Bull. Math. Soc. Sci. Math. Roumanie
Tome 53(101) No. 4, 2010, 373–386

An arithmetic method of counting the subgroups of a finite abelian group

by
Marius Tărnăuceanu

Abstract

The main goal of this paper is to apply the arithmetic method developed in our previous paper [13] to determine the number of some types of subgroups of finite abelian groups.

Key Words: Finite abelian groups, number of subgroups, number of cyclic subgroups, number of elements, matrices of integers.
2010 Mathematics Subject Classification: Primary 20K01; Secondary 20K27, 11C20, 15A36.

1 Introduction

One of the most important problems of the combinatorial abelian group theory is to determine the number of subgroups of a finite abelian group. This topic has enjoyed a constant evolution starting with the first half of the 20^{th} century. Since a finite abelian group is a direct product of abelian p-groups, the above counting problem is reduced to p-groups. Formulas which give the number of subgroups of type μ of a finite p-group of type λ were established by S. Delsarte (see [7]), P.E. Djubjuk (see [8]) and Y. Yeh (see [15]). An excellent survey on this subject together with connections to symmetric functions was written by M.L. Butler (see [5]) in 1994. Another way to find the total number of subgroups of finite abelian p-groups is presented in [6] and applied for rank two p-groups, as well as for elementary abelian p-groups. Also, remind here the paper [1] which gives an explicit formula for the number of subgroups in a finite abelian p-group by using divisor functions of matrices.

The starting point for our discussion is given by the paper [13] (see also Section I.2 of [14]), where we introduced and studied the concept of fundamental group lattice, that is the subgroup lattice of a finite abelian group. These lattices were successfully used to solve the problem of existence and uniqueness of a finite abelian group whose subgroup lattice is isomorphic to a fixed lattice (see Proposition 2.8 (§ 2.1) of [13]). Some steps in finding the total number of subgroups of several particular finite abelian groups have been made in Section 2.2 of [13], too.

The purpose of the current paper is to extend the above study, by applying the fundamental group lattices in counting some different types of subgroups of finite abelian groups. Explicit formulas are obtained for the number of subgroups of a given order in a finite abelian p-group of rank 2, improving Proposition 2.9 (§ 2.2) of [13], and for the number of maximal subgroups and cyclic subgroups of a given order of *arbitrary* finite abelian groups. The number of elements of a prescribed order in such a group will be also found.

The paper is organized as follows: in Section 2 we recall the notion of fundamental group lattice and its basic properties. Section 3 deals with the number of subgroups of finite abelian groups. In Section 4 the precise expressions for the number of cyclic subgroups, as well as for the number of elements of a given order in a finite abelian group will be determined. In the final section some conclusions and further research directions are indicated.

Most of our notation is standard and will usually not be repeated here. Basic definitions and results on lattices (respectively on groups) can be found in [9] (respectively in [12]). For subgroup lattice concepts we refer the reader to [10] and [14].

2 Fundamental group lattices

Let G be an abelian group of order n and $L(G)$ be the subgroup lattice of G. By the fundamental theorem of finitely generated abelian groups, there exist (uniquely determined by G) the numbers $k \in \mathbb{N}^*$, $d_1, d_2, ..., d_k \in \mathbb{N} \setminus \{0,1\}$ satisfying $d_1|d_2|...|\,d_k$, $d_1 d_2 \cdots d_k = n$ and

$$G \cong \bigtimes_{i=1}^{k} \mathbb{Z}_{d_i}.$$

This decomposition of a finite abelian group into a direct product of cyclic groups together with the form of subgroups of $\mathbb{Z}^k$ (see Lemma 2.1, § 2.1, [13]) leads us to the concept of fundamental group lattice, defined in the following manner:

Let $k{\geq}1$ be a natural number. Then, for each $(d_1, d_2, ..., d_k) \in (\mathbb{N}\setminus\{0,1\})^k$, we consider the set $L_{(k;d_1,d_2,...,d_k)}$ consisting of all matrices $A = (a_{ij}) \in \mathcal{M}_k(\mathbb{Z})$ which have the following properties:

i) $a_{ij} = 0$, for any $i > j$,

ii) $0 \leq a_{1j}, a_{2j}, ..., a_{j-1j} < a_{jj}$, for any $j = \overline{1,k}$,

iii) 1) $a_{11}|d_1$,

2) $a_{22}|\left(d_2, d_1\,\dfrac{a_{12}}{a_{11}}\right)$,

$$3)\ a_{33} \Big| \left(d_3, d_2\, \frac{a_{23}}{a_{22}}, d_1\, \frac{\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}{a_{22}a_{11}}\right),$$

