American Journal of Mathematics and Statistics 2017, 7(4): 166-168
DOI: 10.5923/j.ajms.20170704.04

Exhibition of Normal Distribution in Finite *p*-groups

Adebisi Sunday Adesina*, Michael Enioluwafe

Department of Mathematics, University of Ibadan, Ibadan, Nigeria

Abstract Suppose that *G* is a group of order p^m and $n \le m$. Let $S_n(G)$ be the number of subgroups of order p^n in *G*. Then, the number of subgroups of order p^n is normally distributed with respect to *n*, where n is a positive integer.

Keywords *p*-groups, Hall's enumeration principle, Elementary abelian group, Trivial subgroup, Symmetric distribution

1. Introduction

Finite *p*-groups are ideal objects for combinatorial and cohomological investigations. Some of its basic properties were proved by Sylow, Frobenius, and Burnside. But, namely, Philip Hall (1904-1982) laid the foundations of modern *p*-group theory (Ber. Y [10]). Normally, Blackburn also made very outstanding achievements after Hall. A common method of investigation in algebra is to break up a complex structure into simpler substructures. The hope is that by repeated application of this procedure, one will eventually arrive at structures that are easy to understand. It may then be possible, in some sense, to synthesis these substructures, so as to reconstruct the original one. While it is rare for the procedure just described to be brought to such a perfect state of completion, the analytic synthetic method can yield valuable information and suggest new concepts. Group theory in general, considers how far this can be used. (Kurosh A.G., 1960) [12]. In this work we examine the basic properties of any *p*-group which put them in categories and hence define the individual and general characterisations.

The hall enumeration principle [10] paves way for counting the subgroups of given structures.

Definition: Let *p* be a prime. A group *G* is said to be a *p*-group if the order of every element of G is a power of *p*. A group which is finite is a *p*-group if and only if the order of G is a power of *p*.

Remark: (Kuk A.) [13] Let *G* be a group of order *m*, and let *p* be a prime. If p^d is the highest power of *p* which divides *m*, where *d* is an integer, then the subgroup of order p^d is called a sylow *p*-subgroup of *G*.

* Corresponding author:
adesinasunday@yahoo.com (Adebisi Sunday Adesina)
Published online at http://journal.sapub.org/ajms

Definition: Elementary Abelian Group: Let *G* be a *p*-group. If G is abelian and all its elements (with the exception of the identity) have order *p*; then, the order of *G*, $|G| = p^m$ for some $m \in \mathbb{N}$. In this case, *G* is a direct product of *m* groups of order *p*. We then say that *G* is an elementary abelian *p*-group.

Remark: Two elementary abelian *p*-groups of the same order p^m are isomorphic [Ber.Y].

We denote such group by E_{p^m} and call it the elementary abelian *p*-group.

Let $E = E_{p^m}$ be the elementary abelian group of order p^m, $0 \le n \le m$. (see [7], [8], [9]).

Set $\gamma_n^m = S_n(E)$.

Let $m \ge n$. Then the following assertions are true (see [10], [11]):

(a) $\gamma_n^m = \dfrac{(p^m - 1)\cdots(p^m - p^{n-1})}{(p^n - 1)\cdots(p^n - p^{n-1})}$

(b) $\gamma_n^m = \gamma_{m-n}^m$

(c) $\gamma_n^{m+1} = \gamma_n^m + p^{m-n+1} \cdot \gamma_{n-1}^m$ for $1 \le n \le m$

(d) $\gamma_{m-1}^m = 1 + p + \cdots + p^{m-1}$

(e) If $m > 2$, then $\gamma_{m-2}^m \equiv 1 + p (\bmod p^2)$.

Main Result

The number of subgroups of order p^n in a finite *p*-group of order p^m is normally distributed with respect to the positive integer $n \le m$.

Hence, by defining a probability function on *G*, assuming that the area under the graph is a unit, it is possible to estimate the number of subgroups of *G*.

This is one of the main objectives of studying the modern finite *p*-groups.

2. Proof of Results

Definition: Suppose that G is any group such that $e \in G$ is the identity, then $H_1 = G$ and $H_2 = \{e\}$ are both subgroups of G called the trivial subgroups of G.

By computation, from (a) above, considering simple even and odd cases (for m = 4 & m = 5 respectfully), we have that:

(1) For m = 4, $\gamma_0^4 = 1$, the trivial subgroup of G (the identity).

$$\gamma_1^4 = \frac{p^4-1}{p-1} = p^3+p^2+p+1,$$

$$\gamma_2^4 = \frac{(p^4-1)(p^4-p)}{(p^2-1)(p^2-p)} = (p^2+1)(p^2+p+1),$$

$$\gamma_3^4 = \frac{p^4-1}{p-1} = (p+1)(p^2+1) = p^3+p^2+p+1,$$

$\gamma_4^4 = 1$, the trivial subgroup G

(2) For m = 5

$$\gamma_0^5 = 1$$

$$\gamma_1^5 = \frac{p^5-1}{p-1} = p^4+p^3+p^2+1$$

$$\gamma_2^5 = \frac{(p^5-1)(p^4-1)}{(p^2-1)(p-1)} = (p^2+1)(p^4+p^3+p^2+p+1)$$

$$\gamma_3^5 = \frac{(p^5-1)(p^5-p)(p^5-p^2)}{(p^3-1)(p^3-p)(p^3-p^2)} = (p^2+1)(p^4+p^3+p^2+p+1)$$

