Malaysian Journal of Mathematical Sciences 18(2): 259–266 (2024)
https://doi.org/10.47836/mjms.18.2.03

Malaysian Journal of Mathematical Sciences

Journal homepage: https://mjms.upm.edu.my

The Squared-Zero Product Probability of Some Ring of Matrices over Integers Modulo Prime

Zaid, N.[1,2], Sarmin, N. H.*[2], and Khasraw, S. M. S.[3]

[1]*Centre for Foundation, Language and General Studies, Asia Metropolitan University, 81750 Johor Bahru, Johor, Malaysia*
[2]*Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia*
[3]*Department of Mathematics, College of Education, Salahaddin University-Erbil, Kurdistan Region, Iraq*

E-mail: nhs@utm.my
**Corresponding author*

Received: 6 November 2023
Accepted: 25 January 2024

Abstract

Recently, the study of probabilities in ring theory has shown a significant increase in the field of algebra. Many interesting algebraic structures were modeled to find their probabilities in certain finite rings. In this paper, we introduce a new type of probability in finite rings, namely the squared-zero product probability. The aim is to study the square property and the zero product property of the ring. The focus of this study is the ring of matrices of dimension two over integers modulo prime p. To obtain the probability, the order of the square-annihilator of the ring is determined. The results found show that the squared-zero product probability of the ring is dependent on the value of p.

Keywords: ring theory; probability theory; ring of matrices.

1 Introduction

In the field of mathematics, ring theory plays a fundamental role in defining various algebraic structures which can provide understanding in many mathematical subjects. Some examples of rings include the ring of integers [12], Hamiltonian ring [13], and the rings of a special class [10]. Furthermore, ring theory has been applied in various mathematical branches including cryptography [5], functional analysis [1], graph theory [6], coding theory [4], as well as probability theory [8]. In this paper, we focus on the relation between ring theory and probability theory.

While ring theory and probability theory are two distinct areas, there are situations in which both areas overlap. In ring theory, probability theory has been extensively applied to study the tendencies that certain algebraic properties of a ring hold. In this paper, we study the probability that a square of an element of a finite ring is zero. This probability is then called the squared-zero product probability. The squared-zero product probability is determined for the ring of matrices of dimension two over integers modulo prime p.

This paper consists of five sections. The first section is the introduction of the study. The second section provides some previous works done on probability in finite rings. The third section presents a new probability defined in this study, namely the squared-zero product probability. Next, the fourth section gives the results obtained in this study. Finally, the conclusion of the study is presented in the fifth section.

2 Probabilistic Characterizations in Finite Rings

This section provides a literature review of studies done on probabilities associated with finite rings. The application of probability theory in ring theory began in 1976 when MacHale [8] studied the probability that two elements of a finite noncommutative ring commute. In the study, the probability is defined as $\Pr(R) = \dfrac{\{a \in R | ab = ba\}}{|R|^2}$, where a and b are elements in a noncommutative ring R. In the study, MacHale [8] also found that $\Pr(R) \leq \dfrac{5}{8}$.

Following the study, many researchers started to gain interest in finding the probabilistic characterizations in finite rings. This includes the study done by Dutta and Nath [3] on the relative commuting probability. The authors defined the relative commuting probability of a finite ring as the probability that a randomly chosen pair of elements, one from the ring R and the other from its subring S, commute. The probability is mathematically written as,

$$\Pr(S, R) = \frac{|\{(a, b) \in S \times R | ab = ba\}|}{|S||R|}.$$

Following that, Rehman et al. [11] introduced another type of probability in finite rings called the probability of product. The study was done on the ring of integers $\mathbb{Z}_n$. Just like its name, the objective of the study is to explore the probability that the product of any two randomly chosen elements of a ring is a fixed element of the ring itself. Mathematically, the probability is written as,

$$P_m(\mathbb{Z}_n) = \frac{|\{(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_n | ab = m\}|}{|\mathbb{Z}_n \times \mathbb{Z}_n|},$$

where a, b and m are elements of $\mathbb{Z}_n$.

