International Journal of Algebra, Vol. 6, 2012, no. 5, 249 - 254

Idempotent Elements in Quaternion Rings over $\mathbb{Z}_p$

Michael Aristidou

American University of Kuwait
Department of Science and Engineering
P.O. Box 3323, Safat 13034, Kuwait
maristidou@auk.edu.kw

Andy Demetre

Seattle University
Department of Mathematics
901 12th Ave., P.O. Box 222000
Seattle, WA 98122-1090, USA
demetra@seattleu.edu

Abstract

In this paper, we discuss idempotent elements in the finite ring $\mathbb{H}/\mathbb{Z}_p$. The number of idempotents in $\mathbb{H}/\mathbb{Z}_p$ was found recently in [4]. We provide examples and we establish conditions for idempotency in $\mathbb{H}/\mathbb{Z}_p$.

Mathematics Subject Classification: 15A33, 15A30, 20H25, 15A03

Keywords: quaternion, ring, idempotent

1. Introduction

The quaternions, denoted by $\mathbb{H}$, were first invented by W. R. Hamilton in 1843 as an extension of the complex numbers into four dimensions [6]. Algebraically speaking, $\mathbb{H}$ forms a division algebra (skew field) over $\mathbb{R}$ of dimension 4 ([6], p.195-196). In [2], we studied the finite ring [1] $\mathbb{H}/\mathbb{Z}_p$, where p is a prime, looking into its structure and some of its properties. A more detailed description of the structure $\mathbb{H}/\mathbb{Z}_p$ was given recently by Miguel and Serodio in [4]. 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. In the sections that follow, we examine idempotent elements in $\mathbb{H}/\mathbb{Z}_p$ and provide conditions for idempotency in $\mathbb{H}/\mathbb{Z}_p$.

2. Idempotent Elements in $\mathbb{H}/\mathbb{Z}_p$

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, an element x is of the form:

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

where $a_i \in \mathbb{Z}_p$, p prime, and $i^2 = j^2 = k^2 = p - 1 = -1$. 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 ommit 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 imginary 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 ommitted the case $x = 0$ as trivial).

The next non-simple cases are captured by the following Propositions and Theorem.

Proposition 2.1: Let $x \in \mathbb{H}/\mathbb{Z}_p$, $p \neq 2$, be of the form $x = a_0 + a_1 i$. If x is idempotent, then x is of the form $x = \frac{p+1}{2} + \sqrt{\frac{p^2-1}{4}}i$.

Proof. We have $(a_0 + a_1 i)^2 = (a_0 + a_1 i)(a_0 + a_1 i) = a_0^2 + 2a_0 a_1 i - a_1^2 = (a_0^2 - a_1^2) + 2a_0 a_1 i$. Since x is idempotent, the RHS of the last equation must equal $a_0 + a_1 i$. Hence, we have:

$$a_0^2 - a_1^2 = a_0 \qquad (1)$$
$$2a_0 a_1 = a_1. \qquad (2)$$

From (2), we get $2a_0 a_1 = a_1 \Rightarrow 2a_0 = 1 \Rightarrow a_0 = \frac{p+1}{2}$. From (1), we get $a_0^2 - a_1^2 = a_0 \Rightarrow \frac{(p+1)^2}{4} - a_1^2 = \frac{(p+1)}{2} \Rightarrow a_1^2 = \frac{(p+1)^2}{4} - \frac{(p+1)}{2} \Rightarrow a_1^2 = \frac{p^2-1}{4}$. To see if $\frac{p^2-1}{4}$ is a square $mod p$, we calculate the Legendre Symbol[2] $(\frac{\frac{p^2-1}{4}}{p})$. The multiplicative property of the Legendre Symbol gives us $(\frac{\frac{p^2-1}{4}}{p}) = (\frac{p^2-1}{p})(\frac{1/4}{p})$. But, $(\frac{1/4}{p}) = 1$, since $1/4 = (1/2)^2$. Hence:

$$(\frac{\frac{p^2-1}{4}}{p}) = (\frac{p^2-1}{p}) = (p^2-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & , \text{ if } p \equiv 1 (mod 4) \\ -1 & , \text{ if } p \equiv 3 (mod 4). \end{cases}$$

Therefore, there are *no* idempotents of the form $a_0 + a_1 i$, if $p \equiv 3(mod 4)$. Elements of the form $a_0 + a_1 i$ are idempotent if $p \equiv 1(mod 4)$ and, in that case, $a_0 = \frac{p+1}{2}$ and $a_1 = \sqrt{\frac{p^2-1}{4}}$. □

Remark 2.2: For $p = 2$, notice that (1) and (2) in the proof above imply that an idempotent must satisfy $a_1 = 0$ and $a_0 = 1$. Hence, $x = 1$ is the only idempotent element in this case. For $p = 3$, clearly there are no idempotents of the form $a_0 + a_1 i$. An idempotent *not* of that form though is $2 + i + j$.

