Bull. Math. Soc. Sci. Math. Roumanie
Tome 55(103) No. 4, 2012, 423–428

On the number of cyclic subgroups of a finite Abelian group

by
László Tóth *

Abstract

We prove by using simple number-theoretic arguments formulae concerning the number of elements of a fixed order and the number of cyclic subgroups of a direct product of several finite cyclic groups. We point out that certain multiplicative properties of related counting functions for finite Abelian groups are immediate consequences of these formulae.

Key Words: Finite Abelian group, cyclic subgroup, order of elements, multiplicative arithmetic function.
2010 Mathematics Subject Classification: Primary 20K01, 20K27, Secondary 11A25.

1 Introduction

Consider an arbitrary finite Abelian group G of order $\#G > 1$. Let $c_\delta(G)$ and $c(G)$ denote the number of cyclic subgroups of order δ ($\delta \mid \#G$) and the number of all cyclic subgroups of G, respectively.

Let $\#G = p_1^{a_1} \cdots p_r^{a_r}$ be the prime power factorization of $\#G$ and let $G \simeq G_1 \times \cdots \times G_r$ be the primary decomposition of the group G, where $\#G_i = p_i^{a_i}$ $(1 \leq i \leq r)$. Furthermore, let $L(G)$ and $L(G_i)$ denote the subgroup lattices of G and G_i $(1 \leq i \leq r)$, respectively. It is known the lattice isomorphism $L(G) \simeq L(G_1) \times \cdots \times L(G_r)$. See R. Schmidt [7], M. Suzuki [10]. It follows that

$$c_\delta(G) = c_{\delta_1}(G_1) \cdots c_{\delta_r}(G_r), \tag{1}$$

where $\delta = \delta_1 \cdots \delta_r$ and $\delta_i = p_i^{b_i}$ with some exponents $b_i \leq a_i$ $(1 \leq i \leq r)$. Also,

$$c(G) = c(G_1) \cdots c(G_r). \tag{2}$$

Consider now a p-group $G_{(p)}$ of type $(\lambda_1, \ldots, \lambda_k)$ with $1 \leq \lambda_1 \leq \ldots \leq \lambda_k$. It is known that the number of cyclic subgroups of order p^ν of $G_{(p)}$ is

$$c_{p^\nu}(G_{(p)}) = \frac{p^{k-j_\nu} - 1}{p-1} p^{\lambda_0+\lambda_1+\ldots+\lambda_{j_\nu}+(k-j_\nu-1)(\nu-1)}, \tag{3}$$

*The author gratefully acknowledges support from the Austrian Science Fund (FWF) under the project Nr. M1376-N18.

where $\lambda_{j_\nu} < \nu \leq \lambda_{j_\nu+1}$ and $\lambda_0 = 0$. See G. A. Miller [6], Y. Yeh [13].

For every finite Abelian group G the value of $c_\delta(G)$ is therefore completely determined by formulae (1) and (3). Obviously, $c(G) = \sum_{\delta|\#G} c_\delta(G)$, leading to a formula for $c(G)$.

Recently, formula (3) was recovered by M. Tărnăuceanu [11, Th. 4.3], in a slightly different form, by a method based on properties of certain matrices attached to the invariant factor decomposition of an Abelian group G, i.e., $G \simeq C_{i_1} \times \cdots \times C_{i_s}$, where $i_1 \cdots i_s = \#G$, $i_1 \mid i_2 \mid \ldots \mid i_s$, C_k denoting the cyclic group of order k.

For arbitrary positive integers $r, n_1, \ldots, n_r$ consider in what follows the direct product $C_{n_1} \times \cdots \times C_{n_r}$ and denote by $c(n_1, \ldots, n_r)$ the number of its cyclic subgroups. Let ϕ denote Euler's function.

