International Journal of Mathematics, Statistics and Operations Research
Volume 1; Number 2; 2021 : pp. 163-167

EULERS TOTIENT FUNCTION AS APPLIED TO FINDING THE NUMBER OF CYCLIC SUBGROUPS OF FINITE *p*-GROUPS

S. A. Adebisi[1] and M. Ogiugo[2]

[1]*Department of Mathematics, Faculty of Science, University of Lagos, Nigeria. Email : adesinasunday@yahoo.com*
[2]*Department of Mathematics, School of Science,Yaba College of Technology, Lagos.*

ARTICLEINFO

Received: 28 August 2021
Revised: 21 October 2021
Accepted: 26 November 2021
Online: 30 December 2021

To cite this paper:
S.A. Adebisi & M. Ogiugo (2021). Eulers Totient Function as Applied to Finding the Number of Cycle Subgroups of Finite *p*-Groups. *International Journal of Mathematics, Statistics and Operations Research.* 1(2): pp. 163-167.

ABSTRACT

Given that §(H) is the partially ordered set of cyclic subgroups of a nite group H. Suppose that A is the class of p-groups whose order is p^n for integer $n > 3$. Dene a map; $\beta : A \to (0; 1]$ by $\beta(H) = \frac{|\S(H)|}{|H|}$. This work in an eort to make investigations on the second minimum and maximum value of β alongside their corresponding minimum and maximum points, applies the eulers totient function as to nding the number of cyclic subgroups of nite p-groups.

Key words and phrases: Finite p-Groups, Cyclic subgroups, Dihedral subgroup, Abelian subgroups, Quaternion group, Semi-dihedral group.

AMS Mathematics Subject Classication 2020: Primary : 20D60. Secondary : 20D15

ORCID of the corresponding author: https://orcid.org/0000-0003-3766-0910.

1. INTRODUCTION

Suppose that A represents the class of p-groups which have order p^n for n an integer and $n \geq 3$. Given a nite group $H \in A$ and let §(H) denote its partially ordered set subgroups which are cyclic. Moreso, let $C_r(H)$ be the number of cyclic subgroups of order p^r in H According to Miller (see [3]-[5]), it has been proved that $C_r(H) \equiv 0 (mod p) \; \forall_r \in \{2, 3, \ldots, n\}$. This happens for every p being odd.

2. THE EULERS φ-FUNCTION

The function φ is called Eulers totient function. Here, if m is an integer such that m is a prime p then, $\varphi(p) = p - 1$.

Denition (Euler's Totient Function)

Euler's Totient Function, denoted φ is the number of integers k in the range $1 \le k \le n \ni = gcd(n, k) = 1$. A closed form of this function is given by

$$\varphi(n) = n\Pi_{prime\ p \ni p|n}\left(1-\frac{1}{p}\right)$$

3. MULTIPLICATIVE PROPERTY

Euler's Totient Function satises the multiplicative property–that is, for m, n relatively prime, $\varphi(mn) = \varphi(m)\varphi(n)$. For Example $\varphi(84) = 84 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right) \times \left(1-\frac{1}{7}\right) = 24$.

Denition: (see [1]) An arithmetic function is any function dened on the set of positive integers. An arithmetic function f is called multiplicative if $f(mn) = f(m)f(n)$ whenever m, $n$are relatively prime.

Theorem: If f is a multiplicative function and suppose that $n = p_1^{a_1}p_1^{a_2}...p_s^{a_s}$ is its prime-power factorization, then $f(n) = f(p_1^{a_1})f(p_1^{a_2})...f(p_s^{a_s})$.

Theorem: Eulers phi function φ is multiplicative implies that if $gcd(m, n) = 1$ then, $\varphi(mn) = \varphi(m)\varphi(n)$.

Theorem: For any prime p, we have that $\varphi(pa) = p^a p^{a-1} = p^{a-1}(p-1) = \left(1-\frac{1}{p}\right)$.

Theorem: For any integer $n > 1$, if $n = p_1^{a_1}p_1^{a_2}...p_s^{a_s}$ is the prime-power factorization then, $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_s}\right) = p_1^{a_1-1}p_1^{a_2-1}...p_s^{a_s-1}(p_1-1)(p_2-1)...(p_s-1)$. Since φ is multiplicative, we get $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_1^{a_2})...\varphi(p_s^{a_s}) = p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a-2}\left(1-\frac{1}{p_2}\right)...p_s^{a_s}\left(1-\frac{1}{p_s}\right) = n\Pi_{p|n})\left(1-\frac{1}{p}\right)$, p ranges over the prime divisors of n

Denition (see[2]): The number of cyclic subgroups of a nite group G can be dened as

$$|\S(G)| = \sum_{g\in G}\frac{1}{\varphi(o(g))} \tag{1}$$

where φ is the Eulers totient function and $o(g)$ is the order of the element g of G.

