j + k$. We have $z^2 = (1 + w)^2 = 1 + 2w$, $z^3 = (1 + w)(1 + 2w) = 1 + 2w + w = 1$, therefore $z^4 = z$ and $k = 4$.

v) Case $p = 5, t = 2$. We consider the element $z = 2 + 3i + j + 3k = 2 + 3w, w = i + 2j + k, n_z = 3, n_w = 1, t_w = 0$, then $w^2 = -1$. We have that $\tau = 2$ and $z^2 = 2w$. Therefore $m = 2, C_2 = 0, D_2 = 2$, then $\theta = 4$ and , therefore we work on quaternions. It results $z^{mM} = z^8 = 1$, therefore $z^9 = z$ and $k = 9$.

vi) Case $p = 5, t = 2$. We consider the element $z = 2 + i + j + k = 2 + w$ with $n_z = 2, n_w = 3, t_w = 0, w^2 = 2$ and $\tau = 4$, the order of $\beta = 2$. We have $z^2 = 3 + 4w, z^3 = 4 + w, z^4 = 1 + 4w, z^5 = 4w$, therefore $m = 5, C_5 = 0, D_5 = 4, \theta = 2, M = lcm\{2\tau, \theta\} = 8$. It results that $z^{mM} = z^{40} = 1$, then $z^{41} = z$ and $k = 42$.

vii) Case $p = 11, t = 2$. We consider the element $z = 2i + 7j + 3k$ with $n_z = 7, z^2 = 4$, therefore $m = 2, D_2 = 0, C_2 = 4, \upsilon = 5$, the multiplicative order of $C_2 = 4$. We have $z^{m\upsilon} = z^{10} = 1$ and $k = 11$.

viii) Case $p = 13, t = 3$, therefore we work on octonions. We consider the element $z = 3 + 2f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7 = 3 + w$, $w = 2f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_7$, with $n_z = 6$, $n_w = 10, t_w = 0$. We have $w^2 = 3$ and $\tau = 3$, the order of $\beta = 3$. It results, $z^2 = 12 + 2w, z^3 = 3 + 5w, z^4 = 9w$, then $m = 4, C_4 = 0.D_4 = 9, \theta = 3, M = lcm\{2\tau, \theta\} = 6$. We get $z^{mM} = z^{24} = 1$, then $z^{25} = z$ and $k = 25$.

ix) Case $p = 17, t = 4$, therefore we work on sedenions. The Sedenion algebra is a noncommutative, nonassociative and nonalternative algebra of dimension 16. We consider the element $z = 1 + w, w = \sum_{i=1}^{15} f_i$, with $w^2 = 2$ and $\tau = 8$. It results $z^2 = 3 + 2w, z^3 = 4w$. Then $m = 3, C_3 = 0, D_3 = 4, \theta = 4$. We have $M = lcm\{2\tau, \theta\} = lcm\{16, 4\} = 16$ and $z^{mM} = z^{48} = 1$. It results $z^{49} = z$ and $k = 49$.

Remark 15. The (m, k)-type elements in A_t, with m, n positive integers, are the elements $x \in A_t$ such that $x^m = x^k$, $m \geq k$, smallests with this property. If $n_x \neq 0$, then $x^{m-k} = 1$ and x is an $(m - k + 1)$-potent element. If $n_x = 0$ and $t_x \neq 0$, we have that $t_x^{m-k} = 1$, then x is an $(m - k + 1)$-potent element. Therefore, an (m, k)-type element in A_t is an $(m - k + 1)$-potent element in A_t.

4. A nonunitary ring structure of quaternion Fibonacci elements over $\mathbb{Z}_p$

The Fibonacci numbers was introduced by *Leonardo of Pisa (1170-1240)* in his book *Liber abbaci*, book published in 1202 AD (see [Kos; 01], p. 1-3).

The nth term of these numbers is given by the formula:

$$f_n = f_{n-1} + f_{n-2},\ n \geq 2,$$

where $f_0 = 0, f_1 = 1$.

In [Ho; 63], were defined and studied Fibonacci quaternions over $\mathbb{H}$, defined as follows

$$F_n = f_n 1 + f_{n+1} i + f_{n+2} j + f_{n+3} k,$$

called the nth Fibonacci quaternions.