Theorem 1. *For any $n_1, \ldots, n_r \geq 1$, $c(n_1, \ldots, n_r)$ is given by the formula*

$$c(n_1, \ldots, n_r) = \sum_{d_1|n_1,\ldots,d_r|n_r} \frac{\phi(d_1)\cdots\phi(d_r)}{\phi(\mathrm{lcm}(d_1, \ldots, d_r))}. \tag{4}$$

Formula (4) was derived in [12] using the orbit counting lemma (Burnside's lemma). Consequently, the number of all cyclic subgroups of a finite Abelian group can be given by formula (4) in a more compact form. Namely, consider the invariant factor decomposition of G given above and apply (4) by selecting $r = s$ and $n_1 = i_1, \ldots, n_s = i_s$. Note that (4) can be used also starting with the primary decomposition of G.

In the case $r = 2$, by using the identity $\phi(d_1)\phi(d_2) = \phi(\gcd(d_1, d_2))\phi(\mathrm{lcm}(d_1, d_2))$ $(d_1, d_2 \geq 1)$ we deduce from (4) the next result:

Corollary 1. *For every $n_1, n_2 \geq 1$ the number of cyclic subgroups of $C_{n_1} \times C_{n_2}$ is*

$$c(n_1, n_2) = \sum_{d_1|n_1,d_2|n_2} \phi(\gcd(d_1, d_2)). \tag{5}$$

It is the purpose of the present paper to give another direct proof of Theorem 1, using simple number-theoretic arguments. In fact, we prove the following formulae concerning the number $o_\delta(n_1, \ldots, n_r)$ of elements of order δ in $C_{n_1} \times \cdots \times C_{n_r}$. Let $n := \mathrm{lcm}(n_1, \ldots, n_r)$. Obviously, the order of every element of the direct product is a divisor of n. Let μ be the Möbius function.

Theorem 2. *For every $n_1, \ldots, n_r \geq 1$ and every $\delta \mid n$,*

$$o_\delta(n_1, \ldots, n_r) = \sum_{e|\delta} \gcd(e, n_1)\cdots\gcd(e, n_r)\mu(\delta/e) \tag{6}$$

$$= \sum_{\substack{d_1|n_1,\ldots,d_r|n_r \\ \mathrm{lcm}(d_1,\ldots,d_r)=\delta}} \phi(d_1)\cdots\phi(d_r). \tag{7}$$

Let $c_\delta(n_1, \ldots, n_r)$ denote the number of cyclic subgroups of order δ $(\delta \mid n)$ of the group $C_{n_1} \times \cdots \times C_{n_r}$. Since a cyclic subgroup of order δ has $\phi(\delta)$ generators,

$$c_\delta(n_1, \ldots, n_r) = \frac{o_\delta(n_1, \ldots, n_r)}{\phi(\delta)}. \tag{8}$$

Now (4) follows immediately from (7) and (8) by $c(n_1, \ldots, n_r) = \sum_{\delta|n} c_\delta(n_1, \ldots, n_r)$.

Corollary 2. *For every prime p and every $a_1, \dots, a_r \geq 1$, $1 \leq \nu \leq \max(a_1, \dots, a_r)$,*

$$c_{p^\nu}(p^{a_1}, \dots, p^{a_r}) = \frac{1}{p^{\nu-1}(p-1)} \left(p^{\min(\nu,a_1)+\dots+\min(\nu,a_r)} - p^{\min(\nu-1,a_1)+\dots+\min(\nu-1,a_r)} \right). \quad (9)$$

Here (9) follows at once by (6). In case of a p-group of type $(\lambda_1, \dots, \lambda_k)$ and choosing $r = k$, $a_1 = \lambda_1, \dots, a_k = \lambda_k$, (9) reduces to (3).

The proof of Theorem 2 is contained in Section 2. Additional remarks are given in Section 3. We point out, among others, that the multiplicative properties (1) and (2) are direct consequences of the formulae included in Theorems 1 and 2.

2 Proof of Theorem 2

Let $o(x)$ denote the order of a group element x. Let $G = C_{n_1} \times \dots \times C_{n_r}$ in short. Let $x_i \in C_{n_i}$ such that $o(x_i) = n_i$ $(1 \leq i \leq r)$. Then $G = \{x = (x_1^{i_1}, \dots, x_r^{i_r}) : 1 \leq i_1 \leq n_1, ..., 1 \leq i_r \leq n_r\}$.

