ON THE NUMBER OF CYCLIC SUBGROUPS
OF A FINITE GROUP

MOHAMMAD HOSSEIN JAFARI AND ALI REZA MADADI

Abstract. Let $G$ be a finite group and $m$ a divisor of $|G|$. We prove that $G$ has at least $\tau(m)$ cyclic subgroups whose orders divide $m$, where $\tau(m)$ is the number of divisors of $m$.

1. Introduction

Throughout all groups are assumed to be finite. A well known result in group theory says that a cyclic group of order $n$ has a unique subgroup of order $d$, for any divisor $d$ of $n$, so a cyclic group of order $n$ has exactly $\tau(n)$ (necessarily cyclic) subgroups. A generalization of this result was obtained by Richards in [3]. He proved that a group of order $n$ has at least $\tau(n)$ cyclic subgroups, and the group is cyclic if and only if it has exactly $\tau(n)$ cyclic subgroups. In this paper we generalize Richards’ result and then classify groups of order $n$ with $\tau(n) + 2$ subgroups. Also we obtain a generalization of the Kesava Menon identity [2].

2. Main results

For a group $G$ and a divisor $m$ of $|G|$, let $A_G(m)$ denote the number of cyclic subgroups of $G$ whose orders divide $m$ and $B_G(m)$ denote the number of solutions in $G$ of the equation $x^m = 1$. Also for any natural number $n$ and any subset $\pi$ of prime numbers, we write $n = n_\pi n_{\pi^c}$, where $\pi^c$ is the complement of $\pi$ in prime numbers, and $n_\pi$ and $n_{\pi^c}$ are the $\pi$-part and $\pi^c$-part of $n$, respectively.

The following theorem shows that there is a close connection between the arithmetic functions $A_G$ and $B_G$. Note that for any $n \in \mathbb{N}$, the set $\{d : 1 \leq d \leq n, (d,n) = 1\}$ denoted by $U(\mathbb{Z}_n)$ is the group of integers modulo $n$ under multiplication.
Theorem 2.1. Let $G$ be a group of order $n$ and $m$ a divisor of $n$. Then

$$A_G(m) = \frac{1}{\varphi(n)} \sum_{d \in U(\mathbb{Z}_n)} B_G((m,d-1)),$$

where $\varphi$ is the Euler totient function.

Proof. Let $\Omega$ denote the set $\{x \in G : x^m = 1\}$. Then, obviously, the group $U(\mathbb{Z}_n)$ acts on $\Omega$ via $x.\bar{r} = x^r$, where $x \in \Omega$ and $\bar{r} \in U(\mathbb{Z}_n)$. We claim that $x,y \in \Omega$ have the same orbits if and only if $\langle x \rangle = \langle y \rangle$. If $x$ and $y$ have the same orbits, then, obviously, $\langle x \rangle = \langle y \rangle$. Conversely, suppose that $\langle x \rangle = \langle y \rangle$. Hence there is an $r \in \mathbb{N}$ such that $y = x^r$ and $(r,o(x)) = 1$. Let $\pi, \pi_1,$ and $\pi_2$ be the set of prime divisors of $n$, $o(x)$, and $r$, respectively. It is trivial that $\pi_1 \subseteq \pi$ and $\pi_1 \cap \pi_2 = \emptyset$. Now if we let $\pi_3 = \pi - (\pi_1 \cup \pi_2)$ and $k = n_{\pi_1}n_{\pi_2} + r$, then it is easy to see that $(k,n) = 1$ and $y = x^k$. Thus $y = x.k$, as desired. Therefore, by the claim, the number of the orbits of the action is equal to $A_G(m)$, the number of cyclic subgroups of $G$ whose orders divide $m$. Now, by the Cauchy-Frobenius Lemma, we have

$$A_G(m) = \frac{1}{\varphi(n)} \sum_{d \in U(\mathbb{Z}_n)} \chi(d),$$

where $\chi$ is the permutation character associated with the action. But

$$\chi(d) = |\{x \in \Omega : x.d = x\}|$$
$$= |\{x \in \Omega : x^d = x\}|$$
$$= |\{x \in G : x^m = 1, x^{d-1} = 1\}|$$
$$= |\{x \in G : x^{(m,d-1)} = 1\}|$$
$$= B_G((m,d-1)),$$

and the proof is complete.

