Rend. Sem. Mat. Univ. Politec. Torino
Vol. 69, 1 (2011), 97 – 110

L. Tóth[*]

MENON'S IDENTITY AND ARITHMETICAL SUMS REPRESENTING FUNCTIONS OF SEVERAL VARIABLES

Abstract. We generalize Menon's identity by considering sums representing arithmetical functions of several variables. As an application, we give a formula for the number of cyclic subgroups of the direct product of several cyclic groups of arbitrary orders. We also point out extensions of Menon's identity in the one variable case, which seems not to appear in the literature.

1. Introduction

Menon's identity [9] states, that for every $n \in \mathbb{N} := \{1,2,\ldots\}$,

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(k-1,n) = \phi(n)\tau(n), \tag{1}$$

where ϕ denotes Euler's function and $\tau(n)$ is the number of divisors of n.

This identity has many generalizations derived by several authors. For example, if f is an arbitrary arithmetical function, then

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} f(\gcd(k-1,n)) = \phi(n)\sum_{d\mid n}\frac{(\mu * f)(d)}{\phi(d)} \quad (n\in\mathbb{N}), \tag{2}$$

where $*$ stands for the Dirichlet convolution. Formula (2) was deduced, in an equivalent form, by Kesava Menon [9, Th. 1] for f multiplicative, and by Sita Ramaiah [12, Th. 9.1] in a more general form.

Nageswara Rao [10] proved that

$$\sum_{\substack{k_1,\ldots,k_s=1\\ \gcd(k_1,\ldots,k_s,n)=1}}^{n} \gcd(k_1-a_1,\ldots,k_s-a_s,n)^s = \phi_s(n)\tau(n) \quad (n\in\mathbb{N}), \tag{3}$$

where $a_1,\ldots,a_s \in \mathbb{Z}$, $\gcd(a_1,\ldots,a_s,n)=1$ and $\phi_s(n) = n^s\prod_{p\mid n}(1-1/p^s)$ is the Jordan function of order s.

Richards [11] remarked that for any polynomial g with integer coefficients,

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(g(k),n) = \phi(n)\sum_{d\mid n}\eta_g(d) \quad (n\in\mathbb{N}), \tag{4}$$

[*] The author gratefully acknowledges support from the Austrian Science Fund (FWF) under the project Nr. P20847-N18

where $\eta_g(d)$ stands for the number of solutions x (mod d) of the congruence $g(x) \equiv 0$ (mod d) such that $\gcd(x,d) = 1$. Haukkanen and Wang [7] gave a proof of formula (4) in a more general setting.

In a recent paper Sury [16] showed that

$$\sum_{\substack{k_1,k_2,\ldots,k_r=1\\ \gcd(k_1,n)=1}}^{n} \gcd(k_1-1,k_2,\ldots,k_r,n) = \phi(n)\sigma_{r-1}(n) \quad (n \in \mathbb{N}), \tag{5}$$

where $\sigma_k(n) = \sum_{d|n} d^k$.

Further generalizations of (1) and combinations of the existing ones were given by Haukkanen [3, 4], Haukkanen and McCarthy [5], Haukkanen and Sivaramakrishnan [6], Sivaramakrishnan [13, 14] and others. See also McCarthy [8, Ch. 1,2]. All of these identities represent functions of a single variable.

Note that there are three main methods used in the literature to prove Menon-type identities, namely: (i) the group-theoretic method, based on the Cauchy–Frobenius lemma, called also Burnside's lemma, concerning group actions, see [9, 11, 16]; (ii) elementary number-theoretic methods based on properties of the Dirichlet convolution and of multiplicative functions, see [9, 3, 7, 12]; (iii) the number-theoretic method based on finite Fourier representations and Cauchy products of r-even functions, cf. [5, 6, 8, 10].

Recall the idea of the proof of (1) based on the Cauchy–Frobenius lemma. Let G be an arbitrary group of order n and let $U_n := \{k \in \mathbb{N} : 1 \le k \le n, \gcd(k,n) = 1\}$ be the group of units (mod n). Consider the action of the group U_n on G given by $U_n \times G \ni (k,g) \mapsto g^k$. Here two elements of G belong to the same orbit if and only if they generate the same cyclic subgroup. Hence the number of orbits is equal to the number of cyclic subgroups of G, notation $c(G)$. We obtain, according to the Cauchy–Frobenius lemma, that

$$c(G) = \frac{1}{\phi(n)} \sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \psi(G,k), \tag{6}$$

where $\psi(G,k) := \#\{g \in G : g^k = g\}$ is the number of fixed elements of G.

If $G = C_n$ is the cyclic group of order n, then we have $c(G) = \tau(n)$, $\psi(G,k) = \gcd(k-1,n)$ and (6) gives Menon's identity (1).

Now specialize (6) to the case where G is the direct product of several cyclic groups of arbitrary orders, i.e., $G = C_{m_1} \times \cdots \times C_{m_r}$, where $m_1,\ldots,m_r \in \mathbb{N}$ ($r \in \mathbb{N}$). We deduce that the number of its cyclic subgroups is

$$c(C_{m_1} \times \cdots \times C_{m_r}) = \frac{1}{\phi(q)} \sum_{\substack{k=1\\ \gcd(k,q)=1}}^{q} \gcd(k-1,m_1)\cdots\gcd(k-1,m_r), \tag{7}$$

where $q = m_1 \cdots m_r$.