Then, Khasraw [7] introduced a similar probability as [11], focusing only on elements with product zero. The study was done on finite commutative rings, and it was found that the probability is closely related to the zero divisors of the ring. The study also found that,

$$P(R) \geq \frac{2n + |Z(R)| - 1}{n^2},$$

where $Z(R)$ is the set of zero divisors of the ring R.

Then, Zai et al. [14] extended the study done by Khasraw in [7] to noncommutative rings, and officially named the probability as the zero product probability. The formula of determining the zero product probability of finite rings is given as,

$$P(R) = \frac{|\{(a,b) \in R \times R | ab = 0\}|}{|R \times R|}.$$

Some other studies of probabilities done on the zero product property of a finite ring include the study on semisimple rings done by Dolžan [2] and the study on group rings done by Mohammed Salih [9].

3 The Squared-Zero Product Probability of Finite Rings

In this section, we define a new probability associated with finite rings, namely the squared-zero product probability. This probability is introduced to study the tendency for the square of an element of a finite ring to be zero. To determine the squared-zero product probability, the square-annihilator of the ring needs to be obtained. Hence, the definition of a square-annihilator is given in the following.

Definition 3.1. *Let R be a finite noncommutative ring. Then, the square-annihilator of R is the set of ordered pairs $(x, x) \in R \times R$ such that $xx = 0$. The square-annihilator of R can be mathematically written in the following form;*

$$Ann_{sq}(R) = \{(x, x) \in R \times R | xx = 0\}.$$

Following the definition of the square-annihilator, the squared-zero product probability of a finite ring is defined as the order of the square-annihilator divided by the square of the size of the ring. The formal definition of the squared-zero product probability is given as follows:

Definition 3.2. *Let R be a finite noncommutative ring. Then, the squared-zero product probability of R,*

$$P_{sq}(R) = \frac{|\{(x, x) \in R \times R | xx = 0\}|}{|R \times R|} = \frac{|Ann_{sq}(R)|}{|R|^2}.$$

4 Results and Discussions

This section presents the results obtained in this study. First, the order of square-annihilator is determined for the 2×2 matrices over integers modulo prime, $M_2(\mathbb{Z}_p)$. Throughout this paper, p indicates prime number. To obtain the order of the square-annihilator, the matrices are first divided into six forms, which cover all possible matrices in $M_2(\mathbb{Z}_p)$. The following theorem gives the order of the square-annihilator of $M_2(\mathbb{Z}_p)$.

Theorem 4.1. *Let R be the ring of 2×2 matrices over integers modulo prime, $\mathbb{Z}_p$. Then, the order of the square-annihilator of R is p^2, or in symbols, $|Ann_{sq}(R)| = p^2$.*

Proof. Suppose $R = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \middle| x_1, x_2, x_3, x_4 \in \mathbb{Z}_p \right\}$. To obtain the order of the square-annihilator of R, the calculations are divided into six cases, based on the forms of the matrices in R.

Let, $X = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \in R$.

Case 1: When X is the zero matrix.
Then, all $x_i = 0$ when $i = 1, 2, 3, 4$. Thus, $X = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Since, $XX = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is trivial, this gives $|Ann_{sq}(X)| = 1$.

Case 2: When X has only one zero entry diagonally.
Then, only one of the diagonal entries is not zero while the other entries are zeros. Thus, the possible forms of X are $\begin{bmatrix} x_1 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 0 & x_4 \end{bmatrix}$.
Without loss of generality, take $X = \begin{bmatrix} x_1 & 0 \\ 0 & 0 \end{bmatrix}$. The possible element x_1 in $\mathbb{Z}_p$ can be determined by the following matrix multiplication,

$$\begin{bmatrix} x_1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 & 0 \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p},$$

which is then written as,

$$x_1{}^2 \equiv 0 \pmod{p}.$$

The congruence has no solution since x_1 is nonzero. The case is similar when, $X = \begin{bmatrix} 0 & 0 \\ 0 & x_4 \end{bmatrix}$. Therefore, there is no square-annihilator for this case, which gives, $|Ann_{sq}(X)| = 0$.