Using elementary properties of the order of elements in a group and of the gcd and lcm of integers, respectively we deduce that for every $x = (x_1^{i_1}, \dots, x_r^{i_r}) \in G$,

$$o(x) = \operatorname{lcm}(o(x_1^{i_1}), \dots, o(x_r^{i_r})) = \operatorname{lcm}\left(\frac{o(x_1)}{\gcd(o(x_1), i_1)}, \dots, \frac{o(x_r)}{\gcd(o(x_r), i_r)} \right)$$

$$= \operatorname{lcm}\left(\frac{n_1}{\gcd(n_1, i_1)}, \dots, \frac{n_r}{\gcd(n_r, i_r)} \right) = \operatorname{lcm}\left(\frac{n}{\gcd(n, i_1 n/n_1)}, \dots, \frac{n}{\gcd(n, i_r n/n_r)} \right)$$

$$= \frac{n}{\gcd(i_1 n/n_1, \dots, i_r n/n_r, n)}.$$

Assume that $o(x) = \delta$, where $\delta \mid n$ is fixed. Then $\gcd(i_1 n/n_1, \dots, i_r n/n_r, n) = n/\delta$.

Write $i_1 n/n_1 = j_1 n/\delta, \dots, i_r n/n_r = j_r n/\delta$. Then $\gcd(j_1, \dots, j_r, \delta) = 1$ and $j_1 = \delta i_1/n_1$, ..., $j_r = \delta i_r/n_r$ are integers, that is $\delta i_1 \equiv 0 \pmod{n_1}$, ..., $\delta i_r \equiv 0 \pmod{n_r}$. We obtain, as solutions of these linear congruences, that $i_1 = k_1 n_1/\gcd(\delta, n_1)$ with $1 \leq k_1 \leq \gcd(\delta, n_1)$, ..., $i_r = k_r n_r/\gcd(\delta, n_r)$ with $1 \leq k_r \leq \gcd(\delta, n_r)$.

Therefore, the number of elements of order δ in G is the number of ordered r-tuples $(k_1, \dots, k_r)$ satisfying the conditions

(i) $1 \leq k_1 \leq \gcd(\delta, n_1), \dots, 1 \leq k_r \leq \gcd(\delta, n_r)$ and

(ii) $\gcd\left(k_1 \frac{\delta}{\gcd(\delta,n_1)}, \dots, k_r \frac{\delta}{\gcd(\delta,n_r)}, \delta\right) = 1$.

Using the familiar formula $\sum_{d|n} \mu(d) = 1$ for $n = 1$ and 0 otherwise, this can be written as

$$o_\delta(n_1, \dots, n_r) = \sum_{e|\delta} \mu(e) \sum_{\substack{k_1 \leq \gcd(\delta,n_1) \\ e \mid k_1 \frac{\delta}{\gcd(\delta,n_1)}}} \cdots \sum_{\substack{k_r \leq \gcd(\delta,n_r) \\ e \mid k_r \frac{\delta}{\gcd(\delta,n_r)}}} 1.$$

Here the linear congruence $k_1 \frac{\delta}{\gcd(\delta,n_1)} \equiv 0 \pmod{e}$ has $\gcd(e, \frac{\delta}{\gcd(\delta,n_1)})$ solutions in $k_1 \pmod{e}$, and $(\text{mod } \gcd(\delta, n_1))$ it has exactly

$$\frac{\gcd(\delta, n_1)}{e} \gcd\left(e, \frac{\delta}{\gcd(\delta, n_1)}\right) = \gcd\left(\gcd(\delta, n_1), \frac{\delta}{e}\right) = \gcd\left(\frac{\delta}{e}, n_1\right)$$

solutions (similar for the indexes $2, ..., r$). Hence,

$$o_\delta(n_1, \dots, n_r) = \sum_{e|\delta} \mu(e) \gcd(\delta/e, n_1) \cdots \gcd(\delta/e, n_r)$$

$$= \sum_{e|\delta} \mu(\delta/e) \gcd(e, n_1) \cdots \gcd(e, n_r),$$

which is formula (6).

