International Electronic Journal of Algebra
Volume 27 (2020) 1-12
DOI: 10.24330/ieja.662942

IDEMPOTENTS IN CERTAIN MATRIX RINGS OVER POLYNOMIAL RINGS

Jose Maria P. Balmaceda and Joanne Pauline P. Datu

Received: 4 June 2018; Revised: 12 August 2019; Accepted: 5 October 2019
Communicated by Abdullah Harmancı

Abstract. We determine the forms of the nontrivial idempotents in the ring of 2×2 matrices over the polynomial rings $\mathbb{Z}_{pq}[x]$ and $\mathbb{Z}_{p^2}[x]$, where p and q are any primes. Any such idempotent in the stated rings will be of a form in our list. Our work generalizes the results of Kanwar, Khatkar and Sharma (2017) who identified the forms of idempotents in $M_2(\mathbb{Z}_{2p}[x])$ and $M_2(\mathbb{Z}_{3p}[x])$.

Mathematics Subject Classification (2010): 16S50, 13F20, 13B25
Keywords: Idempotent, matrix ring, polynomial ring

1. Introduction

An element e in a ring R is an idempotent if $e^2 = e$. In a ring with unity, the elements 0 and 1 are idempotents, called trivial idempotents. Integral domains contain only the trivial idempotents. Idempotents other than 0 and 1 are called non-trivial idempotents. Idempotents are important particularly in decompositions of a ring and its modules.

In recent years, certain aspects of idempotents and units and their connections have become of interest to ring theorists (see [1], [6], [8]). In some rings, elements are characterized by the behavior of the units. For example, an (S, k)-ring is a ring in which each element is the sum of k units [3]. Then there exist ring elements that are characterized by both idempotents and units at the same time. For example, clean rings are rings where every element is uniquely the sum of an idempotent and a unit. The article [9] gives a survey on recent results on additive representations of ring elements. In this regard, it will be useful to have a good knowledge of rings with idempotents. A good source would be matrix rings.

Kanwar, Khatkar and Sharma [5] studied idempotents and units in certain matrix rings over polynomial rings. Forms of idempotents in $M_2\left(\mathbb{Z}_{2p}[x]\right)$ for any odd prime p and in $M_2\left(\mathbb{Z}_{3p}[x]\right)$ for any prime greater than 3 were identified as well as the form of units in $M_2\left(\mathbb{Z}_2[x]\right)$ and $M_2\left(\mathbb{Z}_3[x]\right)$.

Motivated by the current interest in idempotents and units in rings, we extend the results of Kanwar et. al. [5]. We generalize the paper's results to the ring of 2×2 matrices $M_2(\mathbb{Z}_{pq}[x])$, over the polynomial ring $\mathbb{Z}_{pq}[x]$ where p and q are distinct primes, and the ring $M_2\left(\mathbb{Z}_{p^2}[x]\right)$ where p is prime.

2. Preliminaries

In this section we gather some definitions, notations and results that will be useful in our study. Basic number theory and concepts on rings, matrices, and polynomials are assumed and can be found in standard references such as [2], [4] and [7]. Euler's generalization of Fermat's Little Theorem and the Chinese Remainder Theorem will be invoked in several proofs.

We will denote the ring of $n \times n$ matrices over a ring R by $M_n(R)$. For a ring R, $E(R)$ denotes the set of all idempotents in R.

The following results from [5] and [6] will be useful.

Proposition 2.1. [5] *Let R be any ring with unity and $a = \sum_{i=0}^{n} a_i x^i$ be an element in $R[x]$ such that $a^2 - a \in R$. If any of the following conditions hold:*

(1) *R has no non-zero nilpotent elements,*
(2) *$a_0 a_i = a_i a_0$ for $1 \leq i \leq n$ and $2a_0 - 1$ is a unit in R,*

then $a \in R$.

Remark. A ring with no non-zero nilpotent elements is called a reduced ring. Equivalently, a ring is reduced if it has no non-zero elements with square zero, that is, $x^2 = 0$ implies $x = 0$. The ring $\mathbb{Z}_n$ is reduced if and only if n is a square-free integer [4]. This is seen by solving the quadratic congruence $x^2 \equiv 0 \ (mod\ n)$ via the Chinese Remainder Theorem.

Corollary 2.2. [6] *If R is a ring all of whose idempotents are in the center of R, then $E(R[x]) = E(R)$.*

Corollary 2.3. [5] *If R is a ring with no non-zero nilpotent elements, then $E(R[x]) = E(R)$.*

Proposition 2.4. [5] *Let R be a commutative ring with only 0 and 1 as its idempotents. Then the trace of every non-trivial idempotent in $M_2(R)$ is 1.*

3. Idempotents in $M_2(\mathbb{Z}_{pq}[x])$

Our main results, given by Theorems 3.9 and 3.10, will be presented in this section. We obtain a complete list of the forms of non-trivial idempotents in $M_2(\mathbb{Z}_{pq}[x])$ where p, q are primes such that $p > q$ as well as the case where $p = q$.

