Stud. Univ. Babeş-Bolyai Math. 69(2024), No. 1, 3–14
DOI: 10.24193/subbmath.2024.1.01

Idempotent and nilpotent elements in octonion rings over $\mathbb{Z}_p$

Michael Aristidou, Philip R. Brown and George Chailos

Abstract. In this paper, we show that the set $\mathbb{O}/\mathbb{Z}_p$, where p is a prime number, does not form a skew field and discuss idempotent and nilpotent elements in the (finite) ring $\mathbb{O}/\mathbb{Z}_p$. We provide examples and establish conditions for idempotency and nilpotency.

Mathematics Subject Classification (2010): 15A33, 15A30, 20H25, 15A03.

Keywords: Quaternion, octonion, ring, skew field, idempotent, nilpotent.

1. Introduction

Quaternions, denoted by $\mathbb{H}$, were first discovered by William. R. Hamilton in 1843 as an extension of complex numbers into four dimensions [10]. Namely, a quaternion is of the form

$$x = a_0 + a_1 i + a_2 j + a_3 k,$$

where a_i are reals and i, j, k are such that $i^2 = j^2 = k^2 = ijk = -1$. Algebraically speaking, $\mathbb{H}$ forms a division algebra (skew field) over $\mathbb{R}$ of dimension 4 ([10], p.195-196).About the same time, John T. Graves discovered the octonions, denoted by $\mathbb{O}$, which are 8-dimensional numbers of the form

$$x = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 + a_4 e_4 + a_5 e_5 + a_6 e_6 + a_7 e_7$$

where a_i are reals and e_i's are mutually anti-commuting roots of unity. (i.e. $e_i^2 = -1$ and $e_i e_j = e_k$, $e_j e_i = -e_k$, $i \neq j$) [6]. Algebraically speaking, $\mathbb{O}$ forms a normed division algebra (skew field) over $\mathbb{R}$ of dimension 8 [6]. It is the largest of the (only) four normed division algebras and it is nonassociative.

Received 27 July 2021; Accepted 14 December 2021.

A study of the structure and some of its properties of the finite ring[2] $\mathbb{H}/\mathbb{Z}_p$, where p is a prime number, was done in [2]. A more detailed description of the structure $\mathbb{H}/\mathbb{Z}_p$ was given by Miguel and Serodio in [20]. Among others, they found the number of zero-divisors, the number of idempotent elements, and provided an interesting description of the zero-divisor graph. In particularly, they showed that the number of idempotent elements in $\mathbb{H}/\mathbb{Z}_p$ is p^2+p+2, for p odd prime. As discussed in [3], the only scalar idempotents in $\mathbb{H}/\mathbb{Z}_p$ are $a_0 = 0, 1$. Furthermore, there are no purely imaginary idempotents in $\mathbb{H}/\mathbb{Z}_p$. On the other hand, in [4], it was shown that nilpotents x in $\mathbb{H}/\mathbb{Z}_p$ are purely imaginary with norm $N(x) = 0$ and $x^2 = 0$.

In the sections that follow, we look at the structure of the finite ring $\mathbb{O}/\mathbb{Z}_p$. The multiplication of octonions followed the Fano Plane and it was programmed in Maple[3]. We give examples of idempotent and nilpotent elements in $\mathbb{O}/\mathbb{Z}_p$ and provide conditions for idempotency and nilpotency in $\mathbb{O}/\mathbb{Z}_p$.

2. Is $\mathbb{O}/\mathbb{Z}_p$ a finite skew field? A counterexample

In [2] we saw that since $\mathbb{Z}_\mathbf{p}$ is a field, then $\mathbb{H}/\mathbb{Z}_p$ is a quaternion algebra. The theory of quaternion algebras over a field $\mathbb{K}$ ($\mathrm{char}\mathbb{K} \neq 2$) tells us that a quaternion algebra Q is either a division ring or $Q = \mathbb{M}_{2\times 2}(\mathbb{K})$ ([16], p.16, 19). Since $\mathbb{H}/\mathbb{Z}_p$ is not a division ring (see [2]), then $\mathbb{H}/\mathbb{Z}_p \cong \mathbb{M}_{2\times 2}(\mathbb{Z}_p)$ if $p \neq 2$.

