Discrete Mathematics 342 (2019) 800–806

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

On a question of Sury

Yan Li [a], Jisoo Yoo [b], Daeyeoul Kim [b,*]

[a] *Department of Applied Mathematics, China Agricultural university, Beijing 100083, China*
[b] *Department of Mathematics and Institute of Pure and Applied Mathematics, Chonbuk National University, 567 Baekje-daero, Deokjin-gu, Jeonju-si, Jeollabuk-do 54896, South Korea*

ARTICLE INFO

Article history:
Received 20 August 2018
Received in revised form 5 November 2018
Accepted 10 November 2018
Available online xxxx

Keywords:
Greatest common divisor
Chinese remainder theorem

ABSTRACT

Sury (2009) proved that the following two sets

$$\{(a_1,\ldots,a_r)|\ a_i\in[1,n],\ a_i\in\mathbb{Z},\ \gcd(a_1,\ldots,a_r,n)=1\}$$

and

$$\{c|\ c\in[1,n^r],\ c\in\mathbb{Z},\ p^r\nmid\gcd(c,n^r),\ \forall\ \text{prime}\ p\}$$

have the same cardinality. And he asked whether there is a natural bijection between the above two sets. In this note, we will construct a natural correspondence between these two sets by p-adic expansion of integers and the Chinese remainder theorem.

1. Introduction

In [9], B. Sury studied the actions of matrix groups on column vectors over $\mathbb{Z}_n$ by left multiplication, where $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}$ is the ring of residue classes modulo n. Using Cauchy–Frobenius–Burnside lemma, he obtained some Menon-type identities. For example, one of his identities is stated as follows:

$$\sum_{\substack{a\in\mathbb{Z}_n^*\\ b_1,\ldots,b_k\in\mathbb{Z}_n}}\gcd(a-1,b_1,\ldots,b_k,n)=\varphi(n)\sigma_k(n),$$

where gcd(,) represents the greatest common divisor, $\mathbb{Z}_n^*$ is the group of units of $\mathbb{Z}_n$, φ is the Euler's totient function and $\sigma_k(n)=\sum_{d|n}d^k$ is the kth divisor function. For other related works on Menon-type identities, see [5,7,8,10–12] and references therein.

In the last section of [9], where Sury analyzed the action of $GL_r(\mathbb{Z}_n)$ on $(\mathbb{Z}_n)^r$, he obtained two sets

$$\mathcal{B}=\mathcal{B}_r(n):=\{(a_1,\ldots,a_r)|\ a_i\in[1,n],\ a_i\in\mathbb{Z},\ \gcd(a_1,\ldots,a_r,n)=1\}\tag{1}$$

and

$$\mathcal{D}=\mathcal{D}_r(n):=\{c|\ c\in[1,n^r],\ c\in\mathbb{Z},\ p^r\nmid\gcd(c,n^r),\ \forall\ \text{prime}\ p\}\tag{2}$$

"which have the same cardinality but there does not seem to be an obvious bijection between them!" ([9, p. 100])

* Corresponding author.
E-mail addresses: liyan_00@cau.edu.cn (Y. Li), yoojs@jbnu.ac.kr (J. Yoo), kdaeyeoul@jbnu.ac.kr (D. Kim).

https://doi.org/10.1016/j.disc.2018.11.008
0012-365X/

Historically, $|\mathcal{B}_r(n)| = \varphi_r(n)$ is the well known arithmetical function defined by Jordan, which is also called Jordan's totient function. ([4, p. 147–155]) One has $\varphi_r(n) = \sum_{d|n} d^r \mu(n/d)$, where μ denotes the Möbius function. C. Jordan [6] obtained the following two formulas, which express the order of the general and special linear groups over $\mathbb{Z}_n$ by Jordan's totient function:

$$|GL_r(\mathbb{Z}_n)| = n^{\frac{r(r-1)}{2}} \prod_{k=1}^{r} \varphi_k(n),$$

$$|SL_r(\mathbb{Z}_n)| = n^{\frac{r(r-1)}{2}} \prod_{k=2}^{r} \varphi_k(n).$$

These two formulas are also contained in [1].

Note that the set $\mathcal{D}_r(n)$ can be written as

$$\mathcal{D}_r(n) = \{c \mid c \in [1, n^r],\ c \in \mathbb{Z},\ \gcd(c, n^r)_r = 1\} \tag{3}$$

where

$$\gcd(a, b)_r := \max\{d^r \mid d^r | a,\ d^r | b\}.$$

Interestingly, from one of the referees, we know that, $|\mathcal{D}_r(n)| = \phi_r(n)$ is Cohen's generalization of the Euler's totient function, which was introduced in the papers [2,3].