$$\vdots$$

$$k)\ a_{kk} \Big| \left(d_k, d_{k-1}\, \frac{a_{k-1k}}{a_{k-1\,k-1}}, d_{k-2}\, \frac{\begin{vmatrix} a_{k-2\,k-1} & a_{k-2k} \\ a_{k-1\,k-1} & a_{k-1k} \end{vmatrix}}{a_{k-1\,k-1}a_{k-2\,k-2}}, ..., d_1\, \frac{\begin{vmatrix} a_{12} & a_{13} & \cdots & a_{1k} \\ a_{22} & a_{23} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{k-1\,k} \end{vmatrix}}{a_{k-1\,k-1}a_{k-2\,k-2}...a_{11}}\right),$$

where by $(x_1, x_2, ..., x_m)$ we denote the greatest common divisor of the numbers $x_1, x_2, ..., x_m \in \mathbb{Z}$. On the set $L_{(k;d_1,d_2,...,d_k)}$ we introduce the next partial ordering relation (denoted by $\leq$), as follows: for $A = (a_{ij})$, $B = (b_{ij}) \in L_{(k;d_1,d_2,...,d_k)}$, put $A \leq B$ if and only if the relations

$$1)'\ b_{11} | a_{11},$$

$$2)'\ b_{22} \Big| \left(a_{22}, \frac{\begin{vmatrix} a_{11} & a_{12} \\ b_{11} & b_{12} \end{vmatrix}}{b_{11}}\right),$$

$$3)'\ b_{33} \Big| \left(a_{33}, \frac{\begin{vmatrix} a_{22} & a_{23} \\ b_{22} & b_{23} \end{vmatrix}}{b_{22}}, \frac{\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \end{vmatrix}}{b_{22}b_{11}}\right),$$

$$\vdots$$

$$k)'\ b_{kk} \Big| \left(a_{kk}, \frac{\begin{vmatrix} a_{k-1\,k-1} & a_{k-1\,k} \\ b_{k-1\,k-1} & b_{k-1\,k} \end{vmatrix}}{b_{k-1\,k-1}}, \frac{\begin{vmatrix} a_{k-2\,k-2} & a_{k-2\,k-1} & a_{k-2\,k} \\ b_{k-2\,k-2} & b_{k-2\,k-1} & b_{k-2\,k} \\ 0 & b_{k-1\,k-1} & b_{k-1\,k} \end{vmatrix}}{b_{k-1\,k-1}b_{k-2\,k-2}}, ..., \frac{\begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ b_{11} & b_{12} & \cdots & b_{1k} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & b_{k-1\,k} \end{vmatrix}}{b_{k-1\,k-1}b_{k-2\,k-2}...b_{11}}\right)$$

hold. Then $(L_{(k;d_1,d_2,...,d_k)}, \leq)$ is a complete modular lattice, which is called a *fundamental group lattice of degree k*.

Moreover, from Proposition 2.2, § 2.1, [13], we know that $L_{(k;d_1,d_2,...,d_k)}$ is isomorphic to $L(G)$ and so the problem of counting the subgroups of G can be translated into an arithmetic problem: finding the number of elements of $L_{(k;d_1,d_2,...,d_k)}$.

On the other hand, if $n = p_1^{n_1} p_2^{n_2} ... p_m^{n_m}$ is the decomposition of n as a product of prime factors and

$$G \cong \bigtimes_{i=1}^{m} G_i$$

is the corresponding primary decomposition of G, then it is well-known that we have

$$L(G) \cong \bigtimes_{i=1}^{m} L(G_i).$$

The above lattice isomorphism shows that

$$|L(G)| = \prod_{i=1}^{m} |L(G_i)|,$$

therefore our counting problem is reduced to p-groups. In this way, we need to investigate only fundamental group lattices of type $L_{(k;p^{\alpha_1},p^{\alpha_2},...,p^{\alpha_k})}$, where p is a prime and $1 \le \alpha_1 \le \alpha_2 \le ... \le \alpha_k$. Concerning these lattices, the following elementary remarks will be very useful:

a) The order of the subgroup of $\bigtimes_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ corresponding to the matrix $A = (a_{ij}) \in L_{(k;p^{\alpha_1},p^{\alpha_2},...,p^{\alpha_k})}$ is