We continue to gather relevant results for completeness.

Proposition 3.1. [5] *If p is a prime and n is a positive integer, the only idempotents of $\mathbb{Z}_{p^n}$ are 0 and 1.*

Corollary 3.2. [5] *Let $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ be the complete prime factorization of the positive integer n. Then $\mathbb{Z}_n$ has 2^m idempotents.*

In the next proposition we give the four idempotents in $\mathbb{Z}_{pq}$, for p and q distinct primes.

Proposition 3.3. [5] *Let p and q be distinct primes. Then the idempotents in $\mathbb{Z}_{pq}$ are 0, 1, p^{q-1} and q^{p-1}.*

The next result shows that if R is a commutative ring, the idempotents in $R[x]$ are precisely the idempotents in R.

Proposition 3.4. [6] *Let R be a commutative ring and $f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. Then f is an idempotent in $R[x]$ if and only if the constant term of f is an idempotent in R and all other coefficients of f are zero.*

We next consider the idempotents in the ring $M_2(R)$ of 2×2 matrices over a commutative ring R. Denote by $\det A$, the determinant of a matrix A. The following is an easy but useful result.

Proposition 3.5. *Let R be a commutative ring and A an idempotent in $M_n(R)$. Then the determinant of A is an idempotent in R.*

Proof. Let A be an idempotent in $M_n(R)$. Since $A = A^2$, we have $\det A = \det A^2 = (\det A)^2$, and hence the determinant of A is an idempotent in R. □

Proposition 3.6. [5] *Let R be a commutative ring and A a nontrivial idempotent in $M_2(R)$. If $\det A = 0$, then the trace of A is an idempotent in R.*

Remark. If R is a commutative ring, then the ring of polynomials $R[x]$ is also commutative. Thus Propositions 3.5 and 3.6 hold for all idempotents in $M_2(R[x])$ as well.

Proposition 3.7. [5] *If R is a commutative ring with no non-zero nilpotent elements then the determinant as well as the trace of every idempotent in $M_2(R[x])$ is in R.*

Remark. The above proposition is applied to the ring $M_2(\mathbb{Z}_{pq}[x])$ where p and q are distinct primes, since $\mathbb{Z}_{pq}$ is a reduced ring.

Clearly, the trivial idempotents in $M_2(\mathbb{Z}_{pq}[x])$ where p and q are primes are the zero matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Now, we give the forms of non-trivial idempotents in $M_2(\mathbb{Z}_{pq}[x])$ where p and q are distinct primes.

We now give necessary conditions for non-trivial idempotents in $M_2(\mathbb{Z}_{pq}[x])$.

Theorem 3.8. *For any distinct primes p and q such that $p > q$ and any non-trivial idempotent A in $M_2(\mathbb{Z}_{pq}[x])$ one of the following holds:*

1. *determinant of A is 0 and trace of A is either 1 or p^{q-1} or q^{p-1},*
2. *determinant of A is q^{p-1} and trace of A is either $q^{p-1}+1$ or $2q^{p-1}$,*
3. *determinant of A is p^{q-1} and trace of A is either $2p^{q-1}$ or $p^{q-1}+1$.*

Proof. Let p and q be distinct primes with $p > q$. Then the idempotents in $\mathbb{Z}_{pq}$ are $0, 1, p^{q-1}, q^{p-1}$ *mod* pq. Now, let $A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix}$ be a non-trivial idempotent of $M_2(\mathbb{Z}_{pq}[x])$. As before, write a, b, c and d for $a(x), b(x), c(x)$ and $d(x)$ respectively, so we have

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\; ; \; A^2 = \begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix}.$$

Since A is an idempotent we have $a = a^2 + bc$, $b = ab + bd$, $c = ac + cd$ and $d = bc + d^2$. From Proposition 3.5, $\det A$ is an idempotent in $\mathbb{Z}_{pq}[x]$, and hence, an idempotent in $\mathbb{Z}_{pq}$. By Proposition 3.3, $\det A$ is either 0 or 1 or p^{q-1} or q^{p-1} *mod* pq. Suppose that $\det A = 1$. Then A is a unit. Multiplying both sides of $A^2 = A$ by A^{-1}, we obtain $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is a trivial idempotent in $M_2(\mathbb{Z}_{pq}[x])$. This is a contradiction, since we assumed A is a non-trivial idempotent. Hence, the determinant of A is either 0 or p^{q-1} or q^{p-1} modulo pq. We now consider each of these possibilities. Since Proposition 3.7 holds for $M_2(\mathbb{Z}_{pq})$, as $\mathbb{Z}_{pq}$ is a reduced ring, the trace of A is in $\mathbb{Z}_{pq}$ i.e. $a + d \in \mathbb{Z}_{pq}$.