In the same paper, the norm formula for the nth Fibonacci quaternions was found:

$$\boldsymbol{n}\left(F_n\right) = F_n \overline{F}_n = 3 f_{2n+3},$$

where $\overline{F}_n = f_n \cdot 1 - f_{n+1} i - f_{n+2} j - f_{n+3} k$ is the conjugate of the F_n in the algebra $\mathbb{H}$.

Fibonacci sequence is also studied when it is reduced modulo m. This sequence is periodic and this period is called *Pisano's period*, $\pi\left(m\right)$. In the following, we consider $m = p$, a prime number and $\left(f_n\right)_{n \geq 0}$, the Fibonacci numbers over $\mathbb{Z}_p$. It is clear that, in general, the sum of two arbitrary Fibonacci numbers is not a Fibonacci numbers, but if these numbers are consecutive Fibonacci numbers, the sentence is true. In the following, we will find conditions when the product of two Fibonacci numbers is also a Fibonacci number. In the following, we work on $A_t, t = 2$, over the field $\mathbb{Z}_p$. We denote this algebra with $\mathbb{H}_p$.

Let $F_1 = a + bi + \left(a + b\right) j + \left(a + 2b\right) k$ and $F_2 = c + di + \left(c + d\right) j + \left(c + 2d\right) k$, two Fibonacci quaternions in $\mathbb{H}_p$. We will find conditions such that $F_1 F_2$ and $F_2 F_1$ are also Fibonacci quaternion elements, that means elements of the same form:

$$A + Bi + \left(A + B\right) j + \left(A + 2B\right) k. \tag{10.}$$

We compute $F_1 F_2$ and $F_2 F_1$ and we obtain that

$$F_1 F_2 = \left(-ac - 3ad - 3bc - 6bd\right) + 2adi + 2a\left(c + d\right) j + \left(2ac + ad + 3bc\right) k \tag{11.}$$

and

$$F_2 F_1 = \left(-ac - 3ad - 3bc - 6bd\right) + 2bci + 2c\left(a + b\right) j + \left(2ac + 3ad + bc\right) k. \tag{12.}$$

By using relation (10), we get the following systems, with c, d as unknowns. From relation (11), we obtain:

$$\begin{cases} \left(-3a - 3b\right) c + \left(-3a - 6b\right) d = 0 \\ \left(-6b - 3a\right) c + \left(-6b\right) d = 0 \end{cases} \tag{13.}$$

From relation (12), we obtain the system:

$$\begin{cases} \left(-3a + 3b\right) c + \left(-3a\right) d = 0 \\ \left(-3a\right) c + \left(-6a - 6b\right) d = 0 \end{cases} \tag{14.}$$

We remark that for $p=3$, the systems (13) and (14) have solutions, therefore, for $p=3$, there is a chance to obtain an algebraic structure on the set $\mathcal{F}_{\pi(p)}$, the set of Fibonacci quaternions over $\mathbb{Z}_p$.

For $p=3$, the Pisano's period is 8, then we have the following Fibonacci numbers: $0,1,1,2,0,2,2,1$. We obtain the following Fibonacci quaternion elements: $F_0=i+j+2k, F_1=1+i+2j, F_2=1+2i+2k, F_3=2+2j+2k$, $F_4=2i+2j+k, F_5=2+2i+j, F_6=2+i+k, F_7=1+j+k$, therefore $\mathcal{F}_{\pi(p)}=\{F_i, i\in\{0,1,2,3,4,5,6,7\}\}$. All these elements are zero norm elements. F_0 and F_4 are nilpotents, F_3, F_5 and F_6 are idempotent elements, F_1,F_2,F_7 are 3-potent elements, By usyng $C++$ software, we computed the sum and the product of these 8 elements. Therefore, we have $F_0F_i=0$, for $i\in\{0,1,...,7\}, F_4F_i=0$, for $i\in\{0,1,...,7\}, F_5F_i=F_i$, for $i\in\{0,1,...,7\}, F_6F_i=F_i$, for $i\in\{0,1,...,7\}$ and

