Acta Univ. Sapientiae, Mathematica, **13**, 1 (2021) 78–87

DOI: 10.2478/ausm-2021-0004

Tripotent elements in quaternion rings over $\mathbb{Z}_p$

Michael Aristidou
Texas A&M University at Galveston,
Galveston TX
email: maristidou@tamu.edu

Kidus Hailemariam
Independent Researcher,
Bloomington MN
email: kidus_tamirat@yahoo.com

Abstract. In this paper, we discuss tripotent[1] elements in the finite ring $\mathbb{H}/\mathbb{Z}_p$. We provide examples and establish conditions for tripotency. We follow similar methods used in [3] for idempotent elements in $\mathbb{H}/\mathbb{Z}_p$.

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 [9]. 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 R of dimension 4 ([9], p.195–196). A study of the finite ring[2] $\mathbb{H}/\mathbb{Z}_p$, where p is a prime number, looking into its structure and some of its properties, was done in [2]. A more detailed description of the structure $\mathbb{H}/\mathbb{Z}_p$ was given by Miguel and Serodio in [6]. 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 $a_0 = 0, 1$. Unlike that, as we will see below, there are scalar tripotents ($a_0 \neq 0, 1$) in

2010 Mathematics Subject Classification: 15A33, 15A30, 20H25, 15A03
Key words and phrases: quaternion, ring, idempotent, tripotent

$\mathbb{H}/\mathbb{Z}_p$. Yet, in both cases, there are no non-zero scalar multiple of the imaginary units (i.e. $x = bi$). Unlike also to the idempotent case, there are also pure imaginary tripotents (i.e. $x = a_1i+a_2j+a_3k$). There are also tripotent elements which are not idempotent. In the sections that follow, we give examples of tripotent elements in $\mathbb{H}/\mathbb{Z}_p$ and provide conditions for tripotency in $\mathbb{H}/\mathbb{Z}_p$.

2 Tripotent elements in $\mathbb{H}/\mathbb{Z}_p$

A quaternion x of the form $x = a_0+a_1i+a_2j+a_3k$ is said to be *tripotent* if $x^3 = x$. For the case of $\mathbb{H}/\mathbb{R}$ (i.e. $a_0, a_1, a_2, a_3 \in \mathbb{R}$), the only tripotent elements are $x = -1, x = 0$ and $x = 1$. However, for the case $\mathbb{H}/\mathbb{Z}_p$ (i.e. $a_0, a_1, a_2, a_3 \in \mathbb{Z}_p$), where p is a prime number, there are other possible tripotents other than, say, the obvious ones.

First notice the following: Take, for example, $p = 5$. If $a_0 \neq 0, a_1 = a_2 = a_3 = 0$, i.e. $\mathbb{H}/\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, a scalar tripotent is 4. For $\mathbb{H}/\mathbb{Z}_7$ is 6, $\mathbb{H}/\mathbb{Z}_{11}$ is 10, etc. In other words, for $\mathbb{H}/\mathbb{Z}_p$ the only scalar tripotent is p–1. This is not hard to show as $(p–1)^3 = (-1)^3 = -1 = p–1$. Furthermore, there are no tripotents that are non-zero scalar multiple of the imaginary units (say $x = bi$) because $x^3 = (bi)^3 = -bi = -x$ $(\neq x)$.

Furthermore, the existence of non-trivial tripotents is guaranteed as follows: As discussed in [2], [3] and [6], $\mathbb{H}/\mathbb{Z}_p$, which is not a division ring, has non-trivial idempotents[3]. But, it is not hard to show that idempotency implies tripotency due to the fact that in any ring $x^2 = x \Rightarrow x^3 = x$. (actually $x^2 = x \Rightarrow x^n = x$, for $n > 0$). Nevertheless, the converse is not true. For example, in $\mathbb{H}/\mathbb{Z}_5$, $3 + i$ is idempotent and hence also tripotent, but $2 + i$ is tripotent but not idempotent. (see also Example 1 and Remark 1).

The following propositions discuss the cases in which a non-scalar quaternion $x \in \mathbb{H}/\mathbb{Z}_p$, where p is a prime number, is tripotent.

Proposition 1 *Let* $x \in \mathbb{H}/\mathbb{Z}_p$ *be a quaternion of the form* $x = a_0 + a_1i$*, where* $a_0, a_1 \neq 0$*. Then,* x *is tripotent if and only if* $a_0^2 = \frac{1-p}{4}$ *and* $a_1^2 = \frac{p-1}{4}$*, where* p *prime number and* $p \neq 2, 3$.