The following corollary can be viewed as a generalization of the well-known Kesava Menon identity [2]. For other generalizations of the Kesava Menon identity, we refer the reader to [5] and [7].

Corollary 2.2. Let $m, n \in \mathbb{N}$ and $m \mid n$. Then

$$\sum_{d \in U(\mathbb{Z}_n)} (m,d-1) = \varphi(n)\tau(m).$$

Proof. Let $G$ be a cyclic group of order $n$. Since $G$ has a unique (necessarily cyclic) subgroup of each divisor of $n$, so $G$ has exactly $\tau(m)$ cyclic subgroups whose orders divide $m$, hence $A_G(m) = \tau(m)$. It is also obvious that $B_G((m,d-1)) = (m,d-1)$ for any $d \in U(\mathbb{Z}_n)$. Now the result follows from the previous theorem.
Before giving another consequence of the above theorem, we will characterize the set \( \{(m,d-1): d \in U(\mathbb{Z}_n)\} \) using the Chinese remainder theorem. In the following, let \( \pi(m) \) be the set of all prime divisors of the natural number \( m \).

Also let \( D(m) \) be the set of all even divisors of \( m \) if \( m \) is even, and the set of all divisors of \( m \) if \( m \) is odd.

**Lemma 2.3.** Let \( m, n \in \mathbb{N} \), \( m | n \). Then \( D(m) = \{(m, d - 1): d \in U(\mathbb{Z}_n)\} \).

**Proof.** Let \( X = \{(m, d - 1): d \in U(\mathbb{Z}_n)\} \). We consider two cases.

1) Suppose that \( m \) is odd. It is clear that \( X \subseteq D(m) \). Conversely, we show that if \( k \in D(m) \), then \( k \in X \). To this end, let \( \sigma = \pi(k), \pi = \pi(m), \pi_1 = \{2\} \), and \( \pi_2 = \pi' - \pi_1 \). Hence \( \sigma \subseteq \pi \) and \( n = n_{\pi_1} n_{\pi_2} \). Now, by the Chinese remainder theorem, the following system of linear congruences

\[
\begin{align*}
    kx &\equiv 1 \pmod{n_{\sigma_2}} \\
    kx &\equiv 1 \pmod{p} \quad \text{if } p \in \pi - \sigma \\
    x &\equiv 1 \pmod{p} \quad \text{if } p \in \sigma \\
    x &\equiv 0 \pmod{2}
\end{align*}
\]

has a simultaneous solution, say \( a \). The last congruence says that \( a \) is even, so \( b = 1 + ka \) is odd. We now show that \( (b, n) = 1 \). Assume by way of contradiction that \( q \) is a prime divisor of \( (b, n) \), and so \( q \) is odd. Also note that \( q \notin \sigma \), for \( q | 1 + ka \). It follows therefore that either \( q \in \pi_2 \) or \( q \in \pi - \sigma \). Suppose first that \( q \in \pi_2 \). Hence \( q | n_{\pi_2} \), and since \( b \equiv 2 \pmod{n_{\pi_2}} \) and \( q | b \), we deduce that \( q = 2 \), a contradiction. Suppose now that \( q \in \pi - \sigma \). Hence \( b \equiv 2 \pmod{q} \), and since \( q | b \), it then follows that \( q = 2 \), again a contradiction. Now we have

\[
(m, b - 1) = (m, ka) = k(m_k, a) = k,
\]

where the last equality follows from the second and third congruences of the above system. Therefore, \( k \in X \), and the proof completes.

