# ON PRIME POWER ABELIAN GROUPS

YENCHIEN YEH

G. A. Miller in two papers [1, 2][1] has discussed the number of subgroups of prime power abelian groups. He has obtained a formula concerning the number of cyclic subgroups of a given prime power abelian group $G$,[2] and proved some theorems relating to subgroups of special types. He predicted there that the general formula for the determination of the number of subgroups of any type could be obtained without difficulty except complexity of calculations. In this paper, however, we get the general formula with a method thoroughly independent of his approach, and it seems that our method is somewhat simpler than his would be.

LEMMA 1. *If $G$ is a prime power abelian group of order $p^{k_1+k_2+\ldots+k_n}$, type $(k_1, k_2, \cdots, k_n)$, where the $k$'s are arranged in ascending order of magnitude, then the number of cyclic subgroups of order $p^h$ in $G$ is*

$$\frac{p^{n-\nu_h}-1}{p-1}\,p^{(n-\nu_h-1)(h-1)+a}, \tag{1}$$

$$\text{where} \quad a=\sum_{\mu=0}^{\nu_h} k_\mu,\ k_{\nu_h}<h\leqq k_{\nu_h+1},\ k_0=0.$$

DEFINITION. Two cyclic subgroups of order $p^h$ are called isomers in $G$ if a generator of one group is the product of an element in $G$ of order less than $p^h$ and a generator of the other group.

The number of elements of order not greater than $p^h$ in $G$ is easily seen to be

$$p^{(n-\nu_h)h+a},$$

$a$ defined as in (1). From Lemma 1, the number of elements of order $p^h$ is

$$\frac{p^{n-\nu_h}-1}{p-1}\,p^{(n-\nu_h-1)(h-1)+a}\cdot p^{h-1}(p-1)=(p^{n-\nu_h}-1)p^{(n-\nu_h)(h-1)+a}.$$

Hence the number of elements of order less than $p^h$ is

$$p^{(n-\nu_h)h+a}-(p^{n-\nu_h}-1)p^{(n-\nu_h)(h-1)+a}=p^{(n-\nu_h)(h-1)+a}.$$

---

Received by the editors February 12, 1947, and, in revised form, April 21, 1947.

[1] Numbers in brackets refer to the references cited at the end of the paper.

[2] [1, p. 259]. We state this here as Lemma 1.

A cyclic group $S$ of order $p^h$ contains $p^{h-1}$ elements of order less than $p^h$, hence corresponding to a given generator $g$ of $S$ there exist just $p^{h-1}$ elements of order $p^h$, each of them is the product of $g$ and an element of order less than $p^h$ in $S$. We have therefore the following lemma.

LEMMA 2. *Every cyclic subgroup of order $p^h$ has*

$$\frac{p^{(n-\nu_h)(h-1)+a}}{p^{h-1}} = p^{(n-\nu_h-1)(h-1)+a}$$

*isomers in $G$ (including itself).*

It is clear that the product of two cyclic subgroups of order $p^h$ is a group of order $p^{2h}$ if and only if these two cyclic subgroups are not isomers.

THEOREM. *Let $G$ be the prime power abelian group as in Lemma* 1.

$$\begin{aligned} (2)\qquad & h_1 = h_2 = \cdots = h_{m_1} > h_{m_1+1} = \cdots = h_{m_1+m_2} > \cdots \\ & > h_{m_1+m_2+\cdots+m_{r-1}+1} = \cdots = h_{m_1+m_2+\cdots+m_r}, \end{aligned}$$

*where $m_1+m_2+\cdots+m_r=m\leqq n$ are $m$ positive integers not greater than $k_n$, with $k_{\nu_i}<h_i\leqq k_{\nu_i+1}$ $(i=1, 2, \cdots, m;\ k_0=0)$. Then the number of subgroups of type* (2) *is given by*

$$(3)\qquad p^H \prod_{i=1}^{m} (p^{n-\nu_i-i+1}-1) \Big/ \prod_{\mu=1}^{r}\prod_{\nu=1}^{m_\mu} (p^\nu - 1)$$

*where*

$$\begin{aligned} H = {} & \sum_{i=1}^{m} (n-\nu_i+1-2i)(h_i-1) \\ & + \frac{1}{2}(m_1^2+m_2^2+\cdots+m_r^2-m^2) + \sum_{i=1}^{m}\sum_{\mu=0}^{\nu_i} k_\mu. \end{aligned}$$

PROOF. We prove this by induction. For $m=1$,

$$H = (n-\nu_1-1)(h_1-1) + \sum_{\mu=0}^{\nu_1} k_\mu,$$

$$\prod_{i=1}^{m} (p^{n-\nu_i-i+1}-1) = p^{n-\nu_1}-1, \qquad \prod_{\mu=1}^{r}\prod_{\nu=1}^{m_\mu} (p^\nu-1) = p-1,$$

(3) reduces to (1), the theorem is therefore true by Lemma 1.