Proof. Let $x = a_0 + a_1i$. Then:

$$x^3 = x \Rightarrow (a_0 + a_1i)^3 = a_0 + a_1i \Rightarrow a_0^3 - 3a_0a_1^2 + (3a_0^2a_1 - a_1^3)i = a_0 + a_1i$$

From the above we have the following two equations:

$$a_0^3 - 3a_0a_1^2 = a_0$$

$$3a_0^2a_1 - a_1^3 = a_1$$

These can be simplified into the following:

$$a_0^2 - 3a_1^2 = 1 \tag{1}$$

$$3a_0^2 - a_1^2 = 1 \tag{2}$$

One can solve for a_0^2 and a_1^2 as follows:

$$a_0^2 - 3a_1^2 = 3a_0^2 - a_1^2 \Rightarrow a_0^2 - 3a_0^2 = 3a_1^2 - a_1^2 \Rightarrow -2a_0^2 = 2a_1^2 \Rightarrow -a_0^2 = a_1^2 \tag{3}$$

Substituting for a_0^2 in (1) and solving for a_1^2 , we get:

$-a_1^2 - 3a_1^2 = 1 \Rightarrow -4a_1^2 = 1 \Rightarrow a_1^2 = \dfrac{-1}{4}$. Since $p = 0\,(\mathrm{mod} p)$, $a_1^2 = \dfrac{p-1}{4}$.

Solving for a_0^2, equation (3) gives: $a_0^2 = -\left(\frac{p-1}{4}\right) = \frac{1-p}{4}$.

To see if the quantities $\frac{p-1}{4}$ and $\frac{1-p}{4}$ are squares $\mathrm{mod} p$, we calculate the *Legendre Symbol*[4] for $\left(\frac{\frac{p-1}{4}}{p}\right)$ and $\left(\frac{\frac{1-p}{4}}{p}\right)$ respectively. The first gives:

$$\left(\frac{\frac{p-1}{4}}{p}\right) = \left(\frac{p-1}{p}\right)\left(\frac{\frac{1}{4}}{p}\right) = \left(\frac{p-1}{p}\right)\cdot 1 = (p-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$$

$$= \begin{cases} 1 & \text{if} \quad p \equiv 1 \pmod 4 \\ -1 & \text{if} \quad p \equiv 3 \pmod 4. \end{cases}$$

Hence, there are *no* tripotents of the form $a_0 + a_1 i$, if $p \equiv 3 \pmod 4$. Elements of the form $a_0 + a_1 i$ are tripotent if $p \equiv 1 \pmod 4$ and, in that case, $a_0^2 = \frac{1-p}{4}$ and $a_1^2 = \frac{p-1}{4}$.

For the converse, it is not hard to show that given $a_0^2 = \frac{1-p}{4}$ and $a_1^2 = \frac{p-1}{4}$, we have that:

$$\begin{aligned} x^3 = (a_0 + a_1 i)^3 &= a_0^3 - 3a_0a_1^2 + (3a_0^2a_1 - a_1^3)i \\ &= a_0(a_0^2 - 3a_1^2) + a_1(3a_0^2 - a_1^2)i \\ &= a_0\left(\frac{1-p}{4} - 3\frac{p-1}{4}\right) + a_1\left(3\frac{1-p}{4} - \frac{p-1}{4}\right)i \\ &= a_0(1-p) + a_1(1-p)i \\ &= a_0 + a_1 i, \quad \text{as} \quad p = 0 \pmod p \\ &= x \end{aligned}$$

Hence, x is tripotent. □

Example 1 *Let* $p = 13$. *Then, we have* $a_0^2 = \frac{1-13}{4} = \frac{-12}{4} = -3 = 10 \pmod{13}$ *and* $a_1^2 = \frac{13-1}{4} = \frac{12}{4} = 3$. *There are many values for* a_0 *and* a_1. *One pair of these possible values is* $a_0 = 6$ *and* $a_1 = 4$, *because* $6^2 = 36 = 10 \pmod{13}$ *and* $4^2 = 16 = 3 \pmod{13}$. *Therefore* $x = 6 + 4i$ *is a tripotent in* $\mathbb{H}/\mathbb{Z}_{13}$. *Notice also that* $x = 6 + 4i$ *is not an idempotent in* $\mathbb{H}/\mathbb{Z}_{13}$.