The real matrix representation of $\mathbb{H}/\mathbb{Z}_p$, where $x = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}/\mathbb{Z}_p$, is achieved by the 4×4 left or right Hamilton Operators as follows:

$$H_x^L = \begin{bmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & -a_3 & a_2 \\ a_2 & a_3 & a_0 & -a_1 \\ a_3 & -a_2 & -a_1 & -a_0 \end{bmatrix} \quad H_x^R = \begin{bmatrix} a_0 & -a_1 & -a_2 & -a_3 \\ a_1 & a_0 & a_3 & -a_2 \\ a_2 & -a_3 & a_0 & a_1 \\ a_3 & a_2 & -a_1 & a_0 \end{bmatrix}$$

But is the finite ring $\mathbb{O}/\mathbb{Z}_p$ a skew field? Consider the elements

$$x_1 = 2e_2 - e_3, x_2 = e_4 + 3e_5$$

in $\mathbb{O}/\mathbb{Z}_5$. Multiplying the two, we get:

$$x_1 \cdot x_2 = (2e_2 - e_3)(e_4 + 3e_5) = 0 (\bmod 5).$$

This shows that $\mathbb{O}/\mathbb{Z}_5$ has zero-divisors, and hence $\mathbb{O}/\mathbb{Z}_5$ is not a skew field. This was also anticipated by some well-known theorem in algebra, by Wedderburn in 1905 ([11], p.361), which says that: “Every finite skew field is a field”. Since $\mathbb{O}/\mathbb{Z}_p$ is not commutative, then it is not a field, and so it is not a skew-field.

So, what is the structure of $\mathbb{O}/\mathbb{Z}_p$? Since $\mathbb{Z}_p$ is a field, then $\mathbb{O}/\mathbb{Z}_p$ is a non-associative octonion algebra. As a matter of fact, is it an alternative, flexible and power associative algebra[4]. It is well known that $\mathbb{O}$ is a skew field, yet it has no ”proper” matrix representation due to the non-associativity. Nevertheless, as $\mathbb{O}$ is an extension of $\mathbb{H}$, by the Cayley-Dickson process, some non-proper 8×8 real matrix representations were introduced, by Tian in [26], through the left and right Hamilton

Operators of quaternions analogous to the one above. Namely:

$$H_x^L = \begin{bmatrix} a_0 & -a_1 & -a_2 & -a_3 & -a_4 & -a_5 & -a_6 & -a_7 \\ a_1 & a_0 & -a_3 & a_2 & -a_5 & a_4 & a_7 & -a_6 \\ a_2 & a_3 & a_0 & -a_1 & -a_6 & -a_7 & a_4 & a_5 \\ a_3 & -a_2 & a_1 & a_0 & -a_7 & a_6 & -a_5 & a_4 \\ a_4 & a_5 & a_6 & a_7 & a_0 & -a_1 & -a_2 & -a_3 \\ a_5 & -a_4 & a_7 & -a_6 & a_1 & a_0 & a_3 & a_2 \\ a_6 & -a_7 & -a_4 & a_5 & a_2 & -a_3 & a_0 & a_1 \\ a_7 & a_6 & -a_5 & -a_4 & a_3 & a_2 & -a_1 & a_0 \end{bmatrix}$$

$$H_x^R = \begin{bmatrix} a_0 & -a_1 & -a_2 & -a_3 & -a_4 & -a_5 & -a_6 & -a_7 \\ a_1 & a_0 & a_3 & -a_2 & a_5 & -a_4 & -a_7 & a_6 \\ a_2 & -a_3 & a_0 & a_1 & a_6 & a_7 & -a_4 & -a_5 \\ a_3 & a_2 & -a_1 & a_0 & a_7 & -a_6 & a_5 & -a_4 \\ a_4 & -a_5 & -a_6 & -a_7 & a_0 & a_1 & a_2 & a_3 \\ a_5 & a_4 & -a_7 & a_6 & -a_1 & a_0 & -a_3 & a_2 \\ a_6 & a_7 & a_4 & -a_5 & -a_2 & a_3 & a_0 & -a_1 \\ a_7 & -a_6 & a_5 & a_4 & -a_3 & -a_2 & a_1 & a_0 \end{bmatrix}$$

Modifying the above over $\mathbb{Z}_p$, one could easily get the left and right 8×8 real representations of $\mathbb{O}/\mathbb{Z}_p$ as follows[5]:

$$H_x^L = \begin{bmatrix} a_0 & p-a_1 & p-a_2 & p-a_3 & p-a_4 & p-a_5 & p-a_6 & p-a_7 \\ a_1 & a_0 & p-a_3 & a_2 & p-a_5 & a_4 & a_7 & p-a_6 \\ a_2 & a_3 & a_0 & p-a_1 & p-a_6 & p-a_7 & a_4 & a_5 \\ a_3 & p-a_2 & a_1 & a_0 & p-a_7 & a_6 & p-a_5 & a_4 \\ a_4 & a_5 & a_6 & a_7 & a_0 & p-a_1 & p-a_2 & p-a_3 \\ a_5 & p-a_4 & a_7 & -a_6 & a_1 & a_0 & a_3 & a_2 \\ a_6 & p-a_7 & p-a_4 & a_5 & a_2 & p-a_3 & a_0 & a_1 \\ a_7 & a_6 & p-a_5 & -a_4 & a_3 & a_2 & p-a_1 & a_0 \end{bmatrix}$$

