Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2016, 3(5):121-127**

ISSN: 2394-2630
CODEN(USA): JSERBR

Research Article

Characteristics of Solutions for Frobenius Equations $x^d = a$ in Finite Groups

Shuker Mahmood

Department of Mathematics, College of Science, Basrah University, Basrah, Iraq

Abstract In this work, we prove that if $\frac{|G|}{r_a}$ is a prime with $d \equiv q \ (\mathrm{mod}\ \frac{|G|}{r_a})$ for some integer number q, where $1 \leq q < \frac{|G|}{r_a}$. Then r_a is a divisor of N_a^d, where $d \in Z^+$ (positive integer), N_a^d is the number of solutions for the Frobenius equation $x^d = a$ in group G of order m, and r_a is a cardinality of C_a (conjugacy class of a) in G. Moreover, in this research we prove that if all elements of the solutions set are conjugate to c for some $c \in G$, then N_a^d divides m. Next, we show that, if $d \equiv \frac{|G|}{r_a} (\mathrm{mod}\ \frac{|G|}{r_a})$. Then N_a^d is a multiple of $|G|$.

Keywords finite groups, Frobenius equation, permutations, conjugate classes, greatest common divisor.

1. Introduction

If there exist elements $b_1, b_2, ..., b_m$ in a finite group G such that for every $b_j \in \{b_i\}_{i=1}^m$, the conjugacy class of b_j in G is $\{b_i\}_{i=1}^m$, then for each positive integer d, the collection of equations $\{x^d = b_i\}_{i=1}^m$ in G is called Frobenius equation in G and denoted by $x^d = b_j$ for some $b_j \in \{b_i\}_{i=1}^m$. Let N_a^d be the number of solutions for the Frobenius equation $x^d = a$ in G. In this paper, we consider the relations between order finite group G and N_a^d for some equations in finite group G. We will express relation linking $|G|$ with the number of the solutions N_a^d of an equation that depend only on the conjugation for all elements in solution and not on all cardinality of the classes in the solution. The number of solutions for the Frobenius equation $x^d = a$ in finite group has been studied by many mathematicians. A fundamental result of Frobenius states that in a finite group G the number of solutions for the equation $(\mathrm{mod}\ \frac{|G|}{r_a})$. Then N_a^d is a multiple of $|G|$. $x^d = e$, where d divides $|G|$, is divisible by d. Here e denotes the identity of group G. Moreover, by using this notation the simplest of Fresenius result states that if d divides $|G|$, then d divides N_e^d (see [3]). Moreover, the Frobenius Theorem was greatly generalized by Hall [5], who proved that if d is a positive integer, and C_a

is a conjugacy class of a has cardinality r_a in group G, then N_a^d is a multiple of $\gcd(d\,r_a,|G|)$. That means it is not necessarily N_a^d divides $|G|$. But in this paper the case of N_a^d divides $|G|$ is determined. Also, in [10] Mann and Martinez proved that for any natural number $m,n\geq 1$, there exists a number $0<k<1$ such that if G is an $m-$generated finite group and $\frac{N_e^d}{|G|}\geq k$, then $N_e^d=|G|$ (i.e., $x^d=e$ for an arbitrary $x\in G$). The inequality $Ord_p(N_e^p)\geq\left\lfloor\frac{n}{p}\right\rfloor-\left\lfloor\frac{n}{p^2}\right\rfloor$ is also shown by ([9] , [4]), where N_e^p is the number of solutions for the equation $x^p=e$ in $G=S_n$ (symmetric group on n letters), p is a prime number and $\lfloor t\rfloor$ denotes the greatest integer $\leq t$. $Ord_p(N_e^p)=\left\lfloor\frac{n}{p}\right\rfloor-\left\lfloor\frac{n}{p^2}\right\rfloor$ provided that $n\equiv 0 \mod p^2$ (see [6]). In this paper we prove that if $\frac{|G|}{r_a}$ is a prime number and $d\equiv q \ (\mathrm{mod}\ \frac{|G|}{r_a})$ for some q, where $1\leq q<\frac{|G|}{r_a}$, then N_a^d is a multiple of r_a. Further, in this research we prove that if all elements of the solutions set are conjugate to c for some $c\in G$, then N_a^d divides $|G|$. Moreover, in this paper the converse of this theorem is not necessarily true in general is explained. Next, we show that, if $d\equiv\frac{|G|}{r_a} \ (\mathrm{mod}\ \frac{|G|}{r_a})$. Then N_a^d is a multiple of $|G|$. Finally, the current work is supported by a number of examples.

