DOI: 10.28919/ejma.2021.1.7

Eur. J. Math. Appl. (2021)1:7
URL: http://ejma.euap.org

A NOTE ON THE NUMBER OF CYCLIC SUBGROUPS OF p-GROUPS

KAIRAN YANG AND RULIN SHEN*

Abstract. Let G be a finite group and $c(G)$ the number of its cyclic subgroups. In this paper we prove that if $|G| = p^n$ then $c(G) \equiv n + 1$(mod p-1).

Given a finite p-group G, write $c(G)$ to denote the number of cyclic subgroups of G, counting the trivial subgroup.

Theorem *Suppose* $|G| = p^n$. *Then* $c(G) \equiv n + 1 (\mathrm{mod\ p} - 1)$.

Lemma *Let* $G=Z \times C$, *where* $|Z| = p$, *and* C *is a nontrivial cyclic* p*-group. Then the number of complements for* Z *in* G *is exactly* p.

Proof. Write $p^r = |C|$, so $r > 0$. If $r = 1$, then G is elementary of order p^2, and the assertion is clear, so assume that $r > 1$. Every complement for Z in G is isomorphic to C, and hence is cyclic of order p^r. Conversely, we claim that every cyclic subgroup X of G of order p^r is a complement for Z. To see this, it suffices to show that $Z \nsubseteq X$. Otherwise, we have $Z < X$, and since X is cyclic, it follows that the elements of Z are p th powers in X. This is a contradiction, however, because all p th powers in G lie in C but $Z \nsubseteq C$.

Now the elements of G that have order less than p^r are exactly the elements of $Z \times B$, where B is the subgroup of C having order p^{r-1}. Thus exactly p^r elements of G have order less than p^r, and hence the number of elements of G that have order p^r is $p^{r+1} - p^r$. Each of these elements generates one of the complements X for Z in G, and each such complement is generated by any one of $\varphi(p^r)$ different elements of order p^r. The number of complements, therefore, is exactly $\frac{(p-1)p^r}{\varphi(p^r)} = p$, as required. □

Proof of Theorem. The result is trivial if $n = 0$, so we assume that $n > 0$, and we proceed by induction on n. Let $Z \lhd G$, with $|Z| = p$, and observe that each cyclic subgroup of G/Z is either of the form U/Z, where U is a cyclic subgroup of G containing Z, or else it is of the form $(V \times Z)/Z$, where V is a nonidentity cyclic subgroup of G not containing Z.

Write u to denote the number of cyclic subgroups U of G that contain Z, and write v to denote the number of nonidentity cyclic subgroups of G that do not contain Z. Then $c(G) = u+v+1$, where the "+1" appears in order to account for the trivial subgroup of G. Now each cyclic subgroup C of G/Z is either of the form $C = U/Z$, where U is one of u different subgroups

Department of Mathematics, Hubei Minzu University, Enshi 445000, Hubei, P.R. China
*Corresponding author
E-mail addresses: 1179392382@qq.com, rshen@hbmy.edu.cn.
Key words and phrases. number of cyclic subgroups; 2-groups; involutions.
Project supported by the NSF of China (Grant No. 12161035).
Received 20/08/2021.

U/Z, or else by the lemma, there are exactly p different subgroups V such that $C = (V \times Z)/Z$. Since $v = c(G) - u - 1$, we have

$$c(G/Z) = u + \frac{v}{p} = u + \frac{c(G) - u - 1}{p},$$

and thus

$$\begin{aligned} c(G) &= p(c(G/Z) - u) + u + 1 \\ &\equiv c(G/Z) + 1 \\ &\equiv (n-1) + 1 + 1 \\ &= n + 1(\text{mod p} - 1), \end{aligned}$$

where the second congruence holds by the inductive hypothesis. □

Next we will give some corollaries. Recalled that a 2-group of maximal class is a dihedral group D_{2^n} $(n \geq 3)$, a semidihedral group $SD_{2^n}(n \geq 4)$ or a generalized quaternion group $Q_{2^n}(n \geq 3)$ (see Theorem 4.5, [1]). By applying the Inclusion-Exclusion Principle, the number of cyclic subgroups of each of the above 2-groups was determined in [2]. To summarize, we have $c(D_{2^n}) = 2^{n-1} + n, c(SD_{2^n}) = 3 \cdot 2^{n-3} + n$ and $c(Q_{2^n}) = 2^{n-2} + n$.

Corollary 1 *Suppose that a p-group G of order p^n is neither cyclic nor a 2-group of maximal class. Then*

(1) $c(G) \equiv pn - p + 2(mod\ p(p-1))$, *and*

(2) $\frac{c(G)-(n+1)}{p-1} \equiv n - 1(mod\ p)$.

Proof. Write $c_{p^i}(G)$ the number of cyclic subgroups of order p^i in G, and next assume that G is neither cyclic nor a 2-group of maximal class. If $i = 1$, then $c_p(G) \equiv 1(mod\ p)$. If $i \geq 2$, then $c_{p^i}(G)$ is a multiple of p (see Lemma 5.15, [3]). It follows that

$$\begin{aligned} c(G) &= 1 + c_p(G) + \sum_{i \geq 2} c_{p^i}(G) \\ &\equiv 1 + c_p(G) \\ &\equiv 2(mod\ p). \end{aligned}$$

Now our main theorem gives another equation $c(G) \equiv n + 1(mod\ p - 1)$. By applying the Chinese Remainder Theorem, we have $c(G) \equiv p(n-1) + 2(mod\ p(p-1))$, the item (1) is proved.

Next for the item (2) we assume that $c(G) = n + 1 + (p-1)m$, where m is an integer. Then $(p-1)m \equiv c_p - n(mod\ p)$, and so $(p-1)m \equiv 1 - n(mod\ p)$. Since $p - 1$ is coprime to p, by the Fermat's Little Theorem it follows that $(p-1)^{p-1} \equiv 1(mod\ p)$, and then

$$\begin{aligned} m &\equiv (p-1)^{p-2}(1-n) \\ &\equiv (-1)^{p-2}(1-n) \\ &\equiv n - 1(mod\ p), \end{aligned}$$

as required. □

References

[1] D. Gorenstein, Finite groups, Chelsea Publishing Company, New York, 1980.

[2] M. Tărnăuceanu, L. Tóth, Cyclicity degrees of finite groups, Acta Math. Hungar. 145 (2015) 489–504. https://doi.org/10.1007/s10474-015-0480-2.

[3] Berkovich, Y., Y. Berkovich, Z. Janko, Groups of prime power order (Vol. 1), Walter de Gruyter GmbH & Co., Berlin, 2008.