Open Journal of Science and Technology
Journal Homepage: http://readersinsight.net/OJST

Research Article

Relative coprime probability for cyclic subgroups of some dihedral groups

Nurfarah Zulkifli[1], Nor Muhainiah Mohd Ali[2*]

[1,2]Department of Mathematical Sciences, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru Malaysia

*Corresponding Author email: normuhainiah@utm.my

Submission: 12 September 2020 Revised: 20 October 2020 Accepted: 28 November 2020

ABSTRACT

A dihedral group is a group of symmetries of a regular n-sided polygon, in other words, a structured operation that will make n-gon to go back to itself through a solid motion. Many researchers have studied various fields of group theory using dihedral groups and one of them is the study of the coprime probability of a group and it is defined as the probability of a random pair of elements in a group G such that the greatest common divisor of the order of x and y, where x and y are in G, is equal to one. The coprime probability of G is then extended to the relative coprime probability G and it is defined as the probability that two randomly selected elements h from H and g from G where H is a subgroup of a group G such that the greatest common divisor of the order of h and order of g, is equal to one. In this research, the concentration is on the generalization of the relative coprime probability for cyclic subgroups of some dihedral groups.

Keywords: *Dihedral Group, Relatively Prime, Cyclic Subgroups, Relative Coprime Probability*

1. INTRODUCTION

A simple explanation on probability is the likeliness something is to happen. For example, after flipping a coin, what is the probability or possibility that the coin will land on tail? Probability theory is very much helpful for making predictions or decisions which also helps in research investigations so that further analysis can be made. Probability is often not just being used by statisticians to solve any uncertainties, but it has also been applied in the field of group theory. Mathematically, the probability of an event to happen is the number of ways it happens divided by total number of outcomes.

In this research, the focus is on the study of the extension of the coprime probability, namely the relative coprime probability. The idea of the coprime probability was motivated by the extension of the prime graph in which it has been explored tremendously in a variety of areas for various groups. Previous researchers have extensively studied this research mainly focusing on the types of graphs and their properties, such as prime graphs (1), coprime graphs (2) and non-coprime graphs (3).

Later, it was discovered that no studies have been done related to the coprime probability. Abd Rhani, Mohd Ali (4) then took the opportunity to explore this area relating to group theory by introducing the coprime probability of a group. The coprime probability is defined as the probability of the order of a random pair of elements in the group are relatively prime or coprime. In their research, the coprime probability for all $p-$groups, where p is a prime number was determined and the result of the research is stated as follows;

Proposition 1: Let G be a $p-\text{groups}$ of order p^n, where $n \geq 1$. Then

$$P_{copr}(G) = \frac{2p^n - 1}{2p^n}.$$

Next, the same objective is used to determine the coprime probability but in these two papers, Zulkifli and Mohd Ali (5) and Zulkifli and Mohd Ali (6) focused on another group which is the nonabelian metabelian group of order at most 24. In Zulkifli and Mohd Ali (5), it was found that when a group G has the same order then the coprime probability of dihedral groups or $p-\text{groups}$ are the same, whereas Zulkifli and Mohd Ali (6) provide the results that shows the coprime probability varies for nonabelian metabelian groups of order 24.

The research become even more interesting when the coprime probability is extended to the relative coprime probability. The extension was inspired by the research of the commutativity degree in which various groups have been used to study the probability obtained in each group. One of the extensions of the commutativity degree that has attracted researchers' attention is the relative commutativity degree, defined as the probability that an element of a subgroup H of a group G commutes with an element of G. There are several types of groups that have been used to study the pattern of the relative commutativity degree, for example, finite groups (7), dihedral groups (8), and nonabelian metabelian groups (9).

Influenced by that matter, the relative coprime probability is introduced to study and understand the pattern that can be found within a group and it is defined as the probability that two randomly selected elements h from H and g from G, where H is a subgroup of a group G such that the greatest common divisor of the order of h and g, is equal to one (10). The relative coprime probability has been determined for cyclic subgroup of nonabelian metabelian groups of order less than 24 and from the results, it can be concluded that the relative coprime probability of the dihedral groups or $p-\text{groups}$ are the same when G has the same order.

Therefore, a deeper understanding of the relative coprime probability will be given priority by generalizing the relative coprime probability for cyclic subgroups of dihedral group, D_n where n is odd prime. Henceforth, this paper is structured as follows: the first part is the introduction in which this section introduces the relative coprime probability together with some literature that are related to this research. Then, a few basic concepts and definitions that are used in this research are provided in Section 2 and finally, the main results of the research are determined and discussed in Section 3 followed by a summary of the whole research in the conclusion section.