2. Preliminaries

In the current work we will support this paper by a number of examples, when $G=A_n\subset S_n$. Moreover, where their elements are studied in past work see [14-16] and they are useful because symmetric groups S_n and Alternating groups A_n are so important in finite groups field, because (Every finite group G is isomorphic to a subgroup of the symmetric group S_n for some $n>1$) (see [2]). Moreover, we know that (Every symmetric group S_n is isomorphic to a subgroup of the alternating group A_{n+2}). That means, if G is a finite group of order n. Then G is isomorphic to a subgroup of the alternating group A_{n+2} .Therefore, we need to introduce some important facts about symmetric and alternating groups.

Definition 2.1 [17].

A partition α is a sequence of nonnegative integers $(\alpha_1,\alpha_2,\ldots)$ with $\alpha_1\geq\alpha_2\geq\ldots$ and $\sum_{i=1}^{\infty}\alpha_i<\infty$. The length $l(\alpha)$ and size $|\alpha|$ of α are defined as $l(\alpha)=Max\{i\in N \mid \alpha_i\neq 0\}$ and $|\alpha|=\sum_{i=1}^{\infty}\alpha_i$. We set $\alpha \vdash n=\{\alpha \ partition \mid |\alpha|=n\}$ for $n\in N$. An element of $\alpha\vdash n$ is called a partition of n, and α_i are the parts of α .

Definition 2.2 [17].

Let $\beta\in S_n$. We define $c_m=c_m^{(n)}=c_m^{(n)}(\beta)$ to be the number of cycles of length m of β .

Remarks: 2.3

(1) Let $\beta \in S_n$, we only write the non-zero components of a partition. Therefore, $\alpha = (\alpha_1, \alpha_2, ..., \alpha_{c(\beta)})$ is a partition of n where $c(\beta)$ is the number of disjoint cycle factors, including the $1-$cycle of β (see [17]).

(2) If $\beta \in C^\alpha$, then $C^\alpha = C^\alpha(\beta)$ the conjugacy class of β in S_n and the cardinality of each $C^\alpha = C^\alpha(\beta)$ can be found as follows:

$$\left|C^\alpha\right| = \frac{n!}{z_{\alpha(\beta)}} \text{ with } z_{\alpha(\beta)} = \prod_{r=1}^{n} r^{c_r}(c_r)! \text{ and } c_r = c_r^{(n)}(\beta) = \left|\{i : \alpha_i = r\}\right| \text{ (see [1]).}$$

(3) If $\beta \in A_n \subset S_n$, then $A(\beta)$ the conjugacy class of β in A_n and either $C^\alpha = A(\beta)$ or C^α splits into two classes $C^{\alpha\pm}$ of A_n where $A(\beta) = C^{\alpha+}$ or $A(\beta) = C^{\alpha-}$ (see [8]).

Theorem: 2.4 [11]

Let $A(\beta)$ be the conjugacy class of β in A_n, $14 > n \notin \theta$ & $(n+1) \notin \theta$, and $\beta \in [n] \cap H$, where $\theta = \{0,1,2,5,6,10,14\}$ and $[n]$ is a class conjugacy of S_n. If p and q are different prime numbers such that $\gcd(p,n) = 1$ and $\gcd(q,n) = 1$, then the solutions of $x^{pq} \in A(\beta)$ in A_n are:

(1) $[n]^-$ if $\beta^{pq} = (\beta^{-1}$ or $\gamma)$, where γ is conjugate to β^{-1}.

(2) $[n]^+$ if $\beta^{pq} = (\beta$ or $\gamma)$, where γ is conjugate to β.

Lemma: 2.5 [13] Let $L = \{m \in N \mid m \equiv q \pmod 5 \text{ for some } q = 1,4\}$. If d is a positive integer such that $\gcd(d,5) = 1$ and $\beta = (b_1, b_2, b_3, b_4, b_5) \in [5]$ of S_5, then the solutions of $x^d \in A(\beta)$ in A_5 are

1. $A(\beta)$, if $d \in L$.
2. $A(\overset{\#}{\beta})$, if $d \notin L$, where $\overset{\#}{\beta} = (b_1, b_3, b_5, b_2, b_4)$.