$$\frac{p^{\sum\limits_{i=1}^{k} \alpha_i}}{\prod\limits_{i=1}^{k} a_{ii}}.$$

b) The subgroup of $\bigtimes_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ corresponding to the matrix $A = (a_{ij}) \in L_{(k;p^{\alpha_1},p^{\alpha_2},...,p^{\alpha_k})}$ is cyclic if and only if $< (\overline{0}^1, \overline{0}^2, ..., \bar{a}_{kk}^k) > \subseteq < (\overline{0}^1, \overline{0}^2, ..., \bar{a}_{k-1\,k-1}^{k-1}, \bar{a}_{k-1\,k}^k) > \subseteq \cdots \subseteq < (\bar{a}_{11}^1 \bar{a}_{12}^2, ..., \bar{a}_{1k}^k) >$, where, for every $i = \overline{1,k}$, we denote by $\bar{x}^i$ the image of an element $x \in \mathbb{Z}$ through the canonical homomorphism: $\mathbb{Z} \to \mathbb{Z}_{p^{\alpha_i}}$.

c) If $A = (a_{ij})$ is an element of $L_{(k;p^{\alpha_1},p^{\alpha_2},\ldots,p^{\alpha_k})}$, then the linear system

$$A^{\top}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} p^{\alpha_1} \\ p^{\alpha_2} \\ \vdots \\ p^{\alpha_k} \end{pmatrix}$$

admits solutions in $\mathbb{Z}^k$.

3 The number of subgroups of a finite abelian group

As we have seen in the previous section, in order to determine the number of subgroups of finite abelian groups it suffices to reduce the study to p-groups and our problem is equivalent to the counting of elements of the fundamental group lattice $L_{(k;p^{\alpha_1},p^{\alpha_2},\ldots,p^{\alpha_k})}$. This consists of all matrices of integers $A = (a_{ij})_{i,j=\overline{1,k}}$ satisfying the conditions:

$$(*)\qquad \left\{\begin{array}{rl}
\text{i)} & a_{ij} = 0, \text{ for any } i > j, \\[1ex]
\text{ii)} & 0 \le a_{1j}, a_{2j}, \ldots, a_{j-1j} < a_{jj}, \text{ for any } j = \overline{1,k}, \\[1ex]
\text{iii)} & 1)\ a_{11} | p^{\alpha_1}, \\[1ex]
 & 2)\ a_{22} \Big| \left(p^{\alpha_2}, p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}\right), \\[2ex]
 & 3)\ a_{33} \Big| \left(p^{\alpha_3}, p^{\alpha_2}\,\dfrac{a_{23}}{a_{22}}, p^{\alpha_1}\,\dfrac{\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}{a_{22}a_{11}}\right), \\[1ex]
 & \vdots \\[1ex]
 & k)\ a_{kk} \Big| \left(p^{\alpha_k}, p^{\alpha_{k-1}}\,\dfrac{a_{k-1k}}{a_{k-1\,k-1}}, p^{\alpha_{k-2}}\,\dfrac{\begin{vmatrix} a_{k-2\,k-1} & a_{k-2k} \\ a_{k-1\,k-1} & a_{k-1k} \end{vmatrix}}{a_{k-1\,k-1}a_{k-2\,k-2}}, \ldots,\right. \\[3ex]
 & \qquad\qquad \left. p^{\alpha_1}\,\dfrac{\begin{vmatrix} a_{12} & a_{13} & \cdots & a_{1k} \\ a_{22} & a_{23} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_{k-1\,k} \end{vmatrix}}{a_{k-1\,k-1}a_{k-2\,k-2}\ldots a_{11}}\right).
\end{array}\right.$$

An explicit formula for $|L_{(k;p^{\alpha_1},p^{\alpha_2},\ldots,p^{\alpha_k})}|$, and consequently for $|L(\mathop{\Large\times}\limits_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}})|$, can be easily obtained in the particular case $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 1$ (see Proposition 2.12, § 2.2, [13]).