$$\begin{aligned}
F_1F_0 &= F_4, F_1^2=F_5, F_1F_2=F_6, F_1F_3=F_7,\\
F_1F_4 &= F_0, F_1F_5=F_1, F_1F_6=F_2, F_1F_7=F_3,
\end{aligned}$$

$$\begin{aligned}
F_2F_0 &= F_4, F_2F_1=F_5, F_2^2=F_6, F_2F_3=F_7,\\
F_2F_4 &= F_0, F_2F_5=F_1, F_2F_6=F_2, F_2F_7=F_{3,}
\end{aligned}$$

$$\begin{aligned}
F_3F_0 &= F_0, F_3F_1=F_1, F_3F_2=F_2, F_3^2=F_3,\\
F_3F_4 &= F_4, F_3F_5=F_5, F_3F_6=F_6, F_3F_7=F_7,
\end{aligned}$$

$$\begin{aligned}
F_7F_0 &= F_4, F_7F_1=F_5, F_7F_2=F_6, F_7F_3=F_7,\\
F_7F_4 &= F_0, F_7F_5=F_1, F_7F_6=F_2, F_7^2=F_3.
\end{aligned}$$

Regarding the sum of two Fibonacci quaternions over $\mathbb{Z}_3$, we obtain:

$$2F_0=F_4, F_0+F_1=F_2, F_0+F_2=F_7, F_0+F_3=F_6, F_0+F_4=0,$$

$$\begin{aligned}
F_0+F_5 &= F_3, F_0+F_6=F_5, F_0+F_7=F_1, 2F_1=F_5, F_1+F_2=F_3,\\
F_1+F_3 &= F_0, F_1+F_4=F_7, F_1+F_5=0, F_1+F_6=F_4, F_1+F_7=F_6,
\end{aligned}$$

$$\begin{aligned}
2F_2 &= F_6, F_2+F_3=F_4, F_2+F_4=F_1, F_2+F_5=F_0, F_2+F_6=0,\\
F_2+F_7 &= F_5, 2F_3=F_7, F_3+F_4=F_5, F_3+F_5=F_2, F_3+F_6=F_1,
\end{aligned}$$

$$\begin{aligned}
F_3+F_7 &= 0, 2F_4=F_0, F_4+F_5=F_6, F_4+F_6=F_0, F_4+F_7=F_2,\\
2F_5 &= F_1, F_5+F_6=F_7, F_5+F_7=F_4, 2F_6=F_2, F_6+F_7=F_0,\\
2F_7 &= F_3.
\end{aligned}$$

From here, we have the following result..

Proposition 16. *$\left(\mathcal{F}_{\pi(3)} \cup \{0\}, +\right)$ is an abelian group of order 9, isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ and $\left(\mathcal{F}_{\pi(3)} \cup \{0\}, +, \cdot\right)$ is a nonunitary and noncommutative ring.*

5. An application in Cryptography

We consider an algebra A_t over $\mathbb{Z}_p$. This algebra is of dimension 2^t. We suppose that we have a text m to be encrypted and the alphabet has p elements, p a prime number. To each letter from alphabet, will corespond a label from 0 to $p-1$, that means we work on $\mathbb{Z}_p$. The encryption algorithm is the following.

1) We will split m in blocks and we will choose the lenght of the blocks of the form 2^t. For a fixed t, we will find an invertible element $q, q \in A_t$, that means $n_q \neq 0$. This element will be the encryption key.

2) Supposing that $m = m_1 m_2 ... m_r$ is the plain text, with m_i blocks of lenght 2^t, formed by the labels of the letters, to each $m_i = m_{i0} m_{i1} ... m_{i2^t-1}$ we will associate an element $v_i \in A_t, v_i = \sum\limits_{j=0}^{2^t-1} m_{ij} f_j$.

3) We compute $qv_i = w_i$, for all $i \in \{1, 2, ..., r\}$. We obtain $w = w_1 w_2 ... w_r$, the encrypted text.

To decrypt the text, we use the decryption key, then we compute $d = q^{-1}$ and $v_i = dw_i$, for all $i \in \{1, 2, ..., r\}$.

