

RESEARCH ARTICLE

Automorphisms of finite cyclic group for generator of 2

Fatin Hanani Hasan^{1*}, Mohd Sham Mohamad², Yuhani Yusof², Siti Hasanah Jusoo², Mohammed Khalid Shahoodh³ and Ekkasit Sangwisut⁴

¹Tunku Abdul Rahman University of Management and Technology, Pahang Branch, Bandar Indera Mahkota, 25200 Kuantan, Pahang, Malaysia

²Centre for Mathematical Sciences, Universiti Malaysia Pahang Al-Sultan Abdullah, Lebuhr Persiaran Tun Khalil Yaakob, 26300 Kuantan, Pahang, Malaysia

³Ministry of Education, General Directorate of Education in Ramadi, 31001 Ramadi, Iraq

⁴Department of Mathematics and Statistics, Faculty of Science and Digital Innovation, Thaksin University, 93110 Phattalung, Thailand

Abstract - Generators are necessary to justify the creation of the automorphisms for finite cyclic q -group, where q is an odd prime. This study identifies generators of previously unclassified automorphism orders for 2-power cyclic groups. This research begins with an overview of cyclic groups and automorphisms, including the properties, to establish a solid foundation. By analysing the automorphisms, the generators are identified according to their specific order within the 2-power group and presented as the primary finding.

Article History

Received : 6 July 2026
 Revised : 14 August 2026
 Accepted : 7 September 2026
 Published : 30 September 2026

Keywords

Automorphism
 Generator
 Finite cyclic group
 Compatible action
 Number theory

1. Introduction

Generators of finite cyclic q -groups, where q denotes an odd prime, form the foundation for studying their automorphism groups, which in turn are essential for understanding group actions and the formation of the nonabelian tensor product. Brown et al. [1] posed significant open questions that have prompted deeper exploration of the theoretical properties of these groups. Among those who advanced this line of inquiry, Visscher [2] examined the automorphisms of cyclic groups in greater depth. Motivated by this context, the present study addresses an unresolved issue with the nonabelian tensor product for cyclic groups. G , a group that is deemed cyclic in group theory if a singular element solely forms it, $g \in G$, often referred to as the group generator. Hence, the mapping $\rho: g \rightarrow g^t$ gives any automorphism of the group G , with t being an integer with $\gcd(t, q^r) = 1$. Dummit and Foote [3] stated that the cyclic group's automorphisms can be shown as follows,

$$\text{Aut}(G) \cong C_{q-1} \times C_{q^{r-1}} \cong C_{(q-1)(q^{r-1})}, \text{ where } q \text{ represents an odd prime and } r \in \mathbb{N}.$$

Furthermore, the authors observed that the automorphisms of q -power order are isomorphic to the instantaneous multiplication for finite cyclic groups, which indicates that identifying the group generator is an essential requirement for determining the order of automorphisms of a q -group. Brescia and Russo [4] defined a cyclic automorphism as one that ensures the subgroup generated by an element and its image is cyclic. Clark [5] has classified generators into four forms, namely 2 , 4 , q^r , or $2q^r$ with q being an odd prime and $r \in \mathbb{N}$. Meanwhile, Broche et al. [6] classified the finite cyclic groups with 2-generator for prime-power order. Asgharzandeh et al. [7] studied the properties and structure of automorphism groups and their applications to free groups, solvable groups, and graphs.

Mohamad [8] explored the generators for 2-power order, as well as the generators for automorphisms of order q^{r-1} , for q -power order, where q is an odd prime, while Shahoodh [9] extended those results. Mohamad [8] also showed that, for two actions to be compatible, their order must be one of the necessary and sufficient factors. Shahoodh [9] examined the latter part of the instantaneous multiplication of the automorphism group for the q -group, which is C_{q^r-1} , calculated both the number and the sum of its automorphisms, and established that each automorphism group has a unique element of order two. Further exploring automorphism groups, Emery [10] addressed the group of automorphisms for finite groups with small order and several general findings on the automorphisms of cyclic groups. In addition, Soleimani [11] established an indicator for the presence of order-preserving automorphisms and connected these results to finite q -groups, where q is an odd prime. Meanwhile, Hirano et al. [12] introduced the concept of uniform factorizations and developed methods for constructing these factorizations for finite groups, with a particular focus on the order of the group.