Assume it to be true for the integer $m$, then the number of sub-

groups of type (2) is given by (3). Let $h_{m+1}$ be a positive integer less than $h_m$, the number of cyclic subgroups of order $p^{h_{m+1}}$ is

$$\frac{p^{n-\nu_{m+1}}-1}{p-1}\,p^{(n-\nu_{m+1}-1)(h_{m+1}-1)+b}, \qquad b=\sum_{\mu=0}^{\nu_{m+1}} k_\mu,$$

where $k_{\nu_{m+1}}<h_{m+1}\leqq k_{\nu_{m+1}+1}$. From Lemma 2, every cyclic subgroup of order $p^{h_{m+1}}$ has

$$p^{(n-\nu_{m+1}-1)(h_{m+1}-1)+b},$$

isomers in $G$, hence there are

$$\frac{p^{n-\nu_{m+1}}-1}{p-1}$$

sets of isomers of order $p^{h_{m+1}}$ in $G$. With the same reason, we see that the number of sets of isomers of order $p^{h_{m+1}}$ in a group of type (2) is

$$\frac{p^m-1}{p-1}\,p^{(m-1)(h_{m+1}-1)}/p^{(m-1)(h_{m+1}-1)}=\frac{p^m-1}{p-1}=M$$

$(\nu_{m+1}=0$, since $h_{m+1}<h_m)$.

Now, let $G^*$ be a subgroup of type (2) in $G$, let $S_1, S_2, \cdots, S_M$ be $M$ cyclic subgroups of order $p^{h_{m+1}}$ in $G^*$ such that no two of them are isomers in $G^*$ and, a fortiori, no two of them are isomers in $G$. The product of $G^*$ and any cyclic subgroup $S$ in $G$, which is an isomer of a certain $S_\nu$, is a group of order less than

$$p^c, \qquad c=\sum_{\nu=1}^{m+1} h_\nu.$$

The number of such subgroups $S$ is easily seen to be

$$\frac{p^m-1}{p-1}\,p^{(n-\nu_{m+1}-1)(h_{m+1}-1)+b}$$

(when $m=n-\nu_{m+1}$, this represents the number of all cyclic subgroups of order $p^{h_{m+1}}$ in $G$; when $m>n-\nu_{m+1}$, subgroup of type (2) does not exist at all). With the exception of these cyclic subgroups, the product of any cyclic subgroup of order $p^{h_{m+1}}$ (in $G$) and $G^*$ is a group of order $p^c$, type $(h_1, h_2, \cdots, h_m, h_{m+1})$.

On the other hand, every group $K$ of type $(h_1, h_2, \cdots, h_m, h_{m+1})$ contains $p^{mh_{m+1}}$ subgroups of type (2). One can find the proof of this in [2, p. 366]. Or, using directly formula (3) (since the theorem is

assumed to be true for the integer $m$), we have here

$$\begin{aligned}
H &= \sum_{i=1}^{m} (m+2-\nu_i-2i)(h_i-1) \\
&\quad + \frac{1}{2}(m_1^2+m_2^2+\cdots+m_r^2-m^2) \\
&\quad + \sum_{\mu=1}^{r} m_\mu(m_{\mu+1}h_{m_1+\cdots+m_{\mu+1}} + m_{\mu+2}h_{m_1+\cdots+m_{\mu+2}} + \cdots \\
&\quad + m_r h_m + h_{m+1}) \\
&= -m_1m_2(h_{m_1+m_2}-1) - m_3(m_1+m_2)(h_{m_1+m_2+m_3}-1) - \cdots \\
&\quad - m_r(m-m_r)(h_m-1) + \frac{1}{2}(m_1^2+\cdots+m_r^2-m^2) + mh_{m+1} \\
&\quad + \sum_{\mu=1}^{r-1} m_\mu(m_{\mu+1}h_{m_1+\cdots+m_{\mu+1}} + \cdots + m_r h_m) \\
&= mh_{m+1} + \frac{1}{2}(m_1+m_2+\cdots+m_r)^2 - \frac{1}{2}m^2 \\
&= mh_{m+1},
\end{aligned}$$

and

$$\prod_{i=1}^{m}(p^{m+2-\nu_i-i}-1) \Big/ \prod_{\mu=1}^{r}\prod_{\nu=1}^{m_\mu}(p^\nu-1) = 1,$$

hence the result.