2) Suppose now that \( m \) is even. Hence \( n \) is even and consequently \( X \subseteq D(m) \). Now we show that if \( k \in D(m) \), then \( k \in X \). To this end, let \( \sigma = \pi(k) \) and \( \pi = \pi(m) \). Hence \( 2 \in \sigma \subseteq \pi \) and \( n = n_{\pi_1} n_{\pi_2} \). Again, by the Chinese remainder theorem, the following system of linear congruences

\[
\begin{align*}
    kx &\equiv 1 \pmod{n_{\sigma_1}} \\
    kx &\equiv 1 \pmod{p} \quad \text{if } p \in \pi - \sigma \\
    x &\equiv 1 \pmod{p} \quad \text{if } p \in \sigma
\end{align*}
\]

has a simultaneous solution, say \( a \). Since \( k \) is even, so \( b = 1 + ka \) is odd. We now show that \( (b, n) = 1 \). Assume by way of contradiction that \( q \) is a prime divisor of \( (b, n) \), and so \( q \) is odd. Again \( q \notin \sigma \) for \( q | 1 + ka \). It follows therefore that either \( q \in \pi' \) or \( q \in \pi - \sigma \). Suppose first that \( q \in \pi' \). Hence \( q | n_{\pi'} \), and since \( b \equiv 2 \pmod{n_{\pi'}} \) and \( q | b \), we deduce that \( q = 2 \), a contradiction. Suppose now that \( q \in \pi - \sigma \). Hence \( b \equiv 2 \pmod{q} \), and since \( q | b \), it then follows that \( q = 2 \), again a contradiction. Now we have

\[
(m, b - 1) = (m, ka) = k(m_k, a) = k,
\]
where the last equality follows from the second and third congruences of the latter system. Therefore, \( k \in X \), and the proof is complete. \( \square \)

There is a classic result in group theory which says that a group \( G \) of order \( n \) is cyclic if and only if the number of solutions in \( G \) of the equation \( x^d = 1 \) is at most \( d \), for any divisor \( d \) of \( n \). We generalize this result in the next theorem.

**Theorem 2.4.** Let \( G \) be a group of order \( n \) and \( m \) a divisor of \( n \). Then the following are equivalent:

1) \( G \) has a unique, and necessarily cyclic, subgroup of order \( m \);
2) the number of solutions in \( G \) of the equation \( x^d = 1 \) is exactly \( d \) for any \( d \in D(m) \);
3) the number of solutions in \( G \) of the equation \( x^d = 1 \) is at most \( d \) for any \( d \in D(m) \).

**Proof.** 1) \( \Rightarrow \) 2): Let \( H \) be the unique, and necessarily cyclic, subgroup of \( G \) of order \( m \). Let \( x \in G \) be arbitrary such that \( x^d = 1 \), where \( d \in D(m) \). We show that \( x \in H \). To this end, it suffices to show that if \( P \) is any Sylow \( p \)-subgroup of \( \langle x \rangle \), then \( P \subseteq H \). Since normalizers grow in \( p \)-groups, so there exists a \( p \)-subgroup \( Q \) of \( G \) such that \( P \subseteq Q \) and \( |Q| = p^s \), where \( m = p^s s \) with \( p \nmid s \).

Now if \( K \) is the unique subgroup of \( H \) of order \( s \), then \( K \) is normal in \( G \), so \( QK \) is a subgroup of \( G \) of order \( m \). By uniqueness of \( H \), we have \( H = QK \). Therefore, \( P \subseteq Q \subseteq H \), and the proof is complete.

2) \( \Rightarrow \) 3): Trivial.

3) \( \Rightarrow \) 1): First we claim that if \( m \) is even, then \( B_G(d) \leq d \) for each odd divisor \( d \) of \( m \).

Let \( d \) be an arbitrary odd divisor of \( m \). Since \( B_G(2) \leq 2 \), so \( G \) has a unique (necessarily central) involution \( z \). Now if \( y^d = 1 \) for some \( y \in G \), then we have \( y^{2d} = 1 = (zy)^{2d} \) and \( (zy)^d \neq 1 \). Thus if we let \( C = \{ x \in G : x^d = 1 \} \) and \( D = \{ x \in G : x^{2d} = 1 \} \), then \( C \cap zC = \emptyset, |zC| = |C| \), and \( C \cup zC \subseteq D \). Since \( |D| = B_G(2d) \leq 2d \), so \( B_G(d) = |C| \leq d \), as desired.

