International Journal of Scientific & Engineering Research Volume 8, Issue 10, October-2017
ISSN 2229-5518

ON THE NUMBER OF SOLUTIONS OF EQUATION $X^n = 1$

ADEBISI, S.A.

ABSTRACT. The number of solutions of the monomial given by $x^n = 1$ forms a group $\mathbb{A}$ say. Thus, let $x = f(n,k)$ be a solution. There exist stochastic differential equations involving $\frac{\partial x}{\partial k}$ and $\frac{\partial x}{\partial n}$ of which the solution has a place and is applicable to the Mckendrick-von Foerster equation, where $n \in \mathbb{Z}\backslash 0$ and $k \in \mathbb{R}$. Moreover, for any equation of second degree, the number of solutions in the function forms a group of order 2.

1. Introduction

In the study of finite p-groups, the main challenges lie in the fact that the number of such groups is very large. Research has shown (for example) that there are exactly 267 non-isomorphic groups of order 2^6 [9], $2,328$ groups of order 2^7 e.t.c. [7].

It therefore becomes an object of curiosity, finding nontrivial properties of almost all p-groups.

Most generally, p-groups have the properties of Nilpotence, Monomiality, Burnside's basis theorem, Counting theorems of Sylow, Miller and Kulakoff.

So, it is natural to seek common properties for sufficiently large sets of p-groups.

Finte p-Groups are ideal instruments for combinatorial and cohomological investigations. Some basic properties were proved by Frobenius, Sylow and Burnside. Eventhough, Philip Hall (1904-1982) laid the foundations of modern p-group theory in his three fundamental papers normally, Blackburn also made a very outstanding achievement in the concept after Hall.

The original theorem on the number of solutions of equation $X^n = 1$ in a finite group was identified with Frobenius . Meanwhile , I . M. Isaac & G.R. Robinson (see [2]) supplied a new proof in this direction (see also [2]) . Suppose that $f_n(G)$ is the number of solutions of the equation $x^n = 1$ in G . Also , let $n(p)$ denote the largest p-power which divides n

This celebrated theorem of Frobenius [1] in a finite group with the Sylow's theorem is the first and most fundamental counting theorem in finite group theory (see [3], [7]).

Theorem (Frobenius).(see [7]) Suppose that G is a finite p-group . If n $\in \mathbb{N}$ and the ooder of G ,$\mid G \mid$ is divisible by n , then the number $f_n(G)$ is a multiple of n . (see [1], [7])

Lemma A : Let $a \in G$ be of order $g = mn$, where $gcd(m,n) = 1$. Then , $a = a(m)a(n)$,where $\mid a(m) \mid = m$, $\mid a(n) = n$, and $a(m)$, $a(n)$ are powers of a

Key words and phrases. Frobenius property, transversal , homomorphism , Mckendrick-von Foerster equation.

International Journal of Scientific & Engineering Research Volume 8, Issue 10, October-2017
ISSN 2229-5518

Suppose that $a = bc = cb$; $o(b) = m$, $o(c) = n$, then , $b = a(m)$,$c = a(n)$.
Proof : From the fact that $gcd(m, n) = 1$ (i.e m and n are relatively prime) $\exists$ x,y $\in \mathbb{Z} \ni mx + ny = 1$. Set $a(m) = a^{ny}$, $a(n) = a^{mx}$; then $a(m)a(n) = a(n)a(m) = a$. We have that $(x, y) = 1 = (x, n) = (y, m)$. If $| a(m) |= m_1$, then $(a(m))^{m_1} = a^{nm_1y} = 1$, so , m_1ny is divisible by mn . Hence m divides m_1 since $(m, ny) = 1$. As $(a(m))^m = a^{mny} = 1$, $| a(m) |= m_1$ divides m . Thus , $m_1 = m$, and so , $| a(m) |= m$. Similarly , $| a(n) = m$. Now , if we assume that $a = bc = cb$ for b,c, $\in G$ and $o(b) = m$, $o(c) = n$. Claiming that $b = a(m)$ and $c = a(n)$, we have that:
$(a(n))^m = (a(m)a(n))^m = a^m = (bc)^m = b^mc^m = c^m$ .Suppose that $x \in \mathbb{Z} \ni mx = 1(modn)$, then $a(n) = (a(n))^{mx} = ((a(n))^m)^x = (c^m)^x = c^{mx} = c^{mx+ny} = c$ $\because o(c) = n$. Thus , $a(m)a(n) = a = bc = ba(n)$. And so , $b = a(m)$
Definition : Transversal : Let Q be a subgroup of a group G . A subset B of G is known as a right transversal for Q in G if B consists of exactly one element from each right coset of Q in G . The left transversal of Q in G can be defined analogously .If G is abelian , then we simply call B a transversal for Q in G . For instance , $B = \{0, 1, 2, 3, 4\}$ is a transversal for $5\mathbb{Z}$ in $(\mathbb{Z}, +)$
Lemma B: (see [7]) Let G be a group . Given that $r = n(p)$, where $n \in \mathbb{N}$ and p is a prime . Let B be a transversal for the conjugacy classes of elements $y \in G$ for which $y^{n/r} = 1$. Then , we have that