Now let $H_1, H_2, \cdots, H_N$ ($N = p^{mh_m+1}$) be the $N$ subgroups of type (2) in $K$, let

$$K = H_\nu \times L_\nu \qquad (\nu = 1, 2, \cdots, N)$$

where $L_\nu$ is a cyclic subgroup of order $p^{h_m+1}$ with generator $l_\nu$. In every $H_\nu$ there are $p^{mh_m+1}$ elements of order not greater than $p^{h_m+1}$, say $g_{\nu 1}, g_{\nu 2}, \cdots, g_{\nu N}$. The $N$ elements $l_\nu g_{\nu\mu}$ ($\mu = 1, 2, \cdots, N$) generate $N$ different cyclic subgroups $L_{\nu 1}, L_{\nu 2}, \cdots, L_{\nu N}$ of order $p^{h_m+1}$ such that

$$H_\nu \times L_{\nu\mu} = H_\nu \times L_\nu = K \qquad (\mu = 1, 2, \cdots, N).$$

Hence every group of type $(h_1, h_2, \cdots, h_m, h_{m+1})$ can be obtained by $p^{2mh_m+1}$ cases of direct production of two groups of type $(h_1, h_2, \cdots, h_m)$ and $(h_{m+1})$ respectively. The number of subgroups of type $(h_1, h_2, \cdots, h_m, h_{m+1})$ in $G$ is therefore

$$
\begin{aligned}
&R_m\left(\frac{p^{n-\nu_{m+1}}-1}{p-1}-\frac{p^m-1}{p-1}\right)p^{(n-\nu_{m+1}-1)(h_{m+1}-1)+b}\Big/p^{2mh_{m+1}}\\
&\quad=R_m\frac{p^m(p^{n-m-\nu_{m+1}}-1)}{p-1}\,p^{(n-\nu_{m+1}-1)(h_{m+1}-1)-2mh_{m+1}+b}\\
&\quad=R_m\frac{p^{n-m-\nu_{m+1}}-1}{p-1}\,p^{(n-\nu_{m+1}+1-2(m+1))(h_{m+1}-1)+(1+m^2-(m+1)^2)/2+b}\\
&\quad=R_{m+1}, \qquad\qquad b=\sum_{\mu=0}^{\nu_{m+1}}k_\mu,
\end{aligned}
\tag{4}
$$

where $R_m$ denotes Formula (3) for subgroups of type (2), $R_{m+1}$ denotes the same formula for subgroups of type $(h_1, h_2, \cdots, h_m, h_{m+1})$.

When $h_{m+1}=h_m$, every group of type $(h_1, h_2, \cdots, h_m, h_{m+1})$ contains

$$\frac{p^{m_r+1}-1}{p-1}\,p^{mh_{m+1}-m_r}$$

subgroups of type $(h_1, h_2, \cdots, h_m)$, so it can be obtained by

$$\frac{p^{m_r+1}-1}{p-1}\,p^{mh_{m+1}-m_r}\cdot p^{mh_{m+1}}=\frac{p^{m_r+1}-1}{p-1}\,p^{2mh_{m+1}-m_r}$$

cases of direct production. Hence instead of (4) we have

$$
\begin{aligned}
&R_m\frac{p^m(p^{n-\nu_{m+1}-m}-1)}{p-1}\,p^{(n-\nu_{m+1}-1)(h_{m+1}-1)+b}\Big/\frac{p^{m_r+1}-1}{p-1}\,p^{2mh_{m+1}-m_r}\\
&\quad=R_m\frac{p^{n-\nu_{m+1}-m}-1}{p^{m_r+1}-1}\,p^{(n-\nu_{m+1}+1-2(m+1))(h_{m+1}-1)+((m_r+1)^2-m_r^2)/2-((m+1)^2-m^2)/2+b}\\
&\quad=R'_{m+1},
\end{aligned}
$$

which represents Formula (3) for subgroups of type $(h_1, h_2, \cdots, h_m, h_{m+1})$, when $h_{m+1}=h_m$.

The theorem is therefore proved by induction.

## References

1. G. A. Miller, *Number of the subgroups of any abelian group*, Proc. Nat. Acad. Sci. U.S.A. vol. 25 (1939) pp. 256–262.

2. ———, *Independent generators of the subgroups of an abelian group*, Ibid. pp. 364–367.

National University of Chekiang