Theorem: 2.6 [12]

Let $A(\beta)$ be the conjugacy class of β in A_n. If p is a prime number and does not divide a, $\beta \in [a^r] \cap H^C$, where $[a^r]$ is a class of S_n, then the solutions of $x^p \in A(\beta)$ are:

1- $[a^r]$ if $(1 \le r \le p)$ and $(a$ is odd or $(a$ and $r)$ are even$)$.

2- $[a^r], [(pa), a^{r-p}], [(pa)^2, a^{r-2p}], ..., [(pa)^m, a^{r-mp}]$

if $[((a$ and $p)$ are odd$)$ or $(p$ is odd and $(a$ and $r)$ are even$)]$ and $[mp \le r < (m+1)p]$.

3- $[a^r], [(pa)^2, a^{r-2p}], [(pa)^4, a^{r-4p}], ..., [(pa)^m, a^{r-mp}]$

if $[(a$ is odd and p is even$)$ or $(a, p$ and r are even$)]$ and $[(mp \le r < (m+1)p)]$ and m is even.

4- $[a^r], [(pa)^2, a^{r-2p}], [(pa)^4, a^{r-4p}], ..., [(pa)^{(m-1)}, a^{r-(m-1)p}]$

If $[(a$ is odd and p is even$)$ or $(a, p$ and r are even$)]$ and $[(mp \le r < (m+1)p)$ and m is odd$]$.

5- $[(pa), a^{r-p}], [(pa)^3, a^{r-3p}], ..., [(pa)^m, a^{r-mp}]$

if $[(a$ and $p)$ are even and r is odd$)]$ and $[(mp \le r < (m+1)p)$ and m is odd$]$.

6- $[(pa), a^{r-p}], [(pa)^3, a^{r-3p}], ..., [(pa)^{(m-1)}, a^{r-(m-1)p}]$

if $[(a$ and $p)$ are even and r is odd$)]$ and $[(mp \le r < (m+1)p)$ and m is even$]$.

7- Does not exist if $[(a$ is even and $(p$ and $r)$ are odd$)]$.

3. Ability on Dividing and Multiplication

In this section we will investigate the ability on dividing and multiplication which are considered between order finite group G and the cardinality r_a in G with N_a^d for some equations in group G under closed conditions.

Theorem 3.1

Let G be a finite group, if $\frac{|G|}{r_a}$ is a prime number and $d \equiv q \ (\mathrm{mod}\ \frac{|G|}{r_a})$ for some q, where $1 \le q < \frac{|G|}{r_a}$.

Then $N_a^d = hr_a$ for some $h \ge 1$.

Proof:

Let G be a finite group of order k and N_a^d the number of solutions for the equation $x^d = a$ in G. Moreover, the conjugacy class C_b in G for any $b \in G$ has order dividing k. But $|C_b| = r_b$, that means $\frac{k}{r_a} \in N - \{0\}$, for any $b \in G$. Suppose that $\frac{k}{r_a} = p$ is prime number and $d \equiv q \ (\mathrm{mod}\ \mathrm{p})$ for some q, where $1 \le q < p$. Therefore, there is an integer number t such that $d = tp + q$, for $1 \le q < p$. However, $1 \le q < p$. This implies $tp + q \ne gp$ for any $g \in Z$. Thus $\gcd(d, p) = 1$ (since p is prime number and $d \ne gp$ for any $g \in Z$), then $\gcd(dr_a, pr_a) = r_a$. But N_a^d is a multiple of $\gcd(d\, r_a, k)$, thus $N_a^d = hr_a$ for $h \ge 1$.

Theorem 3.2

Let $S = \{x \in G \mid x^d \in C_a\}$ be a solution set to the equation $x^d = a$ in finite group G. If there exists $c \in G$ conjugate to all elements in S, then $N_a^d \mid |G|$.

Proof:

For each $b \in G$, there is a conjugacy class C_b of b in G has cardinality r_a. Let $s \in S$, we have s conjugate to c in G ($s \underset{G}{\approx} c) \Rightarrow s \in C_c \Rightarrow S \subseteq C_c$. Moreover, let $t \in C_c$, we have $t \underset{G}{\approx} c \Rightarrow t^d \underset{G}{\approx} c^d$. However, $c^d \underset{G}{\approx} s^d$ and $s^d \underset{G}{\approx} a$, for any $s \in S \Rightarrow t^d \underset{G}{\approx} a \Rightarrow t \in S \Rightarrow C_c \subseteq S$. Hence $S = C_c$, therefore $N_a^d = r_c$. In another direction, the cardinality of each conjugacy class of finite group G divides its order (see [7]). Then $N_a^d \mid |G|$.