Now we prove that \( G \) has a unique subgroup of order \( m \), and that this subgroup is cyclic. Let \( p \) be an arbitrary prime divisor of \( m \) such that \( p^n \mid m \) and \( p^{n+1} \nmid m \). Since \( G \) has a \( p \)-subgroup of order \( p^a \) and \( B_G(p^n) \leq p^a \), so \( G \) has a unique subgroup \( H_p \) of order \( p^a \). This shows that each Sylow \( p \)-subgroup of \( G \) is either cyclic or generalized quaternion. Hence if \( p \) is odd, then \( H_p \) is cyclic. Now suppose that \( p = 2 \). If \( a = 1 \), then, as we know, \( \langle z \rangle \) is the unique (necessarily central) subgroup of \( G \) of order 2. If \( a \geq 2 \), then a Sylow 2-subgroup of \( G \) must be cyclic, because in a generalized quaternion group we have \( B_G(4) \geq 8 \), which contradicts the hypothesis. Hence, again by hypothesis, \( G \) has a unique (necessarily cyclic) subgroup of order \( 2^a \). Therefore, in either case, \( H_2 \) is the unique (necessarily cyclic) subgroup of \( G \) of order \( 2^a \). Now the subgroup \( H = \prod_{p \in \pi(m)} H_p \) is the unique (necessarily cyclic) subgroup of \( G \) of order \( m \), and the proof is complete. \( \square \)
Remark. Notice that the above proof shows that if $G$ has a unique, and necessarily cyclic, subgroup of order $m$, then the number of solutions in $G$ of the equation $x^d = 1$ is exactly $d$ for any divisor $d$ of $m$.

Now we are ready to state our main theorem.

**Theorem 2.5.** Let $G$ be a group of order $n$ and $m$ a divisor of $n$. Then

1) \( A_G(m) \geq \tau(m) \). In other words, $G$ has at least $\tau(m)$ cyclic subgroups whose orders divide $m$.

2) \( A_G(m) = \tau(m) \) if and only if $G$ has a unique, and necessarily cyclic, subgroup of order $m$.

**Proof.** 1) By the Frobenius theorem we have \( B_G((m,d-1)) \geq (m,d-1) \), for any $\bar{d} \in U(\mathbb{Z}_n)$, and so, by Theorem 2.1 and Corollary 2.2, we obtain

\[
A_G(m) \geq \frac{1}{\varphi(n)} \sum_{d \in U(\mathbb{Z}_n)} (m,d-1) = \tau(m).
\]

2) From the proof of the previous part, we know that $A_G(m) = \tau(m)$ if and only if \( B_G((m,d-1)) = (m,d-1) \), for any $\bar{d} \in U(\mathbb{Z}_n)$. Now the result easily follows from Lemma 2.3 and Theorem 2.4. \[\square\]

**Corollary 2.6.** Let $G$ be a group of order $n$ and $\pi$ a set of primes. Then

1) $G$ has at least $\tau(n_{\pi})$ cyclic $\pi$-subgroups;

2) $G$ has exactly $\tau(n_{\pi})$ cyclic $\pi$-subgroups if and only if $G$ has a normal cyclic Hall $\pi$-subgroup.

**Corollary 2.7.** There does not exist a group $G$ of order $n$ having $\tau(n) + 1$ subgroups.

**Proof.** Deny. Then $G$ is not cyclic and so, by Theorem 2.5, $G$ has at least $\tau(n)+1$ cyclic subgroups. Therefore $G$ has at least $\tau(n)+2$ subgroups, contrary to assumption. \[\square\]

Finally we are going to classify groups of order $n$ having $\tau(n) + 2$ subgroups. To do this, we have to characterize minimal noncyclic groups, that is, noncyclic groups all of whose proper subgroups are cyclic. The following proposition which is a characterization of minimal noncyclic groups has also been appeared in [6] as Theorem 2.1. However, our proof is different than theirs.