2. PRELIMINARIES

In this section, some basic concepts on group theory are stated and will be used in this research.

Definition 1 (11) Dihedral group of degree n

For each $n \in \mathbb{N}$ and $n \geq 3$, D_n is denoted as the set of symmetries of a regular $n-\text{gon}$. Furthermore, the order of D_n is $2n$ or equivalently $|D_n| = 2n$. The dihedral groups, D_n can be represent in a form of generators and relations given in the following representation:

$$D_n = \langle a, b \,|\, a^n = 1, b^2 = 1, ab = a^{-1}b \rangle.$$

Definition 2 (10) Relative Coprime Probability of G

Let G be a finite group and H be a subgroup of G. The relative coprime probability of G is defined as follows:

$$P_{copr}(H,G) = \frac{|(h,g) \in H \times G : (|h|,|g|) = 1|}{|H||G|}.$$

3. MAIN RESULTS

The dihedral group, D_n consists of the set of rotations where $R_o = \{a, a^2, \ldots, a^{n-1}\}$ and the set of reflections, $R_e = \{b, ab, a^2b, \ldots, a^{n-1}b\}$, respectively. If $x \in R_o$, then $|x| = n$ whereas if $x \in R_e$, then $|x| = 2$. In this research, H is a subgroup of G where H is a cyclic subgroup. Therefore, $H = \langle e \rangle, \langle a \rangle, \langle b \rangle, \langle ab \rangle, \ldots, \langle a^{n-1}b \rangle$. The relative coprime probability of D_n, where $n \geq 3$ and an odd prime is discussed.

Proposition 2

Let G be dihedral group, D_n, where $n \geq 3$ and an odd prime and H be a cyclic subgroup of G. If the order of H of G is 1, then the relative coprime probability, $P_{copr}(H,G) = 1$.

Proof

Suppose $W = \{(h,g) \in H \times G : (|h|,|g|) = 1, h \in H, g \in G\}$. Let $|H| = 1$, then $H = \langle e \rangle = \{e\}$. So, for $e \in H$ and $\forall g \in G$ then $\gcd(|e|,|g|) = 1$.

Therefore,

$$W = \{(e,g) \in H \times G : (|e|,|g|) = 1\}.$$

Hence,

$$\begin{aligned} P_{copr}(H,G) &= \frac{|W|}{|H||G|} \\ &= \frac{2n}{1\times 2n} \\ &= 1. \end{aligned}$$

Proposition 3

Let G be dihedral group, D_n, where $n \geq 3$ and an odd prime and H be a cyclic subgroup of G. If the order of H of G is 2, then the relative coprime probability, $P_{copr}(H,G) = 3/4$.

Proof

Suppose $W = \{(h,g) \in H \times G : (|h|,|g|) = 1, h \in H, g \in G\}$. Let $|H| = 2$, then $H = \{h_1, h_2\}$. Below are the cases that should be considered in order to find the relative coprime probability for D_n.

Case 1:

For $h_1 \in H$

Let $h_1 = e$ where $|h_1| = 1$ and $\forall g \in G$ then $\gcd(|e|,|g|) = 1$. Suppose $W_a = \{(e,g) \in H \times G : (|e|,|g|) = 1\}$. So, $|W_a| = 2n$.

Case 2:

For $h_2 \in H$

Let $h_2 \in H \setminus e$ and $|h_2| = 2$. For $\forall g \in G,\ g$ is separated to $g = e,\ g \in R_o$ and $g \in R_e$. Below are the cases that need to be considered.

1. If $g = e,$ then $|g| = 1.$ So, $\gcd(|h_2|,|e|) = \gcd(2,1) = 1.$ Therefore, $W_b = \{(h_2,e) \in H \times G : (|h_2|,|e|) = 1\}$. Hence, $|W_b| = 1$.
2. If $g \in R_o$ then $|g| = n.$ This implies that $\gcd(|h_2|,|g|) = \gcd(2,n) = 1.$ So, $W_c = \{(h_2,g) \in H \times G : (|h_2|,|g|) = 1\}$. Hence, $|W_c| = n-1$.
3. If $g \in R_e$ then $|g| = 2.$ This implies that $\gcd(|h_2|,|g|) = \gcd(2,2) = 2.$ Therefore, h and g are not relative coprime.