$$H_x^R = \begin{bmatrix} a_0 & p-a_1 & p-a_2 & p-a_3 & p-a_4 & p-a_5 & p-a_6 & p-a_7 \\ a_1 & a_0 & a_3 & p-a_2 & a_5 & p-a_4 & p-a_7 & a_6 \\ a_2 & p-a_3 & a_0 & a_1 & a_6 & a_7 & p-a_4 & p-a_5 \\ a_3 & a_2 & p-a_1 & a_0 & a_7 & p-a_6 & a_5 & p-a_4 \\ a_4 & p-a_5 & p-a_6 & p-a_7 & a_0 & a_1 & a_2 & a_3 \\ a_5 & a_4 & p-a_7 & a_6 & p-a_1 & a_0 & p-a_3 & a_2 \\ a_6 & a_7 & a_4 & p-a_5 & p-a_2 & a_3 & a_0 & p-a_1 \\ a_7 & p-a_6 & a_5 & a_4 & p-a_3 & p-a_2 & a_1 & a_0 \end{bmatrix}$$

Notice that for the octonionic cases $\mathbb{O}$ and $\mathbb{O}/\mathbb{Z}_p$, we have that $H_{xy}^L \neq H_x^L H_y^L$ because of the non-associativity.

3. Idempotent and nilpotents elements in $\mathbb{O}/\mathbb{Z}_p$

Recall that an element x in a ring R is called idempotent if $x^2 = x$. In the ring $\mathbb{H}/\mathbb{Z}_p$, p prime, in the special case where $x = a_0, a_0 \neq 0$ (i.e., x is a non-zero scalar in $\mathbb{H}/\mathbb{Z}_p$) one quickly observes that if x is idempotent then $x = 1$, for x in 1, 2, ..., p-1, since $(x,p) = 1$. Therefore, the only scalar idempotent in $\mathbb{H}/\mathbb{Z}_p$ is 1 (we omit the case $x = 0$ as trivial). Another simple case is the case where $x = ai, aj$ or $ak, a \neq 0$ (i.e., a non-zero scalar multiple of the imaginary units). Then, $x^2 = (ai)^2 = -a^2 i^2 = -a^2 \neq ai = x$, which shows that there are no idempotents of the form ai, aj or ak. (Again, we omitted the case $x = 0$ as trivial). Examples of proper idempotents[6] and conditions for idempotency in $\mathbb{H}/\mathbb{Z}_p$ were given in [3]. Due to the isomorphism $\mathbb{H}/\mathbb{Z}_p \cong \mathbb{O}[e_i, e_j, e_i e_j]$ (where $e_i \neq e_j$) idempotents in $\mathbb{H}/\mathbb{Z}_p$ will transfer in some subalgebras[7] of $\mathbb{O}/\mathbb{Z}_p$. For example, $x = 4+i+3j+4k$ is idempotent in $\mathbb{H}/\mathbb{Z}_7$ and therefore $x = 4 + e_1 + 3e_2 + 4e_3$ is idempotent in $\mathbb{O}/\mathbb{Z}_7$. Nevertheless, $x = 4 + e_1 + 3e_3 + 4e_5$ is a non-“quaternionic” idempotent in $\mathbb{O}/\mathbb{Z}_7$. Notice that $x = 7i + 4j$ is nilpotent in $\mathbb{H}/\mathbb{Z}_{13}$ and so $x = 7e_1 + 4e_2$ is also nilpotent in $\mathbb{O}/\mathbb{Z}_{13}$. Nevertheless, $x = 4e_1 + e_2 + 3e_3 + 4e_5$ is a non-“quaternionic” nilpotent in $\mathbb{O}/\mathbb{Z}_7$. As we will show below, purely imaginary octonions in $\mathbb{O}/\mathbb{Z}_p$ cannot be idempotents, just as in $\mathbb{H}/\mathbb{Z}_p$ [3]. And nilpotents in $\mathbb{O}/\mathbb{Z}_p$ are purely imaginary, just as in $\mathbb{H}/\mathbb{Z}_p$ [4].

