A GENERALIZATION OF MENON’S IDENTITY WITH RESPECT TO A SET OF POLYNOMIALS

P. Haukkanen and J. Wang*

Abstract: P. Kesava Menon’s elegant identity states that
\[ \sum_{\substack{a \equiv 1 \pmod{n} \\ (a, n) = 1}} (a - 1, n) = \phi(n) \tau(n), \]
where \( \phi(n) \) is Euler’s totient function and \( \tau(n) \) is the number of divisors of \( n \). In this paper we generalize this identity so that, among other things, \( a - 1 \) is replaced with a set \( \{ f_i(a) \} \) of polynomials in \( \mathbb{Z}[a_1, a_2, ..., a_u] \).

1 - Introduction

For positive integers \( u \) and \( n \), let \( S_u(n) \) denote the set of all \( u \)-vectors \( \{ a_i \pmod{n} \} \) such that \( ((a_i)_u) = 1 \), where \( (a_i) \) is the g.c.d. of \( a_1, a_2, ..., a_u \). It is well-known that the cardinality of \( S_u(n) \) is Jordan’s totient \( J_u(n) \). In particular, \( J_1(n) \) is Euler’s totient \( \phi(n) \). For the sake of brevity we write \( S_1(n) = S(n) \).

In [5], P. Kesava Menon established the elegant identity
\[ \sum_{a \in S(n)} (a - 1, n) = \phi(n) \tau(n), \]
where \( \tau(n) \) is the number of divisors of \( n \). Richards [10] mentioned among other things the identity
\[ \sum_{a \in S(n)} \langle f(a), n \rangle = \phi(n) \sum_{d|n} \{ r \in S(d) : f(r) \equiv 0 \pmod{d} \}, \]

Received: September 7, 1995.
AMS Subject Classification: 11A25.
Keywords and Phrases: Menon’s identity, Set of polynomials, Euler’s totient, Jordan’s totient, Regular arithmetical convolution.
* Supported by the Natural Science Foundations of China and Liaoning Province.
where \( f(x) \) is any polynomial with integer coefficients. Nageswara Rao [8] generalized (1.1) to

\[
\sum_{\{a_i\} \in S_u(n)} (a_1 - s_1, \ldots, a_u - s_u, n) = J_u(n) \tau(n),
\]

where \( \{s_i\} \) is a fixed element of \( S_u(n) \). Sita Ramaiah [11, Section 9] considers Menon’s identity with respect to regular convolutions.

In this paper we consider a combination of (1.2) and (1.3) with respect to regular convolutions.

It should be noted that in the literature there are also other generalizations of Menon’s identity (see e.g. [1, 3, 4, 7, 12–17]). The most general identity is given in [3]. This identity arises from the theory of even functions and contains as special cases most of the generalized Menon identities. However, it does not deal with generalized Menon identities with respect to polynomials and therefore does not contain (1.2). We do not consider the identity of [3] here.

2 – Preliminaries

We assume that the reader is familiar with the notion of regular convolution. This notion was introduced by Narkiewicz [9]. Further background material on regular convolution can be found e.g. in [6, 11].

Let \( A \) be a regular convolution. For a positive integer \( k \), denote

\[
A_k(n) = \{d: d^k \in A(n^k)\}.
\]

It is known [11] that \( A_k \) is a regular convolution. The \( A_k \)-convolution of two arithmetical functions \( f \) and \( g \) is given as

\[
(f \ast A_k g)(n) = \sum_{d \in A_k(n)} f(d) g(n/d).
\]

Let \( \mu_{A_k} \) denote the \( A_k \)-analogue of the Möbius function. We then have

\[
(2.1) \quad f(n) = \sum_{d \in A_k(n)} (f \ast A_k \mu_{A_k})(d).
\]

Let \( A \) be a regular convolution, and let \( k, u \) and \( n \) be positive integers. Let \( S_{A,k}^{(u)}(n) \) denote the set of all \( u \)-vectors \( \{a_i\} \) (mod \( n^k \)) such that \( ((a_i), n^k)_{A,k} = 1 \), where \( ((a_i), n^k)_{A,k} \) denotes the greatest \( k \)-th power divisor of \( (a_i) \) which belongs to \( A(n^k) \). The number of elements in \( S_{A,k}^{(u)}(n) \) is denoted by \( \phi_{A,k}^{(u)}(n) \). If \( k = 1 \)
and $A$ is the Dirichlet convolution, then $S_{A,k}^{(u)}(n) = S_u(n)$ and $\phi_{A,k}^{(u)}$ is the Jordan totient $J_u$. The function $\phi_{A,k}^{(u)}$ is thus a generalization of the Jordan totient $J_u$ and therefore a generalization of the Euler totient $\phi$. It is known \cite{3} that

$$\phi_{A,k}^{(u)}(n) = \sum_{d \in A_k(n)} d^{ku} \mu_{A_k}(n/d) .$$

The Möbius inversion formula with respect to regular convolutions gives

$$n^{ku} = \sum_{d \in A_k(n)} \phi_{A,k}^{(u)}(d) .$$

Further, it can be verified that

$$\phi_{A,k}^{(u)}(n) = n^{ku} \prod_{p^t \in A_k(n)} (1 - p^{-kt}) ,$$

where the product is over the $A_k$-primitive prime powers of $n$.