A short direct proof that $\varphi_r(n) = \phi_r(n)$ for every $n, r \geqslant 1$, is the following:

Consider the set

$$A = \{a \in \mathbb{Z}^r \mid 1 \leqslant a \leqslant n^r\}.$$

Group the elements a of A according to the values $\gcd(a, n^r)_r = d^r$, where $d \mid n$. Here

$$a = d^r j,\ \text{with } 1 \leqslant j \leqslant (n/d)^r \text{ and } \gcd(j, (n/d)^r)_r = 1.$$

By the definition of the function ϕ_r, the number of such elements a is exactly $\phi_r(n/d)$. Therefore, $n^r = \sum_{d|n} \phi_r(n/d)$. By Möbius inversion we deduce that $\phi_r(n) = \sum_{d|n} d^r \mu(n/d)$.

Though the sets $\mathcal{B}_r(n)$ and $\mathcal{D}_r(n)$ have the same cardinality, there is no simple bijection between them. For $(a_1, \ldots, a_r) \in \mathcal{B}_r(n)$, try to define

$$(a_1, \ldots, a_r) \mapsto a_1 \cdots a_r.$$

Then $1 \leqslant a_1 \cdots a_r \leqslant n^r$, but $\gcd(a_1 \cdots a_r, n^r)_r = 1$ does not hold in general. For example, take $r = 2,\ n = 6,\ a_1 = 1,\ a_2 = 4$. Then $\gcd(1, 4, 6) = 1$, but $\gcd(1 \cdot 4, 6^2)_2 = \gcd(4, 36)_2 = 4 \neq 1$.

In the end of [9], B. Sury asked the following interesting question of the existence of a natural bijection between $\mathcal{B}_r(n)$ and $\mathcal{D}_r(n)$:

Intriguing question 1.1 (*[9, p. 107]*). *Is there a natural bijection between $\mathcal{B}$ and $\mathcal{D}$?*

In this note, we will give an answer to Sury's question. Our construction is based on p-adic expansion of integers and the Chinese remainder theorem. Throughout this paper, all variables (e.g. a_i, c, n) are integers.

2. Answer to Sury's question

For convenience, we change the subset of positive integers to the subset of non-negative integers. Precisely, let

$$\mathcal{A} := \{(a_1, \ldots, a_r) \mid a_i \in [0, n-1],\ a_i \in \mathbb{Z},\ \gcd(a_1, \ldots, a_r, n) = 1\} \tag{4}$$

and

$$\mathcal{C} := \{c \mid c \in [0, n^r - 1],\ c \in \mathbb{Z},\ p^r \nmid \gcd(c, n^r),\ \forall \text{ prime } p\}. \tag{5}$$

Clearly, there is a natural bijection from $\mathcal{B}$ to $\mathcal{A}$ by mapping a_i to 0 if $a_i = n$ and keeping a_i unchanged otherwise, as this mapping does not affect $\gcd(a_1, a_2, \ldots, a_r, n)$. The same argument gives rise to a natural bijection between $\mathcal{D}$ and $\mathcal{C}$. So, in the following we will only give a natural bijection between sets $\mathcal{A}$ and $\mathcal{C}$.

First, we look at a simple case $n = p$ being a prime.

Under this assumption:

$$\mathcal{A} = \{(a_1, \ldots, a_r) \mid a_i \in [0, p-1]\} - \{(0, \ldots, 0)\}$$

and

$$\mathcal{C} = \{c \mid c \in [0, p^r - 1]\} - \{0\}.$$

The mapping

$$[0, p-1]^r \to [0, p^r - 1]$$

by p-adic expansion

$$(a_1, \ldots, a_r) \mapsto a_1 + a_2 p + \cdots + a_r p^{r-1}$$

gives a natural bijection between $\mathcal{A}$ and $\mathcal{C}$.

Now, we will deal with the more complicated case of $n = p^2$.

Clearly, we obtained

$$\mathcal{A} = \{(a_1, \ldots, a_r) |\ a_i \in [0, p^2 - 1]\} - \{(a_1, \ldots, a_r) |\ \ p|a_i\}$$

and

$$\mathcal{C} = \{c |\ c \in [0, p^{2r} - 1]\} - \{c |\ \ p^r|c\}.$$

For $1 \le i \le r$, let $a_i = a_i^{(0)} + pa_i^{(1)}$ be the p-adic expansion of a_i, i.e., $a_i^{(0)}, a_i^{(1)} \in [0, p-1]$ are integers. Obviously, $p|a_i$ if and only if $a_i^{(0)} = 0$.

