JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA) VOL. 6 NO. 2 (NOV 2023)
Available online at www.jfma.math.fsm.undip.ac.id

IDEMPOTENT ELEMENTS IN MATRIX RING OF ORDER 2 OVER POLYNOMIAL RING $\mathbb{Z}_{p^2q}[x]$

Muchammad Choerul Arifin[1*], Iwan Ernanto[1]

[1] *Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Gadjah Mada, Indonesia*

Email: [1]muchammadchoerularifin11@mail.ugm.ac.id, [2]iwan.ernanto@ugm.ac.id

*Corresponding author

Abstract. An idempotent element in the algebraic structure of a ring is an element that, when multiplied by itself, yields an outcome that remains unchanged and identical to the original element. Any ring with a unity element generally has two idempotent elements, 0 and 1, these particular idempotent elements are commonly referred to as the trivial idempotent elements However, in the case of rings $\mathbb{Z}_n$ and $\mathbb{Z}_n[x]$ it is possible to have non-trivial idempotent elements. In this paper, we will investigate the idempotent elements in the polynomial ring $\mathbb{Z}_{p^2q}[x]$ with p, q different primes. Furthermore, the form and characteristics of non-trivial idempotent elements in $M_2(\mathbb{Z}_{p^2q}[x])$ will be investigated. The results showed that there are 4 idempotent elements in $\mathbb{Z}_{p^2q}[x]$ and 7 idempotent elements in $M_2(\mathbb{Z}_{p^2q}[x])$.

Keywords: Idempotent elements, Matrix ring, Polynomial ring, Matrix ring over polynomial ring.

I. INTRODUCTION

A ring is formally characterized as a nonempty set denoted as R, equipped with two binary operations, namely addition and multiplication, while satisfying specific criteria [1] [2]. Within the ring theory, there exist distinctive elements that conform to specific definitions, including idempotent elements. An idempotent element, by definition, is characterized as an element that, when multiplied by itself, yields an outcome that remains unchanged and identical to the original element. In other words, an element e is called an idempotent element if $e^2 = e$ [1]. Within any ring including a unity element, at least there are two idempotent elements, namely 0 and 1. These particular idempotent elements are commonly referred to as the trivial idempotent elements [3]. However, in the case of rings $\mathbb{Z}_n$ and $\mathbb{Z}_n[x]$ it is possible to have non-trivial idempotent elements [4].

Idempotent elements hold a crucial significance in the study of algebra, particularly within the ring theory. Using these idempotent elements, we can define new classes of these elements such as unit regular elements [5], clean and strongly clean elements [6][7][8], lie regular elements [9], etc. Due to its crucial significance, the study of idempotent elements become one of the interesting topics for researchers.

In recent times, there have been many studies on certain aspects of idempotent elements. In the case of polynomial rings, Kanwar *et al.* [10] showed that in any commutative ring R, the idempotent elements of ring R are equal to the idempotent elements of ring $R[x]$. Furthermore, Kanwar *et al.* [11] also showed the forms of idempotent elements in $M_2(\mathbb{Z}_{2p}[x])$ with p odd primes and $M_2(\mathbb{Z}_{3p}[x])$ with p primes greater than 3. Moreover, Jose *et al.* [12] extended the discussion to the case of $M_2(\mathbb{Z}_{pq}[x])$, where p, q are distinct primes. In this paper, we will investigate in more complex case of idempotent elements in the ring $\mathbb{Z}_{p^2q}[x]$, where p, q are distinct primes. Through this case, the form and characteristics of non-trivial idempotent elements on $M_2(\mathbb{Z}_{p^2q}[x])$ will be investigated.

II. RESULTS AND DISCUSSION

In this section, we will investigate the forms and characteristics of non-trivial idempotent elements in the ring of matrices of order 2 over the polynomial ring $\mathbb{Z}_{p^2q}[x]$, where p, q are distinct primes. First, we will begin by considering the following theorem of idempotent elements in the ring $\mathbb{Z}_{p^2q}$, where p, q are distinct primes.

Theorem 1 *Given p, q are distinct primes. The idempotent elements in $\mathbb{Z}_{p^2q}$ are $0, 1, p^{k(q-1)}$, and $q^{p(p-1)}(mod\, p^2q)$, where k is the smallest positive integer such that $k(q-1)-2$ is positive.*

Proof. Given that x is an idempotent element in $\mathbb{Z}_{p^2q}$, it follows that $x^2 \equiv x\ (mod\, p^2q)$ holds. Then, we obtained $x^2 \equiv x(mod\, p^2)$ and $x^2 \equiv x(mod\, q)$. Since p is a prime number, then $x \equiv 0(mod\, p^2)$ or $x \equiv 1(mod\, p^2)$. Similarly to q, then $x \equiv 0(mod\, q)$ or $x \equiv 1(mod\, q)$. Furthermore, for the case of $x \equiv 0(mod\, p^2)$ and $x \equiv 0(mod\, q)$, then we obtained $x \equiv 0(mod\, p^2q)$. For the case of $x \equiv 1(mod\, p^2)$ and $x \equiv 1(mod\, q)$, we obtained $x \equiv 1(mod\, p^2q)$. Moreover, to find the other 2 idempotent elements, divide into the following 2 cases.