Example 2.3: Let $p = 13$. Then, $a_0 = \frac{p+1}{2} = 7$ and $a_1^2 = \frac{p^2-1}{4} = 42 = 3(mod 13)$. So, $a_1 = 4$ or 9. Therefore, the idempotents are $7 + 4i$ and $7 + 9i$.

Proposition 2.4: Let $x \in \mathbb{H}/\mathbb{Z}_p$ be of the form $x = a_1 i + a_2 j + a_3 k$. Then, x is *not* an idempotent.

Proof. We have that:

$$\begin{aligned}(a_1 i + a_2 j + a_3 k)^2 &= (a_1 i + a_2 j + a_3 k)(a_1 i + a_2 j + a_3 k) \\ &= -a_1^2 + a_1 a_2 k - a_1 a_3 j - a_2 a_1 k - a_2^2 + a_2 a_3 i + a_3 a_1 j - a_3 a_2 i - a_3^2 \\ &= -(a_1^2 + a_2^2 + a_3^2) + (a_2 a_3 - a_2 a_3) i + (a_1 a_3 - a_1 a_3) j + (a_1 a_2 - a_1 a_2) k \\ &= -(a_1^2 + a_2^2 + a_3^2) + 0i + 0j + 0k \\ &= -(a_1^2 + a_2^2 + a_3^2).\end{aligned}$$

As the outcome of the above is a scalar (instead of $a_1 i + a_2 j + a_3 k$), we clearly have that x is not an idempotent. □

The above Proposition helps obtaining the following Theorem which generalizes Prop. 2.1.

Theorem 2.5: Let $x = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}/\mathbb{Z}_p$. Then, x is idempotent if $a_0 = \frac{p+1}{2}$ and $a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4}$.

Proof. We have that:

$$\begin{aligned}(a_0 + a_1 i + a_2 j + a_3 k)^2 &= (a_0 + a_1 i + a_2 j + a_3 k)(a_0 + a_1 i + a_2 j + a_3 k) \\ &= a_0^2 + a_0 a_1 i + a_0 a_2 j + a_0 a_3 k + a_0 a_1 i - a_1^2 + a_1 a_2 k - a_1 a_3 j \\ &\quad + a_0 a_2 j - a_1 a_2 k - a_2^2 + a_2 a_3 i + a_0 a_3 k + a_1 a_3 j - a_2 a_3 i - a_3^2 \\ &= a_0^2 - a_1^2 - a_2^2 - a_3^2 + 2a_0 a_1 i + 2a_0 a_2 j + 2a_0 a_3 k.\end{aligned}$$

As the last portion of the above must equal $a_0 + a_1 i + a_2 j + a_3 k$ (if one is to have idempotency), then we get that:

$$\begin{aligned}a_0 &= a_0^2 - a_1^2 - a_2^2 - a_3^2 \qquad (1)\\ a_1 &= 2a_0 a_1 \qquad (2)\\ a_2 &= 2a_0 a_2 \qquad (3)\\ a_3 &= 2a_0 a_3. \qquad (4)\end{aligned}$$

Equations (2), (3) and (4) imply:

$$\begin{aligned} a_1 = 0 \quad &\text{or} \quad 2a_0 = 1 \\ a_2 = 0 \quad &\text{or} \quad 2a_0 = 1 \\ a_3 = 0 \quad &\text{or} \quad 2a_0 = 1 \end{aligned}$$

from which (last part) we derive that $a_0 = \frac{p+1}{2}$. Using this fact in (1), we also get:

$$\begin{aligned} \frac{p+1}{2} &= \frac{(p+1)^2}{4} - a_1^2 - a_2^2 - a_3^2 \\ a_1^2 + a_2^2 + a_3^2 &= \frac{(p+1)^2}{4} - \frac{p+1}{2} \\ a_1^2 + a_2^2 + a_3^2 &= \frac{p^2-1}{4}. \end{aligned}$$

□

Remark 2.6: Just as in Rem.2.2, for $p = 2$, (1) and (2) in the proof above imply that an idempotent must satisfy $a_1 = 0$ and $a_0 = 1$. Hence, $x = 1$ is the only idempotent element in this case.

