Bull. Aust. Math. Soc. **101** (2020), 201–206
doi:10.1017/S0004972719000601

THE NUMBER OF CYCLIC SUBGROUPS OF FINITE ABELIAN GROUPS AND MENON'S IDENTITY

MARIUS TĂRNĂUCEANU

(Received 27 March 2019; accepted 3 April 2019; first published online 17 May 2019)

Abstract

We give a new formula for the number of cyclic subgroups of a finite abelian group. This is based on Burnside's lemma applied to the action of the power automorphism group. The resulting formula generalises Menon's identity.

2010 *Mathematics subject classification*: primary 11A25; secondary 20D60, 20K01.

Keywords and phrases: Menon's identity, Burnside's lemma, group action, cyclic subgroup, abelian group, power automorphism group.

1. Introduction

Menon's identity [9] is one of the most interesting arithmetical identities.

Menon's identity. *For every positive integer n,*

$$\sum_{a\in\mathbb{Z}_n^*}\gcd(a-1,n)=\varphi(n)\tau(n),$$

where $\mathbb{Z}_n^*$ *is the group of units of the ring* $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$, $\gcd(\cdot,\cdot)$ *is the greatest common divisor,* φ *is Euler's totient function and* $\tau(n)$ *is the number of divisors of n.*

There are several approaches to Menon's identity and many generalisations. There are three main methods used to prove Menon-type identities:

- group-theoretic methods based on Burnside's lemma (also called the Cauchy–Frobenius lemma; see [13]) involving group actions (see [9, 14, 17]);
- elementary number-theoretic methods based on properties of the Dirichlet convolution and multiplicative functions (see [1, 4, 9, 16]);
- number-theoretic methods based on finite Fourier representations and Cauchy products of r-even functions (see [2, 3, 8, 12]).

The generalisations involve additive and multiplicative characters (see [7, 22, 23]), arithmetical functions of several variables (see [20]), actions of subgroups of $\mathrm{GL}_r(\mathbb{Z}_n)$ (see [5, 6, 19]) and residually finite Dedekind domains (see [10, 11]).

Our group-theoretical approach uses Burnside's lemma for a new group action: the natural action of the power automorphism group $\mathrm{Pot}(G)$ on G. First of all, we recall some definitions and results that will be useful to us.

Burnside's lemma. *Let G be a finite group acting on a finite set X and set*

$$\mathrm{Fix}(g) = \{x \in X \mid g \circ x = x\} \quad \textit{for } g \in G.$$

Then the number of distinct orbits is

$$N = \frac{1}{|G|} \sum_{g\in G} |\mathrm{Fix}(g)|. \tag{1.1}$$

In what follows, let G be a finite abelian group of order n and

$$G = G_1 \times \cdots \times G_k$$

be the primary decomposition of G, where G_i is a p_i-group for $i = 1, \ldots, k$. Then every G_i is of type

$$G_i = \mathbb{Z}_{p_i^{\alpha_{i1}}} \times \cdots \times \mathbb{Z}_{p_i^{\alpha_{ir_i}}},$$

where $1 \le \alpha_{i1} \le \cdots \le \alpha_{ir_i}$. We will apply Burnside's lemma to the natural action of the power automorphism group $\mathrm{Pot}(G)$ on G. An automorphism f of G is called a *power automorphism* if $f(H) = H$ for all $H \le G$. The set $\mathrm{Pot}(G)$ of all power automorphisms of G is a subgroup of $\mathrm{Aut}(G)$. As is well known, every power automorphism of a finite abelian group is *universal*, that is, there exists an integer m such that $f(x) = mx$ for all $x \in G$. From [15, Theorem 1.5.6], $\mathrm{Pot}(G)$ has the structure

$$\mathrm{Pot}(G) \cong \mathrm{Pot}(G_1) \times \cdots \times \mathrm{Pot}(G_k) \cong \mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_{1r_1}}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{p_k^{\alpha_{kr_k}}}). \tag{1.2}$$

Our main result can be stated as follows.

Theorem 1.1. *With the above notation,*

$$\prod_{i=1}^{k} \sum_{\substack{1\le m_i\le p_i^{\alpha_{ir_i}} \\ p_i\nmid m_i}} \prod_{j=1}^{r_i} \gcd(m_i - 1, p_i^{\alpha_{ij}}) = \varphi(\exp(G))|L_1(G)|, \tag{1.3}$$

where $\exp(G)$ *is the exponent of G and* $|L_1(G)|$ *is the number of cyclic subgroups of G.*

Clearly, (1.3) gives a new formula to compute the number of cyclic subgroups of a finite abelian group (for other such formulas, see [18, 21]). We exemplify it in a particular case.