1. Case $x \equiv 0(mod\, p^2)$ and $x \equiv 1(mod\, q)$.
   By Chinese Remainder Theorem [13], we obtained
   $$x \equiv M_q x_q (mod\, p^2q),$$
   where $M_q = \frac{p^2q}{q} = p^2$ and $M_q x_q \equiv 1(mod\, q)$. Since $(p^2, q) = 1$, by Euler's Theorem [14] [15], then $p^{\phi(q)} \equiv 1(mod\, q)$, where $\phi(q) = q-1$. Hence, from the previous solution we obtained
   $$x \equiv (p^{q-1})(mod\, p^2q).$$
   However, p^{q-1} is not necessarily greater than p^2. If $p^{q-1} \geq p^2$, then case is solved and the 3^{rd} idempotent element is p^{q-1}. Otherwise, multiply $q-1$ by k, where k is the smallest positive integer such that $p^{k(q-1)} > p^2$. Hence, the 3^{rd} idempotent element is
   $$x \equiv (p^{k(q-1)})(mod\, p^2q),$$
   where k is the smallest positive integer such that $p^{k(q-1)} \geq p^2$.
2. Case $x \equiv 1(mod\, p^2)$ and $x \equiv 0(mod\, q)$.
   Similarly to the first case, the 4^{th} idempotent element is
   $$x \equiv (q^{p(p-1)})(mod\, p^2q).$$

Thus, the idempotent elements of $\mathbb{Z}_{p^2q}$ are $0, 1, p^{k(q-1)}$, and $q^{p(p-1)}$ $(mod\, p^2q)$, where k is the smallest positive integer such that $p^{k(q-1)} \geq p^2$.

□

Example 1 Given a ring $\mathbb{Z}_{12} = \mathbb{Z}_{2^2 3}$. The idempotent elements of this ring are $0, 1, 4$, and 9.

Similar to other rings, polynomial rings also have idempotent elements. In case ring R is a commutative ring, by Corollary 2.3 [11], we obtained $E(\mathbb{Z}_{p^2q}) = E(\mathbb{Z}_{p^2q}[x])$.

The ring of matrices over the ring of polynomials is also known as the determinant and trace of the matrix. Given the following theorem shows that the determinant and trace of an idempotent element matrix are in the ring.

Theorem 2 *Given any commutative ring $(R, +, \times)$ and has only trivial nilpotent elements. Determinant and trace of any idempotent matrix in $M_2(R[x])$ are in R.*

Proof. Let A be a matrix denoted by

$$A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix},$$

is an idempotent matrix in $M_2(R[x])$. Since det(A) is an idempotent element and by Corollary 2.3 [11], then det(A) is idempotent in R i.e. $a(x)d(x) - b(x)c(x) \in R$. Furthermore, since A is an idempotent matrix, then $a(x) = (a(x))^2 + b(x)c(x)$ and $d(x) = (d(x))^2 + b(x)c(x)$. Hence, we obtained

$$\begin{aligned}(a(x) + d(x))^2 &= (a(x))^2 + 2a(x)d(x) + (d(x))^2 \\ &= a(x) + d(x) + 2(a(x)d(x) - b(x)c(x)).\end{aligned}$$

Since det(A) $\in R$, then $(a(x) + d(x))^2 - (a(x) + d(x)) \in R$. Thus, by Proposition 2.1 [11] we obtained trace(A) $\in R$.

$\square$

The trivial idempotent elements in $M_2(\mathbb{Z}_{p^2q}[x])$, where p, q are distinct primes are the zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. We will investigate the forms of non-trivial idempotent matrices on $M_2(\mathbb{Z}_{p^2q}[x])$, where p, q are distinct primes. However, first given the following theorem which explains the conditions on non-trivial idempotent matrices in $M_2(\mathbb{Z}_{p^2q}[x])$.

Theorem 3 *Given p, q are distinct primes and A is a non-trivial idempotent matrix in $M_2(\mathbb{Z}_{p^2q}[x])$. Then, one of the following conditions holds:*

1. *det(A) = 0 and trace(A) = 1 or $p^{k(q-1)}$ or $q^{p(p-1)}$;*
2. *det(A) = $p^{k(q-1)}$ and trace(A) = $p^{k(q-1)} + 1$ or $2p^{k(q-1)}$; or*
3. *det(A) = $q^{p(p-1)}$ and trace(A) = $q^{p(p-1)} + 1$ or $2q^{p(p-1)}$.*

Proof. By Theorem 1 and Corollary 2. 3 [11], the idempotent elements in $\mathbb{Z}_{p^2q}[x]$ are $0, 1, p^{k(q-1)}$, and $q^{p(p-1)} (mod\ p^2q)$, where k is the smallest positive integer such that $k(q-1) - 2$ is positive.