Theorem 3.1. *Let $x \in \mathbb{O}/\mathbb{Z}_p$ be an octonion of the form $x = a_0 + \sum_{i=1}^{7} a_i e_i$. Then x is idempotent if and only if $a_0 = \frac{1+p}{2}$ and $\sum_{i=1}^{7} a_i^2 = \frac{p^2-1}{4}$.*

Proof. We follow the steps given in the proof for the quaternion case in [3]. Since x is idempotent, we have:

$$\begin{aligned} x^2 = x \Rightarrow & \left(a_0 + \sum_{i=1}^{7} a_i e_i\right)\left(a_0 + \sum_{i=1}^{7} a_i e_i\right) = a_0 + \sum_{i=1}^{7} a_i e_i \\ & \Rightarrow a_0^2 + 2a_0 \sum_{i=1}^{7} a_i e_i + \left(\sum_{i=1}^{7} a_i e_i\right)\left(\sum_{i=1}^{7} a_i e_i\right) = a_0 + \sum_{i=1}^{7} a_i e_i \\ & \xrightarrow[\text{Fano}]{\text{distr.}} a_0^2 - \sum_{i=1}^{7} a_i^2 = a_0 \quad \text{and} \quad 2a_0 a_i = a_i \end{aligned}$$

From the 2^{nd} equation, we have that either $a_i = 0$ or $2a_0 = 1$. That is $a_0 = \frac{1+p}{2}$, as $p = 0(\operatorname{mod} p)$. Substituting the latter in the 1^{st} equation, we get $\sum_{i=1}^{7} a_i^2 = \frac{p^2-1}{4}$. □

Corollary 3.2. *Let $x \in \mathbb{O}/\mathbb{Z}_p$ be a purely imaginary octonion of the form*

$$x = \sum_{i=1}^{7} a_i e_i.$$

Then x is not idempotent.

Proof. If x is purely imaginary then $a_0 = 0$. Then from Theorem 3.1, $0 = \dfrac{1+p}{2}$ which is a contradiction. $\square$

Example 3.3. Consider $x = 4 + e_1 + 3e_3 + 4e_5$ in $\mathbb{O}/\mathbb{Z}_7$. Then x is idempotent. Notice that $4 = \dfrac{1+7}{2}$ and $1^2 + 3^2 + 4^2 = 26 = \dfrac{49-1}{4}$ mod(7).

Remark 3.4. To find the number of idempotents in $\mathbb{O}/\mathbb{Z}_p$, one could naturally find how many ways $\frac{P^2-1}{4}$ can be written as a sum of seven or fewer squares. The equation $\displaystyle\sum_{i=1}^{7} a_i^2 = \frac{p^2-1}{4}$ in Theorem 3.1 brings to mind the "sum of seven squares problem", which is to find the different values $r_7(n)$ for which $n = \displaystyle\sum_{i=1}^{7} x_i^2$, $n \in \mathbb{N}$. A formula for square-free values of n were stated without proof by Eisenstein in 1847, and those were extended to all positive integers n by Smith in 1864, also without a proof. Hardy in 1920 developed a method in deriving the proof for $r_k(n)$, where k is odd, but he explicitly showed only the $r_5(n)$ case in [13, 12]. More general results for $\mathrm{r}_7(n)$ were given by Cooper in 2001 [8] and Cooper and Hirschhorn in 2007 [9].

Recall that an element x in a ring R is called nilpotent if $x^k = 0$ for some $k \in \mathbb{N}$. In [4], it was shown that if x in $\mathbb{H}/\mathbb{Z}_p$ is nilpotent then the norm $N(x) = 0$ (where $N(x) = xx^* = \displaystyle\sum_{i=0}^{3} a_i^2$) and, furthermore, that x is purely imaginary and $x^2 = 0$. If $x \in \mathbb{O}/\mathbb{Z}_p$, we have similar results. First, consider the following Lemmas:

Lemma 3.5. *For any $x \in \mathbb{O}/\mathbb{Z}_p$, we have that $x^2 - 2a_0x + N(x) = 0$.*

Proof. Let $x = a_0 + \displaystyle\sum_{i=1}^{7} a_i e_i$. Then the left-hand side of the equation becomes:

$$\begin{aligned}
x^2 - 2a_0x + N(x) &= (a_0 + \sum_{i=1}^{7} a_i e_i)(a_0 + \sum_{i=1}^{7} a_i e_i) - 2a_0x + N(x) \\
&= a_0^2 + 2a_0 \sum_{i=1}^{7} a_i e_i + (\sum_{i=1}^{7} a_i e_i)(\sum_{i=1}^{7} a_i e_i) - 2a_0(a_0 + \sum_{i=1}^{7} a_i e_i) + \sum_{i=0}^{7} a_i^2 \\
&= a_0^2 + \sum_{i=1}^{7} 2a_0 a_i e_i - \sum_{i=1}^{7} a_i^2 - 2a_0(a_0 + \sum_{i=1}^{7} a_i e_i) + \sum_{i=0}^{7} a_i^2 \\
&= a_0^2 + 2a_0 \sum_{i=1}^{7} a_i e_i - \sum_{i=1}^{7} a_i^2 - 2a_0^2 - 2a_0 \sum_{i=1}^{7} a_i e_i + a_0^2 + \sum_{i=1}^{7} a_i^2 \\
&= 0
\end{aligned}$$

$\square$

Lemma 3.6. *Let $x \in \mathbb{O}/\mathbb{Z}_p$. If x is nilpotent, then $N(x) = 0$.*