$$f_n(G) = \sum_{b\in B} | G : C_G(b) | .f_r(C_G(r)) \cdots (*)$$

Proof : By Lemma (A) if $g \in G$ with $g^n = 1$ then , $g = xy$, where $xy = yx$ $o(x) = o(g)(p)$ divides r , $o(y) = \frac{o(g)}{o(g)(p)}$ divides $\frac{n}{r}$. This is a unique expression . $\Rightarrow$

$$f_n(G) = \sum_{y\in G, y^{n/r}=1} f_r(C_G(y)).$$

Definitely , if g is as given , its contribution in $f_r(C_G(y))$ is equal to 1 if y is the p'-part of g and it is zero if y is not a p'-part of g . This contribution of g in $f_n(G)$ is also 1 . Now , since $f_r(C_G(y))$ remains constant as y runs over the index $| G : C_G(b) |$ elements in the conjugacy classes represented by $b \in G$. Hence , this agrees with $(*)$
Definition : A group G has p-Frobenius property if p^φ divides $f_{p^\varphi}(G)$ whenever p^φ divides $| G |$.
Lemma C: Let r be a power of $p \ni t$ divides $| G |$. Suppose that $Q \leq G$ is a subgroup which has the p-Frobenius property . Then r divides $| G : Q | .f_r(Q)$.
Proof : Assume that $r_0 =| Q | (p) \leq r$ Then , $f_r(Q) = f_{r_0}(Q)$ is divisible by r_0 , by the hypothesis , and $| G : Q |$ is divisible by $\frac{|G|(p)}{r_0} \Rightarrow | G | (p)$ divides $| G : Q | f_r(Q)$. Now , since r divides $| G | (p)$, the proof is complete . $\square$
Lemma D : (Cauchy see [7]) Let G be an abelian group . If a prime p divides $| G |$ then $\exists\ g \in G \ni o(g) = p$.
Proof : Assume that the lemma is true $\forall$ proper subgroups of G . One may thus suppose that G has two different maximal subgroups U and $V \ni B = UV$ and $| G | = \frac{|U||V|}{|U\cap V|}$, by the direct formula .Thus p divides either $| U |$ or $| V |$. $\square$
Lemma : G has the p-Frobenius property .

International Journal of Scientific & Engineering Research Volume 8, Issue 10, October-2017
ISSN 2229-5518

Proof : By induction on $\mid G \mid$, let r be a p-power $\ni r$ divides $\mid G \mid$. Suppose that $r =\mid G \mid (p)$ and we apply lemma (B) , and let $n =\mid G \mid$, then we obtain as follows

$$\mid G \mid = n = f_n(G) = \mid B \cap Z(G) \mid .f_r(C_G(b)) + \sum_{b \in B \setminus Z(G)} \mid G : C_G(b) \mid .f_r(C_G(B)).$$

Proceeding by induction , applying lemma (C) , we have that r divides $\mid G : Q \mid$ $f_r(Q)$ for $b \in B \setminus Z(G)$,where $Q = C_G(b)$. And , since r divides $\mid G \mid$, we have that r divides $\mid B \cap \mathbb{Z}(G) \mid .f_r(G)$, by the formula . And so , it suffices to show that $p \nmid \mid B \cap Z(G) \mid$ .We now have that $B \cap Z(G) = \{y \in Z(G) \mid y^{n/r} = 1\}$, that is $\mid B \cap Z(G) \mid = f_{n/r}(Z(G))$. Thus , $p \nmid \mid B \cap Z(G) \mid$, by lemma (D) ,since $p \nmid (n/q)$ Now , let $r < \mid G \mid (p)$. As r divides $\mid G \mid (p)$ and $f_{|G|(p)}(G)$ - $f_r(G)$. Let $\mathcal{G}$ be the set of elements of G having p-power order which exceeds r . Then ,
$f_{|G|(p)}(G)$ - $f_r(G) = \mid \mathcal{G} \mid$. If t is one of such elements and $o(t) = p^k$ ($> r$) , $s \in \mathbb{N}$ then the number of elements of order $> r$ in $\langle t \rangle$ is p^k - r and r divides p^k - r since by assumption , the p-power $r < p^k$. Then , the set $\mathcal{G}$ is partitioned in subsets of cardinalities which are divisible by r . □