Let A be a matrix denoted by

$$A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix},$$

is a non-trivial idempotent matrix in $M_2(\mathbb{Z}_{p^2q}[x])$. By Theorem 2, det($A$) and trace($A$) are $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. If det(A) $= 1$, we obtained A is the identity matrix. A contradiction as a matrix A is a non-trivial idempotent matrix. Hence, det(A) is $0, p^{k(q-1)}$, or $q^{p(p-1)}$.

1. Case det(A) $= 0$.
   By Theorem 2 and Theorem 2.5 [11], trace(A) is $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. If trace(A) $= 0$, then we obtained

$$\begin{aligned} A^2 &= \begin{bmatrix} a(x)(a(x)+d(x)) & b(x)(a(x)+d(x)) \\ c(x)(a(x)+d(x)) & d(x)(a(x)+d(x)) \end{bmatrix} \\ &= \begin{bmatrix} a(x)\cdot 0 & b(x)\cdot 0 \\ c(x)\cdot 0 & d(x)\cdot 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}. \end{aligned}$$

   We obtained that A is a zero matrix. A contradiction as a matrix A is a non-trivial idempotent matrix. Hence, trace(A) $\neq 0$. Note that the following matrices in $M_2(\mathbb{Z}_{p^2q}[x])$

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} p^{k(q-1)} & 0 \\ 0 & 0 \end{bmatrix}, \text{and} \begin{bmatrix} q^{p(p-1)} & 0 \\ 0 & 0 \end{bmatrix}$$

   respectively is a non-trivial idempotent matrix with determinant 0 and its trace is $1, p^{k(q-1)}$, and $q^{p(p-1)}$. Thus, if A is a non-trivial idempotent matrix and det(A) $= 0$, then trace(A) is either $1, p^{k(q-1)}$, or $q^{p(p-1)}$.

2. Case det(A) $= p^{k(q-1)}$.
   Since A is an idempotent matrix, then $a(x) = (a(x))^2 + b(x)$ and $d(x) = (d(x))^2 + b(x)c(x)$. Note that,

$$\begin{aligned} (a(x)+d(x))^2 &= (a(x))^2 + 2a(x)d(x) + (d(x))^2 \\ &= a(x) + d(x) + 2p^{k(q-1)}(mod\, p^2q). \end{aligned}$$

   Let $y = a(x) + d(x)$, then we obtained the quadratic equation $y^2 - y - 2p^{k(q-1)} \equiv 0(mod\, p^2q)$. From this quadratic equation, it follows that

$$y^2 - y - 2p^{k(q-1)} \equiv 0(mod\, p^2) \tag{1}$$
$$y^2 - y - 2p^{k(q-1)} \equiv 0(mod\, q). \tag{2}$$

   Equation (1) is equivalent to $y^2 - y \equiv 0(mod\, p^2)$, then $y \equiv 0(mod\, p^2)$ or $y \equiv 1(mod\, p^2)$. By Euler's Theorem [14] [15], Equation (2) is equivalent to $y^2 - y - 2 \equiv 0(mod\, q)$, then $y \equiv 2(mod\, q)$ or $y \equiv -1\ (mod\, q)$.

   (a) Case $y \equiv 0(mod\, p^2)$ and $y \equiv 2(mod\, q)$.

By Chinese Remainder Theorem [13], then we obtained

$$y \equiv (2M_q y_q)(mod\ p^2 q),$$

where $M_q = p^2$ and $M_q y_q \equiv 1(mod\ q)$. Since $gcd(p^2, q) = 1$, By Euler's Theorem [14] [15], then $p^{\varphi(q)} \equiv 1(mod\ q)$, where $\varphi(q) = q - 1$. Hence, from the previous solution we obtained

$$y \equiv (2p^{q-1})(mod\ p^2 q)$$

However, p^{q-1} is not necessarily greater than p^2. If $p^{q-1} \geq p^2$, then case is solved and the 3^{rd} idempotent element is p^{q-1}. Otherwise, multiply $q-1$ by k, where k is the smallest positive integer such that $p^{k(q-1)} > p^2$. Hence, the 1^{st} solution is

$$y \equiv (2p^{k(q-1)})(mod\ p^2 q).$$

(b) Case $y \equiv 0(mod\ p^2)$ and $y \equiv -1(mod\ q)$.
Similarly to the case (a), the 2^{nd} solution is

$$y \equiv (-p^{k(q-1)})(mod\ p^2 q).$$

(c) Case $y \equiv 1(mod\ p^2)$ and $y \equiv 2(mod\ q)$.
By Chinese Remainder Theorem [13] and Euler's Theorem [14] [15], then we obtained the 3^{rd} solution is

$$\begin{aligned} y &\equiv (q^{p(p-1)} + 2p^{k(q-1)})(mod\ p^2 q) \\ &\equiv (1 + p^{k(q-1)})(mod\ p^2 q). \end{aligned}$$