Example 2.7: Let $p = 5$. Then, $a_0 = \frac{p+1}{2} = 3$ and $a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4} = 6 = 1(mod5)$. One solution is $a_1 = 5, a_2 = 11, a_3 = 5$. Therefore, an idempotent is $3 + 5i + 11j + 5k$. Another is $3 + 6i + 10j + 15k$, and basically one can find them all by solving $a_1^2 + a_2^2 + a_3^2 = 1(mod5)$.

Remark 2.8: To find the number of idempotents in $\mathbb{H}/\mathbb{Z}_p$ one could naturally find how many ways $\frac{p^2-1}{4}$ can be written as a sum of three or fewer squares. From [4], we know that the number is $p^2 + p + 2$, for p odd prime. The equation $a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4}$ brings to mind the classical 'Sum of Three Squares Theorem' which was proved by Gauss in his *Disquisitones Arithmeticae* (S.291) in 1801.[3] 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 $a_1^2 + a_2^2 + a_3^2 = \frac{p^2-1}{4}$. In particularly, $(4, 1, 3, 4)$ is a solution and hence $x = 4 + i + 3j + 4k$ is an idempotent in $\mathbb{H}/\mathbb{Z}_7$. More interestingly, we get solutions even if $\frac{p^2-1}{4} = 4^m(8k + 7), m, k \geq 0$. For example, for $p = 31$: $\frac{p^2-1}{4} = 240 = 4^2(8.1 + 7)$, but $240 = 209 = 23mod31 = 8^2 + 9^2 + 8^2$ (and the idempotent is $16 + 8i + 9j + 8k$). Finally, notice that $2 + i + j$ is an idempotent in $\mathbb{H}/\mathbb{Z}_3$, but $\frac{p^2-1}{4} = \frac{3^2-1}{4} = 2$ is *not* the sum of three squares in $\mathbb{Z}_3$.

Conclusion

We discussed idempotent elements in $\mathbb{H}/\mathbb{Z}_p$ and gave conditions for their existence, as well as some examples. A natural question is to examine nilpotent elements in $\mathbb{H}/\mathbb{Z}_p$, but we leave that as a future project. Another is to study the group structure of the units of $\mathbb{H}/\mathbb{Z}_p$ in more detail. Miguel and Serodio already pointed out in [4] that the group can be generated by two elements. Finally, 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 and nilpotent elements in that finite ring.

Notes

1. Recall that addition and multiplication on $\mathbb{H}/\mathbb{Z}_n$ are defined as follows:

$$\begin{aligned} x+y &= (a_0+a_1i+a_2j+a_3k)+(b_0+b_1i+b_2j+b_3k) \\ &= (a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k \end{aligned}$$

$$\begin{aligned} x\cdot y &= (a_0+a_1i+a_2j+a_3k)\cdot(b_0+b_1i+b_2j+b_3k) \\ &= a_0b_0+(n-1)a_1b_1+(n-1)a_2b_2+(n-1)a_3b_3+ \\ &\quad (a_0b_1+a_1b_0+a_2b_3+(n-1)a_3b_2)i+ \\ &\quad (a_0b_2+(n-1)a_1b_3+a_2b_0+a_3b_1)j+ \\ &\quad (a_0b_3+a_1b_2+(n-1)a_2b_1+a_3b_0)k \end{aligned}$$

2. The Legendre Symbol $(\frac{a}{p})$ is defined as follows:

$$(\frac{a}{p}) = a^{\frac{p-1}{2}} = \begin{cases} 1 & , \text{ if } a \text{ is a qudratic residue } modp \\ -1 & , \text{ if } a \text{ is not a qudratic residue } modp \\ 0 & , \text{ if } p|a. \end{cases}$$

3. For a proof see [8]. Also [1] for a more elementary proof.

References

[1] N. C. Ankeny, Sum of Three Squares, Proceedings of the AMS, Vol.8, 2 (1957), 316-319.

[2] M. Aristidou and A. Demetre, A Note on Quaternion Rings over $\mathbb{Z}_p$, International Journal of Algebra, Vol.3, 15 (2009), 725-728.

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

[4] C. J. Miguel and R. Serodio, On the Structure of Quaternion Rings over $\mathbb{Z}_p$, International Journal of Algebra, Vol.5, 27 (2011), 1313-1325.

[5] R. S. Pierce, Associative Algebras, Springer, 1982.

[6] R. Remmert et all, Numbers, Springer, 1991.

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

[8] J. P. Serre, A Course in Arithmetic, Springer, p.45, 1973.

Received: October, 2011