Miskolc Mathematical Notes
Vol. 22 (2021), No. 2, pp. 763–768
HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2021.3428

A GENERALIZATION OF MENON-RAO-SURY'S IDENTITIES TO ADDITIVE CHARACTERS BY TÓTH'S METHOD

YAN LI, RAN CHEN, AND DAEYEOUL KIM

Received 11 September, 2020

Abstract. In this paper, we obtain a new Menon-type identity:

$$\sum_{\substack{a_1,\ldots,a_s,b_1,\ldots,b_r=1\\ \gcd(a_1,\ldots,a_s,n)=1}}^{n} \gcd(a_1-c_1,\ldots,a_s-c_s,b_1,\ldots,b_r,n)^s\lambda_1(b_1)\cdots\lambda_r(b_r)$$
$$=\varphi_s(n)\sigma_r(\gcd(w_1,\ldots,w_r,n)),$$

where $\lambda_j(b):=\exp(2\pi i w_j b/n)$ is an additive character of $\mathbb{Z}/n\mathbb{Z}$ for $1\leqslant j\leqslant r$, $(c_1,\ldots,c_s)\in\mathbb{Z}^s$ is a fixed vector such that $\gcd(c_1,\ldots,c_s,n)=1$, $\varphi_s(n)=n^s\prod_{p|n}(1-p^{-s})$ is the Jordan's totient function and $\sigma_r(n)=\sum_{d|n}d^r$ is the rth divisor function. This extends Rao's identity ([9]) and Sury's identity ([11]) to additive characters. Following the method of Tóth [14], we also generalize the above identity to arbitrary arithmetic function.

2010 *Mathematics Subject Classification:* 11A07; 11A25

Keywords: Menon's identity, arithmetic function, additive character, divisor function, Jordan's totient function, Dirichlet convolution

1. INTRODUCTION

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

$$\sum_{\substack{a=1\\ \gcd(a,n)=1}}^{n}\gcd(a-1,n)=\varphi(n)\tau(n), \tag{1.1}$$

where gcd(,) represents the greatest common divisor, φ denotes Euler's totient function and $\tau(n)$ is the number of divisors of n. This interesting arithmetic identity was proved by P. K. Menon [6] in 1965 and has lots of generalizations.

Using finite Fourier representations and Cauchy composite of totally even functions, K. Nageswara Rao [9] generalized Menon's identity as follows: for $s\in\mathbb{N}$,

$$\sum_{\substack{a_1,\ldots,a_s=1\\ \gcd(a_1,\ldots,a_s,n)=1}}^{n}\gcd(a_1-c_1,\ldots,a_s-c_s,n)^s=\varphi_s(n)\tau(n), \tag{1.2}$$

where $(c_1,\dots,c_s)\in\mathbb{Z}^s$ is a fixed vector such that $\gcd(c_1,\dots,c_s,n)=1$ and

$$\varphi_s(n):=\#\{(a_1,\dots,a_s)\in\mathbb{Z}^s \mid 1\leqslant a_1,\dots,a_s\leqslant n,\ \gcd(a_1,\dots,a_s,n)=1\} \tag{1.3}$$

is the well known arithmetic function defined by Jordan, usually called Jordan's totient function. Explicitly, Jordan's totient can be computed by

$$\varphi_s(n)=n^s\prod_{p\mid n}(1-p^{-s}), \tag{1.4}$$

where p runs over all prime divisors of n ([1, p.147–155], [5, p.1–2]).

In 2009, B. Sury [11] proved that for $r\geqslant 0$,

$$\sum_{\substack{a,b_1,\dots,b_r=1\\ \gcd(a,n)=1}}^{n}\gcd(a-1,b_1,\dots,b_r,n)=\varphi(n)\sigma_r(n), \tag{1.5}$$

where $\sigma_r(n)=\sum_{d\mid n}d^r$ by using the Cauchy-Frobenius-Burnside lemma.

Recently, Zhao and Cao [19] derived the following elegant Menon-type identity with Dirichlet character:

$$\sum_{\substack{a=1\\ \gcd(a,n)=1}}^{n}\gcd(a-1,n)\chi(a)=\varphi(n)\tau\left(\frac{n}{d}\right), \tag{1.6}$$

where χ is a Dirichlet character modulo n with conductor d.