In what follows we denote $u$-vectors by boldface letters, i.e., $\{a_i\} = \mathbf{a}$.

**Lemma.** Let $d \in A_k(n)$. Then for any $\mathbf{b} \in S_{A,k}^{(u)}(d)$,

$$\left| \left\{ \mathbf{a} \in S_{A,k}^{(u)}(n): \mathbf{a} \equiv \mathbf{b} \pmod{d^k} \right\} \right| = \phi_{A,k}^{(u)}(n)/\phi_{A,k}^{(u)}(d) .$$

**Proof:** Let $p_j^{t_j}, j = 1, 2, ..., v$, be the $A_k$-primitive prime powers such that $p_j^{t_j} \in A_k(n)$, $p_j^{t_j} \nmid d$. Denote

$$T = \left\{ \mathbf{a} \pmod{n^k}: \mathbf{a} \equiv \mathbf{b} \pmod{d^k} \right\} ,$$

$$T_j = \left\{ \mathbf{a} \in T: p_j^{t_j} \nmid (a_i) \right\}, \quad j = 1, 2, ..., v .$$

It is clear that an element $\mathbf{a} \in T$ belongs to $S_{A,k}^{(u)}(n)$ if, and only if, $p_j^{t_j} \nmid (a_i)$ for all $A_k$-primitive prime powers $p_j^{t_j} \in A_k(n)$. If $p_j^{t_j} \in A_k(n)$ and $p_j^{t_j} \nmid d$, then $p_j^{t_j} \nmid (a_i)$. Namely, otherwise $p_j^{t_j} \mid (b_i)$, which contradicts the hypothesis $\mathbf{b} \in S_{A,k}^{(u)}(d)$. Thus $\mathbf{a} \in T$ belongs to $S_{A,k}^{(u)}(n)$ if, and only if, $p_j^{t_j} \nmid (a_i)$ for all $j = 1, 2, ..., v$. So we can deduce that

$$\left| \left\{ \mathbf{a} \in S_{A,k}^{(u)}(n): \mathbf{a} \equiv \mathbf{b} \pmod{d^k} \right\} \right| = \left| T \setminus \bigcup_{j=1}^{v} T_j \right| .$$
By the inclusion-exclusion principle,
\[
\left| \{ a \in S_{A,k}^{(u)}(n) : a \equiv b \pmod{d^k} \} \right| = \\
= |T| + \sum_{j=1}^{v} (-1)^j \sum_{1 \leq e_1 < e_2 < \ldots < e_j \leq v} |T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j}|.
\]

If \( a \in T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j} \), then for all \( i = 1, 2, \ldots, u \) there exists \( x_i = 1, 2, \ldots, n^k/d^k \) such that \( a_i = b_i + x_i d^k \) and
\[
b_i + x_i d^k \equiv 0 \pmod{p_{e_1}^{kt_{e_1}} p_{e_2}^{kt_{e_2}} \ldots p_{e_j}^{kt_{e_j}}}.
\]

Denote briefly \( m_j = p_{e_1}^{kt_{e_1}} p_{e_2}^{kt_{e_2}} \ldots p_{e_j}^{kt_{e_j}} \). Since \( d \in A_k(n) \) and \( p_j^{t_j} \in A_k(n), p_j^{t_j} \nmid d \) for all \( j = 1, 2, \ldots, v \), we have
\[
(m_j, d^k) = 1.
\]

Thus for all \( i = 1, 2, \ldots, u \) there exists a unique \( x_i \) (mod \( m_j \)) satisfying (2.7). Consequently, there exists exactly one \( x_i \) satisfying (2.7) in each of the intervals \([1, m_j], [m_j + 1, 2m_j], \ldots, [(c - 1)m_j + 1, cm_j]\), where \( cm_j = n^k/d^k \). Therefore
\[
|T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j}| = \frac{n^{ku/d^ku}}{m_j^{u}} = \frac{n^{ku/d^ku}}{p_{e_1}^{kut_{e_1}} p_{e_2}^{kut_{e_2}} \ldots p_{e_j}^{kut_{e_j}}}.
\]

Now, by (2.6), we have
\[
\left| \{ a \in S_{A,k}^{(u)}(n) : a \equiv b \pmod{d^k} \} \right| = \\
= \frac{n^{ku/d^ku}}{d^ku} + \sum_{j=1}^{v} (-1)^j \sum_{1 \leq e_1 < e_2 < \ldots < e_j \leq v} \frac{n^{ku/d^ku}}{p_{e_1}^{kut_{e_1}} p_{e_2}^{kut_{e_2}} \ldots p_{e_j}^{kut_{e_j}}} \\
= \frac{n^{ku/d^ku}}{d^ku} \prod_{j=1}^{v} (1 - p_j^{-kut_j}) = \frac{n^{ku/d^ku}}{d^ku \prod_{j=1}^{v} (1 - p_j^{-kut_j})} \\
= \frac{\phi_{A,k}^{(u)}(n)}{\phi_{A,k}^{(u)}(d)}.
\]