Case (1) Determinant of A is 0.

From Proposition 3.6, $a + d$ is an idempotent in $\mathbb{Z}_{pq}[x]$, so we have $a + d = 0$ or 1 or p^{q-1} or q^{p-1} *mod* pq. If $a + d = 0$, then $d = -a$. Now, since $ad - bc = 0$, this

implies that $a^2+bc=0$ and $bc+d^2=0$. So, $A^2=\begin{bmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{bmatrix}=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Thus, A is the zero matrix in $M_2(\mathbb{Z}_{pq}[x])$, which is a contradiction, since A is a non-trivial idempotent.

Note that the matrices $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} p^{q-1} & 0 \\ 0 & 0 \end{bmatrix}$, and $\begin{bmatrix} q^{p-1} & 0 \\ 0 & 0 \end{bmatrix}$ in $M_2(\mathbb{Z}_{pq}[x])$ have determinant 0 and traces 1, p^{q-1} and q^{p-1} respectively.

Case (2) Determinant of A is q^{p-1}.

The equations $a^2+bc=a$ and $bc+d^2=d$ imply $a^2=a-bc$ and $d^2=d-bc$ respectively. From this, we have $(a+d)^2=a^2+2ad+d^2=a-bc+2ad+d-bc=a+d+2(ad-bc)=a+d+2q^{p-1}(mod\ pq)$. We solve the values of $a+d\in\mathbb{Z}_{pq}$ that satisfies this equation. We let $x=a+d$ and solve for the values of x that satisfy the quadratic equation $x^2-x-2q^{p-1}\equiv 0(mod\ pq)$. From this, we have:

$$x^2-x-2q^{p-1}\equiv 0(mod\ p) \tag{1}$$

$$x^2-x-2q^{p-1}\equiv 0(mod\ q) \tag{2}$$

From Euler's Theorem, since $\gcd(p,q)=1$, (1) can be written as $x^2-x-2\equiv 0(mod\ p)$. Hence, $x\equiv 2(mod\ p)$ or $x\equiv -1(mod\ p)$. Also (2) can be written as $x^2\equiv x(mod\ q)$. So we have $x\equiv 0(mod\ q)$ or $x\equiv 1(mod\ q)$. Now, if $x\equiv 2(mod\ p)$ and $x\equiv 0(mod\ q)$ then by Chinese Remainder Theorem and Euler's Theorem [2] with $\gcd(p,q)=1$ we have $x\equiv 2q^{p-1}(mod\ pq)$. Similar computations hold for the next cases. If $x\equiv 2(mod\ p)$ and $x\equiv 1(mod\ q)$ then $x\equiv 2q^{p-1}+p^{q-1}\equiv q^{p-1}+1(mod\ pq)$, since $q^{p-1}+p^{q-1}\equiv 1\ (mod\ pq)$. If $x\equiv -1(mod\ p)$ and $x\equiv 0(mod\ q)$ then $x\equiv -q^{p-1}(mod\ pq)$. Lastly, if $x\equiv -1(mod\ p)$ and $x\equiv 1(mod\ q)$ then $x\equiv -q^{p-1}+p^{q-1}\equiv 1-2q^{p-1}(mod\ pq)$. Hence, the possible values of $a+d\in\mathbb{Z}_{pq}$ that satisfy the equation $(a+d)^2\equiv a+d+2q^{p-1}(mod\ pq)$ are $2q^{p-1}$ or $q^{p-1}+1$ or $-q^{p-1}$ or $1-2q^{p-1}$.

For $p=3$, observe that the cases where $a+d=-q^{p-1}$ and $a+d=1-2q^{p-1}$ coincide with the cases $2q^{p-1}$ and $q^{p-1}+1$ respectively. So for $p\neq 3$, we claim that the cases $a+d=-q^{p-1}$ and $a+d=1-2q^{p-1}$ are not possible traces for an idempotent matrix A with determinant q^{p-1}.

If $a+d=-q^{p-1}$ then $d=-q^{p-1}-a$ with $ad-bc=q^{p-1}$, we get $a^2+bc=a^2+ad-q^{p-1}=a^2+a(-q^{p-1}-a)-q^{p-1}=a^2-q^{p-1}a-a^2-q^{p-1}=-q^{p-1}a-q^{p-1}$; $ab+bd=b(a+d)=-q^{p-1}b$; $ac+cd=c(a+d)=-q^{p-1}c$; and $bc+d^2=ad-q^{p-1}+d^2=(-q^{p-1}-d)d-q^{p-1}+d^2=-q^{p-1}d-d^2-q^{p-1}+d^2=-q^{p-1}(d+1)=-q^{p-1}(-q^{p-1}-a+1)=q^{2(p-1)}+q^{p-1}a-q^{p-1}=q^{p-1}a$. Since A is an idempotent, we have $b=-q^{p-1}b$. It follows that $b(1+q^{p-1})=0$. Similarly, from $c=-q^{p-1}c$,

