KZYJC
ISSN:1001-0920
ISSN: 1001-0920
Volume 38, Issue 07, November, 2023

The Zero Product Probability of Ring of Matrices Based on Euler's Phi-Function

Nurhidayah Zaid[1], Nor Haniza Sarmin[2], Sanhan Muhammad Salih Khasraw[3]

Department of Mathematical Sciences, Faculty of Science, Universiti Teknologi Malaysia, 81310 Johor Bahru, Johor, Malaysia[1,2]
Department of Mathematics, College of Education, Salahaddin University-Erbil, Kurdistan Region, Iraq[3]

ABSTRACT— In the field of algebra, the application of probability theory in ring theory has been widely studied by various researchers. In this paper, a type of probability in finite rings, namely the zero product probability is determined for some ring of 2×2 matrices with a single nonzero entry. To obtain the zero product probability, the exact order of the annihilator of a ring *R* needs to be first determined. The annihilator of *R* is defined as the set of pairs of elements, where the product of elements in each pair is the zero element of *R*. The general formula for the exact order is established using the linear congruence method as well as Euler's phi-function. The zero product probability of *R* is then found by dividing the exact order of the annihilator by the square of the order of *R*. Besides that, a subset of the annihilator, which is the square-annihilator that only focuses on the square attributes of the annihilator is also determined for the same ring. The exact order of the square-annihilator is then used to find the squared-zero product probability of *R*.

KEYWORDS: Ring Theory, Annihilator, Euler's Phi-Function, Zero Product Probability

1. INTRODUCTION

The study of ring theory has long become a topic of interest for various researchers in the field of algebra. Many interesting subjects of a ring have been studied as of today, including the studies on ideals, zero divisors, and annihilators of a ring. In this paper, our focus is to study the zero product property of a finite ring of matrices. This zero product property of a ring has opened up various studies in finite rings, one of them being the zero divisor graph, introduced by [1] in 1988. The zero divisor graph is a graph where its vertices are the zero divisors of a finite ring, and two vertices are adjacent if and only if their product is zero [2]. Much research was done on the zero divisor graph to explore its interesting features. Eventually, the studies done on the zero divisor graph helped [3] to gain an idea in introducing the zero product probability, which is the probability that two elements of a finite ring have product zero.

In determining the zero product probability of a finite ring, the annihilator of the ring plays an important role. An annihilator is defined as the set of pairs of elements of a ring *R* where the product of the elements in a pair is the zero element of *R* [3]. In other words, the annihilator of a finite ring highlights the zero product property of the ring.

In this paper, the exact order of the annihilator is determined for some ring of matrices of dimension two and then the zero product probability of the ring is determined. Besides that, a new type of annihilator of finite rings is introduced, namely the square-annihilator. Eventually, a new type of probability in finite rings is defined based on the definition of the square-annihilator, namely the squared-zero product probability.

This paper consists of four main sections. The first section is the introduction, followed by some literature review on the probabilities related to finite rings which are given in the second section. Then, the third section presents the research methodology used in determining the results of this study, including the Euler's phi-function. Lastly, the fourth section presents the results obtained in this study.

2. Some Probabilities Associated with Finite Rings

Recent years have seen a significant increase in studies on probabilities related to finite rings. It was started back in 1976 when [4] determined the probability that two random elements of a ring commute for noncommutative rings. The probability is written as $P(R)=\frac{|\{x\in R\,|\,xr=rx\}|}{|R|^2}$, where x and r are the elements of the noncommutative ring R.

Much later in 2014, [5] precisely defined the commuting probability of a finite ring R given as $\Pr(R)=\frac{|\{(x,y)\in R\times R\,|\,xy=yx\}|}{|R|^2}$, where R is a finite ring and $|R|$ denotes the cardinality of R.

Another study of commuting probability in rings has been done by [6] in 2017. In the study, the commuting probability is generalized as the relative commuting probability of the subring S in a finite ring R and the mathematical formula is given by: $\Pr(S,R)=\frac{|\{(s,r)\in S\times R\,|\,sr=rs\}|}{|S\times R|}$.

Then, [7] formally defined it as the relative commutativity degree of finite rings which is the probability that a randomly chosen pair of elements one from a subset S of a ring R and the other from R commute. The relative commutativity degree of a finite ring can be mathematically written as $\Pr(S,R)=\frac{|\{(x,y)\in S\times R\,|\,xy=yx\}|}{|S||R|}$, where S is a subring of a finite ring R.

