The Euler's Totient Function and the General Group Theory

[1]S. A. Adebisi*, [2]M. Ogiugo

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

Abstract

Euler's totient function is useful in many ways. It is used in the encryption systems (such as the RSA), which is used for security purposes. The function deals with the prime number theory, and it is useful in the calculation of large calculations also. In this paper, efforts are intensified to calculate the number of distinct cyclic subgroups for a class of finite p-groups.

Keywords: Eulers totient function, Cyclic subgroups, Dihedral subgroup, Abelian subgroups, Quaternion group, Semi-dihedral group.

Introduction

Euler introduced this function in 1763. Initially, Euler used the Greek π for denotation of the function, but because of some issues, his denotation of Greek π didn't get the recognition. And he failed to give it the proper notation sign i.e., ϕ. Hence the function cannot be introduced. Further, ϕ was taken from the Gauss's 1801 Disquisitiones Arithmeticae. The function is also termed as phi function. But J. J. Sylvester, in 1879, included the term totient for this function because of properties and the uses of the functions. The different rules are framed to deal with different kinds of integers given like if integer p is a prime number, then which rule to be applied, etc. all the rules are framed by Euler are practicable and can be used even today while dealing with the same, (please see [1 - 18]). Euler's totient function is useful in many ways. It is used in the RSA encryption system, which is used for security purposes. The function deals with the prime number theory, and it is useful in the calculation of large calculations also. The function is also used in algebraic calculations and elementary numbers. The symbol used to denote the function is ϕ, and it is also called a phi function. The function consists of more theoretical use rather than practical use. The practical use of the function is limited. The function can be better understood through the various practical examples rather than only theoretical explanations. There are various rules for calculating the Euler's totient function, and for different numbers, different rules are to be applied. The function was first introduced in 1763, but because of some issues, it got recognition in 1784, and the name was modified in 1879. The function is a universal function and can be applied everywhere.To know how many prime numbers are coming up to the given integer n Euler's Totient Function is used. It is also called an arithmetic function. For an application or use of Euler's Totient function, two things are important. One is that the gcd formed from given integer n should be multiplicative to each other, and the other is the numbers of gcd should be the prime numbers only. The integer n in this case should be more than 1. From a negative integer, it is not possible to calculate the Euler's Totient Function. The principle, in this case, is that for $\phi(n)$, the multiplicators called m and n should be greater than 1. Hence denoted by $1 < m < n$ and gcd (m, n) = 1. Sign ϕ is the sign used to denote Totient Function.

The Euler's φ-function

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

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

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

Multiplicative Property

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

Definition 2: (see [19]) An arithmetic function is any function defined 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 1: If f is a multiplicative function and suppose that $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is its prime-power factorization, then $f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_s^{a_s})$.

Theorem 2: Euler's phi function $\varphi$is multiplicative implies that if $gcd(m, n) = 1$ then,$\varphi(mn) = \varphi(m)\varphi(n)$

Theorem 3: For any prime p, we have that $\varphi(p^a) = p^{a\smile}p^{a-1} = p^{a-1}(p - 1) = p^a(1 - \frac{1}{p})$

Theorem 4: For any integer $n > 1$, if $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ is the prime-power
factorization then,$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_s})$
$= p_1^{a_1-1} p_2^{a_2-1} \cdots p_s^{a_s-1}(p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$.Since φ is multiplicative,
we get $\varphi(n) = \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_s^{a_s}) = p_1^{a_1}(1 - \frac{1}{p_1})p_2^{a-2}(1 - \frac{1}{p_2}) \cdots p_s^{a_s}(1 - \frac{1}{p_s})$
$= n\Pi_{p|n})(1 - \frac{1}{p})$, p ranges over the prime divisors of n

Definition 3 (see[20]) : The number of cyclic subgroups of a finite group G can be defined as

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

where φ is the Euler's totient function and $o(g)$ is the order of the element g of G

Theorem 5 (see [20]) : 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 $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-1}}$ or to any of the non-abelian groups lasted below:

[i] $M(p^n), n \geq 4$

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

[iii] $Q_{2^n} = \langle a, b | a^{2^{n-1}} = b^4 = 1, bab^{-1} = a^{2^{n-1}-1} \rangle$

[iv] $QD_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1, bab^{-1} = a^{2^{n-2}-1} \rangle, n \geq 4$

Already, the numer of cyclic subgroups of the non-abelian (i) to (iv) were known.