we get $c(1+q^{p-1})=0$. Since $\gcd(q^{p-1}+1, qp)=1$, $b=c=0$. Thus, we have $A=\begin{bmatrix} a & 0 \\ 0 & -q^{p-1}-a \end{bmatrix}$. Since A is an idempotent, a and $-q^{p-1}-a$ must be idempotents in $\mathbb{Z}_{pq}$. For $a=0$, we have $\left(-q^{p-1}\right)^2 = q^{p-1}$. For $a=1$, we get $\left(-q^{p-1}-1\right)^2 = q^{p-1}+2q^{p-1}+1 \equiv 3q^{p-1}+1 \ (mod\ pq)$. For $a=p^{q-1}$, we have $\left(-q^{p-1}-p^{q-1}\right)^2 = q^{p-1}+2q^{p-1}p^{q-1}+p^{q-1}$. Lastly, for $a=q^{p-1}$ we have $\left(-q^{p-1}-q^{p-1}\right)^2 = \left(-2q^{p-1}\right)^2 = 4q^{p-1}$. Notice that $-q^{p-1}-a$ is not an idempotent for $a=0,1,p^{q-1}$ and q^{p-1}. We have a contradiction. So $a+d=-q^{p-1}$ is not a possible trace for an idempotent matrix A with determinant q^{p-1}.

If $a+d=1-2q^{p-1}$ then $d=1-2q^{p-1}-a$. Now, $ab+bd=b(a+d)=(1-2q^{p-1})b$ and $ac+cd=c(a+d)=(1-2q^{p-1})c$. So $A^2=\begin{bmatrix} a^2+bc & (1-2q^{p-1})b \\ (1-2q^{p-1})c & bc+d^2 \end{bmatrix}$. Since A is an idempotent, we have $b(1-2q^{p-1})=b$ which gives us $2bq^{p-1}=0$. Similarly, from $c(1-2q^{p-1})=c$ we have $2cq^{p-1}=0$. Lastly, $ad-bc=q^{p-1}$ implies $a(1-2q^{p-1}-a)-bc=q^{p-1}$. So, $a-2aq^{p-1}-a^2-bc=q^{p-1}$. Since $a^2+bc=a$, we are left with $-q^{p-1}=2aq^{p-1}$. From $a^2+bc=a$, $2bq^{p-1}=0$ and $2cq^{p-1}=0$, we have $(2q^{p-1}a)^2-2(2q^{p-1}a)=0$. Substituting the value of $2aq^{p-1}$ that we just obtained, we have $(-q^{p-1})^2-2(-q^{p-1})=0$. This implies that $q^{p-1}+2q^{p-1}=0$. Hence $3q^{p-1}\equiv 0 \pmod{pq}$, which gives $3q^{p-1}\equiv 0 \pmod{p}$. This is contradiction since p is a prime distinct from 3 and q. So the case where $a+d=1-2q^{p-1}$ is not possible for an idempotent matrix A with determinant q^{p-1}.

Note that the matrices $\begin{bmatrix} q^{p-1} & 0 \\ 0 & q^{p-1} \end{bmatrix}$ and $\begin{bmatrix} q^{p-1} & 0 \\ 0 & 1 \end{bmatrix}$ in $M_2\left(\mathbb{Z}_{pq}[x]\right)$ have determinant q^{p-1} and traces $2q^{p-1}$ and $q^{p-1}+1$ respectively.

Case (3) Determinant of A is p^{q-1}.

As in the previous case, since A is idempotent, we have $(a+d)^2 = a+d+2(ad-bc) = a+d+2p^{q-1} \pmod{pq}$. By performing a similar computation as in Case (2), we see that the possible values of $a+d\in\mathbb{Z}_{pq}$ are $2p^{q-1}$, $p^{q-1}+1$, $-p^{q-1}$ or $1-2p^{q-1}$. We claim that $-p^{q-1}$ and $1-2p^{q-1}$ are not possible traces for an idempotent matrix A with determinant p^{q-1}. In the case where $q=2$, the proof follows from Case 2 in [5, p. 154] . For $q\neq 2$, we apply the same argument that was used in Case (2) by interchanging the roles of p and q with p still greater than q.