Proof. We follow the steps given in the proof for the quaternion case in [4]. If x is nilpotent, then $x^k = 0$ for some k. From Lemma 3.5 above, we have:

$$\begin{aligned} x^2 - 2a_0x + N(x) = 0 &\Rightarrow x(x - 2a_0) = -N(x) \\ &\Rightarrow (x(x - 2a_0))^k = (-N(x))^k \\ &\Rightarrow x^k(x - 2a_0)^k = (-N(x))^k \text{ (see Remark 3.7 below)} \\ &\Rightarrow 0 = (N(x))^k \\ &\Rightarrow N(x) = 0, \text{ because } \mathbb{Z}_\mathbf{p} \text{ is a field.} \end{aligned}$$

□

Remark 3.7. We discuss the statement $(x(x - 2a_0))^k = x^k(x - 2a_0)^k$ in the proof in the Lemma 3.6 above: The statement is taken as obvious, without a proof, in [4] (in Lemma 2.1) for the quaternionic case $\mathbb{H}/\mathbb{Z}_p$, but it deserves a bit more explanation in our case here considering the non-commutativity and non-associativity of $\mathbb{O}/\mathbb{Z}_p$. As we mentioned in Sec.2, $\mathbb{O}/\mathbb{Z}_p$ is an alternative algebra (and flexible). Therefore, it also satisfies the *Moufang Identities*, in particularly the identity $(xy)(zx) = (x(yz))x$. Given this, it is not hard to show the following:

Proposition 3.8. *If A is an alternative algebra such that $xy = yx$, x, $y \in A$, then $(xy)^k = x^k y^k$.*

Proof. We show this for $k = 2$ (the general case follows by iteration). Indeed:

$$\begin{aligned} (xy)^2 = (xy)(xy) \overset{comm.}{=} (yx)(xy) &\overset{Mouf.}{=} (y(xx))y \\ &\overset{altern.}{=} ((yx)x)y \\ &\overset{comm.}{=} ((xy)x)y \\ &\overset{flex.}{=} (x(yx))y \\ &\overset{comm.}{=} (x(xy))y \\ &\overset{altern.}{=} ((xx)y)y \\ &\overset{Mouf.}{=} (xx)(yy) \end{aligned}$$

□

Hence, the statement $(x(x - 2a_0))^k = x^k(x - 2a_0)^k$ is also true in our particular case here, because $\mathbb{O}/\mathbb{Z}_p$ is alternative (and flexible) and $x(x - 2a_0) = (x - 2a_0)x$. It is also clear now why the statement is easy to prove in $\mathbb{H}/\mathbb{Z}_p$, considering that $\mathbb{H}/\mathbb{Z}_p$ is actually associative. Finally, given the above result, one could also obtain the binomial formula $(x + y)^k = \sum_{j=0}^{k} \binom{k}{j} x^j y^{k-j}$, which could also be used to prove the statement in question. That is:

$$
\begin{aligned}
(x(x-2a_0))^k = (x^2-2a_0x)^k &= \sum_{j=0}^{k} \binom{k}{j} (x^2)^j(-2a_0x)^{k-j} \\
&= x^k \sum_{j=0}^{k} \binom{k}{j} x^j(-2a_0)^{k-j} \\
&= x^k(x-2a_0)^k
\end{aligned}
$$

Theorem 3.9. *Let $x \in \mathbb{O}/\mathbb{Z}_p$. Then x is nilpotent if and only if x is purely imaginary and $N(x) = 0$. Furthermore, if x is nilpotent, then $x^2 = 0$.*

Proof. If x is nilpotent, then $x^k = 0$ for some $k > 1$ (where k is the least such natural number). From Lemma 3.6 above, we have that $N(x) = 0$. Combining Lemmas 3.5 and 3.6, we get $x^2 = 2a_0x$. Following the steps given in the proof for the quaternion case in [4], we have:

$$
\begin{aligned}
\text{If } k \text{ is even :} \quad x^2 = 2a_0x &\Rightarrow (x^2)^{k/2} = (2a_0)^{k/2}x^{k/2} \\
&\Rightarrow x^k = (2a_0)^{k/2}x^{k/2} \\
&\Rightarrow 0 = (2a_0)^{k/2}x^{k/2} \\
&\Rightarrow a_0 = 0
\end{aligned}
$$

$$
\begin{aligned}
\text{If } k \text{ is odd :} \quad x^2 = 2a_0x &\Rightarrow (x^2)^{(k+1)/2} = (2a_0)^{(k+1)/2}x^{(k+1)/2} \\
&\Rightarrow (x)^{(k+1)/2} = (2a_0)^{(k+1)/2}x^{(k+1)/2} \\
&\Rightarrow 0 = (2a_0)^{(k+1)/2}x^{k/2} \\
&\Rightarrow a_0 = 0
\end{aligned}
$$