(d) Case $y \equiv 1(mod\ p^2)$ and $y \equiv -1(mod\ q)$.
Similarly to the case (c), the 4^{th} solution is

$$\begin{aligned} y &\equiv (q^{p(p-1)} - \ p^{k(q-1)})(mod\ p^2 q) \\ &\equiv (1 - \ 2p^{k(q-1)})(mod\ p^2 q). \end{aligned}$$

Thus, the solutions of $y = a(x)+d(x)$ are $2p^{k(q-1)}$, $-p^{k(q-1)}$, $1+p^{k(q-1)}$, and $1- 2p^{k(q-1)}$. If $q = 3$, the case of $2p^{k(q-1)}$ coincides with the case of $-p^{k(q-1)}$ and the case of $1+p^{k(q-1)}$ coincides with the case of $1 - \ 2p^{k(q-1)}$. However, if $q \neq 3$, we claimed that the possible values of y are $2p^{k(q-1)}$ or $1 + p^{k(q-1)}$.
First, if $y = -p^{k(q-1)}$. We obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} -p^{k(q-1)}a(x) - p^{k(q-1)} & -p^{k(q-1)}b(x) \\ -p^{k(q-1)}c(x) & a(x)p^{k(q-1)} \end{bmatrix}.$$

Since A is an idempotent, then $(1 + p^{k(q-1)})(b(x)) = (1 + p^{k(q-1)})(c(x)) = 0$. Since $gcd(p^2 q, 1 + p^{k(q-1)}) = 1$, then $b(x) = c(x) = 0$. Hence, we obtained a matrix A is

$$A = \begin{bmatrix} a(x) & 0 \\ 0 & -p^{k(q-1)} - a(x) \end{bmatrix}.$$

Since A is an idempotent, then $a(x)$ and $-p^{k(q-1)} - a(x)$ are also idempotent elements. Since $a(x)$ is an idempotent element, then $a(x)$ is $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. Furthermore, we obtained $-p^{k(q-1)} - a(x)$ is not an idempotent element for $a(x) = 0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. A contradiction, hence $y \neq -p^{k(q-1)}$.
Second, if $y = 1 - 2p^{k(q-1)}$. Similarly to the case above and since A is an idempotent, then $(2p^{k(q-1)})b(x) = (2p^{k(q-1)})c(x) = 0$. Note that,

$$\begin{aligned}(2p^{k(q-1)})b(x)(2p^{k(q-1)})c(x) &= 4b(x)c(x)p^{2k(q-1)} \\ &= 2(2a(x)p^{k(q-1)}) - (2a(x)p^{k(q-1)}) = 0. \qquad (3)\end{aligned}$$

Furthermore, since $a(x)d(x) - b(x)c(x) = p^{k(q-1)}$, then we obtained

$$2a(x)p^{k(q-1)} = -p^{k(q-1)}. \qquad (4)$$

Subtitute Equation (4) to Equation (3), then we obtained

$$3p^{k(q-1)} \equiv 0 \ (mod\ p^2q).$$

Since q is distinct from 3 and p^2, a contradiction as $3p^{k(q-1)} \not\equiv 0 \ (mod\ q)$. Hence, $y \neq 1 - 2p^{k(q-1)}$. Note that the following matrices in $M_2(\mathbb{Z}_{p^2q}[x])$

$$\begin{bmatrix} p^{k(q-1)} & 0 \\ 0 & p^{k(q-1)} \end{bmatrix} \text{ and } \begin{bmatrix} p^{k(q-1)} & 0 \\ 0 & 1 \end{bmatrix}$$

respectively is a non-trivial idempotent matrix with determinant $p^{k(q-1)}$ and its trace is $p^{k(q-1)}$ and $p^{k(q-1)}+1$. Thus, if A is a non-trivial idempotent matrix and det(A) $= p^{k(q-1)}$, then trace(A) is either $2p^{k(q-1)}$ or $p^{k(q-1)} + 1$.