Proposition 3.1. *For $\alpha \in \{0, 1, ..., k\}$, the number of all subgroups of order $p^{k-\alpha}$ in the finite elementary abelian p-group $\mathbb{Z}_p^k$ is 1 if $\alpha = 0$ or $\alpha = k$, and $\sum\limits_{1 \le i_1 < i_2 < ... < i_\alpha \le k} p^{i_1+i_2+...+i_\alpha - \frac{\alpha(\alpha+1)}{2}}$ if $1 \le \alpha \le k-1$. In particular, the total number of subgroups of $\mathbb{Z}_p^k$ is $2 + \sum\limits_{\alpha=1}^{k-1} \sum\limits_{1 \le i_1 < i_2 < ... < i_\alpha \le k} p^{i_1+i_2+...+i_\alpha - \frac{\alpha(\alpha+1)}{2}}$.*

In the general case, our method gives an immediate result in counting the maximal subgroups of $\bigtimes\limits_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$. By the first remark of Section 2, such a subgroup corresponds to a matrix $A = (a_{ij}) \in L_{(k;p^{\alpha_1}, p^{\alpha_2}, ..., p^{\alpha_k})}$ satisfying $\prod\limits_{i=1}^{k} a_{ii} = p$. Then $a_{ii} = p$ for some $i \in \{1, 2, ..., k\}$ and $a_{jj} = 1$ for all $j \neq i$. From the condition ii) of $(*)$ we get $a_{1j} = a_{2j} = \cdots = a_{j-1j} = 0$, for all $j \neq i$. Remark also that the condition iii) is satisfied and thus the elements $a_{1i}, a_{2i}, ..., a_{i-1i}$ can be chosen arbitrarily from the set $\{0, 1, ..., p-1\}$. Therefore we have p^{i-1} distinct solutions of the system $(*)$. Summing up these quantities for $i = \overline{1, k}$, we determine the number of maximal subgroups of the finite abelian p-group $\bigtimes\limits_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$.

Proposition 3.2. *The number of maximal subgroups of $\bigtimes\limits_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ is $\dfrac{p^k - 1}{p - 1}$.*

Next, we return to the problem of finding the total number of subgroups of $\bigtimes\limits_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$. We shall apply our method for rank two abelian p-groups, i.e. when $k = 2$ (clearly, it can be extended in a natural way for an arbitrary k). Note also that the following theorem improves Proposition 2.9, § 2.2, [13], by indicating the number of subgroups of a fixed order in such a group and by giving a proof founded on fundamental group lattices.

Theorem 3.3. *For every $0 \le \alpha \le \alpha_1 + \alpha_2$, the number of all subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in the finite abelian p-group $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is:*

$$\begin{cases} \dfrac{p^{\alpha+1}-1}{p-1}, & \textit{if} \quad 0 \le \alpha \le \alpha_1 \\ \dfrac{p^{\alpha_1+1}-1}{p-1}, & \textit{if} \quad \alpha_1 \le \alpha \le \alpha_2 \\ \dfrac{p^{\alpha_1+\alpha_2-\alpha+1}-1}{p-1}, & \textit{if} \quad \alpha_2 \le \alpha \le \alpha_1+\alpha_2. \end{cases}$$

In particular, the total number of subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ *is*

$$\frac{1}{(p-1)^2}\left[(\alpha_2-\alpha_1+1)p^{\alpha_1+2}-(\alpha_2-\alpha_1-1)p^{\alpha_1+1}-(\alpha_1+\alpha_2+3)p+(\alpha_1+\alpha_2+1)\right].$$

Proof: Let $A=(a_{ij})$ be a solution of $(*)$ for $k=2$, corresponding to a subgroup of order $p^{\alpha_1+\alpha_2-\alpha}$. In this situation, the condition iii) of $(*)$ becomes

$$a_{11}|p^{\alpha_1} \quad \text{and} \quad a_{22}|\left(p^{\alpha_2}, p^{\alpha_1}\frac{a_{12}}{a_{11}}\right).$$

Put $a_{11}=p^i$, where $0 \le i \le \alpha_1$. Then $a_{22}=p^{\alpha-i}$ and so $p^{\alpha-i}|(p^{\alpha_2}, p^{\alpha_1-i}a_{12})$, that is $p^{\alpha-i}|p^{\alpha_1-i}(p^{\alpha_2-\alpha_1+i}, a_{12})$. If $0 \le \alpha \le \alpha_1$, we must have $i \le \alpha$ and the above condition is satisfied by all $a_{12} < p^{\alpha-i}$. So, one obtains $p^{\alpha-i}$ distinct solutions of $(*)$, which implies that the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$(1) \qquad S_1(\alpha)=\sum_{i=0}^{\alpha} p^{\alpha-i}=\frac{p^{\alpha+1}-1}{p-1}\,.$$

Suppose now that $\alpha_1 \le \alpha \le \alpha_2$. Then $p^{\alpha_1-\alpha}|(p^{\alpha_2-\alpha_1+i}, a_{12})$ and thus a_{12} can be any multiple of $p^{\alpha_1-\alpha}$ in the set $\{0,1,...,p^{\alpha-i}-1\}$. It results p^{α_1-i} distinct solutions of $(*)$ and the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$(2) \qquad S_2(\alpha)=\sum_{i=0}^{\alpha_1} p^{\alpha_1-i}=\frac{p^{\alpha_1+1}-1}{p-1}\,.$$