To construct a matrix A with determinant p^{q-1} and trace $2p^{q-1}$ or $p^{q-1}+1$, we consider the least positive residue k of p modulo q. So $p\equiv k \pmod{q}$ with $0<k<q$. Then $p^2\equiv pk \pmod{pq}$. Thus,

$$p^{q-1}\equiv p^{q-3}k^2\equiv \ldots \equiv p^2k^{q-3}\equiv pk^{q-2} \pmod{pq}.$$

So $a+d = 2pk^{q-2}$ or $pk^{q-2}+1$ in $\mathbb{Z}_{pq}$. Clearly, the matrix $\begin{bmatrix} pk^{q-2} & 0 \\ 0 & 1 \end{bmatrix}$ has determinant $pk^{q-2} \equiv p^{q-1} \pmod{pq}$ and trace $pk^{q-2}+1 \equiv p^{q-1}+1 \pmod{pq}$. Moreover the matrix $\begin{bmatrix} pk^{q-2} & 0 \\ 0 & pk^{q-2} \end{bmatrix}$ has determinant $(pk^{q-2})^2 \equiv (p^{q-1})^2 \equiv p^{q-1} \pmod{pq}$ and trace $2pk^{q-2} \equiv 2p^{q-1} \pmod{pq}$. □

We are now ready to state and prove the main result of this paper. The following theorem gives the forms of all non-trivial idempotents in $M_2(\mathbb{Z}_{pq}[x])$. Any such idempotent will be of a form in the list. Moreover, any such matrix in the list gives a non-trivial idempotent of $M_2(\mathbb{Z}_{pq}[x])$.

Theorem 3.9. *For any 2 distinct primes p and q such that $p > q$, any non-trivial idempotent in $M_2(\mathbb{Z}_{pq}[x])$ is one of the following forms:*

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

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

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

(5) $\begin{bmatrix} 1+pa(x) & pb(x) \\ pc(x) & q^{p-1}-pa(x) \end{bmatrix}$, *where* $a(x)\{1+pa(x)\} + pb(x)c(x) = qh(x)$,

(6) $\begin{bmatrix} 1+qa(x) & qb(x) \\ qc(x) & p^{q-1}-qa(x) \end{bmatrix}$, *where* $a(x)\{1+qa(x)\} + qb(x)c(x) = p\phi(x)$,

where $a(x), b(x), c(x), f(x), g(x), h(x), \phi(x) \in \mathbb{Z}_{pq}[x]$ not necessarily non-zero.

Proof. It can be checked that the matrices in (1)-(6) with the given conditions are idempotents in $M_2(\mathbb{Z}_{pq}[x])$. Now, we prove that every non-trivial idempotent in $M_2(\mathbb{Z}_{pq}[x])$ is one of the following stated forms. Now, let $A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix}$ be a non-trivial idempotent in $M_2(\mathbb{Z}_{pq}[x])$. From Theorem 3.8 one of the following holds:

(1) determinant of A is 0 and trace of A is either 1 or p^{q-1} or q^{p-1},
(2) determinant of A is q^{p-1} and trace of A is either $q^{p-1}+1$ or $2q^{p-1}$,
(3) determinant of A is p^{q-1} and trace of A is either $2p^{q-1}$ or $p^{q-1}+1$.

We examine each case separately.

Case (1) Determinant of A is 0.

In this case, the trace of A is either 1 or p^{q-1} or q^{p-1}.

If $a+d=1$ then $d=1-a$ and $ad-bc=0$ give the following: $a^2+bc=a$; $ab+bd=b(a+d)=b$; $ac+cd=c(a+d)=c$ and $bc+d^2=ad+d^2=a(1-a)+(1-a)^2=a-a^2+1-2a+a^2=1-a$. Thus, $A^2=\begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$. It follows that $A=\begin{bmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{bmatrix}$ where $a(x),b(x),c(x)\in\mathbb{Z}_{pq}[x]$ such that $a(x)(1-a(x))=b(x)c(x)$.

If $a+d=p^{q-1}$ then $d=p^{q-1}-a$ and $ad=bc$ give the following: $a^2+bc=a^2+ad=a^2+a(p^{q-1}-a)=a^2+ap^{q-1}-a^2=ap^{q-1}$; $ab+bd=b(a+d)=bp^{q-1}$; $ac+cd=c(a+d)=cp^{q-1}$ and $bc+d^2=ad+(p^{q-1}-a)^2=a(p^{q-1}-a)+(p^{q-1}-a)^2=p^{q-1}(1-a)$. Thus, $A^2=\begin{bmatrix} p^{q-1}a & p^{q-1}b \\ p^{q-1}c & p^{q-1}(1-a) \end{bmatrix}$. Since A is an idempotent, we have $p^{q-1}a=a$, $p^{q-1}b=b$ and $p^{q-1}c=c$ which imply $a(p^{q-1}-1)=0$, $b(p^{q-1}-1)=0$ and $c(p^{q-1}-1)=0$ respectively. Since p^{q-1} is an idempotent in $\mathbb{Z}_{pq}$, it follows that $a=p^{q-1}a'(x)$, $b=p^{q-1}b'(x)$ and $c=p^{q-1}c'(x)$ where $a'(x),b'(x),c'(x)$ are polynomials in $\mathbb{Z}_{pq}[x]$. Since $ad-bc=0$, $p^{q-1}a'(x)(1-a'(x))=p^{q-1}b'(x)c'(x)$ or equivalently $a'(x)(1-a'(x))-b'(x)c'(x)=qf(x)$ for some $f(x)\in\mathbb{Z}_{pq}[x]$. Thus, $A=\begin{bmatrix} p^{q-1}a(x) & p^{q-1}b(x) \\ p^{q-1}c(x) & p^{q-1}(1-a(x)) \end{bmatrix}$, where $a(x),b(x),c(x)\in\mathbb{Z}_{pq}[x]$ such that $a(x)(1-a(x))-b(x)c(x)=qf(x)$ for some $f(x)\in\mathbb{Z}_{pq}[x]$.