Hence, $a_0 = 0$ and therefore x is imaginary. Furthermore, since $a_0 = 0$, from $x^2 = 2a_0x$ we have that $x^2 = 0$. For the converse, since $N(x) = 0$, Lemma 3.5 gives $x^2 = 2a_0x$. Since also x is imaginary ($a_0 = 0$) the equation $x^2 = 2a_0x$ gives $x^2 = 0$. Then for any $k > 1$ we have: $x^k = x^{k-2}x^2 = x^{k-2} \cdot 0 = 0$, so x is nilpotent. $\square$

Example 3.10. Consider $x = 4e_1 + e_2 + 3e_3 + 4e_5$ in $\mathbb{O}/\mathbb{Z}_7$. Then x is nilpotent. Notice that $N(x) = 0^2 + 4^2 + 1^2 + 3^2 + 0^2 + 4^2 + 0^2 + 0^2 = 0 (\operatorname{mod} 7)$.

4. Connection to general rings and applications

There is a lot in the literature on idempotents, nilpotents and k-potents in general, in more general rings R. It would be interesting to see if and how some of these results relate to the ‘special’, in a sense, ring $\mathbb{O}/\mathbb{Z}_p$.

In [16], Hirano and Tominaga proved that in a ring R the following are equivalent: (i) Every element of R is a sum of two commuting idempotents; (ii) R is commutative and every element of R is a sum of two idempotents; (iii) $x^3 = x$, for all x in R.[8]

As $\mathbb{O}/\mathbb{Z}_p$ is not commutative, the above fails. For example, consider the idempotents $a = 3 + e_1$ and $b = 3 + e_2$ in $\mathbb{O}/\mathbb{Z}_5$. Then,

$$x = a + b = (3 + e_1) + (3 + e_2) = 6 + e_1 + e_2 = 1 + e_1 + e_2,$$

but x is not tripotent (indeed, $(1 + e_1 + e_2)^3 = e_1 + e_2 \neq 1 + e_1 + e_2$). The above fails even when the idempotents commute. Take, for example, $a = b = 3 + e_1$ in $\mathbb{O}/\mathbb{Z}_5$.

Also, Mosic in [21] gives the relation between idempotent and tripotent elements in any associative ring R, generalizing the result on matrices by Trenkler and Baksalary [27]. Namely, for any $x \in R$, where 2, 3 are invertible, x is idempotent if and only if x is tripotent and $1 - x$ is tripotent or $1 + x$ is invertible. Notice that even though $\mathbb{O}/\mathbb{Z}_p$ is not associative, the result does hold in some cases. Take for example the tripotent $x = 4 + 3e_1 + e_2 + 4e_3$ in $\mathbb{O}/\mathbb{Z}_7$, which is also an idempotent. It is not hard to check that directly or using the conditions for idempotency in Theorem 3.1 above. Notice also that $1 - x$ is tripotent and $1 + x$ is invertible as $N(x) = 2 \neq 0$. So, we conjecture that Mosic's result may extend to (some) non-associative rings.

Finally, it is interesting to note any possible applications of rings related to the ring $\mathbb{O}/\mathbb{Z}_p$. Malekian and Zakerolhosseini in [19] use octonionic algebras to construct a high speed public key cryptosystem. More specifically, they consider the convolution polynomial rings $R = \mathbb{Z}[x]/(x^N - 1)$, $R_p = \mathbb{Z}_p[x]/(x^N - 1)$ and $R_q = \mathbb{Z}_q[x]/(x^N - 1)$, where p, q are primes such as $q \gg p$. From these they construct the octonionic algebras:

$$\mathbb{A} = \{\, a_0(x) + \sum_{i=1}^{7} a_i(x)e_i \mid a_i(x) \in R \,\},$$

$$\mathbb{A}_p = \{\, a_0(x) + \sum_{i=1}^{7} a_i(x)e_i \mid a_i(x) \ \in R_p \,\},$$

$$\mathbb{A}_q = \{\, a_0(x) + \sum_{i=1}^{7} a_i(x)e_i \mid a_i(x) \in R_q \,\},$$

respectively. Then, the public (and private) key is generated as follows: initially two small octonions $F \in \mathbb{L}_f$ and $G \in \mathbb{L}_g$, where $\mathbb{L}_f, \mathbb{L}_g$ are some specifically constructed subspaces of $\mathbb{A}$, are randomly generated. Namely,

$$F = f_0 + \sum_{i=1}^{7} f_i e_i \mid f_i \in \mathbb{L}_f\,,$$

$$G = g_0 + \sum_{i=1}^{7} g_i e_i \mid g_i \in \mathbb{L}_g\,.$$

The octonion F must be invertible in $\mathbb{A}_p$ and $\mathbb{A}_q$, otherwise a new octionion F is generated. The inverses of F in $\mathbb{A}_p$ and $\mathbb{A}_q$ are denoted by in F_p^{-1} and F_q^{-1}, respectively. The public key, which is an octonion, is then given by $H = F_p^{-1} o\, G \in \mathbb{A}_q$, where o is a multiplication defined on $\mathbb{A}_q$, in terms of the convolution product. Encryption and decryption are done with similar calculations.