Hence,

$$\begin{aligned} P_{copr}(H,G) &= \frac{W}{|H||G|} \\ &= \frac{|W_a| + |W_b| + |W_c|}{|H||G|} \\ &= \frac{(2n) + (1) + (n-1)}{2 \times 2n} \\ &= \frac{3}{4}. \end{aligned}$$

Proposition 4

Let G be dihedral group, D_n, where $n \geq 3$ and an odd prime and H be a cyclic subgroup of G. If the order of H of G is n, then the relative coprime probability, $P_{copr}(H,G) = \frac{n^2+2n-1}{2n^2}$.

Proof

Suppose $W = \{(h,g) \in H \times G : (|h|,|g|) = 1, h \in H, g \in G\}$. Let $|H| = n$, then $H = \langle a \rangle = \{h_m : 1 \leq m \leq n\}$. Below are the cases that should be considered in order to find the relative coprime probability for D_n.

Case 1:

Let $h_m = e$ where $|h_m| = 1$ and $\forall g \in G$ then $\gcd(|h_m|,|g|) = \gcd(|e|,|g|) = 1$. Therefore, $W_d = \{(e,g) \in H \times G : (|e|,|g|) = 1\}$. So, $|W_d| = 2n$.

Case 2:

Let $h_m \in H \setminus e$ and $|h_m| = n$. For $\forall g \in G$, g is separated to $g = e$, $g \in R_o$ and $g \in R_e$. Below are the cases that need to be considered.

If $g = e$, then $|g| = 1$. So, $\gcd(|h_m|,|e|) = \gcd(n,1) = 1$. Therefore, $W_f = \{(h_m,e) \in H \times G : (|h_m|,|e|) = 1\}$.

If $g \in R_o$ then $|g| = n$. This implies that $\gcd(|h_m|,|g|) = \gcd(n,n) = n$. Therefore, h and g are not relative coprime.

If $g \in R_e$ then $|g| = 2$. This implies that $\gcd(|h_m|,|g|) = \gcd(n,2) = 1$. So, $W_i = \{(h_m,g) \in H \times G : (|h_m|,|g|) = 1\}$.

The same steps are repeated for each element in $\langle a \rangle = \{h_m : 1 \leq m \leq n\}$ using Case 2.

Hence,

$$
\begin{aligned}
P_{copr}(H,G) &= \frac{W}{|H||G|} \\
&= \frac{n^2+2n-1}{2n^2}.
\end{aligned}
$$

Propositions 2-4 have shown the relative coprime probability for separate values of n. The results are generalized in Theorem 1.

Theorem 1

Let G be dihedral group, D_n, where $n \geq 3$ and an odd prime and H be a cyclic subgroup of G. Then,

$$P_{copr}(H,G)=\begin{cases}1, & ,\text{if } |H|=1,\\ \frac{3}{4}, & ,\text{if } |H|=2,\\ \frac{n^2+2n-1}{2n^2} & ,\text{if } |H|=n.\end{cases}$$

Proof

Let G be dihedral group, D_n, where $n\geq 3$, n be an odd prime number and H be a cyclic subgroups of G. So, $D_n=\langle a,b \mid a^n=e,b^2=e,bab=a^{-1}\rangle=\{e,a,\ldots,a^{n-1},b,ab,\ldots,a^{n-1}b\}$ and the order for each element is $|e|=1$, $|a^m|=n$ for $1\leq m\leq n-1$ and $|a^m b|=2$ for $1\leq m\leq n$. Also, since H is cyclic subgroup of D_n, then $H=\langle e\rangle,\langle a\rangle,\langle b\rangle,\langle ab\rangle,\ldots,\langle a^{n-1}b\rangle$. Now, let $W=\{(h,g)\in H\times G:(|h|,|g|)=1,h\in H,g\in G\}$. Then some cases that needs to be considered in order to find the relative coprime probability are if $h=e$, $h\in H\setminus e$, $g=e$ and $g\in G\setminus e$. Therefore, the relative coprime probability for cyclic subgroups of D_n, where n is odd prime number is determined.

Case 1:

For $|H|=1$, $H=\langle e\rangle=\{e\}$. Then, by Proposition 2,

$$P_{copr}(H,G)=1.$$

Case 2:

For $|H|=2$, $H=\langle b\rangle,\langle ab\rangle,\ldots,\langle a^m b\rangle$ where $1\leq m\leq n$. Then, by Proposition 3,

$$P_{copr}(H,G)=\frac{3}{4}.$$

Case 3:

For $|H|=n$, $H=\langle a\rangle=\{a^m:1\leq m\leq n\}$. Then, by Proposition 4,

$$P_{copr}(H,G)=\frac{n^2+2n-1}{2n^2}.$$

Next, an example is given to illustrate Theorem 1.