3. Case det(A) $= q^{p(p-1)}$.
   Similarly to the case 2 above, then we obtained the quadratic equation $w^2 - w - 2q^{p(p-1)} \equiv 0(mod\ p^2q)$. From this quadratic equation, it follows that

$$w^2 - w - 2q^{p(p-1)} \equiv 0(mod\ p^2) \qquad (5)$$
$$w^2 - w - 2q^{p(p-1)} \equiv 0(mod\ q). \qquad (6)$$

   By Euler's Theorem [14] [15], Equation (5) is equivalent to $w^2 - w - 2 \equiv 0(mod\ p^2)$, then $w \equiv 2(mod\ p^2)$ or $w \equiv -1(mod\ p^2)$. Equation (6) is quivalent to $w^2 - w \equiv 0(mod\ q)$, then $w \equiv 0(mod\ q)$ or $w \equiv 1(mod\ q)$.

   (a) Case $w \equiv 2(mod\ p^2)$ and $w \equiv 1(mod\ q)$.
   By Chinese Remainder Theorem [13] and Euler's Theorem [14] [15], then we obtained the 1^{st} solution is

$$\begin{aligned} w &\equiv (2q^{p(p-1)} + p^{k(q-1)})(mod\ p^2q) \\ &\equiv (q^{p(p-1)} + 1)(mod\ p^2q). \end{aligned}$$

   (b) Case $w \equiv 2(mod\ p^2)$ and $w \equiv 0(mod\ q)$.

Similarly to the case above, the 2^{nd} solution is

$$w \equiv (2q^{p(p-1)})(mod\, p^2q).$$

(c) Case $w \equiv -1(mod\, p^2)$ and $w \equiv 1(mod\, q)$.
Similarly to the cases above, the 3^{rd} solution is

$$w \equiv (1 - 2q^{p(p-1)})(mod\, p^2q).$$

(d) Case $w \equiv -1(mod\, p^2)$ and $w \equiv 0(mod\, q)$.
Similarly to the cases above, the 4^{th} solution is

$$w \equiv (-q^{p(p-1)})(mod\, p^2q).$$

Thus, the solutions of $w = a(x)+d(x)$ are $q^{p(p-1)}+1, 2q^{p(p-1)}, 1-2q^{p(p-1)}$ and $-q^{p(p-1)}$. We claimed that the possible values of w are $q^{p(p-1)} + 1$ or $q^{p(p-1)}$.
First, if $w = 1 - 2q^{p(p-1)}$. We obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} (a(x))^2 + b(x)c(x) & (1 - 2q^{p(p-1)})b(x) \\ (1 - 2q^{p(p-1)})c(x) & (d(x))^2 + b(x)c(x) \end{bmatrix}.$$

Sine A is an idempotent, then $(2q^{p(p-1)})b(x) = (2q^{p(p-1)})c(x) = 0$. Note that,

$$\begin{aligned} (2q^{p(p-1)})b(x)(2q^{p(p-1)})c(x) &= 4b(x)c(x)q^{2p(p-1)} \\ &= 2(2a(x)q^{p(p-1)}) - (2a(x)q^{p(p-1)}) = 0. \end{aligned} \tag{7}$$

Furthermore, since $a(x)d(x) - b(x)c(x) = q^{p(p-1)}$, then we obtained

$$2a(x)q^{p(p-1)} = -q^{p(p-1)}. \tag{8}$$

Subtitute Equation (8) to Equation (7), then we obtained

$$3q^{p(p-1)} \equiv 0\ (mod\, p^2q).$$

A contradiction as $3q^{p(p-1)} \not\equiv 0(mod\, p^2)$. Hence, $w \neq 1 - 2q^{p(p-1)}$.
Second, if $w = -q^{p(p-1)}$. Similarly to the case above and since A is an idempotent, then $(1 + q^{p(p-1)})(b(x)) = (1 + q^{p(p-1)})(c(x)) = 0$. Since $gcd(p^2q,\, 1 + q^{p(p-1)}) = 1$, then $b(x) = c(x) = 0$. Hence, we obtained a matrix A is

$$A = \begin{bmatrix} a(x) & 0 \\ 0 & -q^{p(p-1)} - a(x) \end{bmatrix}.$$

Since A is an idempotent, then $a(x)$ and $-q^{p(p-1)} - a(x)$ are also idempotent elements. Since $a(x)$ is an idempotent elements, then $a(x)$ is $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. Furthermore, we obtained $-q^{p(p-1)} - a(x)$ is not an idempotent for $a(x) = 0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. A contradiction, hence $w \neq -q^{p(p-1)}$. Note that the following matrices in $M_2(\mathbb{Z}_{p^2q}[x])$

$$\begin{bmatrix} q^{p(p-1)} & 0 \\ 0 & q^{p(p-1)} \end{bmatrix} \text{ and } \begin{bmatrix} q^{p(p-1)} & 0 \\ 0 & 1 \end{bmatrix}$$

respectively is a non-trivial idempotent matrix with determinant $q^{p(p-1)}$ and its trace is $q^{p(p-1)}$ and $q^{p(p-1)}+1$. Thus, if A is a non-trivial idempotent matrix and det$(A) = q^{p(p-1)}$, then trace(A) is either $2q^{p(p-1)}$ or $q^{p(p-1)} + 1$.

