PORTUGALIAE MATHEMATICA
Vol. 53 Fasc. 3 – 1996

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

$$\sum_{\substack{a \pmod n \\ (a,n)=1}} (a-1,n) = \phi(n)\,\tau(n) ,$$

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 $\{f_i(\mathbf{a})\}$ of polynomials in $\mathbf{Z}[a_1, a_2, ..., a_u]$.

1 – Introduction

For positive integers u and n, let $S_u(n)$ denote the set of all u-vectors $\{a_i\}$ $(\bmod n)$ such that $((a_i), n) = 1$, 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

$$\sum_{a\in S(n)} (a-1,n) = \phi(n)\,\tau(n) , \tag{1.1}$$

where $\tau(n)$ is the number of divisors of n. Richards [10] mentioned among other things the identity

$$\sum_{a\in S(n)} (f(a),n) = \phi(n) \sum_{d|n} \Big|\Big\{r\in S(d)\colon\ f(r)\equiv 0 \pmod d\Big\}\Big| , \tag{1.2}$$

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

$$\sum_{\{a_i\}\in S_u(n)} (a_1-s_1,\, ...,\, a_u-s_u,\, n) = J_u(n)\,\tau(n) \ , \tag{1.3}$$

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 wit 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

$$A_k(n) = \{d\colon\ d^k \in A(n^k)\} \ .$$

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

$$(f *_{A_k} g)(n) = \sum_{d\in A_k(n)} f(d)\, g(n/d) \ .$$

Let μ_{A_k} denote the A_k-analogue of the Möbius function. We then have

$$f(n) = \sum_{d\in A_k(n)} (f *_{A_k} \mu_{A_k})(d) \ . \tag{2.1}$$

Let A be a regular convolution, and let k, u and n be positive integers. Let $S^{(u)}_{A,k}(n)$ denote the set of all u-vectors $\{a_i\}\ (\operatorname{mod} n^k)$ 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 $S^{(u)}_{A,k}(n)$ is denoted by $\phi^{(u)}_{A,k}(n)$. If $k = 1$

and A is the Dirichlet convolution, then $S^{(u)}_{A,k}(n) = S_u(n)$ and $\phi^{(u)}_{A,k}$ is the Jordan totient J_u. The function $\phi^{(u)}_{A,k}$ is thus a generalization of the Jordan totient J_u and therefore a generalization of the Euler totient ϕ. It is known [3] that

$$\phi^{(u)}_{A,k}(n) = \sum_{d \in A_k(n)} d^{ku}\, \mu_{A_k}(n/d) \ . \tag{2.2}$$

The Möbius inversion formula with respect to regular convolutions gives

$$n^{ku} = \sum_{d \in A_k(n)} \phi^{(u)}_{A,k}(d) \ . \tag{2.3}$$

Further, it can be verified that

$$\phi^{(u)}_{A,k}(n) = n^{ku} \prod_{p^t \in A_k(n)} (1 - p^{-kut}) \ , \tag{2.4}$$

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 $\mathbf{b} \in S^{(u)}_{A,k}(d)$,*

$$\left|\left\{\mathbf{a} \in S^{(u)}_{A,k}(n)\colon\ \mathbf{a} \equiv \mathbf{b} \pmod{d^k}\right\}\right| = \phi^{(u)}_{A,k}(n)/\phi^{(u)}_{A,k}(d) \ . \tag{2.5}$$

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

$$T = \left\{\mathbf{a} \pmod{n^k}\colon\ \mathbf{a} \equiv \mathbf{b} \pmod{d^k}\right\} \ ,$$
$$T_j = \left\{\mathbf{a} \in T\colon\ p_j^{t_j k} \mid (a_i)\right\} , \qquad j = 1, 2, ..., v \ .$$

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

$$\left|\left\{\mathbf{a} \in S^{(u)}_{A,k}(n)\colon\ \mathbf{a} \equiv \mathbf{b} \pmod{d^k}\right\}\right| = \left|T \setminus \bigcup_{j=1}^{v} T_j\right| \ .$$