Remark 1 *As we have seen already above, there are tripotents which are also idempotents. As we explained already, idempotency implies tripotency, hence the tripotents which are also idempotents satisfy also the conditions of idempotency given in* [3]. *Namely,* $a_0 = \frac{p+1}{2}$ *and* $a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4}$. *Tripotents which are not idempotends, that is 'proper' tridempotents, do not satisfy these additional conditions. It is not hard to see that the conditions for idempotency imply the conditions for tripotency that we provide here, but not vice versa. (see more in Par. 3 for a general condition on when a tripotent is also idempotent). Notice also that in* [3] *it was shown that there are no pure imaginary idempotents of the form* $x = a_1 i + a_2 j + a_3 k$. *Yet, as Proposition 2 below shows, there are tripotents of that form. Hence, all pure imaginary elements are 'proper' tripotents.*

Proposition 2 *Let* $x \in \mathbb{H}/\mathbb{Z}_p$ *be a pure imaginary element of the form* $x = a_1 i + a_2 j + a_3 k$, *where at least two of* a_1, a_2, a_3 *are non-zero. Then,* x *is tripotent if and only if* $a_1^2 + a_2^2 + a_3^2 = p - 1$.

Proof. Let $x = a_1 i + a_2 j + a_3 k$. Then:

$$x^3 = x \Rightarrow (a_1 i + a_2 j + a_3 k)^3 = a_1 i + a_2 j + a_3 k$$

Expanding the above, we get:

$$a_1(-a_1^2 - a_2^2 - a_3^2)i + a_2(-a_1^2 - a_2^2 - a_3^2)j + a_3(-a_1^2 - a_2^2 - a_3^2)k = a_1 i + a_2 j + a_3 k$$

Hence, we obtain the following three equations:

$$a_1(-a_1^2 - a_2^2 - a_3^2) = a_1 \tag{4}$$
$$a_2(-a_1^2 - a_2^2 - a_3^2) = a_2 \tag{5}$$
$$a_3(-a_1^2 - a_2^2 - a_3^2) = a_3. \tag{6}$$

From the above three equations we get:

$$a_1 = 0 \quad \text{or} \quad -a_1^2 - a_2^2 - a_3^2 = 1$$

$$a_2 = 0 \quad \text{or} \quad -a_1^2 - a_2^2 - a_3^2 = 1$$
$$a_3 = 0 \quad \text{or} \quad -a_1^2 - a_2^2 - a_3^2 = 1.$$

From the equation $-a_1^2 - a_2^2 - a_3^2 = 1$, we have $a_1^2 + a_2^2 + a_3^2 = -1$. This can be written also as $a_1^2 + a_2^2 + a_3^2 = p - 1$, as $p \bmod p = 0$.

For the converse, given that $a_1^2 + a_2^2 + a_3^2 = p - 1$, it is not hard to see that: $x^3 = (a_1 i + a_2 j + a_3 k)^3 = a_1(-a_1^2 - a_2^2 - a_3^2)i + a_2(-a_1^2 - a_2^2 - a_3^2)j + a_3(-a_1^2 - a_2^2 - a_3^2)k = a_1(1-p)i + a_2(1-p)j + a_3(1-p)k = a_1 i + a_2 j + a_3 k = x$, as $p \bmod p = 0$. Hence, x is tripotent. □

Example 2 *Let* $p = 5$. *Then, we have* $a_1^2 + a_2^2 + a_3^2 = 5 - 1 = 4$. *We can have different combinations of numbers from* $\mathbb{Z}_5$ *that satisfy the above equation. One such combinations is* $a_1 = 3$, $a_2 = 4$ *and* $a_3 = 2$ (*i.e.* $3^2 + 4^2 + 2^2 = 29 = 4 \bmod 5$). *Hence,* $x = 3i + 4j + 2k$ *is a tripotent in* $\mathbb{H}/\mathbb{Z}_5$.

Theorem 1 *Let* $x \in \mathbb{H}/\mathbb{Z}_p$, *where p is prime and* $p \neq 2, 3$, *be an element of the from* $x = a_0 + a_1 i + a_2 j + a_3 k$, *where* $a_0 \neq 0$ *and at least one of* a_1, a_2, a_3 *is non-zero. Then, x is tripotent if and only if* $a_0^2 = \frac{1-p}{4}$ *and* $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4}$.