Theorem (see [2]): Let $H \in A \ni H$ contains a cyclic maximal subgroups. Given that p is not even. Then, H is isomorphic toabelian type $\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}$ or to M_{p^n}. Otherwise, H is isomorphic to $\mathbb{Z}_2\mathbb{Z}_{2^{n-1}}$ or to any of the non-abelian groups lasted below:

1. $M(p^n)$, $n \geq 4$
2. $D_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1 = bab^{-1} = a^{-1}\rangle$
3. $Q_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1, bab^{-1} = a^{2^{n-1}} - 1\rangle$
4. $QD_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1, bab^{-1} = a^{2^{n-2}-1}\rangle$ $n \geq 4$

In [14], the numer of cyclic subgroups of the non-abelian (i) to (iv) was found.

4. STATEMENT OF PROBLEM

By applying (1) above, we show each of the following:

1. $|\S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}| = |\S(M(p^n))| = 2 + (n-1)p$
2. $|\S(D_{2^n})| = n + 2^{n-1}$
3. $|\S(Q_{2^n})| = n + 2^{n-2}$
4. $|\S(QD_{2^n})| = n + 3{:}2^{n-3}$

Proof of The Results:

5. The abelian type $|\S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}|$ and the modular group

$$|\S(M(P^n))| = 2 + (n-1)p$$

Proof:

$$|\S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}| = \varphi(1) + (p^2 - 1)\cdot\left(\frac{1}{\varphi(p)}\right) + (p^3p^2)\cdot\left(\frac{1}{\varphi(p^2)}\right) + (p^4p^3)\cdot\left(\frac{1}{\varphi(p^3)}\right)$$

$$+ (p^5p^4)\cdot\left(\frac{1}{\varphi(p^4)}\right) + \ldots + (p^np^{n-1})\cdot\left(\frac{1}{\varphi(p^{n-1})}\right)$$

$$= 1 + (p^21)\cdot\left(\frac{1}{(p-1)} + p + p + p + p + p + \ldots + p(n-2) \text{ times}\right)$$

$$= 1 + (p+1)(p-1)\cdot\left(\frac{1}{(p-1)}\right) + (n-2)p = 1 + p + 1 + (n-2)p$$

$$= 2 + (n-1)p$$

6. The Dihedral group $|\S(D_{2^n})| = n + 2^{n-1}$

Proof:

Since $D_{2^n} = \langle a, b | a^{2n-1} = b^2 = 1 = bab^{-1} = a^{-1} \rangle$,

we have that $D_{2^n} = \{1, a, a^2, a^3, \ldots a^{-1+2^{n-1}}, b, ba, ba^2, \ldots, ba^{1+2^{n-1}}\}$.

Now, $a^{n-1} = b^2 = 1$, there exists 2^{n-1} elements of the form a^m, where $m = 2^{n-1}$. We have one of order 2, 2^{m-1} of order m. The remaining 2^{n-1} elements are of order 2 each. We have $\varphi(2) = 1$. Hence, we have $|\S(D_{2^n})| = 2^{n-1} + k$. To find k. For the highest order 2^{n-1}, there are 2^{n-2} of them, followed by the order 2^{n-2}, there are 2^{n-3} of them, and following this order, we have 2^{n-t} of order 2^{n-t+1}. By this analysis, we have,

$$|\S(D^{2^n})| = 2^{n-1} + 2^{n-2}\cdot\left(\frac{1}{\varphi(n-1)}\right) + 2^{n-3}\cdot\left(\frac{1}{\varphi(n-2)}\right) + 2^{n-4}\cdot\left(\frac{1}{\varphi(n-3)}\right)$$

$$+ 2^{n-5}\cdot\left(\frac{1}{\varphi(n-4)}\right) + \ldots + 2^3\cdot\left(\frac{1}{\varphi(16)}\right) + 2^2\cdot\left(\frac{1}{\varphi(8)}\right) + 2\cdot\left(\frac{1}{\varphi(4)}\right)$$