Being motivated by this example and in order to evaluate the right hand side of (7), see Section 4, we generalize in this paper Menon's identity (1), and also (2) and (4), by considering arithmetical sums representing functions of several variables. For example, using simple number-theoretical arguments we derive the following identity:

Let $m_1,\dots,m_r,M \in \mathbb{N}$ (with $r \in \mathbb{N}$), $m := \operatorname{lcm}[m_1,\dots,m_r]$, $m \mid M$ and $\mathbf{a} := (a_1,\dots,a_r) \in \mathbb{Z}^r$. Then

$$\begin{aligned} &\frac{1}{\phi(M)} \sum_{\substack{k=1 \\ \gcd(k,M)=1}}^{M} \gcd(k-a_1,m_1)\cdots\gcd(k-a_r,m_r) \\ (8) \qquad &= \sum_{d_1\mid m_1,\dots,d_r\mid m_r} \frac{\phi(d_1)\cdots\phi(d_r)}{\phi(\operatorname{lcm}[d_1,\dots,d_r])}\eta^{(\mathbf{a})}(d_1,\dots,d_r), \end{aligned}$$

where

$$(9) \qquad \eta^{(\mathbf{a})}(d_1,\dots,d_r) = \begin{cases} 1 & \text{for } \gcd(d_i,a_i)=1\ (1\le i\le r) \text{ and} \\ & \quad \gcd(d_i,d_j) \mid a_i-a_j\ (1\le i,j\le r), \\ 0 & \text{otherwise.} \end{cases}$$

Remark that (8) does not depend on M and it represents a multiplicative function of r variables, to be defined in Section 2. Also, each term of the sum in the right-hand side of (8) is an integer. Therefore the sum in the left-hand side of (8) is a multiple of $\phi(M)$ for any $m_1,\dots,m_r \in \mathbb{N}$.

If $r=2$ and $a_1=a_2=a\in\mathbb{Z}$ with $\gcd(a,m)=1$, then (8) gives

$$(10) \qquad \sum_{\substack{k=1 \\ \gcd(k,M)=1}}^{M} \gcd(k-a,m_1)\gcd(k-a,m_2) \ = \ \phi(M)\sum_{d_1\mid m_1,d_2\mid m_2}\phi(\gcd(d_1,d_2)).$$

If $m_1,\dots,m_r$ are pairwise relatively prime, $M=m=m_1\cdots m_r$ and $\mathbf{a} := (a_1,\dots,a_r) \in \mathbb{Z}^r$, then (8) reduces to

$$(11) \qquad \sum_{\substack{k=1 \\ \gcd(k,m)=1}}^{m} \gcd(k-a_1,m_1)\cdots\gcd(k-a_r,m_r) \ = \ \phi(m)\tau(m_1,a_1)\cdots\tau(m_r,a_r),$$

where $\tau(n,a)$ denotes the number of divisors d of n such that $\gcd(d,a)=1$. Now, if $a_1=\ldots=a_r=a\in\mathbb{Z}$, then the right-hand side of (11) is $\phi(m)\tau(m,a)$.

Note that the arithmetical function of several variables

$$(12) \qquad A(m_1,\dots,m_r) := \frac{1}{m}\sum_{k=1}^{m}\gcd(k,m_1)\cdots\gcd(k,m_r),$$

where $m_1,\dots,m_r\in\mathbb{N}$ and $m:=\operatorname{lcm}[m_1,\dots,m_r]$, as above, was considered by Deitmar, Koyama and Kurokawa [2] in case $m_j \mid m_{j+1}$ $(1\le j\le r-1)$ by studying analytic properties of some zeta functions of Igusa type. The function (12) was investigated in the paper [18].

For $r=1$ and $m_1=m$ (12) reduces to the function

$$A(m) := \frac{1}{m}\sum_{k=1}^{m} \gcd(k,m) = \sum_{d\mid m} \frac{\phi(d)}{d}, \tag{13}$$

of which arithmetical and analytical properties were surveyed in [19].

We also generalize the function (12) and deduce certain single variable extensions of Menon's identity, which seems not to appear in the literature.

2. Preliminaries

We present in this section some basic notions and properties to be used in the paper.

We recall that an arithmetical function of r variables is a function $f:\mathbb{N}^r \to \mathbb{C}$, notation $f\in \mathscr{F}_r$. If $f,g\in\mathscr{F}_r$, then their convolution is defined as

$$(f*g)(m_1,\ldots,m_r) = \sum_{d_1\mid m_1,\ldots,d_r\mid m_r} f(d_1,\ldots,d_r)g(m_1/d_1,\ldots,m_r/d_r). \tag{14}$$

A function $f\in\mathscr{F}_r$ is said to be multiplicative if it is not identically zero and

$$f(m_1n_1,\ldots,m_rn_r) = f(m_1,\ldots,m_r)f(n_1,\ldots,n_r)$$

holds for any $m_1,\ldots,m_r,n_1,\ldots,n_r\in\mathbb{N}$ such that $\gcd(m_1\cdots m_r, n_1\cdots n_r)=1$.