Case 3: When X has only one nonzero entry in the off-diagonal.
Then, only one of the off-diagonal entries is not zero while the other entries are zeros. Thus, the possible forms of X are $\begin{bmatrix} 0 & x_2 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ x_3 & 0 \end{bmatrix}$.

The elements of its square-annihilator are determined using the following matrix multiplication;

$$\begin{bmatrix} 0 & x_2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & x_2 \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p}.$$

From the multiplication, the following equation is formed;

$$x_2 \cdot 0 \equiv 0 \pmod{p},$$

which is always true for all $x_2 \in \mathbb{Z}_p - \{0\}$. This shows that x_2 can be any element in $\mathbb{Z}_p - \{0\}$. Therefore, the order of the square-annihilator for this case is $p-1$. The case is similar when $X = \begin{bmatrix} 0 & 0 \\ x_3 & 0 \end{bmatrix}$. Hence, the order of the square-annihilator for this case,

$$|Ann_{sq}(X)| = 2(p-1) = 2p-2.$$

Case 4: When X has two nonzero entries in a column or row.
Then, any two entries in the same row or column of X are not zero while the other two entries are zeros. Thus, $X = \begin{bmatrix} x_1 & x_2 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ x_3 & x_4 \end{bmatrix}, \begin{bmatrix} x_1 & 0 \\ x_3 & 0 \end{bmatrix}$ or $\begin{bmatrix} 0 & x_2 \\ 0 & x_4 \end{bmatrix}$.

The elements of the square-annihilator are determined using the following matrix multiplication;

$$\begin{bmatrix} x_1 & x_2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ 0 & 0 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p}.$$

From the matrix multiplication, the following system of equations is obtained;

$$\begin{aligned} {x_1}^2 &\equiv 0 \pmod{p}, \\ x_1 x_2 &\equiv 0 \pmod{p}. \end{aligned}$$

From Case 2, it is known that the congruence ${x_1}^2 \equiv 0 \pmod{p}$ has no solution since x_1 is nonzero. This also implies that x_2 has no solution since x_2 is also nonzero. As a result, the matrices with two nonzero entries in a column or row has no square-annihilator. Hence for this case, $|Ann_{sq}(X)| = 0$.

Case 5: When X has three nonzero entries.
Then, $X = \begin{bmatrix} x_1 & x_2 \\ 0 & x_4 \end{bmatrix}, \begin{bmatrix} x_1 & x_2 \\ x_3 & 0 \end{bmatrix}, \begin{bmatrix} x_1 & 0 \\ x_3 & x_4 \end{bmatrix}$ or $\begin{bmatrix} 0 & x_2 \\ x_3 & x_4 \end{bmatrix}$.
Without loss of generality, take $X = \begin{bmatrix} x_1 & x_2 \\ 0 & x_4 \end{bmatrix}$. The elements of the square-annihilator are determined by the following matrix multiplication,

$$\begin{bmatrix} x_1 & x_2 \\ 0 & x_4 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ 0 & x_4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p}.$$

From the matrix multiplication, the following system of equations is formed.

$$\begin{aligned} {x_1}^2 &\equiv 0 \pmod{p}, \\ x_1 x_2 + x_2 x_4 &\equiv 0 \pmod{p}, \\ {x_4}^2 &\equiv 0 \pmod{p}. \end{aligned}$$

From Case 2, it is known that the congruences ${x_1}^2 \equiv 0 \pmod{p}$ and ${x_4}^2 \equiv 0 \pmod{p}$ have no solution since x_1 and x_4 are nonzero. Thus, there is no square-annihilator for the matrices in $M_2(\mathbb{Z}_p)$ with three nonzero entries. Hence for this case, $|Ann_{sq}(X)| = 0$.