Proof. Let $x = a_0 + a_1 i + a_2 j + a_3 k$. Then:

$$x^3 = x \Rightarrow (a_0 + a_1 i + a_2 j + a_3 k)^3 = a_0 + a_1 i + a_2 j + a_3 k.$$

After the multiplications, we get:

$$a_0\big(a_0^2 - 3\big(a_1^2 + a_2^2 + a_3^2\big)\big) + a_1\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big)i + a_2\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big)j + a_3\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big)k = a_0 + a_1 i + a_2 j + a_3 k.$$

Hence, we obtain the following four equations by equating the corresponding coefficients:

$$a_0\big(a_0^2 - 3\big(a_1^2 + a_2^2 + a_3^2\big)\big) = a_0 \tag{7}$$
$$a_1\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big) = a_1 \tag{8}$$
$$a_2\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big) = a_2 \tag{9}$$
$$a_3\big(3a_0^2 - \big(a_1^2 + a_2^2 + a_3^2\big)\big) = a_3. \tag{10}$$

From the above four equations we get the following:

$$a_0 = 0 \quad \text{or} \quad a_0^2 - 3\big(a_1^2 + a_2^2 + a_3^2\big) = 1$$

$$\begin{aligned} a_1 = 0 \quad &\text{or} \quad 3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right) = 1 \\ a_2 = 0 \quad &\text{or} \quad 3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right) = 1 \\ a_3 = 0 \quad &\text{or} \quad 3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right) = 1. \end{aligned}$$

From the first, since $a_0 \neq 0$, we have $a_0^2 - 3\left(a_1^2 + a_2^2 + a_3^2\right) = 1$. In addition, from the last three we have $3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right) = 1$. Let $a_1^2 + a_2^2 + a_3^2 = \lambda$. Then, we have the following two equations:

$$a_0^2 - 3\lambda = 1 \tag{11}$$

$$3a_0^2 - \lambda = 1. \tag{12}$$

Combining the equations, we get:

$$a_0^2 - 3\lambda = 3a_0^2 - \lambda \Rightarrow -2a_0^2 = 2\lambda \Rightarrow a_0^2 = -\lambda.$$

Substituting a_0^2 for $-\lambda$ in (11), we get $\lambda = -\frac{1}{4} = \frac{p-1}{4}$, because $p \bmod p = 0$. Hence, $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4}$. And, since $a_0^2 = -\lambda$, we get $a_0^2 = \frac{1-p}{4}$.
For the converse, given that $a_0^2 = \frac{1-p}{4}$ and $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4}$, it is not hard to see that:

$$\begin{aligned} x^3 = \left(a_0 + a_1 i + a_2 j + a_3 k\right)^3 &= a_0\left(a_0^2 - 3\left(a_1^2 + a_2^2 + a_3^2\right)\right) + \\ &\quad a_1\left(3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right)\right) i + \\ &\quad a_2\left(3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right)\right) j + \\ &\quad a_3\left(3a_0^2 - \left(a_1^2 + a_2^2 + a_3^2\right)\right) k \\ &= a_0\left(\frac{1-p}{4} - 3\frac{p-1}{4}\right) + \\ &\quad a_1\left(3\frac{1-p}{4} - \frac{p-1}{4}\right) i + \\ &\quad a_2\left(3\frac{1-p}{4} - \frac{p-1}{4}\right) j + \\ &\quad a_3\left(3\frac{1-p}{4} - \frac{p-1}{4}\right) k \\ &= a_0(1-p) + a_1(1-p)i + a_2(1-p)j + a_3(1-p)k \\ &= a_0 + a_1 i + a_2 j + a_3 k \ , \text{ as } \ p = 0 \mod p \\ &= x. \end{aligned}$$

Hence, x is tripotent. □

Example 3 *Let* $p = 7$. *Then,* $a_0^2 = \frac{1-7}{4} = \frac{-6}{4}$ *and* $a_1^2+a_2^2+a_3^2 = \frac{7-1}{4} = \frac{6}{4}$. *From the two equations we have* $4a_0^2 = -6 = 1 \pmod 7$ *and* $4(a_1^2+a_2^2+a_3^2) = 6$. *One possible solution is* $a_0 = 3$ *and* $a_1 = 2$, $a_2 = 2$, $a_3 = 2$. *This can be checked as follows:* $4(3^2) = 36 = 1 \pmod 7$ *and* $4(2^2+2^2+2^2) = 48 = 6 \pmod 7$. *Thus, the element* $x = 3+2i+2j+2k$ *is tripotent in* $\mathbb{H}/\mathbb{Z}_7$ *(but not idempotent). Another tripotent is* $x = 4+3i+j+4k$, *which is also idempotent.*