**Proposition 2.8.** Let $G$ be a minimal noncyclic group. Then $G$ is isomorphic to one of the following:

\begin{itemize}
  \item[i)] $\mathbb{Z}_p \times \mathbb{Z}_p$, where $p$ is a prime;
  \item[ii)] $Q_8$;
  \item[iii)] $\langle a, b \mid a^q = b^r = 1, b^{-1}ab = a^s \rangle$, where $r, s \in \mathbb{N}, q \mid s - 1, q \mid s^p - 1$, and $p, q$ are distinct primes.
\end{itemize}
Proposition 2.8. Let \( p \) be a prime number. Then, if \( p \) has the structure of \( G \) for some prime \( p \), then \( G \) is minimal nonabelian. If \( p \) is a product of distinct primes, then \( G \) is isomorphic to one of the following: 1) \( \mathbb{Z}_p \times \mathbb{Z}_p \), 2) \( P \mathbb{Z}_p \), or 3) \( \langle a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle \), where \( r \in \mathbb{N} \).

Proof. By Theorem 6.5.8 in [4], either 1) \( G \) is a p-group for some prime \( p \), or 2) \( G = PQ \), where \( P \in \text{Syl}_p(G) \) is cyclic and \( Q \in \text{Syl}_q(G) \) is an elementary abelian normal subgroup of \( G \) for some distinct primes \( p \) and \( q \). In the first case, since all maximal subgroups of \( G \) are cyclic by assumption, hence by the structure of p-groups with a cyclic maximal subgroup, see Theorem 12.5.1 in [1], we easily deduce that \( G \) is isomorphic to \( Q_p \). In the second case, since \( G \) is minimal noncyclic, so \( Q \) is isomorphic to \( \mathbb{Z}_q \) and it can be seen that \( G \) has the structure mentioned in iii).

The last corollary gives a characterization of groups of order \( n \) having \( \tau(n) + 2 \) subgroups.

Corollary 2.9. Let \( G \) be a group of order \( n \). Then \( G \) has \( \tau(n) + 2 \) subgroups if and only if \( G \) is isomorphic to one of the following:

1) \( V_4 \);
2) \( Q_8 \);
3) \( \langle a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle \), where \( r \in \mathbb{N} \).

Proof. Let \( G \) have \( \tau(n) + 2 \) subgroups. Hence \( G \) is minimal noncyclic. Now, by Proposition 2.8, \( G \) is either \( \mathbb{Z}_p \times \mathbb{Z}_p \), or \( Q_8 \), or \( \langle a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle \), where \( p, q, r, s \) satisfy in some certain conditions. If \( G = \mathbb{Z}_p \times \mathbb{Z}_p \), then \( G \) has \( p + 3 \) subgroups. On the other hand, by hypothesis, \( G \) has \( \tau(p^2) + 2 = 5 \) subgroups. Hence \( p = 2 \) and \( G = V_4 \). Obviously, \( Q_8 \) has \( \tau(8) + 2 = 6 \) subgroups. Finally if \( G = \langle a, b | a^3 = b^2 = 1, b^{-1}ab = a^{-1} \rangle \), then \( n = p'q \). But all subgroups of \( G \) are \( \langle b, a^{(1-s)} \rangle, 1 \leq i \leq q, \langle b^{p^j} \rangle, 1 \leq j \leq r \). Therefore \( G \) has \( 1 + q + 2r \) subgroups. On the other hand, by hypothesis, \( G \) has \( \tau(p'q) + 2 = 4 + 2r \) subgroups. Hence \( q = 3 \). It then follows from \( 3 \nmid s - 1 \) and \( s^p \equiv 1 \pmod{3} \) that \( p = 2 \) and \( s = 2 \). This completes the proof.

\[ \Box \]

References

Mohammad Hossein Jafari  
Department of Pure Mathematics  
Faculty of Mathematical Sciences  
University of Tabriz  
Tabriz 5166616471, Iran  
E-mail address: jafari@tabrizu.ac.ir

Ali Reza Madadi  
Department of Pure Mathematics  
Faculty of Mathematical Sciences  
University of Tabriz  
Tabriz 5166616471, Iran  
E-mail address: a-madadi@tabrizu.ac.ir