$$\gamma_4^5 = \frac{p^5-1}{p-1} = p^4+p^3+p^2+p+1$$

and $\gamma_5^5 = 1$

Note here that for m = 4,

$\gamma_0^4 = \gamma_4^4 = 1.$

$\gamma_1^4 = \gamma_3^4 = p^3+p^2+p+1$

and

$\gamma_2^4 = (p+1)(p^2+1) = p^3+p^2+p+1$

And, for m = 5, we have that

$\gamma_0^5 = \gamma_5^5 = 1,$

$\gamma_1^5 = \gamma_4^5 = p^4+p^3+p^2+p+1$

and

$\gamma_2^5 = \gamma_3^5 = (p^2+1)(p^4+p^3+p^2+p+1).$

Given that, for $m > n$

$$\gamma_n^m = \frac{(p^m-1)\cdots(p^m-p^{n-1})}{(p^n-1)\cdots(p^n-p^{n-1})}$$

where

$$\gamma_n^m = \gamma_{m-n}^m = \frac{(p^m-1)(p^{m-1}-1)(p^{m-2}-1)(p^{m-3}-1)\cdots(p^{m-n+1}-1)}{(p^n-1)(p^{n-1}-1)(p^{n-2}-1)(p^{n-3}-1)\cdots(p-1)}$$

for $n \le m-n$.

Consider the case:

$$\gamma_4^{10} = \frac{(p^{10}-1)(p^9-1)(p^8-1)(p^7-1)}{(p^4-1)(p^3-1)(p^2-1)(p-1)} = \gamma_6^{10}$$

Observe that as n increases from the left (from below), S_n increases to a maximum value at the middle.

Also, as n decreases from the right (from above), S_n increases in value to the same maximum at the middle. This is seen from the simple computation that:

$$\gamma_0^m = \gamma_m^m,\ \gamma_1^m = \gamma_{m-1}^m,$$

$$\gamma_2^m = \gamma_{m-2}^m, \cdots, \gamma_{\frac{1}{2}(m+1)}^m = \gamma_{\frac{1}{2}(m+2)}^m \quad \text{for even } m$$

or $\cdots \gamma_{\frac{1}{2}(m-1)}^m = \gamma_{\frac{1}{2}(m+1)}^m$ for odd m.

Hence, we have the following:

Proposition: The limit of S_n as n increases from below is maximum at $n = \frac{1}{2}m$ for even m and at $n = \frac{1}{2}(m-1)$ or $\frac{1}{2}(m+1)$ for odd m and we write:

$$\lim_{n\downarrow n_0} S_n \to \max \leftarrow \lim_{n\uparrow n_0} S_n$$

Moreover,

$$\sum_{n=0}^{\frac{1}{2}(m-2)=t-1} \gamma_n^m = \sum_{n=\frac{1}{2}(m+2)=t+1}^{m=2t} \gamma_n^m,\ m = 2t,\ t \in \mathbb{N}.$$

and

$$\sum_{n=0}^{\frac{1}{2}(m-1)=t} \gamma_n^m = \sum_{n=\frac{1}{2}(m+1)=t+1}^{m=2t+1} \gamma_n^m,\ m = 2t+1,\ t \in \mathbb{N}.$$

This is a symmetric property.

In particular, when m is odd, we ague that γ_n^m is normally distributed with n, leading to the normal distribution curve.

Where the area under the curve indicates the number of subgroups of order ρ^n.

REFERENCES

[1] Blackburn, N. (1957). On prime power groups in which the derived group has two generators. Proc. Cam. Phil. Soc. 53 (19-27).

[2] Blackburn, N. (1958). On a special class of *p*-groups. Acta Math. 100 (45-92).

[3] Blackburn, N. (1961). Generalizations of certain elementary theorems on *p*-groups, Proc. Lond. Math. Soc. 11 (1-22).

[4] Blackburn, N. (1966). Automorphisms of finite *p*-groups. J. Algebra 3 (28-29).

[5] Blackburn, N. (1973). Note on a paper of Berkovich. J. Algebra 24 (323-334).

[6] Hall, P. (1933). A contribution to the Theory of groups of prime power order. Proc. Lond. Math. Soc. 36 (29-95).

[7] Hall, P. (1940). The classification of prime power groups. J. reine angew Math. 182 (130-141).

[8] Hall, M. (1959). The Theory of Groups Macmillan, New York.

[9] Hall, M. and Senior J.K. (1964). On Groups of order 2^n, ($n \leq 6$). Macmillan, New York.

[10] Yakov Berkovich (2008). Groups of prime power order vol. 1. Walter de Gruyter. GmbH & Co. KG, 10785 Berlin, Germany.

[11] Yakov Berkovich (2005). Alternate proofs of some basic theorems of finite group theory. Glass. Mat. 40, no. 2, (207-233).

[12] Kurosh A. G (1960). The theory of groups. Chelsea Publishing Company.

[13] Kuku A.O. (1992). Abstract Algebra .Ibadan University Press.