Finally, assume that $\alpha_2 \le \alpha \le \alpha_1+\alpha_2$. We must have $\alpha_1-\alpha \le \alpha_2-\alpha_1+i$ and the number of distinct solutions of $(*)$ is again p^{α_1-i}. Thus the number of subgroups of order $p^{\alpha_1+\alpha_2-\alpha}$ in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ is in this case

$$(3) \qquad S_2(\alpha)=\sum_{i=\alpha-\alpha_2}^{\alpha_1} p^{\alpha_1-i}=\frac{p^{\alpha_1+\alpha_2-\alpha+1}-1}{p-1}\,.$$

By using the equalities (1), (2) and (3), one obtains the total number of subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$, namely

$$\sum_{\alpha=0}^{\alpha_1} S_1(\alpha) + \sum_{\alpha=\alpha_1+1}^{\alpha_2} S_2(\alpha) + \sum_{\alpha=\alpha_2+1}^{\alpha_1+\alpha_2} S_3(\alpha) = \frac{1}{(p-1)^2}\left[(\alpha_2-\alpha_1+1)p^{\alpha_1+2}- \right.$$
$$\left. -(\alpha_2-\alpha_1-1)p^{\alpha_1+1}-(\alpha_1+\alpha_2+3)p+(\alpha_1+\alpha_2+1)\right],$$

which completes our proof. □

In the following let us denote by $f_p(i,j)$ the number of all subgroups of the finite abelian p-group $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$ $(i \leq j)$, determined in Theorem 3.3. Note that we have

$$\begin{aligned}
&f_p(i,j) = \\
&= \frac{1}{(p-1)^2}\left[(j-i+1)p^{i+2}-(j-i-1)p^{i+1}-(i+j+3)p+(i+j+1)\right] = \\
&= (j-i+1)p^i+(j-i+3)p^{i-1}+\cdots+(i+j-1)p+(i+j+1).
\end{aligned}$$

Put $f_p(i,j) = f_p(j,i)$, for all $i > j$, and let n be a fixed positive integer and $A_p(n)$ be the matrix $(f_p(i,j))_{i,j=\overline{0,n}}$. Then $A_p(n)$ induces a quadratic form $\sum\limits_{i,j=0}^{n} f_p(i,j)X^iY^j$. Because

$$\det A_p(n) = (p-1)p^{n-1} \det A_p(n-1),$$

by induction on n one easily obtains

$$\det A_p(n) = (p-1)^n p^{\frac{n(n-1)}{2}}, \text{ for any } n \geq 1.$$

Hence, we have proved the next two corollaries.

Corollary 3.4. *The quadratic form* $\sum\limits_{i,j=0}^{n} f_p(i,j)X^iY^j$ *induced by the matrix* $A_p(n)$ *is positive definite, for all* $n \in \mathbb{N}^*$.

Corollary 3.5. *All eigenvalues of the matrix* $A_p(n)$ *are positive, for all* $n \in \mathbb{N}^*$.

4 The number of cyclic subgroups of a finite abelian group

Another interesting application of fundamental group lattices (not studied in [13]) is the counting of cyclic subgroups of finite abelian groups. First of all, we obtain this number for a finite abelian p-group of rank 2. By the second remark of Section 2, the subgroup of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ determined by the matrix $A = (a_{ij})$ is cyclic if and only if $< (\overline{0}^1, \bar{a}^2_{22}) > \subseteq < (\bar{a}^1_{11}, \bar{a}^2_{12}) >$. This necessary and sufficient condition can be rewritten in the following manner.

Lemma 4.1. *The subgroup of* $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ *corresponding to the matrix* $A = (a_{ij}) \in L_{(2;p^{\alpha_1},p^{\alpha_2})}$ *is cyclic if and only if* $a_{22} = \left(p^{\alpha_2}, p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}\right)$.