Now using the identity $\sum_{d|n} \phi(d) = n$,

$$o_\delta(n_1, \dots, n_r) = \sum_{e|\delta} \mu(\delta/e) \sum_{d_1|\gcd(e,n_1)} \phi(d_1) \cdots \sum_{d_r|\gcd(e,n_r)} \phi(d_r)$$

$$= \sum_{d_1|n_1,\dots,d_r|n_r} \phi(d_1) \cdots \phi(d_r) \sum_{ab\,\mathrm{lcm}(d_1,\dots,d_r)=\delta} \mu(a),$$

where the inner sum is 0 unless $\mathrm{lcm}(d_1, \dots, d_r) = \delta$, and in this case it is 1. This gives (7). The proof of Theorem 2 is complete.

3 Remarks

The function $c(n_1, \dots, n_r)$ is representing a multiplicative function of r variables, i.e.,

$$c(n_1 m_1, \dots, n_r m_r) = c(n_1, \dots, n_r) c(m_1, \dots, m_r) \tag{10}$$

holds for any $n_1, \dots, n_r, m_1, \dots, m_r \geq 1$ such that $\gcd(n_1 \cdots n_r, m_1 \cdots m_r) = 1$. Therefore,

$$c(n_1, \dots, n_r) = \prod_p c(p^{e_p(n_1)}, \dots, p^{e_p(n_r)}),$$

where $n_i = \prod_p p^{e_p(n_i)}$ is the prime power factorization of n_i, the product being over the primes p and all but a finite number of the exponents $e_p(n_i)$ are zero ($1 \leq i \leq r$).

The property (10) follows by the next simple number-theoretic argument: According to (4), $c(n_1, \dots, n_r)$ is the r variables convolution of the function $(n_1, \dots, n_r) \mapsto \frac{\phi(n_1) \cdots \phi(n_r)}{\phi(\mathrm{lcm}(n_1,\dots,n_r))}$ with the constant 1 function, both multiplicative. Since convolution preserves the multiplicativity we deduce that $c(n_1, \dots, n_r)$ is multiplicative, too. See [12, Section 2] for details.

Also, let $n_1, \dots, n_r, m_1, \dots, m_r \geq 1$ such that $\gcd(n_1 \cdots n_r, m_1 \cdots m_r) = 1$. Let $n := \mathrm{lcm}(n_1, \dots, n_r)$, $m := \mathrm{lcm}(m_1, \dots, m_r)$. For $\delta \mid nm$ write $\delta = ab$ with $a \mid n$, $b \mid m$ (which are unique). Then,

$$c_\delta(n_1 m_1, \dots, n_r m_r) = c_a(n_1, \dots, n_r) c_b(m_1, \dots, m_r), \tag{11}$$

which follows from (6) by a short computation.

Now, (10) and (11) show the validity of (2) and (1) quoted in the Introduction.

Let $A(n_1, \dots, n_r)$ denote the arithmetic mean of the orders of elements in $C_{n_1} \times \cdots \times C_{n_r}$. From (7) we deduce

Corollary 3. *For every* $n_1, \ldots, n_r \geq 1$,

$$A(n_1, \ldots, n_r) = \frac{1}{n_1 \cdots n_r} \sum_{d_1 | n_1, \ldots, d_r | n_r} \phi(d_1) \cdots \phi(d_r) \operatorname{lcm}(d_1, \ldots, d_r).$$

The function $(n_1, \ldots, n_r) \mapsto A(n_1, \ldots, n_r)$ is also multiplicative. See [1, 2] for further properties of the average of orders of elements in finite Abelian groups.

Consider the special case $n_1 = \ldots = n_r = n$. According to (6),

$$o_\delta(n, \ldots, n) = \sum_{e | \delta} e^r \mu(\delta/r) = \phi_r(\delta) \tag{12}$$

is the Jordan function of order r. Note that $\phi_1(\delta) = \phi(\delta)$ is Euler's function.