If f is multiplicative, then it is determined by the values $f(p^{a_1},\ldots,p^{a_r})$, where p is prime and $a_1,\ldots,a_r\in\mathbb{N}_0:=\{0,1,2,\ldots\}$. More exactly, $f(1,\ldots,1)=1$ and for any $m_1,\ldots,m_r\in\mathbb{N}$,

$$f(m_1,\ldots,m_r) = \prod_p f(p^{e_p(m_1)},\ldots,p^{e_p(m_r)}),$$

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

If $r=1$, i.e., in case of functions of a single variable, we recover the familiar notion of multiplicativity.

For example, the functions $(m_1,\ldots,m_r)\mapsto \gcd(m_1,\ldots,m_r)$ and $(m_1,\ldots,m_r)\mapsto \operatorname{lcm}[m_1,\ldots,m_r]$ are multiplicative for any $r\in\mathbb{N}$.

The convolution (14) preserves the multiplicativity of functions. This property, well known in the one variable case, follows easily from the definitions.

The product and the quotient of (nonvanishing) multiplicative functions are both multiplicative. Let $h\in\mathscr{F}_1$ and $f\in\mathscr{F}_r$ be multiplicative functions. Then the functions

$$(m_1,\ldots,m_r)\mapsto h(m_1)\cdots h(m_r) \quad \text{and} \quad (m_1,\ldots,m_r)\mapsto h(f(m_1,\ldots,m_r))$$

are multiplicative. In particular, the functions $(m_1,\ldots,m_r)\mapsto h(\gcd(m_1,\ldots,m_r))$ and $(m_1,\ldots,m_r)\mapsto h(\operatorname{lcm}[m_1,\ldots,m_r])$ are multiplicative.

The definition and properties of multiplicativity for functions of several variables go back to the work of Vaidyanathaswamy [20]. See also [15].

In the one variable case $\mathbf{1}$, id, id_t and ϕ_t ($t \in \mathbb{C}$) will denote the functions given by $\mathbf{1}(n) = 1$, $\mathrm{id}(n) = n$, $\mathrm{id}_t(n) = n^t$ and $\phi_t(n) = n^t \prod_{p|n}(1-1/p^t)$ ($n \in \mathbb{N}$), respectively.

Let $G = (g_1, \dots, g_r)$ be a system of polynomials with integer coefficients and consider the simultaneous congruences

$$g_1(x) \equiv 0 \pmod{m_1}, \dots, g_r(x) \equiv 0 \pmod{m_r}. \tag{15}$$

Let $N_G(m_1, \dots, m_r)$ denote the number of solutions x (mod $\mathrm{lcm}[m_1, \dots, m_r]$) of (15). Also, let $\eta_G(m_1, \dots, m_r)$ denote the number of solutions x (mod $\mathrm{lcm}[m_1, \dots, m_r]$) of (15) such that $\gcd(x, m_1) = 1$, ..., $\gcd(x, m_r) = 1$. These are other examples of multiplicative functions of several variables, properties which might be known, but we could not locate them in the literature. We give their proof in Lemma 1.

If $r = 1$, $m_1 = m$ and $g_1 = g$, then $N_G(m) := N_g(m)$ is the number of solutions x (mod m) of the congruence $g(x) \equiv 0$ (mod m), which is multiplicative as a function of a single variable. This is well known, see e.g., [1, Th. 5.28].

LEMMA 1. *For every system $G = (g_1, \dots, g_r)$ of polynomials with integer coefficients the functions $(m_1, \dots, m_r) \mapsto N_G(m_1, \dots, m_r)$ and $(m_1, \dots, m_r) \mapsto \eta_G(m_1, \dots, m_r)$ are multiplicative.*

Proof. We prove the multiplicativity of the function N_G. In case of η_G the proof is similar.

Let $m_1, \dots, m_r, n_1, \dots, n_r \in \mathbb{N}$ such that $\gcd(m_1 \cdots m_r, n_1 \cdots n_r) = 1$. Consider the simultaneous congruences (15) together with

$$g_1(x) \equiv 0 \pmod{n_1}, \quad \dots, \quad g_r(x) \equiv 0 \pmod{n_r}, \tag{16}$$

$$g_1(x) \equiv 0 \pmod{m_1 n_1}, \quad \dots, \quad g_r(x) \equiv 0 \pmod{m_r n_r}. \tag{17}$$

If x is any solution of (17), then x is a solution of both (15) and (16).

Conversely, assume that x^* is a solution of (15) and x^{**} is a solution of (16). Consider the simultaneous congruences

$$x \equiv x^* \pmod{\mathrm{lcm}[m_1, \dots, m_r]}, \quad x \equiv x^{**} \pmod{\mathrm{lcm}[n_1, \dots, n_r]}. \tag{18}$$

Let $m := \mathrm{lcm}[m_1, \dots, m_r]$, $n := \mathrm{lcm}[n_1, \dots, n_r]$. Then by the Chinese remainder theorem (18) has a unique solution $\tilde{x}$ (mod mn), where $mn = \mathrm{lcm}[m_1 n_1, \dots, m_r n_r]$. Here $\tilde{x}$ is a solution of (17), completing the proof. □

The following lemma is a known property, it follows easily by the inclusion-exclusion principle, cf. [1, Th. 5.32].