Proposition : (Normalizer/Centralizer-Theorem see [7]) Suppose that $Q \leq G$ then $N_G(Q)/C_G(Q)$ is isomorphic to a subgroup of $Aut(Q)$.

Proof : First , assume that for any $g \in G$, a mapping $\varphi_g : q \mapsto gqg^{-1}$ $(q \in Q)$ is an automorphism of Q . Thus , $g \mapsto \varphi_g$ is a homomorphism of G into $Aut(Q)$ with the kernel $C_G(Q)$.

Proposition I: Suppose that

$$x^n = 1 \qquad (i)$$

Then

(i) The number of solutions of (i) forms a group $\mathbb{A}$
(ii) Define a stochastic process by:

$$x(n,k) = \left\{ \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \right\} \quad \begin{array}{l} n \in \mathbb{R} \setminus 0 \\ k \in \mathbb{Z} \end{array}$$

$$\begin{aligned} \frac{\partial x}{\partial k} &= x'_k = a_1 \mathbb{A} \text{ is a group and} \\ \frac{\partial x}{\partial n} &= x'_n = a_2 \mathbb{A} \text{ is a group; where } a_1, a_2 \in \mathbb{C} \end{aligned}$$

Whence

$$\frac{\partial x}{\partial k} + \frac{\partial x}{\partial n} = x'_k + x'_n = f(k,n,x)$$

which is a type of the differential equation[8]

$$U_t + U_a = -C(t,a,u) \qquad (1)$$

of age - a individuals satisfies the Mckendrick-von Foerster equation given by (1) above.

Existence of Solution

Recall that in (1) if $C(t,a,u)$ is of the form $\frac{cv}{L-a}$, $t > 0$, $0 < a < L$ and $u(t,0) = b(t)$, $t > 0$ where C and L are positive constants, then

$$U_t + U_a = \frac{-cu}{L-a}$$

International Journal of Scientific & Engineering Research Volume 8, Issue 10, October-2017
ISSN 2229-5518

has a solution given by:

$$U = b(t-a)\left(\frac{L-a}{L}\right)^c.$$

Proposition II: For an equation of degree 2, the number of solutions in the function , forms a group of order 2.

Proof: Every equation in degree 2 is always of the form :
$(f(x))^2 = 1 \Rightarrow f(x) = \{-1, 1\}$ from where x is calculated.

Bibliography

[**1**]**:** Berkovich, Y. and Zhmud, E.M. (1998, 1999). Characters of Finite Groups, Parts 1, 2. Translations of Mathematical Monographs 172, 181, AMS Providence RI.

[**2**]**:** Isaacs, I.M. & Robinson, G.R. (1992). On a theorem of Frobenius: Solutions of $x^n = 1$ in finite groups. Amer. Math. Monthly 99 (352-354).

[**3**]**:** Frobenius, G. and Stickelberger, L. (1879). Über Gruppen von Vertauschbaren Elementen, J. reine angew. Math. 86 (217-262).

[**4**]**:** Wielandt, H. (1959). Ein Beweis für die Existenz der Sylow gruppen. Arch. Math. 10 (401-402) (MR26 #504).

[**5**]**:** Parker, C. and Rowley, P. (2002). Symplectic Amalgams Springer. Berlin.

[**6**]**:** Dolfi, S. (1995). Arithmetical conditions on the length of the conjugacy classes of a finite group. J. Algebra 174 (753-771).

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

[**8**]**:** Körezlioglu & A.S. Üstünel (1992) Stochastic Analysis and Related Topics. Birkhäuser Boston Berlin.

[**9**]**:** Simon A., Levin et.al. Applied Mathematical Ecology. Springer-Verlag.

Department of Mathematical Sciences, Anchor University, Lagos.
E-mail address: sadebisi@aul.edu.ng