For many years, researchers were mainly focusing on the commuting probability of finite rings. In 2019, [8] studied another type of probability called the probability of product in the ring of integers $\mathbb{Z}_n$, where the aim was to obtain a desirable product in finite commutative rings, specifically $\mathbb{Z}_n$. The probability, denoted as $P_m(\mathbb{Z}_n)$, is the probability that the product of two randomly chosen elements of $\mathbb{Z}_n$, say x,y is m, where m is fixed. The probability is written as $P_m(\mathbb{Z}_n)=\frac{|\{(x,y)\in\mathbb{Z}_n\times\mathbb{Z}_n\,|\,x\cdot y=m\}|}{|\mathbb{Z}_n\times\mathbb{Z}_n|}$.

From the study, [8] had found several interesting results which includes the resemblance of the probability with the Chinese Remainder Theorem for some cases when m is fixed as 0 or 1. In general, the authors found that the computation of the probability in $\mathbb{Z}_n$ is mainly related to the greatest common divisor, $\gcd(x,n)$ of any element x in $\mathbb{Z}_n$.

Another probability associated to the product of ring elements had been introduced by [3]. The author defined the probability that the product of two randomly chosen elements in a finite ring is zero. The study was done on finite commutative rings with identity 1. The definition of the probability is given in the following.

Definition 2.1 [3] Let R be a finite commutative ring. The probability that two elements chosen at random

ISSN: 1001-0920
Volume 38, Issue 07, November, 2023

(with replacement) from a ring R have product zero, $P(R) = \frac{|\{(x,y) \in R \times R \mid xy = yx = 0\}|}{|R \times R|}$.

Then, [9] extended the probability that two elements of a finite ring have product zero, focusing on noncommutative ring. Following the study, the probability is then named as the zero product probability. The definition of the zero product probability of noncommutative rings is given as follows:

Definition 2.2 [9] Let R be a noncommutative ring. Then, the zero product probability of R,

$$P(R) = \frac{|\{(x,y) \in R \times R \mid xy = 0\}|}{|R \times R|}.$$

In this paper, our focus is to determine the zero product probability of the ring of 2×2 matrices over integers modulo p^n with a single nonzero entry, where p is prime and n is any positive integer. The methods of obtaining the zero product probability is given in the next section.

3. Research Methodology

The results in this paper are divided into two main parts which are determining the general formulas for the order of the annihilator and square-annihilator of some finite ring of matrices, as well as finding the general formula in computing the zero product probability and squared-zero product probability of the ring.

Firstly, the general formula for computing the order of the annihilator of the ring of 2×2 matrices over integers modulo p^n with a single nonzero entry, denoted as R, is determined using the definition of the annihilator. Since the ring considered is a noncommutative ring, the definition of the annihilator of a noncommutative ring is provided as follows:

Definition 3.1 Let R be a noncommutative ring. Then, the annihilator of R is the set of ordered pairs $(x,y) \in R \times R$ such that $xy = 0$. Mathematically, the set is written as: $Ann(R) = \{(x,y) \in R \times R \mid xy = 0\}$.

To form the general formula, a linear system is formed based on the product of the matrices. The linear system is then solved using the linear congruence method, where the number of possible solutions of the system is obtained. The number of possible solutions is the order of the annihilator for each form. The following theorem states the method of determining the number of solutions of a linear congruence, by using the greatest common divisor of two constants.

Theorem 3.1 [10] The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a,n)$. If $d \mid b$, then the congruence has d mutually incongruent solutions modulo n.

Also, to solve the linear congruence system, the Euler's phi-function plays a significant role in determining the number of solutions of the congruence. The Euler's phi-function is provided as follows:

Definition 3.2 [10] The Euler's phi-function, denoted as $\phi(n)$, is the number of positive integers less than or equal to n that are relatively prime to n, for $n \geq 1$.

The following theorem gives the formula to directly calculate the value of $\phi(n)$ for prime-power integers.

Theorem 3.2 [10] Let p is a prime and k is any positive integer, then $\phi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$.

Next, the general formula for the zero product probability of R is formed using the Definition 2.2. To form the general formula, the results on the order of the annihilator which have been found earlier are used.