If $a+d=q^{p-1}$ then $d=q^{p-1}-a$ and $ad-bc=0$ give the following: $a^2+bc=a^2+ad=a^2+a(q^{p-1}-a)=aq^{p-1}$; $ab+bd=b(a+d)=bq^{p-1}$; $ac+cd=c(a+d)=cq^{p-1}$ and $bc+d^2=ad+d^2=a(q^{p-1}-a)+(q^{p-1}-a)^2=q^{p-1}(1-a)$. Thus, $A^2=\begin{bmatrix} q^{p-1}a & q^{p-1}b \\ q^{p-1}c & q^{p-1}(1-a) \end{bmatrix}$. Since A is an idempotent, we have $q^{p-1}a=a$, $q^{p-1}b=b$ and $q^{p-1}c=c$ which imply $a(q^{p-1}-1)=0$, $b(q^{p-1}-1)=0$ and $c(q^{p-1}-1)=0$ respectively. From our previous case, it follows that $A=\begin{bmatrix} q^{p-1}a(x) & q^{p-1}b(x) \\ q^{p-1}c(x) & q^{p-1}(1-a(x)) \end{bmatrix}$ where $a(x),b(x),c(x)\in\mathbb{Z}_{pq}[x]$ such that $a(x)(1-a(x))-b(x)c(x)=pg(x)$ for some $g(x)\in\mathbb{Z}_{pq}[x]$.

Case (2) Determinant of A is q^{p-1}.

In this case, the trace of A is either $q^{p-1}+1$ or $2q^{p-1}$.

If $a+d=2q^{p-1}$ then $d=2q^{p-1}-a$ and $ad-bc=q^{p-1}$ give the following: $a^2+bc=a^2+ad-q^{p-1}=a^2+a(2q^{p-1}-a)-q^{p-1}=2aq^{p-1}-q^{p-1}$; $ab+bd=$

$b(a+d) = 2q^{p-1}b$; $ac+cd = c(a+d) = 2q^{p-1}c$ and $bc+d^2 = ad - q^{p-1} + (2q^{p-1}-a)^2 = a(2q^{p-1}-a) - q^{p-1} + (2q^{p-1}-a)^2 = 3q^{p-1} - 2q^{p-1}a$. Thus, $A^2 = \begin{bmatrix} 2aq^{p-1} - q^{p-1} & 2q^{p-1}b \\ 2q^{p-1}c & 3q^{p-1} - 2q^{p-1}a \end{bmatrix}$. Since A is an idempotent, we have $2q^{p-1}b = b$ and $2q^{p-1}c = c$ which imply $b(2q^{p-1}-1) = 0$ and $c(2q^{p-1}-1) = 0$ respectively. Since q^{p-1} is an idempotent in $\mathbb{Z}_{pq}$, $2q^{p-1}-1$ is a unit. It follows that $b = c = 0$. So we have, $A = \begin{bmatrix} a & 0 \\ 0 & 2q^{p-1}-a \end{bmatrix}$. Both a and $2q^{p-1}-a$ must be idempotents in $\mathbb{Z}_{pq}[x]$ since A is an idempotent. Observe that $2q^{p-1}-a$ is an idempotent only for $a = q^{p-1}$. Thus, $A = \begin{bmatrix} q^{p-1} & 0 \\ 0 & q^{p-1} \end{bmatrix}$.

If $a+d = q^{p-1}+1$ then $d = q^{p-1}+1-a$ and $ad-bc = q^{p-1}$ give the following: $a^2+bc = a^2+ad-q^{p-1} = a^2+a(q^{p-1}+1-a) - q^{p-1} = aq^{p-1}+a-q^{p-1}$; $ab+bd = b(a+d) = b(q^{p-1}+1)$; $ac+cd = c(a+d) = c(q^{p-1}+1)$ and $bc+d^2 = ad-q^{p-1}+d^2 = a(q^{p-1}+1-a)-q^{p-1}+(q^{p-1}+1-a)^2 = 2q^{p-1}+1-a(q^{p-1}+1)$. Thus, $A^2 = \begin{bmatrix} aq^{p-1}+a-q^{p-1} & b(q^{p-1}+1) \\ c(q^{p-1}+1) & 2q^{p-1}+1-a(q^{p-1}+1) \end{bmatrix}$. Since A is an idempotent, we get $q^{p-1}a = q^{p-1}$, $bq^{p-1} = 0$ and $cq^{p-1} = 0$. Thus $A = \begin{bmatrix} 1+pa(x) & pb(x) \\ pc(x) & q^{p-1}-pa(x) \end{bmatrix}$ where $a(x), b(x), c(x) \in \mathbb{Z}_{pq}[x]$ such that $a(x)\{1+pa(x)\} + pb(x)c(x) = qh(x)$ for some $h(x) \in \mathbb{Z}_{pq}[x]$.