In [4], Li, Hu and Kim further extended identities (1.5) and (1.6) to multiplicative and additive characters:

$$\begin{aligned}&\sum_{\substack{a,b_1,\dots,b_r=1\\ \gcd(a,n)=1}}^{n}\gcd(a-1,b_1,\dots,b_r,n)\chi(a)\lambda_1(b_1)\cdots\lambda_r(b_r)\\ =&\varphi(n)\sigma_r\left(\gcd\left(n/d,w_1,\dots,w_r\right)\right),\end{aligned} \tag{1.7}$$

where for $1\leqslant j\leqslant r$, $b\mapsto\lambda_j(b):=\exp(2\pi i w_j b/n)$ with $w_j\in\mathbb{Z}$ is an additive character and d is the conductor of a Dirichlet character χ.

In [14], Tóth presented a generalization of (1.7) to arbitrary arithmetic function F, whose proof is short and elegant,

$$\begin{aligned}&\sum_{a_1,\dots,a_s,b_1,\dots,b_r=1}^{n}F(\gcd(a_1-c_1,\dots,a_s-c_s,b_1,\dots,b_r,n))\chi_1(a_1)\cdots\chi_s(a_s)\\ &\lambda_1(b_1)\cdots\lambda_r(b_r)=\varphi(n)^s\chi_1^*(c_1)\cdots\chi_s^*(c_s)\sum_{\substack{m\mid\gcd(n/d_1,\dots,n/d_s,w_1,\dots,w_r)\\ \gcd(n/m,c_1\cdots c_s)=1}}\frac{m^r(\mu*F)(n/m)}{\varphi(n/m)^s},\end{aligned} \tag{1.8}$$

where $(c_1,c_2,\dots,c_s)\in\mathbb{Z}^s$ is an arbitrary vector; χ_j are Dirichlet characters modulo n with conductors d_j and associated primitive characters $\chi_j^*(1\leqslant j\leqslant s)$; $\mu*F$ is the Dirichlet convolution of F and Möbius function μ.

Note that when $s=1$, $c_1=1$ and $F(a)=a$, (1.8) reduces to (1.7) by $\mu * F = \varphi$.

For other related works on Menon's identity, see [2, 3, 7, 8, 10, 12, 13, 15–18] and references therein.

The initial aim of this note is to generalize Rao's identity (1.2) and Sury's identity (1.5) to additive characters, which is the following theorem.

Theorem 1. *Let $n \in \mathbb{N}$. For $s \in \mathbb{N}$, let $(c_1,\dots,c_s) \in \mathbb{Z}^s$ be a fixed vector such that $\gcd(c_1,\dots,c_s,n)=1$. For $r \geqslant 0$, denote $b \mapsto \lambda_j(b) = \exp(2\pi i w_j b/n)$ to be an additive character of $\mathbb{Z}/n\mathbb{Z}$ where $1 \leqslant j \leqslant r$. Then, the following identity holds.*

$$\begin{aligned}\sum_{\substack{a_1,\dots,a_s,b_1,\dots,b_r=1\\ \gcd(a_1,\dots,a_s,n)=1}}^{n} &\gcd(a_1-c_1,\dots,a_s-c_s,b_1,\dots,b_r,n)^s \lambda_1(b_1)\cdots\lambda_r(b_r)\\ =&\varphi_s(n)\sigma_r(\gcd(w_1,\dots,w_r,n)),\end{aligned} \tag{1.9}$$

where $\varphi_s(n)$ is the Jordan's totient function of order s determined by (1.3) or (1.4), and $\sigma_r(n)=\sum_{d|n} d^r$ is the r-th divisor function.