Example 1.2. The finite abelian group

$$G = \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{72} \cong (\mathbb{Z}_2 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^3}) \times (\mathbb{Z}_3 \times \mathbb{Z}_{3^2})$$

has $\exp(G) = 2^3 3^2 = 72$ and so $\varphi(\exp(G)) = \varphi(72) = 24$. Then (1.3) leads to

$$\begin{aligned}|L_1(G)| &= \frac{1}{24}\Bigg(\sum_{\substack{1\le m_1\le 2^3\\ 2\nmid m_1}} \prod_{j=1}^{3} \gcd(m_1-1, 2^{\alpha_{1j}})\Bigg)\Bigg(\sum_{\substack{1\le m_2\le 3^2\\ 3\nmid m_2}} \prod_{j=1}^{2} \gcd(m_2-1, 3^{\alpha_{2j}})\Bigg)\\ &= \frac{1}{24}(\gcd(0,2^1)\gcd(0,2^2)\gcd(0,2^3) + \gcd(2,2^1)\gcd(2,2^2)\gcd(2,2^3)\\ &\quad + \gcd(4,2^1)\gcd(4,2^2)\gcd(4,2^3) + \gcd(6,2^1)\gcd(6,2^2)\gcd(6,2^3))\\ &\quad \cdot (\gcd(0,3^1)\gcd(0,3^2) + \gcd(1,3^1)\gcd(1,3^2) + \gcd(3,3^1)\gcd(3,3^2)\\ &\quad + \gcd(4,3^1)\gcd(4,3^2) + \gcd(6,3^1)\gcd(6,3^2) + \gcd(7,3^1)\gcd(7,3^2))\\ &= \frac{1}{24}(64+8+32+8)(27+1+9+1+9+1) = 224.\end{aligned}$$

We remark that if the group G is cyclic of order n, then $r_i = 1$ for $i = 1, \ldots, k$, $\exp(G) = p_1^{\alpha_{11}} \cdots p_k^{\alpha_{k1}} = n$ and $|L_1(G)| = \tau(n)$. Thus equality (1.3) becomes

$$\prod_{i=1}^{k} \sum_{\substack{1\le m_i\le p_i^{\alpha_{i1}}\\ p_i\nmid m_i}} \gcd(m_i-1, p_i^{\alpha_{i1}}) = \varphi(n)\tau(n). \tag{1.4}$$

Since

$$\mathbb{Z}^*_{p_1^{\alpha_{11}}} \times \cdots \times \mathbb{Z}^*_{p_k^{\alpha_{k1}}} \cong \mathbb{Z}^*_n,$$

(1.4) can be rewritten as

$$\sum_{\substack{1\le m\le n\\ \gcd(m,n)=1}} \gcd(m-1, n) = \varphi(n)\tau(n),$$

that is, we have recovered Menon's identity.

Two immediate consequences of Theorem 1.1 are the following.

Corollary 1.3. *Let m and n be two positive integers, $l = \operatorname{lcm}(m,n)$ and $p_1, \ldots, p_k$ be the primes dividing l. Write $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$, where α_i and β_i may be zero. Then*

$$|L_1(\mathbb{Z}_m \times \mathbb{Z}_n)| = \frac{1}{\varphi(l)} \prod_{i=1}^{k} \sum_{\substack{1\le m_i\le p_i^{\max\{\alpha_i,\beta_i\}}\\ p_i\nmid m_i}} \gcd(m_i-1, p_i^{\alpha_i})\gcd(m_i-1, p_i^{\beta_i}). \tag{1.5}$$

Corollary 1.4. *Let n be a positive integer and $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the decomposition of n as a product of prime factors. Then, for every $r \in \mathbb{N}^*$,*

$$|L_1(\mathbb{Z}_n^r)| = \frac{1}{\varphi(n)} \prod_{i=1}^{k} \sum_{\substack{1\le m_i\le p_i^{\alpha_i}\\ p_i\nmid m_i}} \gcd(m_i-1, p_i^{\alpha_i})^r. \tag{1.6}$$

Note that (1.4) can be obtained from (1.5) or (1.6) by taking $m = 1$ or $r = 1$, respectively. Thus, these equalities can be also seen as generalisations of Menon's identity.