LEMMA 2. *Let $n, d, x \in \mathbb{N}$ such that $d \mid n$, $1 \le x \le d$, $\gcd(x, d) = 1$. Then*

$$\#\{k \in \mathbb{N} : 1 \le k \le n, k \equiv x \pmod{d}, \gcd(k, n) = 1\} = \phi(n)/\phi(d).$$

3. Main results

For $m_1,\dots,m_r \in \mathbb{N}$ ($r \in \mathbb{N}$) let $m := \operatorname{lcm}[m_1,\dots,m_r]$ and let $M \in \mathbb{N}$, $m \mid M$. Let $F = (f_1,\dots,f_r)$ be a system of arithmetical functions of one variable and $G = (g_1,\dots,g_r)$ be a system of polynomials with integer coefficients.

Consider the arithmetical functions of r variables

$$S_F^{(G)}(m_1,\dots,m_r) := \frac{1}{M}\sum_{k=1}^{M} f_1(\gcd(g_1(k),m_1))\cdots f_r(\gcd(g_r(k),m_r)), \tag{19}$$

$$R_F^{(G)}(m_1,\dots,m_r) := \frac{1}{\phi(M)}\sum_{\substack{k=1\\ \gcd(k,M)=1}}^{M} f_1(\gcd(g_1(k),m_1))\cdots f_r(\gcd(g_r(k),m_r)). \tag{20}$$

THEOREM 1. *If F and G are arbitrary systems of arithmetical functions and polynomials with integer coefficients, respectively, then for any $m_1,\dots,m_r \in \mathbb{N}$,*

$$S_F^{(G)}(m_1,\dots,m_r) = \sum_{d_1\mid m_1,\dots,d_r\mid m_r} \frac{(\mu * f_1)(d_1)\cdots(\mu * f_r)(d_r)}{\operatorname{lcm}[d_1,\dots,d_r]} N_G(d_1,\dots,d_r), \tag{21}$$

which does not depend on M.

Proof. Writing $f_i = \mathbf{1} * (\mu * f_i)$ $(1 \le i \le r)$ we obtain

$$\begin{aligned} S_F^{(G)}(m_1,\dots,m_r) &= \frac{1}{M}\sum_{k=1}^{M} \sum_{d_1\mid \gcd(g_1(k),m_1)} (\mu * f_1)(d_1) \cdots \sum_{d_r\mid \gcd(g_r(k),m_r)} (\mu * f_r)(d_r) \\ &= \frac{1}{M}\sum_{d_1\mid m_1,\dots,d_r\mid m_r} (\mu * f_1)(d_1)\cdots(\mu * f_r)(d_r) \sum_{\substack{1\le k\le M\\ g_1(k)\equiv 0 \pmod{d_1},\dots,g_r(k)\equiv 0 \pmod{d_r}}} 1, \end{aligned}$$

where the inner sum is $(M/\operatorname{lcm}[d_1,\dots,d_r])N_G(d_1,\dots,d_r)$. □

COROLLARY 1. *If F is a system of multiplicative arithmetical functions and G is any system of polynomials with integer coefficients, then the function $(m_1,\dots,m_r) \mapsto S_F^{(G)}(m_1,\dots,m_r)$ is multiplicative.*

Proof. By Theorem 1 and Lemma 1 the function $S_F^{(G)}$ is the convolution of multiplicative functions; hence it is multiplicative. □

For the function $A(m_1,\dots,m_r)$ given by (12) we have the next representation.

COROLLARY 2 ([18, Prop. 12], $f_1 = \ldots = f_r = \operatorname{id}$, $g_1(x) = \ldots = g_r(x) = x$).

$$\frac{1}{M}\sum_{k=1}^{M} \gcd(k,m_1)\cdots\gcd(k,m_r) = \sum_{d_1\mid m_1,\dots,d_r\mid m_r} \frac{\phi(d_1)\cdots\phi(d_r)}{\operatorname{lcm}[d_1,\dots,d_r]}, \tag{22}$$

which is multiplicative.

For other special choices of F and G similar results can be derived if the values $N_G(d_1,\dots,d_r)$ are known, but we turn our attention to the function $R_F^{(G)}(m_1,\dots,m_r)$ defined by (20).

THEOREM 2. *If F and G are arbitrary systems of arithmetical functions and polynomials with integer coefficients, respectively, then for any $m_1,\dots,m_r\in\mathbb{N}$,*

$$R_F^{(G)}(m_1,\dots,m_r) = \sum_{d_1|m_1,\dots,d_r|m_r} \frac{(\mu * f_1)(d_1)\cdots(\mu * f_r)(d_r)}{\phi(\operatorname{lcm}[d_1,\dots,d_r])}\eta_G(d_1,\dots,d_r), \tag{23}$$

which does not depend on M.