In fact, following the method of [14], we will get a more general result:

Theorem 2. *Let F be an arbitrary arithmetic function. For $s \in \mathbb{N}$, let $(c_1,\dots,c_s) \in \mathbb{Z}^s$ be an arbitrary vector with $\gcd(c_1,\dots,c_s,n)=g$, and λ_j be additive characters as defined above, with $w_j \in \mathbb{Z} (1 \leqslant j \leqslant r)$. Then*

$$\begin{aligned}\sum_{\substack{a_1,\dots,a_s,b_1,\dots,b_r=1\\ \gcd(a_1,\dots,a_s,n)=1}}^{n} &F(\gcd(a_1-c_1,\dots,a_s-c_s,b_1,\dots,b_r,n))\lambda_1(b_1)\cdots\lambda_r(b_r)\\ =&\varphi_s(n)\sum_{\substack{m|\gcd(w_1,\dots,w_r,n)\\ \gcd(n/m,g)=1}} \frac{m^r(\mu*F)(n/m)}{\varphi_s(n/m)}.\end{aligned} \tag{1.10}$$

Note that for $F(n)=n^s, \mu*F=\varphi_s$. Therefore, (1.10) reduces to (1.9) whenever $F(n)=n^s$ and $\gcd(c_1,\dots,c_s,n)=1$. So we will only prove Theorem 2.

2. Proof of the main result

Denote $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$ to be the quotient ring of $\mathbb{Z}$ modulo n and let

$$\mathcal{M}_s(n) := \{(a_1,\dots,a_s) \in \mathbb{Z}_n^s \mid \gcd(a_1,\dots,a_s,n)=1\} \tag{2.1}$$

i.e., $\mathcal{M}_s(n)$ consists of vectors of $\mathbb{Z}_n^s$ with maximal order. Clearly the cardinality of $\mathcal{M}_s(n)$ is $\varphi_s(n)$.

To prove Theorem 2, we need the following lemma.

Lemma 1. *Assume $m \mid n$. Under the natural homomorphism*

$$\mathbb{Z}_n^s \xrightarrow{\pi} \mathbb{Z}_m^s : (a_1,\dots,a_s) \longmapsto (a_1,\dots,a_s) \mod m,$$

$\mathcal{M}_s(n)$ maps surjectively to $\mathcal{M}_s(m)$ and each vector of $\mathcal{M}_s(m)$ has $\varphi_s(n)/\varphi_s(m)$ pre-images in $\mathcal{M}_s(n)$.

Proof. Clearly, $\pi(\mathcal{M}_s(n)) \subset \mathcal{M}_s(m)$. For the left part, first consider the prime power case: $n = p^u$. Assume $m = p^v$ with $0 \leqslant v \leqslant u$. The case $v = 0$ is trivial since $\mathcal{M}_s(m) = \mathbb{Z}_m^s$ has only one element. For $v > 0$, a vector β of $\mathbb{Z}_m^s$ belongs to $\mathcal{M}_s(m)$ if and only if some component of β does not divide by p. This implies that each pre-image of $\beta \in \mathcal{M}_s(m)$ in $\mathbb{Z}_n^s$ lies in $\mathcal{M}_s(n)$. Therefore, each vector of $\mathcal{M}_s(m)$ has $(n/m)^s = \varphi_s(n)/\varphi_s(m)$ pre-images in $\mathcal{M}_s(n)$.

The general case can be deduced by the Chinese remainder theorem.

Let $n = \prod_{j=1}^{t} p_j^{u_j}$ be the prime factorization of n. Denote $n_j = p_j^{u_j}$ for $1 \leqslant j \leqslant t$. We have the natural isomorphism

$$\mathbb{Z}_n^s \cong \mathbb{Z}_{n_1}^s \times \mathbb{Z}_{n_2}^s \times \cdots \times \mathbb{Z}_{n_t}^s.$$

Under this isomorphism,

$$\mathcal{M}_s(n) \stackrel{1:1}{\longleftrightarrow} \mathcal{M}_s(n_1) \times \mathcal{M}_s(n_2) \times \cdots \times \mathcal{M}_s(n_t). \tag{2.2}$$

Similarly, let $m = \prod_{j=1}^{t} p_j^{v_j}$ and $m_j = p_j^{v_j}$ for $1 \leqslant j \leqslant t$. Then

$$\mathcal{M}_s(m) \stackrel{1:1}{\longleftrightarrow} \mathcal{M}_s(m_1) \times \mathcal{M}_s(m_2) \times \cdots \times \mathcal{M}_s(m_t). \tag{2.3}$$