Proof: If $< (\overline{0}^1, \bar{a}^2_{22}) > \subseteq < (\bar{a}^1_{11}, \bar{a}^2_{12}) >$, then we can choose an integer x such that $(\overline{0}^1, \bar{a}^2_{22}) = x(\bar{a}^1_{11}, \bar{a}^2_{12})$. It results $p^{\alpha_1} | x a_{11}$ and $p^{\alpha_2} | x a_{12} - a_{22}$, therefore there exist $y, z \in \mathbb{Z}$ satisfying $x a_{11} = y p^{\alpha_1}$ and $x a_{12} - a_{22} = z p^{\alpha_2}$. These equalities imply that $a_{22} = -z p^{\alpha_2} + y p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}$, which together with the condition 2) of iii) in $(*)$ show that $a_{22} = \left(p^{\alpha_2}, p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}\right) \cdot$

Conversely, suppose that $a_{22} = \left(p^{\alpha_2}, p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}\right) \cdot$ Then there are $y, z \in \mathbb{Z}$ with $a_{22} = -z p^{\alpha_2} + y p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}} \cdot$ Taking $x = y\,\dfrac{p^{\alpha_1}}{a_{11}} \in \mathbb{Z}$, we easily obtain $(\overline{0}^1, \bar{a}^2_{22}) = x(\bar{a}^1_{11}, \bar{a}^2_{12})$ and so $< (\overline{0}^1, \bar{a}^2_{22}) >$ is contained in $< (\bar{a}^1_{11}, \bar{a}^2_{12}) >$. □

By using the above lemma, the problem of finding the number of cyclic subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ reduces to an elementary arithmetic exercise.

Theorem 4.2. *For every* $0 \le \alpha \le \alpha_2$*, the number of cyclic subgroups of order* p^α *in the finite abelian p-group* $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ *is:*

$$\begin{cases} 1, & \text{if} \quad \alpha = 0 \\ p^\alpha + p^{\alpha-1}, & \text{if} \quad 1 \le \alpha \le \alpha_1 \\ p^{\alpha_1}, & \text{if} \quad \alpha_1 < \alpha \le \alpha_2. \end{cases}$$

In particular, the number of all cyclic subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ *is*

$$2 + 2p + \cdots + 2p^{\alpha_1 - 1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1}.$$

Proof: Denote by $g^2_p(\alpha)$ the number of cyclic subgroups of order p^α in $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$ and let $A{=}(a_{ij}) \in L_{(2;p^{\alpha_1},p^{\alpha_2})}$ be the matrix corresponding to such a subgroup. Then $a_{11} | p^{\alpha_1}$, $a_{22}{=}\left(p^{\alpha_2}, p^{\alpha_1}\,\dfrac{a_{12}}{a_{11}}\right)$ and $a_{11}a_{22}{=}p^{\alpha_1+\alpha_2-\alpha}$. Taking $a_{11}{=}p^i$ with $0 \le i \le \alpha_1$, we obtain

$$a_{22} = p^{\alpha_1+\alpha_2-\alpha-i} = (p^{\alpha_2}, p^{\alpha_1-i}a_{12}) = p^{\alpha_1-i}(p^{\alpha_2-\alpha_1+i}, a_{12}),$$

which implies that

$$p^{\alpha_2-\alpha} = \left(p^{\alpha_2-\alpha_1+i}, a_{12}\right). \tag{4}$$

Clearly, for $\alpha = 0$ it results $a_{11} = p^{\alpha_1}$, $a_{22} = p^{\alpha_2}$, $a_{12} = 0$, and thus

$$g_p^2(0) = 1. \tag{5}$$

For $1 \le \alpha \le \alpha_1$ we must have $\alpha_1 - \alpha \le i$. If $i = \alpha_1 - \alpha$, the condition (4) is equivalent to $p^{\alpha_2-\alpha}|a_{12}$, therefore a_{12} can be chosen in p^α ways. If $\alpha_1-\alpha+1 \le i$, (4) is equivalent to

$$p^{\alpha_2-\alpha}|a_{12} \;\text{ and }\; p^{\alpha_2-\alpha+1} \nmid a_{12}.$$

There are $p^{\alpha_1-i} - p^{\alpha_1-i-1}$ elements of the set $\{0, 1, ..., p^{\alpha_1+\alpha_2-\alpha-i}\}$ which satisfy the previous relations. So, one obtains

$$g_p^2(\alpha) = p^\alpha + \sum_{i=\alpha_1-\alpha+1}^{\alpha_1} \left(p^{\alpha_1-i} - p^{\alpha_1-i-1}\right) = p^\alpha + p^{\alpha-1}, \text{ for } 1 \le \alpha \le \alpha_1. \tag{6}$$