Notes

1. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ and $\mathbb{O}$ are the only normed division algebras. This was proved by Hurwitz in 1898 [17].

2. "+" and "." on $\mathbb{H}$ are defined in [14, p. 124]. As $p = 0 (\mathrm{mod}\, p)$ on $\mathbb{H}/\mathbb{Z}_p$ they are defined as follows:

$$\begin{aligned}
x + y &= (a_0 + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)\\
&= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k\\
x \cdot y &= (a_0 + a_1 i + a_2 j + a_3 k) \cdot (b_0 + b_1 i + b_2 j + b_3 k)\\
&= a_0 b_0 + (p-1)a_1 b_1 + (p-1)a_2 b_2 + (p-1)a_3 b_3 +\\
&\quad (a_0 b_0 + a_1 b_0 + a_2 b_3 + (p-1)a_3 b_2)j +\\
&\quad (a_0 b_2 + (p-1)a_1 b_3 + a_2 b_0 + a_3 b_1)j +\\
&\quad (a_0 b_3 + a_1 b_2 + (p-1)a_2 b_1 + a_3 b_0)k
\end{aligned}$$

3. Fano Plane (Figure 1); Multiplication table (Figure 2); Program in Maple (Figure 3):

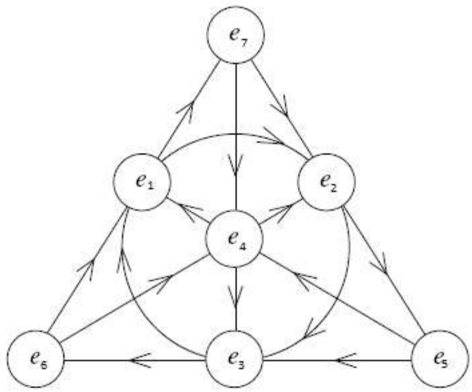

Figure 1. Fano Plane

e_ie_j	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_0	e_0	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	$-e_0$	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	$-e_0$	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	$-e_0$	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	$-e_0$	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	$-e_0$	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	$-e_0$	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	$-e_0$

Figure 2. Multiplication table

```
> HypercomplexLib :=`C:\\Hypercomplex\\Hypercomplex.mla`;
> libname:=HypercomplexLib,libname; ### now Maple will find the lib
                 HypercomplexLib := C:\Hypercomplex\Hypercomplex.mla
  libname := "C:\Hypercomplex\Hypercomplex.mla", "C:\Program Files\Maple 18\lib", "."      (1)
> with(Hypercomplex) :
> setHypercomplex(octonion) :
> i2·i7
                                   -i5                                                     (2)
> (2 i2 - i3)·(i4 + 3 i5) mod 5;
                                    0                                                      (3)
> (4 + i1 + 3 i3 + 4 i5)·(4 + i1 + 3 i3 + 4 i5) mod 7;
                          4 + i1 + 3 i3 + 4 i5                                             (4)
> (4 i1 + i2 + 3 i3 + 4 i5)·(4 i1 + i2 + 3 i3 + 4 i5) mod 7;
                                    0                                                      (5)
```

Figure 3. Maple program

4. Accordingly, the following hold: $(xx)y = x(xy)$ (alternative), $x(yx) = (xy)x$ (flexible), $\langle x\rangle$ is power associative for all x.

5. These representations are given in [11] without a proof. The proof for $\mathbb{O}/\mathbb{Z}_p$ is actually straightforward, following the exact steps in the proofs of Theorems 2.1 and 2.3 in [26] for the case of $\mathbb{O}$.

6. In Herstein [14, p. 130], we have as an exercise that: In a ring R, if $x^2 = x$, for all x in R, then R is commutative. It is not hard to show that the converse is not true. (e.g. $\mathbb{F} = \mathbb{Z}_3$, 2 is not idempotent). Actually, a field $\mathbb{F}$ has only trivial idempotents. Hence, in $\mathbb{H}/\mathbb{Z}_p$ some elements are non-trivial idempotents and they were described in [3].

7. Namely, the seven quaternionic subalgebras of $\mathbb{O}$ each generated by the seven "line" (including the circle) in the Fano Plane.