$$+ 1\cdot\left(\frac{1}{\varphi(2)}\right) 2^{n-1} + 2^{n-2}\cdot\left(\frac{1}{2^{n-1}}\cdot\frac{1}{2}\right) + 2^{n-3}\cdot\left(\frac{1}{2^{n-2}}\cdot\frac{1}{2}\right) + 2^{n-4}\cdot\left(\frac{1}{2^{n-3}}\cdot\frac{1}{2}\right)$$

$$+ 2^{n-5}\cdot\left(\frac{1}{2^{n-4}}\cdot\frac{1}{2}\right) + \ldots + 2^3\cdot\left(\frac{1}{16}\cdot\frac{1}{2}\right) + 2^2\cdot\left(\frac{1}{8}\cdot\frac{1}{2}\right) + 2\cdot\left(\frac{1}{4}\cdot\frac{1}{2}\right)$$

$$+ 1\cdot\left(\frac{1}{2}\cdot\frac{1}{2}\right)$$

$= 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + \ldots + 1$ in n places.

$= 2^{n-1} + n$

7. The Quaternion Group $|\S(Q_{2^n})| = n + 2^{n-2}$

Proof :

$$|\S(Q_{2n})| = \varphi(1) + \cdot\left(\frac{1}{\varphi(2)}\right) + (2 + 2^{n-1})\cdot\left(\frac{1}{\varphi(2^2)}\right) + (2^2)\cdot\left(\frac{1}{\varphi(2^3)}\right) + (2^3)\cdot\left(\frac{1}{\varphi(2^4)}\right)$$

$$+ \ldots + (2^{n-2})\cdot\left(\frac{1}{\varphi(2^{n-1})}\right)$$

$= 1 + 1 + (2 + 2^{n-1})\cdot\left(\frac{1}{2}\right) + 1 + 1 + 1 + 1 + 1 + 1(n-3)$ times

$= 2 + 2^{n-2} + 1 + n - 3$

$= n + 2^{n-2}$

8. The Quasidihedral Group $|\S(QD_{2^n})| = n + 3.2^{n-3}$

Proof:

$$|\S(QD_{2^n})| = \varphi(1) + (1 + 2^{n-2})\cdot\left(\frac{1}{\varphi(2)}\right) + (2 + 2^{n-2})\cdot\left(\frac{1}{\varphi(2^2)}\right) + (2^2)\cdot\left(\frac{1}{\varphi(2^3)}\right)$$

$$+ (2^3)\cdot\left(\frac{1}{\varphi(2^4)}\right) + (2^4)\cdot\left(\frac{1}{\varphi(2^5)}\right) + \ldots + (2^{n-2})\cdot\left(\frac{1}{\varphi(2^{n-1})}\right)$$

$$= 1 + (1 + 2^{n-2})(1) + (2 + 2^{n-2})\cdot\left(\frac{1}{2}\right) + (2^2)\cdot\left(\frac{1}{8\left(\frac{1}{2}\right)}\right) + (2^3)\cdot\left(\frac{1}{2^4\left(\frac{1}{2}\right)}\right)$$

$$+ (2^4)\cdot\left(\frac{1}{2^5\left(\frac{1}{2}\right)}\right) + (2^5)\cdot\left(\frac{1}{2^6\left(\frac{1}{2}\right)}\right) + \ldots + (2^{n-2})\cdot\left(\frac{1}{2^{n-2}\left(\frac{1}{2}\right)}\right)$$

$$= 3 + 2^{n-2} + 2^{n-3} + 1 + 1 + 1 + 1 + 1 + 1(n-3) \text{ times}$$

$$= 3 + 2^{n-2} + 2^{n-3} + n - 3$$

$$= n + 2^{n-2} + 2^{n-3}$$

$$= n + 2^{n-3}(2 + 1)$$

$$= n + 3\cdot 2^{n-3}$$

References

1. Annie Xu and Emily Zhu Euler's Totient Function and More! Number Theory September 18, 2016)
2. Lazorec M., Rulin S. and Marius T. (2020) 2nd minimum/maximum value of the no. of cyclic subgroups of nite *p*-groups. arXiv:2001.10521v1[math.GR]
3. Miller G.A. An extension of Sylow's theorem, Proc. London Math. Soc. (2) 2 (1905). 142-143 4 S. A. ADEBISI1 AND M. OGIUGO 2
4. Qu, H., Finite non-elementary abelian *p*-groups whose number of sub-groups is maximal, Israel J. Math. 195 (2013) 773-781.
5. Richard I.M., A remark on the number of cyclic subgroups of a nite group, Amer. Math. Monthly 91 (1984), no.9, 571-572