Proof. Similar to the proof of Theorem 1,

$$R_F^{(G)}(m_1,\dots,m_r) = \frac{1}{\phi(M)}\sum_{\substack{k=1\\ \gcd(k,M)=1}}^{M}\ \sum_{d_1|\gcd(g_1(k),m_1)}(\mu * f_1)(d_1)\ \cdots \sum_{d_r|\gcd(g_r(k),m_r)}(\mu * f_r)(d_r)$$

$$= \frac{1}{\phi(M)}\sum_{d_1|m_1,\dots,d_r|m_r}(\mu * f_1)(d_1)\cdots(\mu * f_r)(d_r) \sum_{\substack{1\le k\le M\\ \gcd(k,M)=1\\ g_1(k)\equiv 0 \pmod{d_1},\dots,g_r(k)\equiv 0 \pmod{d_r}}} 1,$$

where the inner sum is $(\phi(M)/\phi(\operatorname{lcm}[d_1,\dots,d_r]))\eta_G(d_1,\dots,d_r)$ by Lemma 2. □

In the one variable case ($r=1$) Theorem 2 is a special case of [7, Theorem], giving, with $f_1=f$, $g_1=g$, $m_1=m$,

$$R_f^{(g)}(m) := \frac{1}{\phi(m)}\sum_{\substack{k=1\\ \gcd(k,m)=1}}^{m} f(\gcd(g(k),m)) = \sum_{d|m}\frac{(\mu * f)(d)}{\phi(d)}\eta_g(d), \tag{24}$$

and for $f=\mathrm{id}$ this reduces to (4).

COROLLARY 3. *Assume that $g_1=\ldots=g_r=g$ and $m_1,\dots,m_r$ are pairwise relatively prime. Then*

$$R_F^{(G)}(m_1,\dots,m_r) = R_{f_1}^{(g)}(m_1)\cdots R_{f_r}^{(g)}(m_r). \tag{25}$$

Proof. For any $d_1\mid m_1,\dots,d_r\mid m_r$, $\eta_G(\operatorname{lcm}[d_1,\dots,d_r]) = \eta_g(d_1\cdots d_r) = \eta_g(d_1)\cdots\eta_g(d_r)$ and obtain from (23) that

$$R_F^{(G)}(m_1,\dots,m_r) = \sum_{d_1|m_1}\frac{(\mu * f_1)(d_1)}{\phi(d_1)}\eta_g(d_1)\cdots\sum_{d_r|m_r}\frac{(\mu * f_r)(d_r)}{\phi(d_r)}\eta_g(d_r),$$

giving (25) using the notation of (24). □

COROLLARY 4. *If F is a system of multiplicative arithmetical functions and G is any system of polynomials with integer coefficients, then the function $(m_1,\dots,m_r)\mapsto R_F^{(G)}(m_1,\dots,m_r)$ is multiplicative.*

Proof. By Theorem 2 and Lemma 1 the function $R_F^{(G)}$ is the convolution of multiplicative functions; hence it is multiplicative. □

In case of multiplicative functions f_i $(1 \le i \le r)$ we can assume that $m_i > 1$ $(1 \le i \le r)$, since for $m_i = 1$ the corresponding factors of (20) are equal to 1.

COROLLARY 5 ($f_1 = \mathrm{id}_{t_1}, \ldots, f_r = \mathrm{id}_{t_r}$).

$$\begin{aligned} R_{t_1,\ldots,t_r}^{(G)}(m_1,\ldots,m_r) &:= \frac{1}{\phi(M)} \sum_{\substack{k=1 \\ \gcd(k,M)=1}}^{M} (\gcd(g_1(k),m_1))^{t_1} \cdots (\gcd(g_r(k),m_r))^{t_r} \\ &= \sum_{d_1|m_1,\ldots,d_r|m_r} \frac{\phi_{t_1}(d_1)\cdots\phi_{t_r}(d_r)}{\phi(\mathrm{lcm}[d_1,\ldots,d_r])} \eta_G(d_1,\ldots,d_r), \end{aligned}$$

representing a multiplicative function.

COROLLARY 6 ($f_1 = \ldots = f_r = \mathrm{id}$).

$$\begin{aligned} R_r^{(G)}(m_1,\ldots,m_r) &:= \frac{1}{\phi(M)} \sum_{\substack{k=1 \\ \gcd(k,M)=1}}^{M} \gcd(g_1(k),m_1)\cdots\gcd(g_r(k),m_r) \\ &= \sum_{d_1|m_1,\ldots,d_r|m_r} \frac{\phi(d_1)\cdots\phi(d_r)}{\phi(\mathrm{lcm}[d_1,\ldots,d_r])} \eta_G(d_1,\ldots,d_r), \end{aligned}$$

representing a (positive) integer-valued multiplicative function.

Proof. The function $(m_1,\ldots,m_r) \mapsto \phi(m_1)\cdots\phi(m_r)/\phi(\mathrm{lcm}[m_1,\ldots,m_r])$ is multiplicative and its values are integers, since $\phi(p^{e_1})\cdots\phi(p^{e_r})/\phi(\mathrm{lcm}[p^{e_1},\ldots,p^{e_r}])$ are integers for any prime p and any $e_1,\ldots,e_r \in \mathbb{N}$. □

COROLLARY 7 ($f_1 = \mathrm{id}_{t_1}, \ldots, f_r = \mathrm{id}_{t_r}$, $g_1(x) = x - a_1, \ldots, g_r(x) = x - a_r$). *For any* $\mathbf{a} := (a_1,\ldots,a_r) \in \mathbb{Z}^r$,

$$\begin{aligned} R_{t_1,\ldots,t_r}^{(\mathbf{a})}(m_1,\ldots,m_r) &:= \frac{1}{\phi(M)} \sum_{\substack{k=1 \\ \gcd(k,M)=1}}^{M} (\gcd(k-a_1,m_1))^{t_1} \cdots (\gcd(k-a_r,m_r))^{t_r} \\ &= \sum_{d_1|m_1,\ldots,d_r|m_r} \frac{\phi_{t_1}(d_1)\cdots\phi_{t_r}(d_r)}{\phi(\mathrm{lcm}[d_1,\ldots,d_r])} \eta^{(\mathbf{a})}(d_1,\ldots d_r), \qquad (26) \end{aligned}$$

where $\eta^{(\mathbf{a})}(d_1,\ldots,d_r)$ *is defined by* (9).