Example 17. We consider the word MATHEMATICS and the key SINE. We work on an alphabet with 29 letters, including blank space, denoted with "*", "." and ",". The labels of the letters are done in the below table

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z	*	.	,	
20	21	22	23	24	25	26	27	28	

We consider $t = 2$, therefore we work on quaternions. We will add an "A" at the end of word "MATHEMATICS", to have multiple of 4 lenght text, therefore, we will encode the text "MATHEMATICSA". We have the following blocks MATH, EMAT, ICSA, with the corresponding quaternions $v_1 = 12 + 19j + 7k$, for MATH, $v_2 = 4 + 12i + 19k$, for EMAT and $v_3 = 8 + 2i + 18j$ for ICSA. The key is $q = 18 + 8i + 13j + 4k$, it is an invertible element, with the nonzero norm, $n_q = 22$. We have $w_1 = qv_1 = 28 + 24i + 7j + 7k$, corresponding to the message ",YHH", $w_2 = qv_2 = 16 + 2i + 6j + 28k$, corresponding to the message "QCG," and $w_3 = qv_3 = 10 + 28i + j + 5k$, corresponding to the message "K,BF". Therefore, the encrypted message is ",YHHQCG,K,BF". The decryption key is $d = q^{-1} = 14 + 26i + 6j + 13k$. For decryption, we will compute

$dw_1 = 12 + 19j + 7k = v_1$, $dw_2 = 4 + 12i + 19k = v_2$, $dw_3 = 8 + 2i + 18j = v_3$, and we find the initial text "MATHEMATICSA".

Conclusion. In this paper we studied properties of some special elements in algebras obtained by the Cayley-Dickson process and we find an algebraic structure(nonunitary and noncommutative ring) over Fibonacci quaternions over $\mathbb{Z}_3$. Moreover, an encryption method by using these elements is also provided. As a further research, we intend to study other special elements in the idea of finding another good properties.

References

[Ba; 01] Baez, J.C., *The Octonions*, B. Am. Math. Soc., **39(2)**(2001), 145-205, http://www.ams.org/journals/bull/
2002-39-02/S0273-0979-01-00934-X/S0273-0979-01-00934-X.pdf.

[Ho; 63] Horadam, A. F., *Complex Fibonacci Numbers and Fibonacci Quaternions*, Amer. Math. Monthly **70**(1963), 289-291.

[Kos; 01] Koshy, T., *Fibonacci and Lucas Numbers with Applications*, A Wiley-Interscience publication, U.S.A, 2001.

[MS; 11] Miguel, C. J., Serodio R., *On the Structure of Quaternion Rings over* $\mathbb{Z}p$, International Journal of Algebra, 5(27)(2011), 1313-1325.

[McC; 80] McCrimmon, K., *Pre-book on Alternative Algebras*, 1980, http://mysite.science.uottawa.ca/neher/Papers/alternative/ http://mysite.science.uottawa.ca/neher/Papers/a
2.2.Composition%20algebras.pdf.

[Mo; 15] Mosić Dijana, *Characterizations of k-potent elements in rings*, Annali di Matematica, 194(2015), 1157–1168, DOI 10.1007/s10231-014-0415-5

[RPC; 22] Ratanaburee, P., Petapirak, M., Chuysurichay, S., *On (m, k) - type elements in the ring of integers modulo n*, Songklanakarin J. Sci. Technol., 44 (5)(2022), 1179–1184.

[Sc; 66] Schafer, R. D., *An Introduction to Nonassociative Algebras,* Academic Press, New-York, 1966.

[Sc; 54] Schafer, R. D., *On the algebras formed by the Cayley-Dickson process,* Amer. J. Math., **76**(1954), 435-446.

[Wu; 10] Y. Wu, *k-Potent Matrices - Construction and Applications in Digital Image Encryption*, Recent Advances in Applied Mathematics, Proceedings of the 2010 American Conference on Applied Mathematics, USA, 2010, 455–460.

Cristina FLAUT
Faculty of Mathematics and Computer Science, Ovidius University,
Bd. Mamaia 124, 900527, Constanţa, România,

http://www.univ-ovidius.ro/math/
e-mail: cflaut@univ-ovidius.ro; cristina_flaut@yahoo.com

Andreea BAIAS
PhD student at Doctoral School of Mathematics,
Ovidius University of Constanţa, România,
e-mail: andreeatugui@yahoo.com