[i] $|\S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}| = |\S(M(p^n))| = 2 + (n-1)p$

[ii] $|\S(D_{2^n})| = n + 2^{n-1}$

[iii] $|\S(Q_{2^n})| = n + 2^{n-2}$

[iv] $|\S(QD_{2^n})| = n + 3.2^{n-3}$

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 :

$|\S(\mathbb{Z}_p \times \mathbb{Z}_{p^{n-1}}| = \varphi(1) + (p^2-1).(\frac{1}{\varphi(p)}) + (p^{3\smile}p^2).(\frac{1}{\varphi(p^2)}) + (p^{4\smile}p^3).(\frac{1}{\varphi(p^3)}) + (p^{5\smile}p^4).(\frac{1}{\varphi(p^4)})$
$+ \cdots + (p^{n\smile}p^{n-1}).(\frac{1}{\varphi(p^{n-1})}) = 1 + (p^{2\smile}1).(\frac{1}{(p-1)} + p + p + p + p + p + \cdots + p(n-2) times)$
$= 1 + (p+1)(p-1).(\frac{1}{(p-1)}) + (n-2)p = 1 + p + 1 + (n-2)p = 2 + (n-1)p$

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

Proof :

Since $D_{2^n} = \langle a, b | a^{2^{n-1}} = b^2 = 1 = bab^{-1} = a^{-1} \rangle$,
we have that $D_{2^n} = \{1, a, a^2, a^3, \cdots a^{-1+2^{n-1}}, b, ba, ba^2, \cdots, ba^{-1+2^{n-1}}\}$.

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, $|\S(D_{2^n})| = 2^{n-1} + 2^{n-2}.(\frac{1}{\varphi(n-1)}) + 2^{n-3}.(\frac{1}{\varphi(n-2)}) + 2^{n-4}.(\frac{1}{\varphi(n-3)})$ $+ 2^{n-5}.(\frac{1}{\varphi(n-4)}) + \cdots + 2^3.(\frac{1}{\varphi(16)}) + 2^2.(\frac{1}{\varphi(8)}) + 2.(\frac{1}{\varphi(4)}) + 1.(\frac{1}{\varphi(2)})2^{n-1} + 2^{n-2}.(\frac{1}{2^{n-1}}.\frac{1}{2})$ $+ 2^{n-3}.(\frac{1}{2^{n-2}}.\frac{1}{2}) + 2^{n-4}.(\frac{1}{2^{n-3}}.\frac{1}{2}) + 2^{n-5}.(\frac{1}{2^{n-4}}.\frac{1}{2}) + \cdots + 2^3.(\frac{1}{16}.\frac{1}{2}) + 2^2.(\frac{1}{8}.\frac{1}{2})$ $+ 2.(\frac{1}{4}.\frac{1}{2}) + 1.(\frac{1}{2}.\frac{1}{2}) = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + \cdots + 1$ in n places. $= 2^{n-1} + n$

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

Proof :

$|\S(Q_{2^n})| = \varphi(1) + .(\frac{1}{\varphi(2)}) + (2 + 2^{n-1}).(\frac{1}{\varphi(2^2)}) + (2^2).(\frac{1}{\varphi(2^3)}) + (2^3).(\frac{1}{\varphi(2^4)}) + (2^4).(\frac{1}{\varphi(2^5)})$
$+ \cdots + (2^{n-2}).(\frac{1}{\varphi(2^{n-1})}) = 1 + 1 + (2 + 2^{n-1}).(\frac{1}{2}) + 1 + 1 + 1 + 1 + 1 + 1(n-3)times$
$= 2 + 2^{n-2} + 1 + n - 3 = n + 2^{n-2}$

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

Proof :