Clearly, the following diagram commutes.

$$\begin{array}{ccc} \mathcal{M}_s(n) & \stackrel{1:1}{\longrightarrow} & \mathcal{M}_s(n_1) \times \mathcal{M}_s(n_2) \times \cdots \times \mathcal{M}_s(n_t) \\ \big\downarrow \pi & & \big\downarrow \pi_1 \times \cdots \times \pi_t \\ \mathcal{M}_s(m) & \stackrel{1:1}{\longrightarrow} & \mathcal{M}_s(m_1) \times \mathcal{M}_s(m_2) \times \cdots \times \mathcal{M}_s(m_t) \end{array} \tag{2.4}$$

We have proved that for each j, $\mathcal{M}_s(m_j)$ has $\varphi_s(n_j)/\varphi_s(m_j)$ pre-images in $\mathcal{M}_s(n_j)$. By (2.4) and the multiplicative property of φ_s, we get the desired result. □

Proof of Theorem 2. Let S be the left hand side of (1.10). Using the identity $F(n) = \sum_{m|n}(\mu * F)(m)$, we get

$$\begin{aligned} S &= \sum_{\substack{a_1,\ldots,a_s,b_1,\ldots,b_r=1 \\ \gcd(a_1,\ldots,a_s,n)=1}}^{n} \lambda_1(b_1)\cdots\lambda_r(b_r) \sum_{m|\gcd(a_1-c_1,\ldots,a_s-c_s,b_1,\ldots b_r,n)} (\mu * F)(m) \\ &= \sum_{m|n} (\mu * F)(m) \sum_{\substack{a_1,\ldots,a_s=1 \\ \gcd(a_1,\ldots,a_s,n)=1 \\ (a_1,\ldots,a_s) \\ \equiv (c_1,\ldots,c_s) \pmod m}}^{n} 1 \sum_{\substack{b_1,\ldots,b_r=1 \\ (b_1,\ldots,b_r) \\ \equiv (0,\ldots,0) \pmod m}}^{n} \lambda_1(b_1)\cdots\lambda_r(b_r). \end{aligned} \tag{2.5}$$

The condition $(a_1,\ldots,a_s) \equiv (c_1,\ldots,c_s) \pmod{m}$ requires that

$$\gcd(g,m) = \gcd(c_1,\ldots,c_s,m) = \gcd(a_1,\ldots,a_s,m) = 1$$

since $\gcd(a_1,\ldots,a_s,n) = 1$. Then using Lemma 1, we get

$$\sum_{\substack{a_1,\ldots,a_s=1 \\ \gcd(a_1,\ldots,a_s,n)=1 \\ (a_1,\ldots,a_s) \\ \equiv(c_1,\ldots,c_s) \pmod{m}}}^{n} 1 = \frac{\varphi_s(n)}{\varphi_s(m)} \tag{2.6}$$

if $\gcd(g,m) = 1$; and otherwise it equals to 0.

Substituting (2.6) to (2.5) and using the orthogonality of characters, we get

$$\begin{aligned} S &= \sum_{\substack{m|n \\ \gcd(m,g)=1 \\ \frac{n}{m}|\gcd(w_1,\ldots,w_r)}} (\mu * F)(m) \frac{\varphi_s(n)}{\varphi_s(m)} \left(\frac{n}{m}\right)^r \\ &= \varphi_s(n) \sum_{\substack{m|\gcd(w_1,\ldots,w_r,n) \\ \gcd(n/m,g)=1}} m^r \frac{(\mu * F)(n/m)}{\varphi_s(n/m)} \end{aligned} \tag{2.7}$$

which concludes the proof. □

ACKNOWLEDGEMENT

The first author is supported by the Laboratory Open Project funded by the State Key Laboratory of Cryptology in Beijing and the corresponding author is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07041132).

REFERENCES

[1] L. Dickson, "History of the theory of numbers, vol. i: Divisibility and primality," *Chelsea Publishing Co.*, 1966.