Apart from that, a new type of annihilator is defined on finite rings, namely the squared-annihilator. The definition of the square-annihilator of a finite ring is given as follows:

Definition 3.3 Let R be a finite ring. Then, the square-annihilator of R is the set of ordered pairs $(x,x) \in R \times R$ such that $xx = 0$. Mathematically, the set is written as: $Ann_{sq}(R) = \{(x,x) \in R \times R \mid xx = 0\}$.

To find the exact order of the square-annihilator of R, the same method as finding the exact order of the annihilator of R is used.

Next, based on the definition of the squared-annihilator of R, a new type of probability, namely the squared-zero product probability is found for R. The definition of the squared-zero product probability is given below.

Definition 3.4 Let R be a finite ring. Then, the squared-zero product probability of R is:

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

4. Results and Discussions

This section presents the results of this study, which includes the order of the annihilator, the order of the square-annihilator, the zero product probability as well as the squared-zero product probability of R.

4.1 The Order of the Annihilator of R

In this subsection, the order of the annihilator of R, denoted as $Ann(R)$, is computed and its general formula is found by using the Euler's phi-function, as stated in the following theorem.

Theorem 4.1 Given a ring $S = \left\{ \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \middle| y_1, y_2, y_3, y_4 \in \mathbb{Z}_{p^n} - \{0\} \right\}$ and the ring $R = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{Z}_{p^n} - \{0\} \right\}$ is a subset of S. Then, the order of the annihilator of R, $|Ann(R)| = p^{4n-1} - p^{3n-1}$.

Proof. First, the number of possible elements $X \in R$ and $Y \in S$ where $XY = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is determined by using the following matrix multiplication.

$$\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (\text{mod } p^n).$$

This gives the following linear congruences.

ISSN: 1001-0920
Volume 38, Issue 07, November, 2023

$$xy_1 \equiv 0 \pmod{p^n} \tag{4.1}$$

$$xy_2 \equiv 0 \pmod{p^n}, \tag{4.2}$$

where y_3 and y_4 can be any element in $\mathbb{Z}_{p^n}$.

To solve the congruences, the proof is divided into *n* cases, which are when $\gcd(x, p^n) = 1, p, p^2, \cdots, p^{n-2}$, p^{n-1}.

Case 1: When $\gcd(x, p^n) = 1.$

Based on Theorem 3.2, it is found that there are $p^n - p^{n-1}$ possible values of x where $\gcd(x, p^n) = 1$. Hence, the number of possible elements of *X*, $|X| = p^n - p^{n-1}$. Next, to find $|Y|$, based on Theorem 3.1, the number of solution for the entries y_1 and y_2 is $|y_1| = |y_2| = \gcd(x, p^n) = 1$. Then, based on Congruence 4.1 and Congruence 4.2, $|y_3| = |y_4| = p^n$. Thus, for this case, the order of the annihilator, $|Ann(R)| = |X||Y| = (p^n - p^{n-1})(1)(1)(p^n)(p^n) = p^{3n} - p^{3n-1}$.

Case 2: When $\gcd(x, p^n) = p.$

Based on Theorem 3.2, $|X| = p^{n-1} - p^{n-2}$. Next, to find $|Y|$, based on Theorem 3.1, the number of solution for the entries y_1 and y_2 is $|y_1| = |y_2| = \gcd(x, p^n) = p$. Meanwhile, based on Congruence 4.1 and Congruence 4.2, $|y_3| = |y_4| = p^n$. Thus, for this case, the order of the annihilator, $|Ann(R)| = (p^{n-1} - p^{n-2})(p)(p)(p^n)(p^n) = p^{3n+1} - p^{3n}$.

For the next cases, namely Case 3, Case 4, …, Case $n-1$, the proof follows where the number of possible elements in *X* is found based on Theorem 3.2, while the number of solutions for the entries y_1 and y_2 is the greatest common divisor of x and p^n. The calculations for Case $n-1$ is provided in the following.

Case $n-1$: When $\gcd(x, p^n) = p^{n-2}.$

Based on Theorem 3.2, $|X| = p^2 - p.$ Next, to find $|Y|$, based on Theorem 3.1, the number of solution for the entries y_1 and y_2 is $|y_1| = |y_2| = \gcd(x, p^n) = p^{n-2}$. Meanwhile, based on Congruence 4.1 and Congruence 4.2, $|y_3| = |y_4| = p^n$. Thus, for this case, the order of the annihilator, $|Ann(R)| = (p^2 - p)(p^{n-2})(p^{n-2})(p^n)(p^n) = p^{4n-2} - p^{4n-3}$.