Case (3) Determinant of A is p^{q-1}.

In this case, the trace of A is either $2p^{q-1}$ or $p^{q-1}+1$.

Consider the least positive residue k of p modulo q. So $p \equiv k \pmod q$ with $0 < k < q$. Then $p^2 \equiv pk \pmod{pq}$, so that $p^{q-1} \equiv k^{q-2}p \pmod{pq}$. Then the trace $a+d$ of A is either $2p^{q-1} \equiv 2k^{q-2}p \pmod{pq}$ or $p^{q-1}+1 \equiv k^{q-2}p+1 \pmod{pq}$.

Suppose $a+d = 2k^{q-2}p$, so that $d = 2k^{q-2}p - a$. Along with $ad-bc = p^{q-1}$, we obtain the following:

$$\begin{aligned} a^2+bc &= a^2+ad-p^{q-1} = a(a+d) - p^{q-1} \\ &= 2ak^{q-2}p - 2k^{q-2}p = 2k^{q-2}p(a-1); \\ ab+bd &= b(a+d) = 2k^{q-2}pb; \\ ac+cd &= c(a+d) = 2k^{q-2}pc; \text{ and} \\ bc+d^2 &= ad-p^{q-1}+d^2 = d(a+d) - k^{q-2}p \\ &= (2k^{q-2}p-a)2k^{q-2}p - k^{q-2}p = 3k^{q-2}p - 2k^{q-2}pa. \end{aligned}$$

Thus, $A^2 = \begin{bmatrix} 2k^{q-2}p(a-1) & 2k^{q-2}pb \\ 2k^{q-2}pc & 3k^{q-2}p - 2k^{q-2}pa \end{bmatrix}$. Since A is idempotent, we have $2k^{q-2}pb = b$ and $2k^{q-2}pc = c$ which imply $(2k^{q-2}p-1)b = 0$ and $(2k^{q-2}p-1)c = 0$ respectively. Since $2k^{q-2}p - 1$ is a unit in $\mathbb{Z}_{pq}$, we have $b = c = 0$. Hence we have $A = \begin{bmatrix} a & 0 \\ 0 & 2k^{q-2}p - a \end{bmatrix}$. Since A is an idempotent, both a and $2k^{q-2}p - a = 2p^{q-1} - a$ must be idempotents. However, this is true only for $a = p^{q-1}$. Therefore, $A = \begin{bmatrix} p^{q-1} & 0 \\ 0 & p^{q-1} \end{bmatrix}$.

Now suppose $a + d = k^{q-2}p + 1$, so that $d = k^{q-2}p + 1 - a$. Along with $ad - bc = p^{q-1}$, we obtain the following:

$$\begin{aligned} a^2 + bc &= a^2 + ad - p^{q-1} = a(a+d) - p^{q-1} \\ &= ak^{q-2}p + a - k^{q-2}p; \\ ab + bd &= b(a+d) = b(k^{q-2}p + 1); \\ ac + cd &= c(a+d) = c(k^{q-2}p + 1); \text{ and} \\ bc + d^2 &= ad - p^{q-1} + d^2 = d(a+d) - k^{q-2}p \\ &= (k^{q-2}p + 1 - a)(k^{q-2}p + 1) - k^{q-2}p = 2k^{q-2}p + 1 - a(k^{q-2}p + 1). \end{aligned}$$

Thus, $A^2 = \begin{bmatrix} ak^{q-2}p + a - k^{q-2}p & b(k^{q-2}p + 1) \\ c(k^{q-2}p + 1) & 2k^{q-2}p + 1 - a(k^{q-2}p + 1) \end{bmatrix}$. Since A is an idempotent, we have $ak^{q-2}p + a - k^{q-2}p = a$, $b(k^{q-2}p + 1) = b$, and $c(k^{q-2}p + 1) = c$, which imply $ak^{q-2}p = k^{q-2}p$, $bk^{q-2}p = 0$, and $ck^{q-2}p = 0$, respectively. Hence, $A = \begin{bmatrix} 1 + qa(x) & qb(x) \\ qc(x) & p^{q-1} - qa(x)) \end{bmatrix}$, where $a(x), b(x), c(x) \in \mathbb{Z}_{pq}[x]$ such that $a(x)\{1 + qa(x)\} + qb(x)c(x) = p\alpha(x)$, for some $\alpha(x) \in \mathbb{Z}_{pq}[x]$. □

Remark: All computations in Theorems 3.8 and 3.9 are performed modulo pq where p and q are primes such that $p > q$. For our next theorem, computations are performed modulo p^2 where p is prime.