By the inclusion-exclusion principle,

$$\left|\left\{\mathbf{a} \in S^{(u)}_{A,k}(n) \colon\ \mathbf{a} \equiv \mathbf{b} \,(\operatorname{mod} d^k)\right\}\right| = \tag{2.6}$$

$$= |T| + \sum_{j=1}^{v} (-1)^j \sum_{1 \le e_1 \le e_2 < \ldots < e_j \le v} |T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j}| \ .$$

If $\mathbf{a} \in T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j}$, 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

$$b_i + x_i\, d^k \equiv 0 \ (\operatorname{mod} p_{e_1}^{kt_{e_1}}\, p_{e_2}^{kt_{e_2}} \cdots p_{e_j}^{kt_{e_j}}) \ . \tag{2.7}$$

Denote briefly $m_j = p_{e_1}^{kt_{e_1}}\, p_{e_2}^{kt_{e_2}} \cdots p_{e_j}^{kt_{e_j}}$. Since $d \in A_k(n)$ and $p_j^{t_j} \in A_k(n)$, $p_j^{t_j} \not| d$ 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 $x_i \ (\operatorname{mod} m_j)$ satisfying (2.7). Consequently, there exists exactly one x_i satisfying (2.7) in each of the intervals $[1, m_j]$, $[m_j + 1, 2m_j]$, ..., $[(c-1)m_j + 1, c\, m_j]$, where $c\, m_j = n^k/d^k$. Therefore

$$|T_{e_1} \cap T_{e_2} \cap \ldots \cap T_{e_j}| = \frac{n^{ku}/d^{ku}}{m_j^u} = \frac{n^{ku}/d^{ku}}{p_{e_1}^{kut_{e_1}}\, p_{e_2}^{kut_{e_2}} \cdots p_{e_j}^{kut_{e_j}}} \ .$$

Now, by (2.6), we have

$$\left|\left\{\mathbf{a} \in S^{(u)}_{A,k}(n) \colon\ \mathbf{a} \equiv \mathbf{b} \,(\operatorname{mod} d^k)\right\}\right| =$$

$$= \frac{n^{ku}}{d^{ku}} + \sum_{j=1}^{v} (-1)^j \sum_{1 \le e_1 < e_2 < \ldots < e_j \le v} \frac{n^{ku}/d^{ku}}{p_{e_1}^{kut_{e_1}}\, p_{e_2}^{kut_{e_2}} \cdots p_{e_j}^{kut_{e_j}}}$$

$$= \frac{n^{ku}}{d^{ku}} \prod_{j=1}^{v} (1 - p_j^{-kut_j}) = \frac{n^{ku} \prod_{p^t \in A_k(n)} (1 - p^{-kut})}{d^{ku} \prod_{p^t \in A_k(d)} (1 - p^{-kut})}$$

$$= \frac{\phi^{(u)}_{A,k}(n)}{\phi^{(u)}_{A,k}(d)} \ .$$

This completes the proof. ∎

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 $\mathbf{Z}[x_1, x_2, ..., x_u]$. Let $N_F(n)$ denote the number of elements $\mathbf{a} \in S^{(u)}_{A,k}(n)$ such that $f_i(\mathbf{a}) \equiv 0 \pmod{n^k}$ for every $i = 1, 2, ..., s$ and let T_F be the A_k-convolution of N_F and the ζ-function, i.e.,

$$T_F(n) = \sum_{d \in A_k(n)} N_F(d)\,\zeta(n/d) = \sum_{d \in A_k(n)} N_F(d)\ . \tag{3.1}$$

Theorem. *Let g be any arithmetical function. Then*

$$\sum_{\mathbf{a} \in S^{(u)}_{A,k}(n)} g\Big(\big((f_i(\mathbf{a})), n^k\big)^{1/k}_{A,k}\Big) = \phi^{(u)}_{A,k}(n) \sum_{d \in A_k(n)} (g *_{A_k} \mu_{A_k})(d)\, N_F(d)/\phi^{(u)}_{A,k}(d)\ . \tag{3.2}$$