[2] M. H. Jafari and A. R. Madadi, "On the number of cyclic subgroups of a finite group," *Bull. Korean Math. Soc.*, vol. 54, pp. 2141–2147, 2017, doi: 10.4134/BKMS.b160783.

[3] Y. Li, X. Hu, and D. Kim, "A generalization of Menon's identity with Dirichlet characters," *Int. J. Number Theory*, vol. 14, no. 10, pp. 2631–2639, 2018, doi: 10.1142/S1793042118501579.

[4] Y. Li, X. Hu, and D. Kim, "A Menon-type identity with multiplicative and additive characters," *Taiwanese J. Math.*, vol. 23, no. 3, pp. 545–555, 2019, doi: 10.11650/tjm/180702.

[5] Y. Li, J. Yoo, and D. Kim, "On a question of Sury," *Discrete Math.*, vol. 342, no. 3, pp. 800–806, 2019, doi: 10.1016/j.disc.2018.11.008.

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

[7] C. Miguel, "A Menon-type identity in residually finite Dedekind domains," *J. Number Theory*, vol. 164, pp. 43–51, 2016, doi: 10.1016/j.jnt.2015.12.018.

[8] V. S. Ramaiah, "Arithmetical sums in regular convolutions," *J. Reine Angew. Math.*, vol. 303-304, pp. 265–283, 1978, doi: 10.1515/crll.1978.303-304.265.

[9] K. N. Rao, "On certain arithmetical sums," *Lecture Notes Math.*, vol. 251, pp. 181–192, 1972.

[10] R. Sivaramakrishnan, "A number-theoretic identity," *Publ. Math. Debrecen*, vol. 21, pp. 67–69, 1974.

[11] B. Sury, "Some number-theoretic identities from group actions," *Rendiconti del Circolo Matematico di Palermo*, vol. 58, pp. 99–108, 2009, doi: 10.1007/s12215-009-0010-6.

[12] L. Tóth, "Menon's identity and arithmetical sums representing functions of several variables," *Rend. Semin. Mat. Univ. Politec. Torino*, vol. 69, no. 1, pp. 97–110, 2011.

[13] L. Tóth, "Menon-type identities concerning Dirichlet characters," *Int. J. Number Theory*, vol. 14, no. 4, pp. 1047–1054, 2018, doi: 10.1142/S179304211850063X.

[14] L. Tóth, "Short proof and generalization of a Menon-type identity by Li, Hu and Kim," *Taiwanese J. Math.*, vol. 23, no. 3, pp. 557–561, 2019, doi: 10.11650/tjm/180904.

[15] L. Tóth, "Menon-type identities concerning additive characters," *Arab. J. Math.*, vol. 9, no. 3, pp. 697–705, 2020, doi: 10.1007/s40065-019-0259-3.

[16] M. Tărnăuceanu, "A generalization of Menon's identity," *J. Number Theory*, vol. 132, pp. 2568–257, 2012, doi: 10.1016/j.jnt.2012.05.012.

[17] J. Wang and P. Haukkanen, "High degree analogs of Menon's identity," *Indian Journal of Mathematics*, vol. 39, no. 1, pp. 37–42, 1997.

[18] Y. Wang and C. Ji, "A generalization of Arai-Carlitz's identity," *Ramanujan J.*, vol. 53, no. 3, pp. 585–594, 2020, doi: 10.1007/s11139-019-00236-y.

[19] X.-P. Zhao and Z.-F. Cao, "Another generalization of Menon's identity," *Int. J. Number Theory*, vol. 13, no. 9, pp. 2373–2379, 2017, doi: 10.1142/S1793042117501299.

Authors' addresses

Yan Li
China Agricultural university, Department of Applied Mathematics, Beijing 100083, China, State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100083, China
E-mail address: liyan_00@cau.edu.cn

Ran Chen
China Agricultural university, Department of Applied Mathematics, Beijing 100083, China
E-mail address: 1151136728@cau.edu.cn

Daeyeoul Kim
(**Corresponding author**) Jeonbuk National University, Department of Mathematics and Institute of Pure and Applied Mathematics, 567 Baekje-daero, South Korea
E-mail address: kdaeyeoul@jbnu.ac.kr