Proof. It is well known that for $d_1,\ldots,d_r \in \mathbb{N}$ the simultaneous congruences

$$x \equiv a_1 \ (\mathrm{mod}\ d_1), \ldots, x \equiv a_r \ (\mathrm{mod}\ d_r)$$

admit solutions if and only if $\gcd(d_i,d_j) \mid a_i - a_j$ $(1 \le i,j \le r)$ and in this case there is a unique solution $\overline{x}$ (mod $\operatorname{lcm}[d_1,\ldots,d_r]$). Here

$$\gcd(\overline{x},d_1)=\gcd(a_1,d_1),\ \ldots,\ \gcd(\overline{x},d_r)=\gcd(a_r,d_r)$$

and we obtain for the values of $\eta^{(\mathbf{a})}(d_1,\ldots,d_r)$ formula (9). □

For $t_1=\ldots=t_r=1$ we obtain from (26) formula (8) given in the Introduction.

COROLLARY 8 ($r=2$, $f_1=f_2=\mathrm{id}$).

$$\begin{aligned} R_2^{(G)}(m_1,m_2) \quad &:= \quad \frac{1}{\phi(M)} \sum_{\substack{k=1\\ \gcd(k,M)=1}}^{M} \gcd(g_1(k),m_1)\gcd(g_2(k),m_2) \\ &= \sum_{d_1\mid m_1,d_2\mid m_2} \phi(\gcd(d_1,d_2))\eta_G(d_1,d_2). \end{aligned}$$

Proof. Use that $\phi(a)\phi(b)=\phi(\gcd(a,b))\phi(\operatorname{lcm}[a,b])$ for any $a,b\in\mathbb{N}$, which holds for any multiplicative function written instead of ϕ. □

COROLLARY 9 ($r=2$, $f_1=f_2=\mathrm{id}$, $g_1(x)=x-a_1$, $g_2(x)=x-a_2$, $a_1,a_2\in\mathbb{Z}$).

$$R_2^{(a_1,a_2)}(m_1,m_2) \quad := \quad \frac{1}{\phi(M)} \sum_{\substack{k=1\\ \gcd(k,M)=1}}^{M} \gcd(k-a_1,m_1)\gcd(k-a_2,m_2)$$

$$(27) \qquad = \sum_{\substack{d_1\mid m_1,d_2\mid m_2\\ \gcd(d_1,a_1)=1,\gcd(d_2,a_2)=1\\ \gcd(d_1,d_2)\mid a_1-a_2}} \phi(\gcd(d_1,d_2)).$$

COROLLARY 10 ($r=2$, $f_1=f_2=\mathrm{id}$, $g_1(x)=x-a_1$, $g_2(x)=x-a_2$, $|a_1-a_2|=1$).

Let $a_1,a_2\in\mathbb{Z}$ with $|a_1-a_2|=1$. The multiplicative function $R_2^{(a_1,a_2)}(m_1,m_2)$, given by (27) *can be represented as*

$$(28) \qquad R_2^{(a_1,a_2)}(m_1,m_2) = \sum_{\substack{d_1\mid m_1,d_2\mid m_2\\ \gcd(d_1,a_1)=1,\gcd(d_2,a_2)=1\\ \gcd(d_1,d_2)=1}} 1,$$

and for any prime p and any $u,v\in\mathbb{N}$,

$$(29) \qquad R_2^{(a_1,a_2)}(p^u,p^v) = \begin{cases} u+v+1, & p\nmid a_1, p\nmid a_2,\\ u+1, & p\nmid a_1, p\mid a_2,\\ v+1, & p\mid a_1, p\nmid a_2,\\ 1, & p\mid a_1, p\mid a_2. \end{cases}$$

Now we deduce formula (10) given in the Introduction.

COROLLARY 11 ($r=2,\ f_1=f_2=\mathrm{id},\ g_1(x)=g_2(x)=x-a,\ a\in\mathbb{Z},\ \gcd(a,m)=1$). *If* $\gcd(a,m)=1$, *then*

$$R_2^{(a)}(m_1,m_2) := \frac{1}{\phi(M)} \sum_{\substack{k=1\\ \gcd(k,M)=1}}^{M} \gcd(k-a,m_1)\gcd(k-a,m_2)$$

$$= \sum_{d_1\mid m_1, d_2\mid m_2} \phi(\gcd(d_1,d_2)). \tag{30}$$

Note that other special systems of F and G can be considered too. We give the following example.