Remark 2 *The equation* $a_1^2+a_2^2+a_3^2 = \frac{p-1}{4}$ *brings to mind the classic 'Sum of Three Squares Theorem' which was proved by Gauss in his Disquisitiones Arithmeticae in 1801.*[5] *As that theorem says, an integer n can be the sum of three squares if and only if* $n \neq 4^m(8k+7), m, k, \geq 0$. *So, clearly, when* $n = 7$ *one does not have solutions to the equation* $a_1^2+a_2^2+a_3^2 = n$. *But, in our case (in this special 'modp' version), one does get solutions for* $p = 7$ *to the equation* $a_1^2+a_2^2+a_3^2 = \frac{p-1}{4}$, *as Example 3 above shows. More interestingly, we get solutions even if* $\frac{p-1}{4} = 4^m(8k+7), m, k, \geq 0$. *For example, for* $p = 113$, $\frac{p-1}{4} = \frac{113-1}{4} = 28 = 4^1(8.0+7)$, *but* $28 = 141 \pmod{113} = 4^2+5^2+10^2$. *And, given that* $a_0^2 = \frac{1-113}{4} = -28 = 85 \pmod{113}$, *the tripotent is* $56+4i+5j+10k$.

3 Connection to general rings and applications

There is a lot in the literature regarding tripotents, 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 $\mathbb{H}/\mathbb{Z}_p$.

In Zhou et al. [14] (Theorem 2.1), we are informed that in a commutative ring R every x is the sum of two idempotents if and only if $x^3 = x$. As $\mathbb{H}/\mathbb{Z}_p$ is not commutative, the above fails. For example, consider the idempotents $a = 3+i$ and $b = 3+j$ in $\mathbb{H}/\mathbb{Z}_5$. Then, $x = a+b = (3+i)+(3+j) = 6+i+j = 1+i+j$, but x is not tripotent (because $1^2 \neq \frac{1-5}{4}$ and $1^2+1^2 \neq \frac{5-1}{4}$ from the Theorem 1 above). The above fails even when the idempotents commute. Take, for example, $a = b = 3+i$ in $\mathbb{H}/\mathbb{Z}_5$.

Also, Mosic in [7] gives the relation between idempotent and tripotent elements in any associative ring R, generalizing the result on matrices by Baksalary and Trenkler [12]. 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). Since $\mathbb{H}/\mathbb{Z}_p$ is associative, the result holds. As we have seen already in Par.2 above, idempotency implies tripotency. But for a tripotent to be idempotent it is also required that $1-x$ is tripotent. Take for example the tripotents in our Example 3 above. Namely, $x = 4+3i+j+4k$ and $x = 3+2i+2j+2k$ in

$\mathbb{H}/\mathbb{Z}_7$. The first is also an idempotent, but the second is not. It is not hard to check that directly or using the conditions for idempotency in [3]. Notice also that for the first case we have $1-x$ is tripotent (and $1+x$ is invertible as the $N(x) = 2 \neq 0$), where in the second case is $1-x$ is not tripotent (nor $1+x$ is invertible as the $N(x) = 0$). More generally, in $\mathbb{H}/\mathbb{Z}_p$, one can see the conditions given by Mosic as follows: Theorem 1 says that if $x = a_0 + a_1 i + a_2 j + a_3 k$ is tripotent then $a_0^2 = \frac{1-p}{4}$ and $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4}$. If $1-x$ is also a tripotent, then $(1-a_0)^2 = \frac{1-p}{4}$ and $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4}$. Equating the corresponding first terms, one has $a_0^2 = (1-a_0)^2 \Rightarrow 1 - 2a_0 + a_0^2 \Rightarrow 2a_0 = 1 \Rightarrow a_0 = \frac{1}{2} = \frac{p+1}{2}$, which is the first condition for idempotency in [3]. (the second condition in [3] is also true by simply noticing that $a_1^2 + a_2^2 + a_3^2 = \frac{p-1}{4} = \frac{p^2-1}{4}$).