This means that the number of elements of order δ ($\delta \mid n$) in the direct product $C_n \times \cdots \times C_n$, with r factors, is $\phi_r(\delta) = \delta^r \prod_{p|\delta}(1 - 1/p^r)$. This is a less known group-theoretic interpretation of the Jordan function. See G. A. Miller [4, 5], J. Schulte [8, Th. 7].

Hence the number of cyclic subgroups of order δ ($\delta \mid n$) of the group $C_n \times \cdots \times C_n$, with r factors, is $\phi_r(\delta)/\phi(\delta)$.

Note that the function $k \mapsto \phi_r(k)/(k^{r-2}\phi(k)) = k \prod_{p|k}(1+1/p+1/p^2+\ldots+1/p^{r-1})$ $(r \geq 2)$ was considered quite recently in [9], in connection with Robin's inequality and the Riemann hypothesis.

As a byproduct we obtain from (7) and (12) that for every positive integer δ,

$$\sum_{\operatorname{lcm}(d_1, \ldots, d_r) = \delta} \phi(d_1) \cdots \phi(d_r) = \phi_r(\delta), \tag{13}$$

where the sum is over all ordered r-tuples $(d_1, \ldots, d_r)$ such that $\operatorname{lcm}(d_1, \ldots, d_r) = \delta$. The function in the left hand side of (13) is the von Sterneck function, cf. [3, p. 14].

A final remark: The number $s(n_1, n_2)$ of all subgroups of the group $C_{n_1} \times C_{n_2}$ is given by

$$s(n_1, n_2) = \sum_{d_1 | n_1, d_2 | n_2} \gcd(d_1, d_2) \quad (n_1, n_2 \geq 1). \tag{14}$$

Compare (14) to (5). A proof of (14) will be presented elsewhere.

References

[1] J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht, I. E. Shparlinski, Average order in cyclic groups, *J. Théor. Nombres Bordeaux*, **16** (2004), 107–123.

[2] F. Luca, I. E. Shparlinski, Average multiplicative orders of elements modulo n, *Acta Arith.*, **109** (2003), 387–411.

[3] P. J. McCarthy, *Introduction to Arithmetical Functions*, Springer, 1986.

[4] G. A. Miller, On the totitives of different orders, *Amer. Math. Monthly*, **11** (1904), 129–130.

[5] G. A. Miller, Some relations between number theory and group theory, *American J. Math.*, **27** (1905), 315–322.

[6] G. A. Miller, Number of the subgroups of any given Abelian group, *Proc. Nat. Acad. Sci. U.S.A.*, **25** (1939), 258–262.

[7] R. Schmidt, *Subgroup Lattices of Groups*, de Gruyter Expositions in Mathematics 14, de Gruyter, Berlin, 1994.

[8] J. Schulte, Über die Jordansche Verallgemeinerung der Eulerschen Funktion, *Results Math.*, **36** (1999), 354–364.

[9] P. Solé, M. Planat, The Robin inequality for 7-free integers, *Integers*, **11** (2011), Article A65, 8 pp.

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

[11] M. Tărnăuceanu, An arithmetic method of counting the subgroups of a finite abelian group, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, **53(101)** (2010), 373–386.

[12] L. Tóth, Menon's identity and arithmetical sums representing functions of several variables, *Rend. Sem. Mat. Univ. Politec. Torino*, **69** (2011), 97–110.

[13] Y. Yeh, On prime power Abelian groups, *Bull. Amer. Math. Soc.*, **54** (1948), 323–327.

Received: 28.03.2012,
Revised: 05.06.2012,
Accepted: 23.06.2012.

Institute of Mathematics, Department of Integrative Biology, Universität für Bodenkultur, Gregor Mendel-Straße 33, A-1180 Wien, Austria
and
Department of Mathematics, University of Pécs, Ifjúság u. 6, H-7624 Pécs, Hungary
E-mail: ltoth@gamma.ttk.pte.hu