2. Proof of Theorem 1.1

The natural action of $\mathrm{Pot}(G)$ on G is

$$f \circ a = f(a) \quad \text{for } (f, a) \in \mathrm{Pot}(G) \times G.$$

By using the direct decompositions of $\mathrm{Pot}(G)$ and G in Section 1, it can be written as

$$(f_1, \dots, f_k) \circ (a_1, \dots, a_k) = (f_1(a_1), \dots, f_k(a_k)), \quad (f_i, a_i) \in \mathrm{Pot}(G_i) \times G_i,\ i = 1, \dots, k.$$

First of all, we will prove that two elements $a, b \in G$ are contained in the same orbit if and only if they generate the same cyclic subgroup of G. Indeed, if a and b belong to the same orbit, then there exists $f \in \mathrm{Pot}(G)$ such that $b = f(a)$. Since f is universal, it follows that $b = ma$ for some integer m. Then $b \in \langle a \rangle$, and so $\langle b \rangle \subseteq \langle a \rangle$. On the other hand, since a group automorphism preserves the element orders, $o(a) = o(b)$. Therefore $\langle a \rangle = \langle b \rangle$. Conversely, assume that $\langle a \rangle = \langle b \rangle$, where $a = (a_1, \dots, a_k)$ and $b = (b_1, \dots, b_k)$. Then $\langle a_i \rangle = \langle b_i \rangle$, for $i = 1, \dots, k$. This implies that for every i there is an integer m_i such that $b_i = m_i a_i$ and $\gcd(m_i, o(a_i)) = 1$. Remark that if $a_i = 1$ then we must have $m_i = 1$, while if $a_i \neq 1$ then $\gcd(m_i, p_i) = 1$. Consequently, in both cases $p_i \nmid m_i$. This shows that the map

$$f_i : G_i \longrightarrow G_i, \quad f_i(x_i) = m_i x_i \quad \text{for } x_i \in G_i,$$

is a power automorphism of G_i. Then $f = (f_1, \dots, f_k) \in \mathrm{Pot}(G)$ and $f(a) = b$, that is, a and b are contained in the same orbit. Thus, the number of distinct orbits is

$$N = |L_1(G)|.$$

Next we will focus on the right-hand side of (1.1). Note that the group isomorphism (1.2) leads to

$$|\mathrm{Pot}(G)| = \prod_{i=1}^{k} |\mathrm{Aut}(\mathbb{Z}_{p_i^{\alpha_{ir_i}}})| = \prod_{i=1}^{k} \varphi(p_i^{\alpha_{ir_i}}) = \varphi\Big(\prod_{i=1}^{k} p_i^{\alpha_{ir_i}}\Big) = \varphi(\exp(G)).$$

Also, for every $f = (f_1, \dots, f_k) \in \mathrm{Pot}(G)$ and every $a = (a_1, \dots, a_k) \in G$,

$$a \in \mathrm{Fix}(f) \Longleftrightarrow a_i \in \mathrm{Fix}(f_i) \quad \text{for each } i = 1, \dots, k,$$

implying that

$$|\mathrm{Fix}(f)| = \prod_{i=1}^{k} |\mathrm{Fix}(f_i)|.$$

On the other hand, since $\mathrm{Pot}(G_i) \cong \mathrm{Aut}(\mathbb{Z}_{p_i^{\alpha_{ir_i}}})$, every f_i is of type

$$f_i(x_i) = m_i x_i \quad \text{with } p_i \nmid m_i.$$

Then for $x_i = (x_{i1}, \dots, x_{ir_i}) \in G_i$,

$$\begin{aligned} x_i \in \mathrm{Fix}(f_i) &\iff (m_i - 1)x_{ij} = 0 \text{ in } \mathbb{Z}_{p_i^{\alpha_{ij}}} \quad \text{for } j = 1, \dots, r_i \\ &\iff p_i^{\alpha_{ij}} \mid (m_i - 1)x_{ij} \quad \text{for } j = 1, \dots, r_i \\ &\iff \frac{p_i^{\alpha_{ij}}}{\gcd(m_i - 1, p_i^{\alpha_{ij}})} \,\Big|\, x_{ij} \quad \text{for } j = 1, \dots, r_i \\ &\iff x_{ij} = c\frac{p_i^{\alpha_{ij}}}{\gcd(m_i - 1, p_i^{\alpha_{ij}})} \quad \text{with } c = 0, \dots, \gcd(m_i - 1, p_i^{\alpha_{ij}}) - 1 \\ &\qquad \text{for } j = 1, \dots, r_i. \end{aligned}$$