Finally, it is interesting to note any possible applications of idempotents, tripotent or more generally k-potent ring elements. Wu in [13] applies k-potent matrices in digital image encryption. A series of encryption key matrices is used, via matrix multiplications, to mask an image by altering the gray level of each pixel of the image. The original image then is transformed into a different image. k-potent matrices, and their 'variations', are used for the encryption key matrices. Wu defines them all via the equation: $A = \alpha I + \beta A$, where $\alpha\beta = 0, \alpha, \beta \in \{-1, 0, 1\}$ and $k \geq 2$. (e.g. A is *periodic* with period $k-1$ if $A^k = A$ and k is the least positive integer as such, A is *skew-unipotent* if $A^k = -I$, etc).

4 Conclusion

In this paper, we talked about tripotent elements in $\mathbb{H}/\mathbb{Z}_p$. Unlike idempotents, there are scalar tripotents ($a_0 \neq 0, 1$) in $\mathbb{H}/\mathbb{Z}_p$. Yet, in both cases, there are no non-zero scalar multiple of the imaginary units (i.e. $x = bi$). Unlike also to the idempotent case, there are also pure imaginary tripotents (i.e. $x = a_1 i + a_2 j + a_3 k$). There are also tripotent elements which are not idempotent. We provided examples of non-trivial tripotents and we established conditions for tripotency. The methodology we followed and the conditions we found were very similar as the one(s) in [3]. An interesting and possibly harder project is to look at the structure of $\mathbb{O}/\mathbb{Z}_p$, where $\mathbb{O}$ is the octonion division algebra, and discuss idempotent, tripotent and nilpotent elements in that finite ring.

Notes

1. Recall that x is *idempotent* if $x^2 = x$, and x is *tripotent* if $x^3 = x$. In general, x is *k-potent* if $x^k = x$, for some k.
2. $+$ and $\cdot$ on $\mathbb{H}$ are defined in ([5], p.124). As $p = 0 \pmod p$, on $\mathbb{H}/\mathbb{Z}_p$ they are defined as follows:

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

3. In Herstein ([5], p.130), we have that: In a ring $\mathbb{F}$, if $x^2 = x$, for all x, then $\mathbb{F}$ 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]. Interestingly, in Herstein ([5], p.136) we also have that: In a ring $\mathbb{F}$, if $x^3 = x$, for all x, then $\mathbb{F}$ is commutative. The latter is much harder to establish, but a solution (with an interesting story behind it) can be found in [4].
4. The *Legendre Symbol* $\left(\frac{a}{p}\right)$ is defined as follows:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } a \text{ is a qudratic residue mod } p \\ -1 & \text{if } a \text{ is not a qudratic residue mod } p \\ 0 & \text{if } p/a. \end{cases}$$

5. For a proof see ([11], p.45). Also see [1] for a more elementary proof.

Acknowledgements

The authors would like to thank Dr. Philip Brown for his valuable comments and corrections on an earlier draft, and the referee for his/her review, comments and suggestions on the article.

References

[1] N. C. Ankeny, Sum of Three Squares, *Proc. Amer. Math. Soc.*, **8** (2) (1957), 316–319.

[2] M. Aristidou and A. Demetre, A Note on Quaternion Rings over $\mathbb{Z}_p$, *Int. J. Algebra*, **3** (15) (2009), 725–728.

[3] M. Aristidou and A. Demetre, Idempotent Elements in Quaternion Rings over $\mathbb{Z}_p$, *Int. J. Algebra*, **6** (5) (2012), 249–254.

[4] P. Damianou, Commutative Rings (in Greek), Proceedings of the 9^{th} Cyprus Conference of Mathematics Education and Science, Cyprus, 2007, 165–166.

[5] I. N. Herstein, *Topics in Algebra*, 2^{nd} ed., Wiley, NY, 1975.

[6] C. J. Miguel and R. Serodio, On the Structure of Quaternion Rings over $\mathbb{Z}_p$, *Int. J. Algebra*, **5** (27) (2011), 1313–1325.

[7] D. Mosic, Characterizations of k-potent Elements in Rings, *Ann. Mat. Pura Appl.*, **194** (4) (2015), 1157–1168

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

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

[10] R. D. Schafer, *An Introduction to Nonassociative Algebrass*, Academic Press, NY, 1966.

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

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

[13] 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.

[14] Z. Ying, T. Kosan and Y. Zhou, Rings in Which Every Element is a Sum of Two Tripotents, *Canad. Math. Bull.*, **59** (3) (2016), 661–672.

Received: October 22, 2020