Example: 3.3

Let $d = 22$ and $a = (a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (1\ 6\ 2\ 5\ 4\ 7\ 3)$ in $G = A_7$. Find N_a^d and discuss ability to divide order group G.

Solution:

By (Theorem 2.4) we have the solution set is $S = \{[7]^+\} = \{A(a)\}$, and $N_a^d = \frac{(7)!}{2 \times 7} = 360$. Let $c = a \in A_7$, we have $c \in A(a) = [7]^+$. Hence c conjugate to all elements in S and $N_a^d = 360$ divides $|A_7| = \frac{(7)!}{2} = 2520$.

Example: 3.4

Let $d=17$ and $a=(a_1,a_2,a_3,a_4,a_5)=(1\ 3\ 4\ 2\ 5)$ in $G=A_5$. Find N_a^d and discuss ability to divide order group G.

Solution:

By (Lemma 2.5) we have the solution set is $S=\{[5]^-\}=\{A(\overset{\#}{a})\}$, where $\overset{\#}{a}=(a_1,a_3,a_5,a_2,a_4)=(5\ 2\ 1\ 3\ 4)$ and $N_a^d=\frac{(5)!}{2\times 5}=12$, where $A(5\ 2\ 1\ 3\ 4)=\{(1\ 2\ 3\ 5\ 4),$ $(1\ 5\ 4\ 2\ 3),(1\ 2\ 5\ 4\ 3),(1\ 3\ 2\ 4\ 5),(1\ 4\ 2\ 5\ 3),(1\ 3\ 5\ 2\ 4),(1\ 2\ 4\ 3\ 5),(1\ 4\ 5\ 3\ 2),(1\ 4\ 3\ 2\ 5),$ $(1\ 5\ 2\ 3\ 4),(1\ 5\ 3\ 4\ 2),(1\ 3\ 4\ 5\ 2)\}$. Let $c=\overset{\#}{a}\in A_5$, we have $c\in A(\overset{\#}{a})=[5]^-$. Hence c conjugate to all elements in S and $N_a^d=12$ divides $|A_5|=\frac{(5)!}{2}=60$.

Example: 3.5

Find N_a^d and discuss ability to divide order group G.

(1) If $d=3$ and $a=(4\ \ 2)(1\ 3)(7\ 6)(8\ 5)$ in $G=A_8$.

(2) If $d=5$ and $a=(3\ 1\ \ 2)(6\ 4\ 5)$ in $G=A_6$.

Solution:

1) By (Theorem 2.6) we have the solution set is $S=\{[2^4],[2,6]\}$, and $N_a^d=\frac{(8)!}{2^4\times(4)!}+\frac{(8)!}{2\times 6}=3465$.

Here we note that there is not exist any element in group A_8 conjugate with all elements in the classes $[2^4]$ and $[2,6]$ simultaneously, because all elements in class $[2^4]$ have structure different of all elements in class $[2,6]$.

Moreover, $N_a^d=3465$ does not divides $|A_8|=\frac{(8)!}{2}=20160$.

2) By (Theorem 2.6) we have the solution set is $S=\{[3^2]\}$, and $N_a^d=\frac{(6)!}{3^2\times(2)!}=40$. Let $c=a\in A_6$, we have $c\in A(a)=[3^2]$. Hence c conjugate to all elements in S and $N_a^d=40$ divides $|A_6|=\frac{(6)!}{2}=360$.

Remark: 3.6

The converse of theorem (3.2) is not necessarily true in general.

Example: 3.7

Let $d=3$ and $a=(1)$ in $G=A_3$. Find N_a^d and discuss ability to divide order group G.

Solution:

By (Theorem 2.6) we have the solution set is $S=\{[1^3],[3]^+,[3]^-\}$, and $N_a^d=1+\frac{(3)!}{3}=3$. Here we have $N_a^d=3$ divides $|A_3|=\frac{(3)!}{2}=3$. However, there is no element in A_3 conjugate to all elements in S. Therefore, the converse of theorem (1.1) is not necessarily true in general.

Theorem: 3.8

Let G be a finite group, if $d \equiv \frac{|G|}{r_a} (\bmod \frac{|G|}{r_a})$. Then $N_a^d = h|G|$ for some $h \geq 1$.