Mention that if $\alpha_1 < \alpha \le \alpha_2$, then the condition $\alpha_1 - \alpha \le i$ is satisfied by all $i = \overline{1, \alpha_1}$, and hence

$$g_p^2(\alpha) = \sum_{i=0}^{\alpha_1} \left(p^{\alpha_1-i} - p^{\alpha_1-i-1}\right) = p^{\alpha_1}, \text{ for } \alpha_1 < \alpha \le \alpha_2. \tag{7}$$

Now, the equalities (5)-(7) give us the total number of cyclic subgroups of $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}}$, namely

$$\begin{aligned} 1 + \sum_{\alpha=1}^{\alpha_1} \left(p^\alpha + p^{\alpha-1}\right) + \sum_{\alpha=\alpha_1+1}^{\alpha_2} p^{\alpha_1} = \\ = \frac{1}{p-1}\left[(\alpha_2 - \alpha_1 + 1)p^{\alpha_1+1} - (\alpha_2 - \alpha_1 - 1)p^{\alpha_1} - 2\right] = \\ = 2 + 2p + \cdots + 2p^{\alpha_1-1} + (\alpha_2 - \alpha_1 + 1)p^{\alpha_1} \end{aligned}$$

and our proof is finished. □

The above method can be used for an arbitrary $k > 2$, too. In order to do this we need to remark that

$$g_p^2(\alpha) = \frac{p^\alpha h_p^1(\alpha) - p^{\alpha-1} h_p^1(\alpha - 1)}{p^\alpha - p^{\alpha-1}}, \text{ for all } \alpha \ne 0,$$

where

$$h_p^1(\alpha) = \begin{cases} p^\alpha, & \text{if } \quad 0 \le \alpha \le \alpha_1 \\ p^{\alpha_1}, & \text{if } \quad \alpha_1 \le \alpha. \end{cases}$$

This equality extends to the general case in the following way.

Theorem 4.3. *For every* $1 \leq \alpha \leq \alpha_k$, *the number of cyclic subgroups of order* p^α *in the finite abelian p-group* $\bigtimes_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ *is*

$$g_p^k(\alpha) = \frac{p^\alpha h_p^{k-1}(\alpha) - p^{\alpha-1} h_p^{k-1}(\alpha-1)}{p^\alpha - p^{\alpha-1}},$$

where

$$h_p^{k-1}(\alpha) = \begin{cases} p^{(k-1)\alpha}, & \textit{if} \quad 0 \leq \alpha \leq \alpha_1 \\ p^{(k-2)\alpha+\alpha_1}, & \textit{if} \quad \alpha_1 \leq \alpha \leq \alpha_2 \\ \vdots & \\ p^{\alpha_1+\alpha_2+\ldots+\alpha_{k-1}}, & \textit{if} \quad \alpha_{k-1} \leq \alpha. \end{cases}$$

Note that $g_p^k(0) = 1$ and the number of all cyclic subgroups of $\bigtimes_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ can be easily determined from Theorem 4.3. Since the numbers of cyclic subgroups and of elements of a given order in a finite abelian p-group are closely connected (through the well-known Euler's function φ), we also infer the following consequence of Theorem 4.3.

Corollary 4.4. *The number of all elements of order* p^α, $1 \leq \alpha \leq \alpha_k$, *in the finite abelian p-group* $\bigtimes_{i=1}^{k} \mathbb{Z}_{p^{\alpha_i}}$ *is*

$$g_p^k(\alpha)\varphi(p^\alpha) = g_p^k(\alpha)\left(p^\alpha - p^{\alpha-1}\right) = p^\alpha h_p^{k-1}(\alpha) - p^{\alpha-1} h_p^{k-1}(\alpha-1).$$

As we have seen in Section 2, counting the subgroups of finite abelian groups can be reduced to p-groups. The same thing can be also said for cyclic subgroups and for elements of a given order in an arbitrary finite abelian group G. Suppose that $p_1^{n_1} p_2^{n_2} ... p_m^{n_m}$ is the decomposition of $|G|$ as a product of prime factors and let $\bigtimes_{i=1}^{m} G_i$ be the corresponding primary decomposition of G. Then every cyclic subgroup H of order $p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{a_m}$ of G can be uniquely written as a direct product $\bigtimes_{i=1}^{m} H_i$, where H_i is a cyclic subgroup of order $p_i^{\alpha_i}$ of G_i, $i = \overline{1, m}$. This remark leads to the following result, that generalizes Theorem 4.3. and Corollary 4.4.