This then leads to the last case, illustrated in the following.

Case n: When $\gcd(x, p^n) = p^{n-1}.$

Based on Theorem 3.2, $|X| = p - 1$. Next, to find $|Y|$, based on Theorem 3.1, the number of solution for the entries y_1 and y_2 is $|y_1| = |y_2| = \gcd(x, p^n) = p^{n-1}$. Meanwhile, based on Congruence 4.1 and Congruence 4.2, $|y_3| = |y_4| = p^n$. Thus, for this case, the order of the annihilator of *R*, $|Ann(R)| = (p-1)(p^{n-1})(p^{n-1})(p^n)(p^n) = p^{4n-1} - p^{4n-2}$.

Now combining all cases from Case 1 until Case *n*, the order of the annihilator,

$$|Ann(R)| = p^{3n} - p^{3n-1} + p^{3n+1} - p^{3n} - p^{3n+1} + \ldots + p^{4n-3} + p^{4n-2} - p^{4n-3} + p^{4n-1} - p^{4n-2}.$$

By telescoping sum,

$$\begin{aligned} |Ann(R)| &= p^{4n-1} + (p^{4n-2} - p^{4n-2}) + (p^{4n-3} - p^{4n-3}) + \ldots + (p^{3n+1} - p^{3n+1}) + (p^{3n} - p^{3n}) - p^{3n-1} \\ &= p^{4n-1} - p^{3n-1}. \end{aligned}$$ □

4.2 The Order of the Square-Annihilator of R

In this subsection, the order of the square-annihilator of *R*, denoted as $Ann_{sq}(R)$, is computed and its general formula is found as stated in the following theorem.

Theorem 4.2 Given a ring $R = \left\{ \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{Z}_{p^n} - \{0\} \right\}$. Then, the order of the square-annihilator of *R*,

$$|Ann_{sq}(R)| = \begin{cases} p^{\frac{n}{2}} - 1; & \text{when } n \text{ is even,} \\ p^{\frac{n-1}{2}} - 1; & \text{when } n \text{ is odd.} \end{cases}$$

Proof. To obtain the possible elements $x \in \mathbb{Z}_{p^n} - \{0\}$, the following matrix multiplication is considered.

$$\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (\text{mod } p^n),$$

which is then written as $x^2 \equiv 0 \pmod{p^n}$. When *n* is even, *n* can be written as 2*m*, where *m* is any positive integer. Eventually, $p^n = p^{2m} = (p^m)(p^m)$. Hence, when *n* is even, p^n is a perfect square. Solving for x,

$$\begin{aligned} x^2 &\equiv 0 \pmod{p^m} \\ x &= \underbrace{p^m, 2p^m, 3p^m, \cdots, (p^m - 1)p^m}_{p^m - 1 \text{ times}}. \end{aligned}$$

Thus, when *n* is even, $|Ann_{sq}(R)| = p^m - 1 = p^{\frac{n}{2}} - 1$.

Meanwhile, when *n* is odd, it can be written as $2m-1$. Eventually, based on the fundamental theorem of arithmetic, p^n can be represented as a product of prime numbers: $p^n = p^{2m-1} = (p^m)(p^m)(p)$. Solving for x, the calculations are divided into two forms. The first form is $x^2 \equiv 0 (\text{mod } p)$, which has no solution in $\mathbb{Z}_{p^n} - \{0\}$. Then, the second form is $x^2 \equiv 0 \pmod{p^m}$, which results in $x = \underbrace{p^m, 2p^m, 3p^m, \cdots, (p^m - 1)p^m}_{p^m - 1 \text{ times}}$.

Therefore, the order of the square-annihilator when n is odd, $|Ann_{sq}(R)| = p^{m-1} - 1 = p^{\frac{n+1}{2}-1} - 1 = p^{\frac{n-1}{2}} - 1$. □

4.3 The Zero Product Probabilities of R

In this subsection, the zero product probability and squared-zero product probability of R are determined by using their definitions.