Despite these advancements, no complete classification has existed for generators of automorphisms with specific orders in 2-power cyclic groups, a significant gap that this paper addresses. To address this gap, this paper utilises the Groups, Algorithms, and Programming (GAP) Software [13] to compute the number of generators according to their specific order for these groups. Having established the theoretical foundation, the preliminary results on the automorphism are presented in the next section.

2. Methodology

The subsequent theorem describes the structure of the automorphism group of a finite cyclic q -group's of q -power order as the direct product of two finite cyclic groups.

Theorem 2.1

Let q be an odd prime and $r \in \mathbb{N}$. Suppose that G is a cyclic group of order q^r , subsequently $\text{Aut}(G) \cong C_{q-1} \times C_{q^{r-1}} \cong C_{(q-1)q^{r-1}}$, and $|\text{Aut}(G)| = (q-1)q^{r-1}$.

The Euler's φ -function is introduced next, as it determines the number of automorphisms of a finite cyclic group by counting the positive integers not exceeding n that are relatively prime to n . This concept is fundamental to the analysis of automorphism group structures throughout this study.

Definition 2.1 Euler's φ -function

The Euler Phi-function, $\varphi(m)$ is defined as

$$\varphi(m) = |\{k \in \mathbb{Z}: 1 \leq k \leq m, \gcd(k, m) = 1\}|, m \geq 1.$$

Theorem 2.2 explains the order of any given integer, a .

Theorem 2.2

Let z be an integer modulo m with order l and let $h > 0$. Then, the order of z^h is $\left(\frac{1}{\gcd(h, l)}\right)$ modulo m .

The classification of the generators is presented as follows.

Theorem 2.3

Let $n \geq 2$. Then, U_n is cyclic if and only if it has one of the following forms: 2, 4, q^r , or $2q^r$ where q is an odd prime and $r \in \mathbb{N}$.

The following proposition establishes the existence of a unique element of order two in the automorphisms of the finite cyclic q -group.

Proposition 2.1

Every automorphism group of a finite cyclic q -group contains exactly one element of order two.

The Binomial Theorem is recalled below since it is required in several proofs involving powers of group elements and their corresponding automorphisms.

Theorem 2.4 Binomial Theorem

For any integer n and any real numbers x and y ,

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k, \quad (1)$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (2)$$

represents the binomial coefficient.

Fermat's Little Theorem is introduced below. Fermat's Little Theorem is essential to identify the order of elements in cyclic groups. This theorem is particularly useful in proving results related to automorphisms and their properties in this study.

Theorem 2.5 Fermat's Little Theorem

Suppose q is a prime number, and let a be an integer such that q does not divide a . Then, $a^{q-1} \equiv 1 \pmod{q}$.

The findings and discussion on generators, presented in the specific order for the 2-power group, were built upon these preliminary results and are presented in the following section.

3. Results and Discussion

Assume that $n \geq 2$, where U_n is cyclic if and only if it has one of the following forms: 2, 4, q^r , or $2q^r$ where q is an odd prime and $r \in \mathbb{N}$. This study considers only the case in which the generator is 2. Moreover, if an integer z modulo m has order l and $h > 0$, z^h has order $\left(\frac{1}{\gcd(h, l)}\right)$ modulo m . Therefore, the corresponding generators of specific order are presented below.

Table 1. Classification of automorphism group generators by order

Result	Generator	Order
Proposition 3.1	$\rho: g \rightarrow g^{q^r-1}$	2
Theorem 3.1	$\rho: g \rightarrow g^{q-1}$	$2q^{r-1}$
Theorem 3.2	$\rho: g \rightarrow g^{2q^r-1}$	$q-1$
Proposition 3.2	$\rho: g \rightarrow g^2$	$(q-1)(q^{r-1})$
Proposition 3.3	$\rho: g \rightarrow g^d$	dq

In order to prove the preceding statement, we explore various statements, lemmas, and theorems.

Proposition 3.1

Suppose $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$ is a finite cyclic group with q -power order, where q denotes an odd prime and $r \geq 2$. Then, $\rho: g \rightarrow g^{q^r-1}$ is an automorphism of $\text{Aut}(C_{q^r})$ with order 2.

Proof

Consider the automorphism $\rho: g \rightarrow g^{q^r-1}$ of $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$, where $r \geq 2$. Then, $(q^r - 1)^2 = q^{2r} - 2q^r + 1 \equiv 1 \pmod{q^r}$.

Therefore, $\rho: g \rightarrow g^{q^r-1}$ is an automorphism of order 2. ■

The following lemma is required to determine the automorphisms of order $2q^{r-1}$, where q is an odd prime and $r \geq 2$.