COROLLARY 12 ($r=2,\ f_1=f_2=\mathrm{id},\ g_1(x)=g_2(x)=x^2-a,\ \gcd(a,m)=1$). *For every* $m=\mathrm{lcm}[m_1,m_2]$ *odd with* $\gcd(a,m)=1$,

$$\sum_{\substack{k=1\\ \gcd(k,m)=1}}^{m} \gcd(k^2-a,m_1)\gcd(k^2-a,m_2)$$

$$= \phi(m) \sum_{d_1\mid m_1, d_2\mid m_2} \phi(\gcd(d_1,d_2)) \prod_{p\mid \mathrm{lcm}[d_1,d_2]} \left(1+\left(\frac{a}{p}\right)\right),$$

which is a multiple of $\phi(m)$, *where* $\left(\frac{a}{p}\right)$ *is the Legendre symbol.*

In particular, for $a=1$ *and every* m_1,m_2 *odd,*

$$\sum_{\substack{k=1\\ \gcd(k,m)=1}}^{m} \gcd(k^2-1,m_1)\gcd(k^2-1,m_2) = \phi(m) \sum_{d_1\mid m_1, d_2\mid m_2} \phi(\gcd(d_1,d_2)) 2^{\omega(\mathrm{lcm}[d_1,d_2])}$$

and where $\omega(n)$ *denotes the number of distinct prime factors of* n.

Proof. The congruence $x^2\equiv a \pmod{p^e}$ has $1+\left(\frac{a}{p}\right)$ solutions (mod p^e) for any prime $p>2$, $p\nmid a$ and any $e\in\mathbb{N}$. Therefore, $\eta_g(n)=\prod_{p\mid n}\left(1+\left(\frac{a}{p}\right)\right)$ for any $n\in\mathbb{N}$ odd with $\gcd(n,a)=1$. Apply Corollary 6. □

4. The number of cyclic subgroups of the direct product of several cyclic groups

THEOREM 3. *Let* $m_1,\ldots,m_r\in\mathbb{N}$. *The number of cyclic subgroups of the group* $C_{m_1}\times\cdots\times C_{m_r}$ *is given by the formula*

$$c(C_{m_1}\times\cdots\times C_{m_r}) = \sum_{d_1\mid m_1,\ldots,d_r\mid m_r} \frac{\phi(d_1)\cdots\phi(d_r)}{\phi(\mathrm{lcm}[d_1,\ldots,d_r])}, \tag{31}$$

representing a multiplicative function of r variables.

In particular, the number of cyclic subgroups of $C_{m_1} \times C_{m_2}$ is

$$c(C_{m_1} \times C_{m_2}) = \sum_{d_1|m_1, d_2|m_2} \phi(\gcd(d_1, d_2)), \tag{32}$$

and for any prime p and any $u, v \in \mathbb{N}$ with $u \geq v$,

$$c(C_{p^u} \times C_{p^v}) = 2\left(1 + p + p^2 + \ldots + p^{v-1}\right) + (u - v + 1)\, p^v. \tag{33}$$

Proof. Formula (31) follows at once from (7), deduced in the Introduction, by applying (8) with $a_1 = \ldots = a_r = 1$ and $M = m_1 \cdots m_r$. For the case $r = 2$ see Corollary 11. The values of $c(C_{p^u} \times C_{p^v})$ are easily obtained by (32). □

Note that certain formulae for the number of cyclic subgroups of the p-group $C_{p^{\alpha_1}} \times \cdots \times C_{p^{\alpha_r}}$ $(\alpha_1, \ldots, \alpha_r \in \mathbb{N})$, including (33) were deduced in the recent paper [17, Section 4] by a different method. Formulae (31) and (32) are given, without proof, in [21] in cases $r = 3$, $m_1 = m_2 = m_3$ and $r = 2$, $m_1 = m_2$, respectively.

5. Further remarks

In case $r = 1$ formulae (21) and (23) can be used to deduce new identities, representing functions of a single variable, if the values $N_{g_1}(n)$, respectively $\eta_{g_1}(n)$ $(n \in \mathbb{N})$ are known. As examples, we point out the next identities.

COROLLARY 13. *Let $j \in \mathbb{N}$. For every $n \in \mathbb{N}$,*

$$\frac{1}{n} \sum_{k=1}^{n} \gcd(k^j, n) = \sum_{d|n} \frac{\phi(d) N^{(j)}(d)}{d}, \tag{34}$$

where the multiplicative function $N^{(j)}$ is given by $N^{(j)}(p^a) = p^{[(j-1)a/j]}$ for every prime power p^a ($a \in \mathbb{N}$), $[y]$ denoting the greatest integer $\leq y$.

Proof. Apply formula (21) for $r = 1$, $f_1 = \text{id}$, $g(x) = x^j$ where the number of solutions of the congruence $x^j \equiv 0 \pmod{p^a}$ is $p^{[(j-1)a/j]}$, as it can be checked easily. □

In what follows, consider formula (23) for $r = 1$, $f_1 = \text{id}$ and $g_1 = g$. Then (23) reduces to (4).

COROLLARY 14. *Let $a, b \in \mathbb{Z}$ with $\gcd(b, n) = 1$. Then for every $n \in \mathbb{N}$,*

$$\sum_{\substack{k=1 \\ \gcd(k,n)=1}}^{n} \gcd(bk - a, n) = \phi(n)\tau(n, a). \tag{35}$$

Proof. Apply formula (4) in case of the linear polynomial $g(x) = bx - a$. Here $\eta_g(n) = 1$ for $\gcd(a, n) = 1$ and $\eta_g(n) = 0$ otherwise. □

For $a=b=1$ (35) reduces to (1).