Case 6: When all entries in X are nonzero.
Then, all entries x_1, x_2, x_3 and x_4 are nonzero. To obtain the order of square-annihilator, the following matrix multiplication is performed,

$$\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \pmod{p}.$$

From the matrix multiplication, the following system of equations is formed;

$$x_1{}^2 + x_2x_3 \equiv 0 \pmod{p}, \tag{1}$$
$$x_2x_3 + x_4{}^2 \equiv 0 \pmod{p}, \tag{2}$$
$$x_1x_2 + x_2x_4 \equiv 0 \pmod{p}, \tag{3}$$
$$x_1x_3 + x_3x_4 \equiv 0 \pmod{p}. \tag{4}$$

Since all entries are nonzero, it can be said that there are $p-1$ possible entries for x_1. By elimination method operated on equation (1) and equation (2),

$$x_1{}^2 - x_4{}^2 \equiv 0 \pmod{p},$$
$$x_1{}^2 \equiv x_4{}^2 \pmod{p},$$
$$x_1 \equiv \pm x_4 \pmod{p}.$$

This shows that either $x_1 = x_4$ or x_4 is the additive inverse of x_1. Therefore, in either way, the value of x_4 is dependent on the value of x_1.

Meanwhile, to obtain the possible values for x_2 and x_3, it can be seen from equation (3) that,

$$x_2(x_1 + x_4) \equiv 0 \pmod{p}.$$

From this equation, $x_2 \in \mathbb{Z}_p - \{0\}$ since $x_1 + x_4 \in \mathbb{Z}_p - \{0\}$ as the ring is always closed under addition. Therefore, the number of possible values of x_2 is $p-1$. Then, from equation (1),

$$x_3 \equiv -\frac{x_1{}^2}{x_2} \pmod{p}.$$

This shows that the values of x_3 depends on x_2.

Hence, for this case, the order of the square-annihilator of R is

$$|Ann_{sq}(X)| = (p-1)(p-1)(1)(1) = p^2 - 2p + 1.$$

All the above cases have covered all possible matrices $X \in R$. Thus, combining all of the cases, it is found that the order of the square-annihilator of R is

$$|Ann_{sq}(R)| = 1 + 2p - 2 + p^2 - 2p + 1 = p^2.$$

□

The following example presents the order of the square-annihilator of the ring of matrices of dimension two over $\mathbb{Z}_p$ when $p = 2$.

Example 4.1. *Given a finite ring* $R = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \middle| x_1, x_2, x_3, x_4 \in \mathbb{Z}_2 \right\}$. *Based on Definition 3.1, it is found that the square-annihilator of* R,

$$Ann_{sq}(R) = \left\{ \left(\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right), \left(\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \right), \right.$$
$$\left. \left(\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right), \left(\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right) \right\}.$$

The result is consistent with Theorem 4.1, where the order of the square-annihilator,

$$|Ann_{sq}(R)| = (2)^2 = 4.$$

The next theorem presents the squared-zero product probability of $M_2(\mathbb{Z}_p)$, found by using its definition.

Theorem 4.2. *Let R be the ring of matrices of dimension two over $\mathbb{Z}_p$. Then, the squared-zero product probability of R, $P_{sq}(R) = \dfrac{1}{p^6}$.*

Proof. Suppose R is the ring of matrices of dimension two over $\mathbb{Z}_p$. According to Definition 3.2, the squared-zero product probability of R is the order of the square-annihilator of R divided by the square of the order of R. Based on Theorem 4.1, the order of the square-annihilator of R is $|Ann_{sq}(X)| = p^2$. Since $|R| = p^4$, then the squared-zero product probability of R,

$$P_{sq}(R) = \frac{p^2}{(p^4)^2} = \frac{1}{p^6}.$$

□

The following example presents the squared-zero product probability of the ring of matrices of dimension two over $\mathbb{Z}_p$ when $p = 2$.