This completes the proof. \(\Box\)

**Remark.** Let \( D(b, d, n) \) denote the arithmetic progression
\[
D(b, d, n) = \{ b, b + d, \ldots, b + (n - 1)d \},
\]
where \( (b, d) = 1 \). Let \( \phi(b, d, n) \) denote the number of elements in \( D(b, d, n) \) that are relatively prime to \( n \) (see [2]). A direct consequence of the above lemma is that

\[
\phi(b, d, n) = d \phi(n)/\phi(d) .
\]

This result could be generalized to the general case of the lemma, that is, with respect to \( k, u \) and \( A \).

3 – The identity

Let \( F = \{f_1, f_2, ..., f_s\} \) be a set of polynomials in \( \mathbb{Z}[x_1, x_2, ..., x_u] \). Let \( N_F(n) \) denote the number of elements \( a \in S^{(u)}_{A,k}(n) \) such that \( f_i(a) \equiv 0 \) (mod \( n^k \)) for every \( i = 1, 2, ..., s \) and let \( T_F \) be the \( A_k \)-convolution of \( N_F \) and the \( \zeta \)-function, i.e.,

\[
(3.1) \quad T_F(n) = \sum_{d \in A_k(n)} N_F(d) \zeta(n/d) = \sum_{d \in A_k(n)} N_F(d) .
\]

**Theorem.** Let \( g \) be any arithmetical function. Then

\[
(3.2) \quad \sum_{a \in S^{(u)}_{A,k}(n)} g\left(\left(\left(f_i(a), n^k\right)^{1/k}_{A,k}\right)\right) = \phi^{(u)}_{A,k}(n) \sum_{d \in A_k(n)} (g * A_k \mu_{A_k})(d) N_F(d)/\phi^{(u)}_{A,k}(d) .
\]

**Proof:** By (2.1),

\[
\sum_{a \in S^{(u)}_{A,k}(n)} g\left(\left(f_i(a), n^k\right)^{1/k}_{A,k}\right) = \sum_{a \in S^{(u)}_{A,k}(n)} \sum_{d \in A_k(n)} \sum_{d^k \mid (f_i(a))} (g * A_k \mu_{A_k})(d)
\]

\[
= \sum_{d \in A_k(n)} (g * A_k \mu_{A_k})(d) \sum_{a \in S^{(u)}_{A,k}(n)} \sum_{d^k \mid (f_i(a))} 1
\]

\[
= \sum_{d \in A_k(n)} (g * A_k \mu_{A_k})(d) \sum_{a \in S^{(u)}_{A,k}(n)} \sum_{d^k \mid (f_i(b))} \left\{ a \in S^{(u)}_{A,k}(n) : b \equiv b \pmod{d^k} \right\} .
\]
By the lemma,
\[
\sum_{a \in S_{A,k}^{(u)}(n)} g\left((f_i(a), n^k)_{A,k}\right)^{1/k} = \sum_{d \in A_k(n)} (g * A_k \mu A_k)(d) N_F(d) \phi_{A,k}^{(u)}(n)/\phi_{A,k}^{(u)}(d)
\]
\[
= \phi_{A,k}^{(u)}(n) \sum_{d \in A_k(n)} (g * A_k \mu A_k)(d) N_F(d)/\phi_{A,k}^{(u)}(d).
\]
This completes the proof. $\blacksquare$

**Corollary.** We have

\[
(3.3) \quad \sum_{a \in S_{A,k}^{(u)}(n)} \left( (f_i(a), n^k)_{A,k} \right)^u = \phi_{A,k}^{(u)}(n) T_F(n).
\]

**Proof:** Take $g(n) = n^{ku}$ in the theorem and apply (2.2) and (3.1). $\blacksquare$

**Example 1:** If $F = \{f\}$, $k = u = 1$ and $A$ is the Dirichlet convolution, then (3.3) reduces to (1.2). If $f(x) = x - 1$, then (1.2) reduces to (1.1).

**Example 2:** If $F = \{x_1 - s_1, x_2 - s_2, ..., x_u - s_u\}$, $s \in S_u(n)$, $k = 1$ and $A$ is the Dirichlet convolution, then $N_F(n) = 1$, $T_F(n) = \tau(n)$ and therefore (3.3) reduces to (1.3).

**REFERENCES**


Penti Haukkanen,
Department of Mathematical Sciences, University of Tampere,
P.O. Box 607, FIN-33101 Tampere – FINLAND

and

Jun Wang,
Institute of Mathematical Sciences, Dalian University of Technology,
Dalian 116024 – PEOPLE’S REPUBLIC OF CHINA