□

The main discussion in this paper follows. The forms of non-trivial idempotent elements in ring $M_2(\mathbb{Z}_{p^2q}[x])$ are presented in list form in the following theorem.

Theorem 4 *Given p, q are distinct primes. The non-trivial idempotent matrix form in ring $M_2(\mathbb{Z}_{p^2q}[x])$ can be expressed in one of the following matrix forms:*

1. $\begin{bmatrix} p^{k(q-1)} & 0 \\ 0 & p^{k(q-1)} \end{bmatrix}$ *and* $\begin{bmatrix} q^{p(p-1)} & 0 \\ 0 & q^{p(p-1)} \end{bmatrix}$;
2. $\begin{bmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{bmatrix}$, *where* $a(x)(1-a(x)) - b(x)c(x) = 0$;
3. $\begin{bmatrix} p^{k(q-1)}a(x) & p^{k(q-1)}b(x) \\ p^{k(q-1)}c(x) & p^{k(q-1)}(1-a(x)) \end{bmatrix}$, *where* $a(x)(1-a(x)) - b(x)c(x) = qf(x)$;
4. $\begin{bmatrix} q^{p(p-1)}a(x) & q^{p(p-1)}b(x) \\ q^{p(p-1)}c(x) & q^{p(p-1)}(1-a(x)) \end{bmatrix}$, *where* $a(x)(1-a(x)) - b(x)c(x) = p^2g(x)$;
5. $\begin{bmatrix} 1+qa(x) & qb(x) \\ qc(x) & p^{k(q-1)} - qa(x) \end{bmatrix}$, *where* $a(x)(1+qa(x)) + qb(x)c(x) = p^2h(x)$;
6. $\begin{bmatrix} 1+p^2a(x) & p^2b(x) \\ p^2c(x) & p^{k(q-1)} - p^2a(x) \end{bmatrix}$, *where* $a(x)(1+p^2a(x)) + p^2b(x)c(x) = q\phi(x)$

where $a(x), b(x), c(x), f(x), g(x), h(x), \phi(x) \in \mathbb{Z}_{p^2q}[x]$.

Proof. Let A be a matrix denoted by

$$A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix},$$

is a non-trivial idempotent matrix in $M_2(\mathbb{Z}_{p^2q}[x])$. By Theorem 3, divide into the following 3 cases.

1. Case det$(A) = 0$.
First, if trace$(A) = 1$. Since $a(x) + d(x) = 1$ and $a(x)d(x) - b(x)c(x) = 0$, then $a(x) = (a(x))^2 + b(x)c(x)$, $b(x) = b(x)(a(x) + d(x))$, $c(x) = c(x)(a(x) + d(x))$, and $d(x) = (d(x))^2 + b(x)c(x)$. Hence, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} a(x) & b(x) \\ c(x) & 1 - a(x) \end{bmatrix}.$$

Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} a(x) & b(x) \\ c(x) & 1 - a(x) \end{bmatrix}$$

where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2q}[x]$ such that $a(x)(1 - a(x)) - b(x)c(x) = 0$. This matrix is the 2^{nd} non-trivial idempotent matrix form.
Second, if trace$(A) = p^{k(q-1)}$. Similarly to the case above, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} p^{k(q-1)}a(x) & p^{k(q-1)}b(x) \\ p^{k(q-1)}c(x) & p^{k(q-1)}(1 - a(x)) \end{bmatrix}.$$

Since A is an idempotent, then $p^{k(q-1)}a(x) = a(x),\ p^{k(q-1)}b(x) = b(x),\ p^{k(q-1)}c(x) = c(x)$. Since det$(A) = 0$, then we obtained

$$a(x)(1 - a(x)) - b(x)c(x) = qf(x),$$

where $f(x) \in \mathbb{Z}_{p^2q}[x]$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} p^{k(q-1)}a(x) & p^{k(q-1)}b(x) \\ p^{k(q-1)}c(x) & p^{k(q-1)}(1 - a(x)) \end{bmatrix},$$

where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2q}[x]$ such that $a(x)(1 - a(x)) - b(x)c(x) = qf(x)$. This matrix is the 3^{rd} non-trivial idempotent matrix form.
Third, if trace$(A) = q^{p(p-1)}$. Similarly to the cases above, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} q^{p(p-1)}a(x) & q^{p(p-1)}b(x) \\ q^{p(p-1)}c(x) & q^{p(p-1)}(1 - a(x)) \end{bmatrix}.$$

Since A is an idempotent, then $q^{p(p-1)}a(x) = a(x),\ q^{p(p-1)}b(x) = b(x),\ q^{p(p-1)}c(x) = c(x)$. Since det$(A) = 0$, then we obtained

$$a(x)(1 - a(x)) - b(x)c(x) = p^2g(x),$$

where $g(x) \in \mathbb{Z}_{p^2q}[x]$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} q^{p(p-1)}a(x) & q^{p(p-1)}b(x) \\ q^{p(p-1)}c(x) & q^{p(p-1)}(1 - a(x)) \end{bmatrix},$$

where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2q}[x]$ such that $a(x)(1-a(x)) - b(x)c(x) = p^2g(x)$. This matrix is the 4^{th} non-trivial idempotent matrix form.