COROLLARY 15. *Let $n\in\mathbb{N}$. Then*

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(k^2-1,n)=\phi(n)h(n), \tag{36}$$

where

$$h(n)=\begin{cases}\tau(m^2), & n=m \text{ odd},\\ 2\tau(m^2), & n=2m,\ m \text{ odd},\\ 4(\ell-1)\tau(m^2), & n=2^\ell m,\ \ell\ge 2,\ m \text{ odd}.\end{cases} \tag{37}$$

Proof. Apply formula (4) for the polynomial $g(x)=x^2-1$. Any solution of $x^2\equiv 1$ (mod n) is coprime to n; hence $\eta_g(n)=N_g(n)$. For the number $N_g(p^a)$ of solutions of $x^2\equiv 1$ (mod p^a) it is well known that $N_g(p^a)=2$ (p odd prime, $a\in\mathbb{N}$), $N_g(2)=1$, $N_g(4)=2$, $N_g(2^\ell)=4$ ($\ell\ge 3$). □

Finally, let $j\in\mathbb{N}$ be fixed. Group the prime factors of $n\in\mathbb{N}$ according to the values $\gcd(p-1,j)=d$ and write $n=\prod_{d\mid j} n_d$, where for any $d\mid j$,

$$n_d = \prod_{\substack{p^k\|n\\ \gcd(p-1,j)=d}} p^k.$$

COROLLARY 16. *For every $n\in\mathbb{N}$ odd,*

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(k^j-1,n) = \phi(n)\prod_{d\mid j}\tau(n_d^d). \tag{38}$$

Proof. For $g(x)=x^j-1$ we have $\eta_g(n)=N_g(n)$ with $\eta(p^a)=\gcd(j,p-1)$ for every p odd prime and $a\in\mathbb{N}$. Apply formula (4). Now, for $F(n):=\sum_{d\mid n}\eta_g(d)$ one has $F(p^a)=1+a\gcd(j,p-1)=\tau(p^{a\gcd(j,p-1)})$ for any p odd prime and $a\in\mathbb{N}$. □

COROLLARY 17 ($j=6$). *For every $n\in\mathbb{N}$ odd,*

$$\sum_{\substack{k=1\\ \gcd(k,n)=1}}^{n} \gcd(k^6-1,n) = \phi(n)\tau(A^6)\tau(B^2), \tag{39}$$

where A is the product, with multiplicity, of the prime factors $p\equiv 1$ (mod 6) of n, and $B=n/A$.

References

[1] APOSTOL T. M. *Introduction to Analytic Number Theory*. Springer, 1976.

[2] DEITMAR A., KOYAMA S. AND KUROKAWA N. Absolute zeta functions. *Proc. Japan Acad. Ser. A Math. Sci. 84* (2008), 138–142.

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

[4] HAUKKANEN P. On a gcd-sum function. *Aequationes Math. 76* (2008), 168–178.

[5] HAUKKANEN P. AND MCCARTHY P. J. Sums of values of even functions. *Portugal. Math. 48* (1991), 53–66.

[6] HAUKKANEN P. AND SIVARAMAKRISHNAN R. On certain trigonometric sums in several variables. *Collect. Math. 45* (1994), 245–261.

[7] HAUKKANEN P. AND WANG J. A generalization of Menon's identity with respect to a set of polynomials. *Portugal. Math. 53* (1996), 331–337.

[8] MCCARTHY P. J. *Introduction to Arithmetical Functions*. Universitext. Springer, 1986.

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

[10] NAGESWARA RAO K. *On certain arithmetical sums*. Lecture Notes Math. Springer, 1972, pp. 181–192.

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

[12] SITA RAMAIAH V. Arithmetical sums in regular convolutions. *J. Reine Angew. Math. 303/304* (1978), 265–283.

[13] SIVARAMAKRISHNAN R. A number-theoretic identity. *Publ. Math. Debrecen 21* (1974), 67–69.

[14] SIVARAMAKRISHNAN R. Square reduced residue systems (mod r) and related arithmetical functions. *Canad. Math. Bull. 22* (1979), 207–220.

[15] SIVARAMAKRISHNAN R. *Classical Theory of Arithmetic Functions*. Monographs and Textbooks in Pure and Applied Mathematics, Vol. 126. Marcel Dekker, 1989.

[16] SURY B. Some number-theoretic identities from group actions. *Rend. Circ. Mat. Palermo (2) 58* (2009), 99–108.

[17] TĂRNĂUCEANU M. 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.

[18] TÓTH L. Some remarks on a paper of V. A. Liskovets. submitted.

[19] TÓTH L. A survey of gcd-sum functions. *J. Integer Sequences 13* (2010). Article 10.8.1, 23 pp.

[20] VAIDYANATHASWAMY R. The theory of multiplicative arithmetic functions. *Trans. Amer. Math. Soc. 33* (1931), 579–662.

[21] The On-Line Encyclopedia of Integer Sequences, items A060648, A064969.

AMS Subject Classification: 11A25, 11A07, 20D60, 20K27

László TÓTH
Department of Mathematics University of Pécs
Ifjúság u. 6, H-7624 Pécs, HUNGARY
and
Institute of Mathematics, Department of Integrative Biology Universität für Bodenkultur
Gregor Mendel-Straße 33, A-1180 Wien, AUSTRIA
e-mail: `ltoth@gamma.ttk.pte.hu`

Lavoro pervenuto in redazione il 15.06.2011