8. A ring R is called a *tripotent ring* if $x^3 = x$, for all x in R. The fact that a tripotent ring is commutative is found as an exercise in Hernstein [14, p. 136]. Several proofs of this fact have been given since the 60's [5]. In Bourbaki, we find it also as an exercise with guided steps/hints for the proof [7, p. 176]. See also [23]. Interestingly, a more general result by Jacobson was already known in the 40's [18]. Namely, if in a ring R there exists an integer $n > 1$ such that $x^n = x$, for every x in R, then R is commutative. For a proof of Jacobson's Theorem see [5], [15].

References

[1] Ankeny, N.C., *Sum of three squares*, Proc. Amer. Math. Soc., **8**(2)(1957), 316-319.

[2] Aristidou, M., Demetre, A., *A note on quaternion rings over* $\mathbb{Z}_p$, Int. J. Alg., **3**(15)(2009), 725-728.

[3] Aristidou, M., Demetre, A., *Idempotent elements in quaternion rings over $\mathbb{Z}_p$*, Int. J. Alg., **6**(5)(2012), 249-254.

[4] Aristidou, M., Demetre, A., *Nilpotent elements in quaternion rings over $\mathbb{Z}_p$*, Int. J. Alg., **6**(14)(2012), 663-666.

[5] Ayoub, R., Ayoub, C., *On the commutativity of rings*, Am. Math. Mon., **71**(3)(1964), 267-271.

[6] Baez, J.C., *The octonions*, Bull. Amer. Math. Soc., **39**(2002), 145-205.

[7] Bourbaki, N., *Elements of Mathematics – Algebra I*, Hermann, 1974.

[8] Cooper, S., *Sums of five, seven and nine squares*, Ramanujan J., **6**(2002), 469-490.

[9] Cooper, S., Hirschhorn, M., *On the number of primitive representations of integers as sums of squares*, Ramanujan J., **13**(2007), 7-25.

[10] Ebbinghaus, H.D., Hermes, H., Hirzebruch, F., Koecher, M., Mainzer, K., Neukirch, J., Prestel, A., Remmert, R., *Numbers*, Springer, NY, 1991.

[11] Halici, S., Karatas, A., $\mathbb{O}/\mathbb{Z}_p$ *Octonion algebra and its matrix representations*, Palest. J. Math., **6**(1)(2017), 307-313.

[12] Hardy, G.H., *On the representations of a number as the sum of any number of squares, and in particular of five or seven*, Proc. Nat. Acad. Sci., U.S.A., **4**(1918), 189-193.

[13] Hardy, G.H., *On the representation of a number as the sum of any number of squares, and in particular of five*, Trans. Amer. Math. Soc., **21**(1920), 255-284.

[14] Herstein, I.N., *Topics in Algebra*, 2nd ed., Wiley, 1975.

[15] Herstein, I.N., *Wedderburn's theorem and a theorem of Jacobson*, Am. Math. Mon., **68**(3)(1961), 249-251.

[16] Hirano, Y., Tominaga, H., *Rings in which every element is the sum of two idempotents*, Bull. Austral. Math. Soc., **37**(2)(1988), 161-164.

[17] Hurwitz, A., *Über die Composition der quadratischen Formen von Beliebig Vielen Variabeln*, Nachr. Ges. Wiss. Göttingen, (1898), 309-316.

[18] Jacobson, N., *Structure theory for algebraic algebras of bounded degree*, Ann. of Math., **46**(1945), 695-707.

[19] Malekian, E., Zakerolhosseini, A., *OTRU: A non-associative and high speed public key cryptosystem*, 15th CSI International Symposium on Computer Architecture and Digital Systems, Iran, 2010, 83-90.

[20] Miguel, C.J., Serodio, R., *On the structure of quaternion rings over $\mathbb{Z}_p$*, Int. J. Alg., **5**(27)(2011), 1313-1325.

[21] Mosic, D., *Characterizations of k-potent elements in rings*, Ann. Mat. Pura Appl., **194**(4)(2015), 1157-1168.

[22] Pierce, R.S., *Associative Algebras*, Springer, 1982.

[23] van der Poorten, A., *Concerning commuting*, Austral. Math. Soc. Gazette, **194**(1994), 68.

[24] Schafer, R., *An Introduction to Nonassociative Algebras*, Academic Press, 1996.

[25] Serre, J.P., *A Course in Arithmetic*, Springer, 1973.

[26] Tian, Y., *Matrix representations of octonions and their applications*, Adv. Appl. Clifford Algebr., **10**(1)(2000), 61-90.

[27] Trenkler, G., Baksalary, O.M., *On k-potent matrices*, Electron. J. Linear Algebra, **26**(2013), 446-470.

Michael Aristidou
Texas A&M University at Galveston,
Galveston, TX, USA
e-mail: maristidou@tamu.edu

Philip R. Brown
Texas A&M University at Galveston,
Galveston, TX, USA
e-mail: brownp@tamug.edu

George Chailos
University of Nicosia,
Nicosia, Cyprus
e-mail: chailos.g@unic.ac.cy