ISSN: 1001-0920
Volume 38, Issue 07, November, 2023

Theorem 4.3 Given a finite ring $R=\left\{\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{Z}_{p^n} - \{0\}\right\}$. Then, the zero product probability of *R*,

$$P(R) = p^{4n-9} - p^{3n-9}.$$

Proof. Based on Theorem 4.1, the number of the annihilators of *R*, $|Ann(R)| = p^{4n-1} - p^{3n-1}$. Therefore, based on Definition 2.2, the zero product probability of *R*, $P(R) = \frac{|Ann(R)|}{|R|^2} = \frac{p^{4n-1} - p^{3n-1}}{(p^4)^2} = p^{4n-9} - p^{3n-9}$. □

Theorem 4.4 Given a ring $R=\left\{\begin{bmatrix} x & 0 \\ 0 & 0 \end{bmatrix} \middle| x \in \mathbb{Z}_{p^n} - \{0\}\right\}$. Then, the squared-zero product probability of *R*,

$$P_{sq}(R) = \begin{cases} \frac{p^{\frac{n}{2}} - 1}{p^8}; & \text{when } n \text{ is even,} \\ \frac{p^{\frac{n-1}{2}} - 1}{p^8}; & \text{when } n \text{ is odd.} \end{cases}$$

Proof. According to Theorem 4.2, when *n* is even, the order of the square-annihilator of *R* is $p^{\frac{n}{2}} - 1$. Meanwhile, when *n* is odd, the order of the square-annihilator of *R* is $p^{\frac{n-1}{2}} - 1$. Therefore, by Definition 3.4, the squared-zero product probability of *R* is $\frac{p^{\frac{n}{2}} - 1}{p^8}$ when *n* is even and $\frac{p^{\frac{n-1}{2}} - 1}{p^8}$ when *n* is odd. □

5. Conclusion

In this paper, a new type of annihilator of a finite ring, namely the square-annihilator is introduced. Then, the exact order of the annihilator and square-annihilator are determined for the ring of 2×2 matrices over integers modulo p^n with a single nonzero entry, where *p* is prime and *n* is any positive integer. The exact orders are stated in theorems and have been proved using Euler's phi-function. These results are then used to establish the general formula of the zero product probability and the squared-zero product probability of the ring, using their definitions. In addition, for future studies, other forms of matrices such as the diagonal matrix, the upper triangular matrix and the lower triangular matrix can be studied for their annihilator, square-annihilator, zero product probability and squared-zero product probability.

6. Acknowledgement

This work was funded by the Ministry of Higher Education Malaysia (MoHE) under Fundamental Research Grant Scheme (FRGS/1/2020/STG06/UTM/01/2).

7. References

[1] Beck, I., "Coloring of Commutative Rings" Journal of Algebra, Volume 116, 1988, pp. 208-226.

[2] Anderson, D. F. and Livingston, P. S. "The Zero-Divisor Graph of Commutative Ring" Journal of Algebra, Volume 217, 1999, pp. 434-447.

[3] Khasraw, S.M.S., "What is the Probability that Two Elements of a Finite Ring Have Product Zero?" Malaysian Journal of Fundamental and Applied Sciences, Volume 16, Issue 4, 2020, pp. 497-499.

[4] MacHale, D., "Commutativity in Finite Rings" The American Mathematical Monthly, Volume 83, Issue 1, 1976, pp. 30-32.

[5] Buckley, S. M., MacHale, D. and Aine, N. S., "Finite Rings with Many Commuting Pairs of Elements" Preprint, 2014.

[6] Dutta, J., Basnet, D. K. and Nath, R. K., "On Commuting Probability of Finite Rings" Indagationes Mathematicae, Volume 28, 2017, pp. 372-382.

[7] Dutta, P. and Nath, R. K., "On Relative Commuting Probability of Finite Rings" Miskolc Mathematical Notes Volume 20, Issue 1, 2019, pp. 225-232.

[8] Rehman, S., Baig, A. Q. and Haider, K., "A Probabilistic Approach Toward Finite Commutative Rings" Southeast Asian Bulletin of Mathematics, Volume 43, 2019, pp. 413-418.

[9] Omar Zai, N. A. F., Sarmin, N. H. and Zaid, N, "The Zero Product Probability of Some Finite Rings" Menemui Matematik, Volume 42, Issue 2, 2020, pp. 51-58.

[10] Burton, D. M. Elementary Number Theory. Boston: McGraw-Hill, 2002.