Corollary 4.5. *Under the previous hypotheses, for every* $(\alpha_1, \alpha_2, ..., \alpha_m) \in \mathbb{N}^m$ *with* $\alpha_i \leq n_i$, $i = \overline{1, m}$, *the number of cyclic subgroups (respectively of elements) of order* $p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ *in* G *is*

$$\prod_{i=1}^{m} g_{p_i}^{k_i}(\alpha_i)$$

(*respectively*

$$\prod_{i=1}^{m} g_{p_i}^{k_i}(\alpha_i)\varphi(p_i^{\alpha_i})),$$

where k_i *denotes the number of direct factors of* G_i, $i = \overline{1, m}$.

5 Conclusions and further research

All our previous results show that the arithmetic method introduced in [13] and applied in this paper can constitute an alternative way to study the subgroups of finite abelian groups. Clearly, it can successfully be used in solving many computational problems in (finite) abelian group theory. These will surely be the subject of some further research.

Finally, we mention several open problems concerning this topic.

Problem 5.1. Extend Theorem 3.3, by indicating explicit formulas for the number of subgroups of a fixed order and for the total number of subgroups of a finite abelian p-group of an *arbitrary* rank.

Problem 5.2. Let G be a finite abelian group. Use the description of $L(G)$ given by the above arithmetic method and the well-known description of $Aut(G)$ to determine the characteristic subgroups of G.

Problem 5.3. By using the defining relations of a fundamental group lattice, create a computer algebra program that generates the subgroups of a finite abelian group.

Problem 5.4. Let G_1 be a finite abelian group and G_2 be a finite group such that $\mid G_1 \mid = \mid G_2 \mid = n$. Denote $\pi_e(G_i) = \{o(a) \mid a \in G_i\}$ and, for every divisor d of n, let $n_i(d)$ be the number of elements of order d in G_i, $i = 1, 2$ (remark that the numbers $n_1(d)$ are known, by Corollary 4.5). Is it true that the conditions

a) $\pi_e(G_1) = \pi_e(G_2)$,

b) $n_1(d) = n_2(d)$, for all d,

imply the group isomorphism $G_1 \cong G_2$? (In other words, study whether a finite abelian group is determined by the set of its element orders and by the numbers of elements of any fixed order).

Acknowledgement. The authors are grateful to the reviewers for their remarks which improve the previous version of the paper.

References

[1] Bhowmik, G., *Evaluation of the divisor function of matrices*, Acta Arith. **74** (1996), 155-159.

[2] Bhowmik, G., Ramaré, O., *Average orders of multiplicative arithmetical functions of integer matrices*, Acta Arith. **66** (1994), 45-62.

[3] Bhowmik, G., Ramaré, O., *Algebra of matrix arithmetic*, J. Algebra **210** (1998), 194-215.

[4] Birkhoff, G., *Subgroups of abelian groups*, Proc. Lond. Math. Soc. **38** (1934, 1935), 385-401.

[5] Butler, M.L., *Subgroup lattices and symmetric functions*, Mem. Amer. Math. Soc., vol. 112, no. **539**, 1994.

[6] Călugăreanu, Gr.G., *The total number of subgroups of a finite abelian group*, Sci. Math. Jpn. (1) **60** (2004), 157-167.

[7] Delsarte, S., *Functions de Möbius sur les groupes abeliens finis*, Ann. of Math. **49** (1948), 600-609.

[8] Djubjuk, P.E., *On the number of subgroups of a finite abelian group*, Izv. Akad. Nauk SSR Ser. Mat. **12** (1948), 351-378.

[9] Grätzer, G., *General lattice theory*, Academic Press, New York, 1978.

[10] Schmidt, R., *Subgroup lattices of groups*, de Gruyter Expositions in Mathematics 14, de Gruyter, Berlin, 1994.

[11] Suzuki, M., *On the lattice of subgroups of finite groups*, Trans. Amer. Math. Soc. **70** (1951), 345-371.

[12] Suzuki, M., *Group theory*, I, II, Springer Verlag, Berlin, 1982, 1986.

[13] Tărnăuceanu, M., *A new method of proving some classical theorems of abelian groups*, Southeast Asian Bull. Math. (6) **31** (2007), 1191-1203.

[14] Tărnăuceanu, M., *Groups determined by posets of subgroups*, Ed. Matrix Rom, Bucureşti, 2006.

[15] Yeh, Y., *On prime power abelian groups*, Bull. Amer. Math. Soc. **54** (1948), 323-327.

Received: 15.09.2008
Revised: 05.02.2010
Accepted: 11.05.2010

Faculty of Mathematics
"Al.I. Cuza" University
Iaşi, Romania
E-mail: tarnauc@uaic.ro