2. Case det$(A) = p^{k(q-1)}$.
First, if trace$(A) = p^{k(q-1)} + 1$. Similarly to the case 1, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} p^{k(q-1)}a(x) + a(x) - p^{k(q-1)} & (p^{k(q-1)}+1)b(x) \\ (p^{k(q-1)}+1)c(x) & 1 + 2p^{k(q-1)} - (p^{k(q-1)}+1)a(x) \end{bmatrix}.$$

Since A is an idempotent, then $p^{k(q-1)}(a(x)-1) = p^{k(q-1)}b(x) = p^{k(q-1)}c(x) = 0$. Hence, we obtained $a(x) = 1 + qa(x), b(x) = qb(x), c(x) = qc(x)$. Since det$(A) = p^{k(q-1)}$, then we obtained

$$a(x)(1 + qa(x)) + qb(x)c(x) = p^2h(x),$$

where $h(x) \in \mathbb{Z}_{p^2q}[x]$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} 1 + qa(x) & qb(x) \\ qc(x) & p^{k(q-1)} - qa(x) \end{bmatrix},$$

where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2q}[x]$ such that $a(x)(1 + qa(x)) + qb(x)\,c(x) = p^2h(x)$. This matrix is the 5^{th} non-trivial idempotent matrix form.
Second, if trace$(A) = 2p^{k(q-1)}$. Similarly to the case above, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} 2p^{k(q-1)}a(x) - p^{k(q-1)} & 2p^{k(q-1)}b(x) \\ 2p^{k(q-1)}c(x) & 3p^{k(q-1)} - 2p^{k(q-1)}a(x) \end{bmatrix}.$$

Since A is an idempotent, then $(2p^{k(q-1)} - 1)b(x) = (2p^{k(q-1)} - 1)c(x) = 0$. Since $p^{k(q-1)}$ is an idempotent, then $2p^{k(q-1)} - 1$ is a unit. Hence, we obtained $b(x) = c(x) = 0$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} a(x) & 0 \\ 0 & 2p^{k(q-1)} - a(x) \end{bmatrix}.$$

Since A is an idempotent, then $a(x)$ and $2p^{k(q-1)} - a(x)$ are also idempotent elements. Since $a(x)$ is an idempotent elements, then $a(x)$ is $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. Furthermore, we obtained $2p^{k(q-1)} - a(x)$ is an idempotent element for $a(x) = p^{k(q-1)}$. Hence, we obtained a matrix A is

$$A = \begin{bmatrix} p^{k(q-1)} & 0 \\ 0 & p^{k(q-1)} \end{bmatrix}.$$

This matrix is the 1^{st} non-trivial idempotent matrix form.

3. Case det$(A) = q^{p(p-1)}$.

First, if trace(A) $= q^{p(p-1)} + 1$. Similarly to the case 2, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} q^{p(p-1)}a(x) + a(x) - q^{p(p-1)} & (q^{p(p-1)} + 1)b(x) \\ (q^{p(p-1)} + 1)c(x) & 1 + 2q^{p(p-1)} - (q^{p(p-1)} + 1)a(x) \end{bmatrix}.$$

Since A is an idempotent, then $q^{p(p-1)}(a(x) - 1) = q^{p(p-1)}b(x) = q^{p(p-1)}c(x) = 0$. Hence, we obtained $a(x) = 1 + p^2a(x), b(x) = p^2b(x), c(x) = p^2c(x)$. Since det($A$) $= q^{p(p-1)}$, then we obtained

$$a(x)(1 + p^2a(x)) + p^2b(x)c(x) = q\phi(x),$$

where $\phi(x) \in \mathbb{Z}_{p^2q}[x]$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} 1 + p^2a(x) & p^2b(x) \\ p^2c(x) & p^{k(q-1)} - p^2a(x) \end{bmatrix},$$

where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2q}[x]$ such that $a(x)(1 + p^2a(x)) + p^2b(x)c(x) = q\phi(x)$. This matrix is the 6^{th} non-trivial idempotent matrix form.
Second, if trace(A) $= 2q^{p(p-1)}$. Similarly to the case 2, we obtained a matrix A^2 is

$$A^2 = \begin{bmatrix} 2q^{p(p-1)}a(x) - q^{p(p-1)} & 2q^{p(p-1)}b(x) \\ 2q^{p(p-1)}c(x) & 3q^{p(p-1)} - 2q^{p(p-1)}a(x) \end{bmatrix}.$$