Consequently,

$$|\mathrm{Fix}(f_i)| = \prod_{j=1}^{r_i} \gcd(m_i - 1, p_i^{\alpha_{ij}}).$$

Thus, the right-hand side of (1.1) becomes

$$\begin{aligned} \frac{1}{\varphi(\exp(G))} \sum_{f \in \mathrm{Pot}(G)} |\mathrm{Fix}(f)| &= \frac{1}{\varphi(\exp(G))} \sum_{f_1 \in \mathrm{Pot}(G_1)} \cdots \sum_{f_k \in \mathrm{Pot}(G_k)} |\mathrm{Fix}(f_1)| \cdots |\mathrm{Fix}(f_k)| \\ &= \frac{1}{\varphi(\exp(G))} \prod_{i=1}^{k} \Big(\sum_{f_i \in \mathrm{Pot}(G_i)} |\mathrm{Fix}(f_i)| \Big) \\ &= \frac{1}{\varphi(\exp(G))} \prod_{i=1}^{k} \sum_{\substack{1 \le m_i \le p_i^{\alpha_{ir_i}} \\ p_i \nmid m_i}} \prod_{j=1}^{r_i} \gcd(m_i - 1, p_i^{\alpha_{ij}}), \end{aligned}$$

as desired.

Acknowledgement

The author is grateful to the reviewer for remarks which improved the previous version of the paper.

References

[1] P. Haukkanen, 'Menon's identity with respect to a generalized divisibility relation', *Aequationes Math.* **70** (2005), 240–246.

[2] P. Haukkanen and P. J. McCarthy, 'Sums of values of even functions', *Port. Math.* **48** (1991), 53–66.

[3] P. Haukkanen and R. Sivaramakrishnan, 'On certain trigonometric sums in several variables', *Collect. Math.* **45** (1994), 245–261.

[4] P. Haukkanen and J. Wang, 'A generalisation of Menon's identity with respect to a set of polynomials', *Port. Math.* **53** (1996), 331–337.

[5] Y. Li and D. Kim, 'A Menon-type identity with many tuples of group of units in residually finite Dedekind domains', *J. Number Theory* **175** (2017), 42–50.

[6] Y. Li and D. Kim, ‘Menon-type identities derived from actions of subgroups of general linear groups’, *J. Number Theory* **179** (2017), 97–112.

[7] Y. Li, X. Hu and D. Kim, ‘A Menon-type identity with multiplicative and additive characters’, *Taiwanese J. Math.* (2019), to appear.

[8] P. J. McCarthy, *Introduction to Arithmetical Functions*, Universitext (Springer, New York, 1986).

[9] P. K. Menon, ‘On the sum $\sum(a-1,n)[(a,n)=1]$’, *J. Indian Math. Soc.* **29** (1965), 155–163.

[10] C. Miguel, ‘Menon’s identity in residually finite Dedekind domains’, *J. Number Theory* **137** (2014), 179–185.

[11] C. Miguel, ‘A Menon-type identity in residually finite Dedekind domains’, *J. Number Theory* **164** (2016), 43–51.

[12] K. Nageswara Rao, ‘On certain arithmetical sums’, in: *The Theory of Arithmetic Functions*, Lecture Notes in Mathematics, 251 (eds. A. A. Gioia and D. L. Goldsmith) (Springer, Berlin, Heidelberg, 1972), 181–192.

[13] P. Neumann, ‘A lemma that is not Burnside’s’, *Math. Sci.* **4** (1979), 133–141.

[14] I. M. Richards, ‘A remark on the number of cyclic subgroups of a finite group’, *Amer. Math. Monthly* **91** (1984), 571–572.

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

[16] V. Sita Ramaiah, ‘Arithmetical sums in regular convolutions’, *J. Reine Angew. Math.* **303/304** (1978), 265–283.

[17] B. Sury, ‘Some number-theoretic identities from group actions’, *Rend. Circ. Mat. Palermo* **58** (2009), 99–108.

[18] 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.

[19] M. Tărnăuceanu, ‘A generalization of Menon’s identity’, *J. Number Theory* **132** (2012), 2568–2573.

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

[21] L. Tóth, ‘On the number of cyclic subgroups of a finite abelian group’, *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)* **55**(103) (2012), 423–428.

[22] L. Tóth, ‘Menon-type identities concerning Dirichlet characters’, *Int. J. Number Theory* **14** (2018), 1047–1054.

[23] X.-P. Zhao and Z.-F. Cao, ‘Another generalization of Menon’s identity’, *Int. J. Number Theory* **13** (2017), 2373–2379.

MARIUS TĂRNĂUCEANU, Faculty of Mathematics,
“Al.I. Cuza” University, Iaşi, Romania
e-mail: tarnauc@uaic.ro