$|\S(QD_{2^n})| = \varphi(1) + (1 + 2^{n-2}).(\frac{1}{\varphi(2)}) + (2 + 2^{n-2}).(\frac{1}{\varphi(2^2)}) + (2^2).(\frac{1}{\varphi(2^3)}) + (2^3).(\frac{1}{\varphi(2^4)})$
$+ (2^4).(\frac{1}{\varphi(2^5)}) + \cdots + (2^{n-2}).(\frac{1}{\varphi(2^{n-1})}) = 1 + (1 + 2^{n-2})(1) + (2 + 2^{n-2}).(\frac{1}{2})$
$+ (2^2).(\frac{1}{8(\frac{1}{2})}) + (2^3).(\frac{1}{2^4(\frac{1}{2})}) + (2^4).(\frac{1}{2^5(\frac{1}{2})}) + (2^5).(\frac{1}{2^6(\frac{1}{2})}) + \cdots + (2^{n-2}).(\frac{1}{2^{n-1}(\frac{1}{2})})$
$= 3 + 2^{n-2} + 2^{n-3} + 1 + 1 + 1 + 1 + 1 + 1(n-3)times$
$= 3 + 2^{n-2} + 2^{n-3} + n - 3 = n + 2^{n-2} + 2^{n-3} = n + 2^{n-3}(2 + 1) = n + 3.2^{n-3}$ □

Some Other Applications of The Euler's Totient Functions

There are many other areas where the concept of the Euler's totient functions are very applicable (please see [10 - 20]): The function is in applications in the elementary number theory. It can be applied to the prime numbers theory, and in large calculations.. For the purpose of defining the RSA encryption system which is applied for internet security encryption, the function is used.

References

[1] Y.G. Chen and H. Tian, Diophantine equations involving Euler's totient function, in Acta Arithmetica 191 (2019) 33–65.

[2] H. Bai, Diophantine equations involving Euler function, in arXiv preprint arXiv:2001.08246 (2020).

[3] Qu, H., Finite non-elementary abelian p-groups whose number of subgroups is maximal, Israel J. Math. 195 (2013) 773-781.

[4] Miller G.A. An extension of Sylow's theorem, Proc. London Math. Soc. (2) 2 (1905). 142-143

[5] Richard I.M., A remark on the number of cyclic subgroups of a finite group, Amer. Math. Monthly 91 (1984), no.9, 571-572

[6] B. Faye and F. Luca, On the equation $\phi(X^m - 1) = X^n - 1$, International Journal of Number Theory 11(05) (2015) 1691–1700.

[7] M.T. Damir, B. Faye, F. Luca and A. Tall, Members of Lucas sequences whose Euler function is a power of 2, Fibonacci Quarterly 52(1) (2014) 3–9.

[8] B. Faye, F. Luca and A. Tall, On the equation $\phi(5^m - 1) = 5^n - 1$, in Bulletin of the Korean Mathematical Society 52(2) (2015) 513–524.

[9] B. Faye and F. Luca, Pell numbers whose Euler function is a Pell number, in Publications de l'Institut Mathematique 101(115) (2017) 231–245.

[10] F. Luca, Arithmetic functions of Fibonacci numbers, in Fibonacci Quarterly 41(4) (2003) 382–384.

[11] F. Luca, Euler indicators of binary recurrence sequences, in Collectanea Mathematica (2002) 133–156.

[12] F. Luca, Multiply perfect numbers in Lucas sequences with odd parameters, in Publicationes Mathematicae-Debrecen 58(1-2) (2001) 121–155.

[13] F. Luca, On the Euler function of repdigits, in Czechoslovak Mathematical Journal 58(1) (2008) 51–59.

[14] F. Luca and B. De Weger, $\sigma_k(F_m) = F_n$, in New Zealand J. Math 40 (2010) 1–13.

[15] F. Luca and F. Nicolae, $\phi(F_m) = F_n$, in Integers 9 (2009) A30.

[16] F. Luca and P. Stanica, The Euler Function of Fibonacci and Lucas Numbers and Factorials, in Naval Postgraduate School Monterey CA Dept of Applied Mathematics (2013)

[17] J.C. Saunders, Diophantine equations involving the Euler totient function, in Journal of Number Theory 209 (2020) 347–358.

[18] Lazorec M., Rulin S.& Marius T. (2020) 2nd minimum/maximum value of the no. of cyclic subgroups of finite p-groups. arXiv:2001.10521v1[math.GR]

[19] Annie Xu and Emily Zhu Euler's Totient Function and More Number Theory September 18, 2016.

[20] J.C. Saunders, The Euler Totient Function on Lucas Sequences
Arxiv:2110.04247v3[math.NT]25 Oct., 2021