Proof: By (2.1),

$$\begin{aligned}
&\sum_{\mathbf{a} \in S^{(u)}_{A,k}(n)} g\Big(\big((f_i(\mathbf{a})), n^k\big)^{1/k}_{A,k}\Big) = \\
&\qquad = \sum_{\mathbf{a} \in S^{(u)}_{A,k}(n)} \sum_{\substack{d \in A_k(n) \\ d^k | (f_i(\mathbf{a}))}} (g *_{A_k} \mu_{A_k})(d) \\
&\qquad = \sum_{d \in A_k(n)} (g *_{A_k} \mu_{A_k})(d) \sum_{\substack{\mathbf{a} \in S^{(u)}_{A,k}(n) \\ d^k | (f_i(\mathbf{a}))}} 1 \\
&\qquad = \sum_{d \in A_k(n)} (g *_{A_k} \mu_{A_k})(d) \sum_{\substack{\mathbf{b} \in S^{(u)}_{A,k}(d) \\ d^k | (f_i(\mathbf{b}))}} \Big|\Big\{\mathbf{a} \in S^{(u)}_{A,k}(n) \colon\ \mathbf{a} \equiv \mathbf{b} \pmod{d^k}\Big\}\Big|\ .
\end{aligned}$$

By the lemma,

$$\begin{aligned}\sum_{\mathbf{a}\in S^{(u)}_{A,k}(n)} g\Big(\big((f_i(\mathbf{a})),n^k\big)^{1/k}_{A,k}\Big) &= \sum_{d\in A_k(n)} (g *_{A_k} \mu_{A_k})(d)\, N_F(d)\, \phi^{(u)}_{A,k}(n)/\phi^{(u)}_{A,k}(d) \\ &= \phi^{(u)}_{A,k}(n) \sum_{d\in A_k(n)} (g *_{A_k} \mu_{A_k})(d)\, N_F(d)/\phi^{(u)}_{A,k}(d)\ .\end{aligned}$$

This completes the proof. ∎

Corollary. *We have*

$$\sum_{\mathbf{a}\in S^{(u)}_{A,k}(n)} \big((f_i(\mathbf{a})),n^k\big)^{u}_{A,k} = \phi^{(u)}_{A,k}(n)\, T_F(n)\ . \tag{3.3}$$

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

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 $F=\{x_1-s_1, x_2-s_2, ..., x_u-s_u\}$, $\mathbf{s}\in S_u(n)$, $k=1$ 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

[1] FUNG, F. – A number-theoretic identity arising from Burnside's orbit formula, *Pi Mu Epsilon J.,* 9 (1994), 647–650.

[2] GARCIA, P.G. and LIGH, S. – A generalization of Euler's ϕ-function, *Fibonacci Quart.,* 21 (1983), 26–28.

[3] HAUKKANEN, P. and MCCARTHY, P.J. – Sums of values of even functions, *Portugaliae Math.,* 48 (1991), 53–66.

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

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

[6] MCCARTHY, P.J. – *Introduction to Arithmetical Functions*, Universitext, Springer-Verlag, New York, 1986.

[7] NAGESWARA RAO, K. – Unitary class division of integers mod n and related arithmetical identities, *J. Indian Math. Soc.,* 30 (1966), 195–205.

[8] NAGESWARA RAO, K. – On certain arithmetical sums, *Springer-Verlag Lecture Notes in Math.,* 251 (1972), 181–192.

[9] Narkiewicz, W. – On a class of arithmetical convolutions, *Colloq. Math.,* 10 (1963), 81–94.

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

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

[12] Sivaramakrishnan, R. – Generalization of an arithmetic function, *J. Indian Math. Soc.,* 33 (1969), 127–132.

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

[14] Sivaramakrishnan, R. – Multiplicative even functions $(\operatorname{mod} r)$. I Structural properties, *J. Reine Angew. Math.,* 302 (1978), 32–43.

[15] Venkataraman, T. – A note on the generalization of an arithmetic function in k-th power residue, *Math. Stud.,* 42 (1974), 101–102.

[16] Venkatramaiah, S. – On a paper of Kesava Menon, *Math. Stud.,* 41 (1973), 303–306.

[17] Venkatramaiah, S. – A note on certain totient functions, *Math. Ed.,* 18 (1984), 66–71.

Pentti 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