Lastly, we give the forms of non-trivial idempotents in $M_2(\mathbb{Z}_{p^2}[x])$ where p is prime.

Theorem 3.10. *For any prime p, the non-trivial idempotents in $M_2(\mathbb{Z}_{p^2}[x])$ are of the form $\begin{bmatrix} a(x) & b(x) \\ c(x) & 1 - a(x) \end{bmatrix}$, where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2}[x]$ not necessarily non-zero such that $a(x)\{1 - a(x)\} = b(x)c(x)$.*

Proof. It can be checked that the matrix of the said form is an idempotent. We have shown that if p is prime then the idempotents in $\mathbb{Z}_{p^2}$ are the trivial idempotents

0 and 1. Now, let $A = \begin{bmatrix} a(x) & b(x) \\ c(x) & d(x) \end{bmatrix}$ be a non-trivial idempotent of $M_2(\mathbb{Z}_{p^2}[x])$. For convenience, we write a, b, c and d for $a(x), b(x), c(x)$ and $d(x)$. Since A is an idempotent we have $a = a^2 + bc$, $b = ab + bd$, $c = ac + cd$ and $d = bc + d^2$. Since the determinant of A is an idempotent in $\mathbb{Z}_{p^2}$. It follows that $\det A$ is either 0 or 1. If $\det A = 1$, then $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ which is a trivial idempotent in $M_2\left(\mathbb{Z}_{p^2}[x]\right)$. This is a contradiction, since we assumed A is a non-trivial idempotent. Thus $\det A = 0$. From Proposition 3.6, we have $a + d = 0$ or 1. If $a + d = 0$ then $d = -a$. This implies that $a^2 + bc = 0$ and $bc + d^2 = 0$. So A is the zero matrix. Again, we arrive at a contradiction since we assumed A is a non-trivial idempotent. Observe that $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ has determinant 0 and trace 1.

If $a+d = 1$ then $d = 1-a$ and $ad-bc = 0$ give the following: $a^2+bc = a$; $ab+bd = b(a + d) = b$; $ac + cd = c(a + d) = c$ and $bc + d^2 = ad + d^2 = a(1 - a) + (1 - a)^2 = a - a^2 + 1 - 2a + a^2 = 1 - a$. Thus, $A^2 = \begin{bmatrix} a & b \\ c & 1-a \end{bmatrix}$. Hence $A = \begin{bmatrix} a(x) & b(x) \\ c(x) & 1-a(x) \end{bmatrix}$ where $a(x), b(x), c(x) \in \mathbb{Z}_{p^2}[x]$ such that $a(x)(1 - a(x)) = b(x)c(x)$. □

Acknowledgement. We thank the reviewers for the valuable comments and suggestions to improve the work.

References

[1] P. N. Anh, G. F. Birkenmeier and L. van Wyk, *Idempotents and structures of rings*, Linear Multilinear Algebra, 64(10) (2016), 2002-2029.

[2] D. M. Burton, Elementary Number Theory, 6th Edition, Tata McGraw-Hill Education Pvt. Ltd., 2006.

[3] M. Henriksen, *Two classes of rings generated by their units*, J. Algebra, 31 (1974), 182-193.

[4] T. W. Hungerford, Abstract Algebra: An Introduction, 3rd Edition, Cengage Learning, 2012.

[5] P. Kanwar, M. Khatkar and R. K. Sharma, *Idempotents and units of matrix rings over polynomial rings*, Int. Electron. J. Algebra, 22 (2017), 147-169.

[6] P. Kanwar, A. Leroy and J. Matczuk, *Idempotents in ring extensions*, J. Algebra, 389 (2013), 128-136.

[7] E. D. Nering, Linear Algebra and Matrix Theory, 2nd Edition, John Wiley & Sons Inc., 1970.

[8] W. K. Nicholson and Y. Zhou, *Rings in which elements are uniquely the sum of an idempotent and a unit*, Glasg. Math. J., 46(2) (2004), 227-236.

[9] A. K. Srivastava, *Additive representations of elements in rings: a survey*, in Algebra and its Applications, Springer Proc. Math. Stat., Springer, Singapore, 174 (2016), 59-73.

Jose Maria P. Balmaceda and **Joanne Pauline P. Datu** (Corresponding Author)
Institute of Mathematics
College of Science
University of the Philippines
1101 Diliman, Quezon City, Philippines
e-mails: joey@math.upd.edu.ph (J. M. P. Balmaceda)
jpdatu2@up.edu.ph (J. P. P. Datu)