Example 1

Let $G=D_{3.}$. Then,

$$D_{3.}=\langle a,b \mid a^3=b^2=1,bab=a^{-1}\rangle.$$

By referring to Cayley table of D_3, $D_3=\{e,a,a^2,b,ab,a^2b\}$ and the order for each element is $|e|=1$, $|b|=|ab|=|a^2b|=2$, and $|a|=|a^2|=3$. Let H be a cyclic subgroup of G, then

$H = \langle e \rangle, \langle a \rangle, \langle b \rangle, \langle ab \rangle, \langle a^2 b \rangle$ and the order for each H is $|\langle e \rangle| = 1,$ $|\langle a \rangle| = 3,$ and $|\langle b \rangle| = |\langle ab \rangle| = |\langle a^2 b \rangle| = 2.$ Then, the relative coprime probability of D_3 is shown as follows.

Case 1

For $|H| = 1,$ then $H = \langle e \rangle.$ Thus, by Proposition 2,

$$P_{copr}(H, G) = 1.$$

Case 2

For $|H| = 2,$ then $H = \langle b \rangle, \langle ab \rangle, \langle a^2 b \rangle.$ Thus, by Proposition 3, for $H = \langle b \rangle,$

$$P_{copr}(H, G) = 3/4.$$

Same goes when $H = \langle ab \rangle$ and $H = \langle a^2 b \rangle.$

Case 3

If $|H| = 3,$ then $H = \langle a \rangle = \{e, a, a^2\}.$ Thus, by Proposition 4,

$$P_{copr}(H, G) = \frac{3^2 + 2(3) - 1}{2(3)^2} = \frac{7}{9}.$$

4. CONCLUSION

The relative coprime probability for cyclic subgroups of D_n where n is an odd prime is generalized. The result showed that if $|H| = 1$ then $P_{copr}(H, D_n) = 1,$ if $|H| = 2$ then $P_{copr}(H, D_n) = 3/4,$ and if $|H| = n$ then $P_{copr}(H, D_n) = \frac{n^2 + 2n - 1}{2n^2}.$

It is recommended that further research on this matter can be done such as the relative coprime probability for cyclic subgroups of D_n where n is even can be generalized. Apart from that, the relative coprime probability for noncyclic subgroups of D_n can also be obtained.

Reference:

1. Williams J, editor The prime graph components of finite groups. The Santa Cruz Conference on Finite Groups (Univ California, Santa Cruz, Calif, 1979) Proc Sympos Pure Math; 1980.
2. Ma XL, Wei HQ, Yang LY. The coprime graph of a group. International Journal of Group Theory. 2014;3(3):13-23.
3. Mansoori F, Erfanian A, Tolue B, editors. Non-coprime graph of a finite group. AIP Conference Proceedings; 2016: AIP Publishing LLC.
4. Abd Rhani N, Mohd Ali NM, Sarmin NH, Erfanian A. The Co-Prime Probability of p-Groups. Journal of Mathematics & Computing Science. 2019;5(1):53-6.

5. Zulkifli N, Mohd Ali NM. Co-prime Probability for Nonabelian Metabelian Groups of Order Less than 24 and Their Related Graphs. Matematika. 2019;35(3).

6. Zulkifli N, Mohd Ali NM. Co-prime Probability for Nonabelian Metabelian Groups of Order 24 and Their Related Graphs. Discovering Mathematics (Menemui Matematik). 2019;41(2):68-79.

7. Erfanian A, Rezaei R, Lescot P. On the relative commutativity degree of a subgroup of a finite group. Communications in Algebra. 2007;35(12):4183-97.

8. Abdul Hamid M, Mohd Ali NM, Sarmin NH, Abd Manaf FN, editors. Relative commutativity degree of some dihedral groups. AIP Conference Proceedings; 2013: American Institute of Physics.

9. Abu Bakar F, Mohd Ali NM, Abd Rhani N, editors. The relative commutativity degree of noncyclic subgroups of nonabelian metabelian groups of order at most 14. AIP Conference Proceedings; 2017: AIP Publishing LLC.

10. Zulkifli N. Co-prime and relative co-prime probability for nonabelian metabelian groups of order at most 24 with their related graphs. Skudai, Johor: Universiti Teknologi Malaysia; 2019.

11. Dummit DS, Foote RM. Abstract algebra: Wiley Hoboken; 2004.