Lemma 3.1

Assume that q is an odd prime. Then,

$$(q-1)^{2q^{n-2}} \equiv s_n q^n + 1 - 2q^{n-1},$$

for some integer s_n , where $n \geq 2$.

Proof

Proceed by mathematical induction on n . For the base case, let $n = 2$,

$$(q-1)^{2q^{2-2}} = (q-1)^2 = q^2 - 2q + 1.$$

the statement is true by letting $s_2 = 1$.

Assume the statement holds for some $n \geq 2$. Consider:

$$(q-1)^{2q^{n-2+1}} = ((q-1)^{2q^{n-2}})^q.$$

Applying the inductive hypothesis yields

$$(s_n q^n + 1 - 2q^{n-1})^q.$$

By Theorem 2.4,

$$\begin{aligned} (s_n q^n + 1 - 2q^{n-1})^q &= ((s_n q - 2)q^{n-1} + 1)^q \\ &= ((s_n q - 2)q^{n-1})^q + \binom{q}{1} ((s_n q - 2)q^{n-1})^{q-1} + \dots + \binom{q}{q-1} (s_n q - 2)q^{n-1} + 1 \\ &= Rq^{n+1} + s_n q^{n+1} + 1 - 2q^n \\ &= s_{n+1} q^{n+1} + 1 - 2q^n \end{aligned}$$

where $s_{n+1} = R + s_n$ for some integer R . Thus, the statement holds for $n + 1$. Hence, the statement is valid for every $n \geq 2$. ■

The following lemma is required to determine the automorphisms of order $2q^{r-1}$ where q is an odd prime and $r \geq 2$.

Lemma 3.2

Let q is an odd prime. Then

$$(q-1)^{q^{n-2}} \equiv s_n q^n + q^{n-1} - 1$$

for some integer, s_n where $n \geq 2$.

Proof

Proceed by mathematical induction on n . For the base case, let $n = 2$,

$$(q-1)^{q^{2-2}} = q-1$$

the statement is true by letting $s_2 = 0$.

Assuming the statement is true for some $n \geq 2$. Consider:

$$(q-1)^{q^{n-1+1}} = ((q-1)^{q^{n-1}})^q.$$

Applying the inductive hypothesis yields

$$(s_n q^n + q^{n-1} - 1)^q.$$

Through the application of Theorem 2.4,

$$\begin{aligned} (s_n q^n + q^{n-1} - 1)^q &= ((s_n q + 1)q^{n-1} - 1)^q \\ &= ((s_n q + 1)q^{n-1})^q + \binom{q}{1} ((s_n q + 1)q^{n-1})^{q-1} + \dots + \binom{q}{q-1} (s_n q + 1)q^{n-1} - 1 \\ &= Rq^{n+1} + s_n q^{n+1} + q^n - 1 \\ &= s_{n+1} q^{n+1} + q^n - 1 \end{aligned}$$

where $s_{n+1} = R + s_n$ and R is some integer. Thus, for $n+1 > 2$, the assertion is true. Hence, the statement is valid for every $n \geq 2$. ■

The following theorem states the automorphisms of order $2q^{r-1}$ where q denotes an odd prime and $r \geq 2$.

Theorem 3.1

Let $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$ where q is an odd prime and $r \geq 2$. Then, $\rho: g \rightarrow g^{q^{-1}}$ is an automorphism of $\text{Aut}(C_{q^r})$ with order $2q^{r-1}$.

Proof

By Theorem 2.1, G is a cyclic group of order q^r where q represents an odd prime and $r \geq 2$. Hence, $\text{Aut}(G) \cong C_{q-1} \times C_{q^{r-1}} \cong C_{(q-1)q^{r-1}}$, and $|\text{Aut}(G)| = (q-1)q^{r-1}$. In determining the claim, where ρ is an automorphism of order $2q^{r-1}$, the following condition holds:

- i. $(q-1)^{2q^{r-1}} \equiv 1 \pmod{q^r}$,
- ii. $(q-1)^{q^{r-1}} \not\equiv 1 \pmod{q^r}$.

Lemma 3.1 implies that

$$(q-1)^{2q^{r-1}} \equiv s_{r+1} q^{r+1} + 1 - 2q^r \equiv 1 \pmod{q^r}$$

holds for all $r \geq 2$ Hence, Lemma 3.2 shows that condition (ii) contradicts the existence of a subgroup of order $2q^{r-1}$. Therefore, ρ is an automorphism of order $2q^{r-1}$. ■

The ensuing theorem shows the automorphisms of order $q-1$ where q represents an odd prime.