Proof:

Let $\frac{|G|}{r_a} = q$ for some $q \in N - \{0\}$ and $d \equiv \frac{|G|}{r_a} (\bmod \frac{|G|}{r_a})$. Therefore, there is an integer number t such that $d = q(t+1)$. However, $\gcd(dr_a, |G|) = \gcd(qr_a(t+1), qr_a) = qr_a$. But N_a^d is a multiple of $\gcd(d\, r_a, |G|)$, thus $N_a^d = hqr_a = h|G|$ for $h \geq 1$.

4. Conclusion and Discussions

The general purpose of this research was to investigate the relations between order finite group G and the cardinality r_a in G with N_a^d for some equations in group G under new conditions. Moreover, the theorems, presented in this paper, is quite basic in study ability on dividing and multiplication which are considered between each pair of these terms N_a^d, r_a and $|G|$. This paper is an attempt to establish underlying results which hopefully will help others to answer some or all of these questions:

1) If there exist at least two elements are not conjugate in finite group G, but each of them is conjugate to some elements of the solutions set. Now, what is the ability on dividing and multiplication which can be considered between each pair of these terms N_a^d, r_a and $|G|$?
2) Let $x^d = a$ be an equation in group G with $|G| > 1$, and it satisfies one of these theorems [(3.1), (3,2), (3.8)]. Is there any Isomorphism $(f : G \cong A_n)$, satisfy the same theorem for equation $f(x)^d = f(a)$ in alternating group A_n for some $n > 1$?

References

[1]. Bump D., *Lie groups* (2004), Springer-Verlag, New York.
[2]. Childs N. L. and Corradino J. (2007), *Cayley's Theorem and Hopf Galois structures for semidirect products of cyclic groups*, Journal of Algebra, 308, 236–251.
[3]. Finkelstein H. (1978), *Solving Equations in Groups: A Survey of Frobenius Theorem*, Periodica Mathematica Hungarica, 9 (3), 187-204.
[4]. Grady M. and Newmanm M. (1994), *Residue periodicity in subgroup counting functions, In: The Rademacher Legacy to Mathemati*cs, Contemporary Mathematics, 166, 265-273.
[5]. Hall M. (1959), *The theory of groups*, Macmillan.
[6]. Ishihara H., Ochiai H., Takegahara Y., and Yoshida T. (2001), *$p-$divisibility of the number of solutions of $x^d = 1$ in a symmetric group*, Annals of Combinatorics, 5, 197-210.
[7]. Joshi D. K. (2003), *Foundations of discrete mathematics*, New Age International publishers.
[8]. James G. and Kerber A. (1984), *The representation theory of the symmetric group*, Addison Welsey Publishing, Cambridge University Press.
[9]. Katsurada H., Takegahara Y. and T. Yoshida (2000), *The number of homomorphisms from a finite abelian group to a symmetric group*, Communications in Algebra, 28 (5), 2271-2290.
[10]. Mann M. and Martinesz C. (1996), *The exponent of finite groups*, Archiv der Mathematik, 67, 8-10.
[11]. Shuker M. and Andrew R. (2011), *Solving the class equation $x^d = \beta$ in an alternating group for each $\beta \in H_n \cap C^\alpha$ and $n \notin \theta$*, Journal of the Association of Arab Universities for Basic and Applied Sciences, Science Direct, 10, 42–50.

[12]. Shuker M. and Andrew R. (2012), *Solving the class equation* $x^d = \beta$ *in an alternating group for each* $\beta \in H_n{}^c \cap C^\alpha$ *and* $n > 1$, Advances in Linear Algebra and Matrix Theory, 2, 13-19.

[13]. Shuker M. and Andrew R. (2014), *Solving the class equation* $x^d = \beta$ *in an alternating group for all* $n \in \theta$ *and* $\beta \in H_n \cap C^\alpha$, Journal of the Association of Arab Universities for Basic and Applied Sciences, Science Direct, 16, 38–45.

[14]. Shuker Mahmood and Andrew Rajah, The Ambivalent Conjugacy Classes of Alternating Groups, published in Pioneer Journal of Algebra, Number Theory and its Applications, Vol.1, No.2,(2011), 67-72.

[15]. Shuker Mahmood, The Permutation Topological Spaces and their Bases, Basrah Journal of Science, University of Basrah, Vol.32(1), (2014), 28-42.

[16]. Shuker Mahmood, Obtaining the suitable k for (3+2k)- cycles, Basrah Journal of Science, University of Basrah, (2016) to appear.

[17]. Zeindler D. (2010), *Permutation matrices and the moments of their characteristic polynomial*, Electronic Journal of Probability, 15 (34), 1092-1118.