Since A is an idempotent, then $(2q^{p(p-1)} - 1)b(x) = (2q^{p(p-1)} - 1)c(x) = 0$. Since $q^{p(p-1)}$ is an idempotent, then $2q^{p(p-1)} - 1$ is a unit. Hence, we obtained $b(x) = c(x) = 0$. Furthermore, we obtained a matrix A is

$$A = \begin{bmatrix} a(x) & 0 \\ 0 & 2q^{p(p-1)} - a(x) \end{bmatrix}.$$

Since A is an idempotent, then $a(x)$ and $2q^{p(p-1)} - a(x)$ are also idempotent elements. Since $a(x)$ is an idempotent, then $a(x)$ is $0, 1, p^{k(q-1)}$, or $q^{p(p-1)}$. Furthermore, we obtained $2q^{p(p-1)} - a(x)$ is an idempotent element for $a(x) = q^{p(p-1)}$. Hence, we obtained a matrix A is

$$A = \begin{bmatrix} q^{p(p-1)} & 0 \\ 0 & q^{p(p-1)} \end{bmatrix}.$$

This matrix is the 1^{st} non-trivial idempotent matrix form.

□

III. CONCLUSIONS

Idempotent elements in ring $\mathbb{Z}_{p^2q}$ are 4 elements, i.e. $0, 1, p^{k(q-1)}$, and $q^{p(p-1)}$. Furthermore, the idempotent elements in the polynomial ring $\mathbb{Z}_{p^2q}[x]$ coincides with the ring $\mathbb{Z}_{p^2q}(E(\mathbb{Z}_{p^2q}[x] = E(\mathbb{Z}_{p^2q}))$. Moreover, there are 7 non-trivial idempotent matrix forms in $M_2(\mathbb{Z}_{p^2q}[x])$.

REFERENCES

[1] Malik D. S., J. N. Mordeson and M. K. Son, *Fundamentals of Abstract Algebra*. International Edition. United States of America: The McGraw-Hill Publishing Company, 1997.

[2] Herstein, I. N, *Topics in Algebra*. 2nd Edition, New York: John Wiley and Sons, 1975.

[3] Malman, Bartosz, "Zero-Divisors and Indempotents In Group Rings" [Master's Thesis, Lund University], Centrum Scientarium Mathematicarum, 2014.

[4] Thomas Q. Sibley, "Idempotents á La Mod", *The College Mathematics Journal*, vol. 43, no. 5, pp. 401–404, 2012.

[5] K. R. Goodearl, *Von Neumann Regular Rings*. Second edition, Malabar: Robert E. Krieger Publishing Co., Inc., 1991.

[6] Nicholson, W. Keith, "Lifting Idempotents and Exchange Rings", *Trans. Amer. Math. Soc.*, vol. 229, pp. 269-278, 1977.

[7] Nicholson, W. Keith, "Strongly Clean Rings and Fitting's Lemma", *Communications in Algebra*. vol. 27(8), pp. 3583-3592, 1999.

[8] Kanwar, P., A. Leroy, and J. Matczuk, "Clean Elements in Polynomial Rings", *Noncommutative Rings and their Applications, Contemp. Math., Amer. Math. Soc*. pp: 197-204, 2015.

[9] R. K. Sharma, Pooja Yadav, and P. Kanwar, "Lie Regular Generators of General Linear Groups", *Communications in Algebra*. vol 40, pp. 1304-1315, 2012.

[10] Kanwar, P., A. Leroy and J. Matczuk, "Idempotents in Ring Extensions", *Journal of Algebra*, vol. 389, pp. 128-136, 2013.

[11] Kanwar, P., M. Khatkar and R. K. Sharma, "Idempotents and Units of Matrix Rings Over Polynomial Rings", *International Electronic Journal of Algebra*, vol. 22, pp. 147-169, 2017.

[12] Jose Maria, P. Balmaceda, and Joanne Pauline P. Datu, "Idempotents In Certain Matrix Rings Over Polynomial Rings", *International Electronic Journal of Algebra*, vol. 27, pp. 1-12, 2020.

[13] C. Ding, D. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography.* Singapore: World Scientific Publishing Co. Pte. Ltd, 1996.

[14] Koshy Thomas, *Elementary Number Theory with Applications*. 2nd Edition. United Kingdom: Acedemic Press of Elsevier, 2007.

[15] Burton, David M, *Elementary Number Theory*. 6th Edition. New Delhi: Tata McGraw-Hill Publishing Company Limited, 2007.