Theorem 3.2

Let $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$ where q is an odd prime and $r \geq 2$. Then, $\rho: g \rightarrow g^{2q^{r-1}}$ is an automorphism with an order of $q-1$ in $\text{Aut}(C_{q^r})$.

Proof

Theorem 2.1 gives $\text{Aut}(G) \cong C_{q-1} \times C_{q^{r-1}} \cong C_{(q-1)q^{r-1}}$, and $|\text{Aut}(G)| = (q-1)q^{r-1}$. Since $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$, the element 2 serves as a generator of the automorphism group with $(q-1)q^{r-1}$ being the largest possible order of an automorphism. To establish the order of ρ , it is sufficient to show that:

- i. $2^{(q-1)q^{r-1}} \equiv 1 \pmod{q^r}$,
- ii. $2^{\frac{1}{2}(q-1)q^{r-1}} \not\equiv 1 \pmod{q^r}$.

Condition (i) shows that $\rho^{q-1}(g) = g$ which verifies that applying ρ exactly $q-1$ times returns g to itself. For condition (ii), the exponent in the expression is half of the maximum order of the automorphism, which contradicts the subgroup of order $q-1$. Therefore, ρ is an automorphism of order $q-1$. ■

The automorphism of the order $(q-1)q^{r-1}$ is established in the following proposition, where q denotes an odd prime number and $r \geq 2$.

Proposition 3.2

Let $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$ where q is an odd prime and $r \geq 2$. Hence, $\rho: g \rightarrow g^2$ is an automorphism with an order of $(q-1)q^{r-1}$ in $\text{Aut}(C_{q^r})$.

Proof

To determine the order of the automorphism $\rho: g \rightarrow g^2$ for the cyclic group $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$, where q is an odd prime number and $r \geq 2$, the smallest positive integer n needs to be found first, such that $(g^2)^n \equiv g \pmod{q^r}$, which implies that $2^n \equiv 1 \pmod{q^r}$ or similarly, if G is cyclic of order q^r , for $\rho^n(g) = g$ to hold, it needs $2^n \equiv 1 \pmod{q^r}$ to be satisfied.

By Theorem 2.5, $2^{q-1} \equiv 1 \pmod{q}$. As q is an odd prime, q^r has an order $\phi(q^r) = (q-1)q^{r-1}$. For the higher power q^r , the results need to be extended. Therefore, the order of 2 modulo q^r is multiplied by a factor of q^{r-1} due to the additional structure introduced by the higher powers of q . Hence, $2^{(q-1)q^{r-1}} \equiv 1 \pmod{q^r}$.

Since the automorphism $\rho: g \rightarrow g^2$, the smallest n such that $\rho^n(g) = g$ corresponds to finding the smallest n for which $2^n \equiv 1 \pmod{q^r}$. Thus, the order of the automorphism ρ is $(q-1)q^{r-1}$. ■

The following proposition shows the automorphism of order dq , where d represents a unique odd prime divisor of $q-1$, q denotes an odd prime number, and $d < q$.

Proposition 3.3

Let $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$ where q denotes an odd prime number and $r \geq 2$. Then, $\rho: g \rightarrow g^d$ is an automorphism with an order of dq in $\text{Aut}(C_{q^r})$, where d represents a unique odd prime divisor of $q-1$, and $d < q$.

Proof

To determine the order of the automorphism $\rho: g \rightarrow g^d$ for the cyclic group $G = \langle g \rangle \cong C_{q^r} = \langle 2 \rangle$, where q is an odd prime number, $r \geq 2$ and d represents a unique odd prime divisor of $q-1$, and $d < q$, the smallest positive integer n needs to be found first, such that $(g^d)^n \equiv g \pmod{q^r}$, which implies that $d^n \equiv 1 \pmod{q^r}$ or similarly, if G is cyclic of order q^r , for $\rho^n(g) = g$ to hold, it needs $d^n \equiv 1 \pmod{q^r}$ to be satisfied.