Example 4.2. *Given a finite ring $R = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \middle| x_1, x_2, x_3, x_4 \in \mathbb{Z}_2 \right\}$. Based on Theorem 4.2, the squared-zero product probability of R, $P_{sq}(R) = \dfrac{1}{2^6} = \dfrac{1}{64}$.*

5 Conclusion

In this paper, a new type of probability in finite rings, namely the squared-zero product probability is defined and its general formula is established for the ring of 2×2 matrices over integers modulo prime, $M_2(\mathbb{Z}_p)$. To formulate the general formula of the probability, the general formula of the order of its square-annihilator is also formed. It is found that the general formula of the square-annihilator of $M_2(\mathbb{Z}_p)$ depends on the value of p.

Acknowledgement The authors would like to acknowledge the Ministry of Higher Education Malaysia (MoHE) for the funding of this study through the Fundamental Research Grant Scheme (FRGS/1/2020/STG06/UTM/01/2). The first author would also like to express her sincere gratitude to Universiti Teknologi Malaysia (UTM) for the financial support through the UTM Zamalah Scholarship.

Conflicts of Interest The authors declare no conflict of interest.

References

[1] I. Cho (2018). Adelic analysis and functional analysis on the finite adele ring. *Opuscula Mathematica*, *38*(2), 139–185. https://doi.org/10.7494/OpMath.2018.38.2.139.

[2] D. Dolžan (2022). The probability of zero multiplication in finite rings. *Bulletin of the Australian Mathematical Society*, *106*(1), 83–88. https://doi.org/10.1017/S0004972721001246.

[3] P. Dutta & R. K. Nath (2019). On relative commuting probability of finite rings. *Miskolc Mathematical Notes*, *20*(1), 225–232. https://doi.org/10.18514/MMN.2019.2274.

[4] M. Greferath (2009). An introduction to ring-linear coding theory. In *Gröbner Bases, Coding, and Cryptography*, pp. 219–238. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-93806-4_13.

[5] B. Hurley & T. Hurley (2011). Group ring cryptography. *International Journal of Pure and Applied Mathematics*, *69*(1), 67–86.

[6] M. A. Khan (2021). Contributions to generalized derivation on prime near-ring with its application in the prime graph. *Malaysian Journal of Mathematical Sciences*, *15*(1), 109–123. https://mjms.upm.edu.my/lihatmakalah.php?kod=2021/January/15/1/109-123.

[7] S. M. S. Khasraw (2020). What is the probability that two elements of a finite ring have product zero? *Malaysian Journal of Fundamental and Applied Sciences*, *16*(4), 497–499. https://doi.org/10.11113/mjfas.v16n4.1914.

[8] D. MacHale (1976). Commutativity in finite rings. *The American Mathematical Monthly*, *83*(1), 30–32. https://doi.org/10.1080/00029890.1976.11994032.

[9] H. Mohammed Salih (2022). On the probability of zero divisor elements in group rings. *International Journal of Group Theory*, *11*(4), 253–257. https://doi.org/10.22108/ijgt.2021.126694.1664.

[10] T. Nagaiah & M. R. Valluri (2022). A special class of rings. *Malaysian Journal of Mathematical Sciences*, *16*(1), 143–151. https://doi.org/10.47836/mjms.16.1.11.

[11] S. Rehman, A. Q. Baig & K. Haider (2019). A probabilistic approach toward finite commutative rings. *Southeast Asian Bulletin of Mathematics*, *43*(3), 413–418.

[12] C. Schwarzweller (1999). The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, *8*(1), 29–34.

[13] M. Woronowicz (2023). New results for the additive groups of Hamiltonian rings. *Communications in Algebra*, pp. 1–9. https://doi.org/10.1080/00927872.2023.2286338.

[14] N. A. F. O. Zai, N. H. Sarmin & N. Zaid (2020). The zero product probability of some finite rings. *Menemui Matematik*, *42*(2), 51–58. https://myjms.mohe.gov.my/index.php/dismath/article/view/13044.