Consider d as a unique odd prime divisor of $q-1$, and $d < q$. Given that $d^d \equiv 1 \pmod{q}$. For the higher power q^r , the results need to be extended. Therefore, the order of d modulo q^r is multiplied by a factor of q^{r-1} due to the additional structure introduced by the higher powers of q . Hence, $d^{d(q^{r-1})} \equiv 1 \pmod{q^r}$. While q^{r-1} represents the refined congruence conditions associated with q^r , in the context of automorphisms, this condition simplifies into a linear relationship proportional to q . Thus, $d^{dq} \equiv 1 \pmod{q^r}$.

Since the automorphism $\rho: g \rightarrow g^d$, the smallest n such that $\rho^n(g) = g$ corresponds to finding the smallest n for which $d^n \equiv 1 \pmod{q^r}$. Thus, the order of the automorphism ρ is dq . ■

The following section provides a synopsis of this paper.

4. Conclusions

This paper presents the generators of automorphisms for finite cyclic groups of 2-power orders. It expands previous classifications by offering specific order-based findings, enabling clearer group compatibility analysis. The results contribute to group theory and open avenues for further research in cryptographic structures and cyclic group isomorphisms.

Acknowledgement

All the authors would like to express their gratitude to Universiti Malaysia Pahang Al-Sultan Abdullah for the support.

Funding

This research received no specific grant from any funding agency in the public, private, or not-for-profit sectors.

Declaration of Competing Interest

The authors declare no conflict of interest.

CRediT Authorship Contribution Statement

Fatin Hanani Hasan: Conceptualization; Methodology; Analysis; Data curation; Investigation; Resources; Software; Visualization; Writing - original draft; Project administration

Mohd Sham Mohamad: Supervision; Conceptualization; Validation; Analysis; Writing - review & revise

Yuhani Yusof: Supervision; Conceptualization; Validation; Analysis; Writing - review & revise

Siti Hasanah Jusoo : Writing - review & revise

Mohammed Khalid Shahoodh: Methodology; Validation; Writing - review & revise

Ekkasit Sangwisut: Analysis; Validation; Writing - review & revise

Availability of the Data and Materials

Data sharing does not apply to this article as no new data were created or analysed in this study.

Ethical Declarations

No artificial intelligence tools were used in the preparation of this manuscript. All content was developed manually by the authors. This study did not involve human participants or animals. Ethical approval was therefore not required.

Generative Artificial Intelligence Declarations

The authors have not utilised any AI resources or tools in the preparation of this article.

References

- [1] Brown R, Johnson DL, Robertson DL. Some computations of non-abelian tensor products of groups. *Journal of Algebra*. 1987;111(1):177-202.
- [2] Visscher M. On the nonabelian tensor product of groups. *Proceedings of the American Mathematical Society*. 1998;126(5):1269-77.
- [3] Dummit DS, Foote RM. *Abstract algebra*. 3rd ed. Hoboken (NJ): John Wiley and Sons; 2004.
- [4] Brescia M, Russo A. On groups in which many automorphisms are cyclic. *Mathematics*. 2022;10(2):262.
- [5] Clark WE. *Elementary abstract algebra*. LibreTexts. 2021. Retrieved from [https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Elementary_Abstract_Algebra_\(Clark\);](https://math.libretexts.org/Bookshelves/Abstract_and_Geometric_Algebra/Elementary_Abstract_Algebra_(Clark);) 7 September 2026.
- [6] Asgharzadeh M, Golshani M, Herden D, Shelah S. On groups well represented as automorphism groups of groups. *Journal of Commutative Algebra*. Forthcoming. Retrieved from <https://arxiv.org/abs/2407.09279>; 7 September 2026.
- [7] Mohamad MS. Compatibility conditions and nonabelian tensor products of finite cyclic groups of p-power order. PhD Thesis. Malaysia: Universiti Teknologi Malaysia, 2012.
- [8] Shahoodh MK. Compatible pair of actions for finite cyclic groups of p-power order. PhD Thesis. Malaysia: Universiti Malaysia Pahang, 2018.
- [9] Emery S. About automorphisms of some finite groups. Master's Thesis. USA: West Chester University, 2021.
- [10] Soleimani R. A note on automorphisms of finite p-groups. *Journal of Mathematical Extension*. 2021;15(3):1-9. Retrieved from <https://doi.org/10.30495/JME.2021.1484>; 7 September 2026.
- [11] Hirano Y, Ohtsuka Y, Uenami K. Uniform cyclic group factorizations of finite groups. *Communications in Algebra*. 2023;51(1):1-13.
- [12] GAP Group. GAP—Groups, algorithms, and programming, Version 4.16.0. 2026. Retrieved from <https://www.gap-system.org>; 7 September 2026.