So, there is a one-to-one correspondence between $\mathcal{A}$ and

$$\mathcal{A}_{digit} := \{(a_1^{(0)}, a_1^{(1)}, \ldots, a_r^{(0)}, a_r^{(1)}) |\ a_i^{(j)} \in [0, p-1]\} - \{(a_1^{(0)}, a_1^{(1)}, \ldots, a_r^{(0)}, a_r^{(1)}) |\ \ a_i^{(0)} = 0\}.$$

There is a natural bijection from $\mathcal{A}_{digit}$ to $\mathcal{C}$ by rearranging digits:

$$(a_1^{(0)}, a_1^{(1)}, a_2^{(0)}, a_2^{(1)}, \ldots, a_r^{(0)}, a_r^{(1)}) \longmapsto c = a_1^{(0)} + a_2^{(0)} p + \cdots + a_r^{(0)} p^{r-1} + a_1^{(1)} p^r + \cdots + a_r^{(1)} p^{2r-1}.$$

It is easily checked that $a_1^{(0)} = a_1^{(1)} = \cdots = a_r^{(0)} = 0$ if and only if $p^r|c$. Hence, there is a natural bijection between $\mathcal{A}$ and $\mathcal{C}$. The prime square case reveals the general path to prime higher power case.

Proposition 2.1. *Let $n = p^m$ be a prime power. For $a_i \in [0, p^m - 1]$, let*

$$a_i = a_i^{(0)} + a_i^{(1)} p + \cdots + a_i^{(m-1)} p^{m-1} \tag{6}$$

be the p-adic expansion of a_i (i.e., $a_i^{(j)} \in [0, p-1]$). Then the map E_p from $[0, p^m - 1]^r$ to $[0, p^{mr} - 1]$ satisfying

$$\begin{aligned}(a_1, \ldots, a_r) \longmapsto\ & (a_1^{(0)} + a_2^{(0)} p + \cdots + a_r^{(0)} p^{r-1}) \\ & + (a_1^{(1)} + a_2^{(1)} p + \cdots + a_r^{(1)} p^{r-1}) p^r \\ & \vdots \\ & + (a_1^{(m-1)} + a_2^{(m-1)} p + \cdots + a_r^{(m-1)} p^{r-1}) p^{(m-1)r}\end{aligned} \tag{7}$$

gives a natural bijection between $\mathcal{A}$ and $\mathcal{C}$.

Proof. Similarly, we note that

$$\mathcal{A} = \{(a_1, \ldots, a_r) |\ a_i \in [0, p^m - 1]\} - \{(a_1, \ldots, a_r) |\ \ p|a_i\}$$

and

$$\mathcal{C} = \{c |\ c \in [0, p^{mr} - 1]\} - \{c |\ p^r|c\}.$$

Because $p|a_i \iff a_i^{(0)} = 0$, and $a_1^{(0)} = a_2^{(0)} = \cdots = a_r^{(0)} = 0$ corresponds to $p^r|c$, $\mathcal{A}$ is bijective to $\mathcal{C}$ under the map E_p. This concludes the proof. $\square$

Now, we consider the general case by the Chinese remainder theorem. Let $n = p_1^{m_1} \cdots p_s^{m_s}$ be the prime factorization of n with $p_1, p_2, \ldots, p_s$ distinct primes. Let $n_k := p_k^{m_k}$ for $1 \le k \le s$. For $(a_1, \ldots, a_r) \in [0, n-1]^r$, let $(a_{1,k}, \ldots, a_{r,k}) \in [0, n_k - 1]^r$ be the vector such that

$$(a_1, \ldots, a_r) \equiv (a_{1,k}, \ldots, a_{r,k}) \pmod{n_k},$$

where $1 \le k \le s$. Since

$$\gcd(a_1, \ldots, a_r, n) = \prod_{k=1}^{s} \gcd(a_1, \ldots, a_r, n_k) = \prod_{k=1}^{s} \gcd(a_{1,k}, \ldots, a_{r,k}, n_k),$$

by the Chinese remainder theorem, there is a natural bijection between $\mathcal{A}$ and the set $\prod_{k=1}^{s} \mathcal{A}_{p_k}$, which maps

$$(a_1, \ldots, a_r) \longmapsto \prod_{k=1}^{s} (a_{1,k}, \ldots, a_{r,k}), \tag{8}$$

where

$$\mathcal{A}_{p_k} = \{(a_{1,k}, \ldots, a_{r,k}) | \, a_{i,k} \in [0, n_k - 1], \ \gcd(a_{1,k}, \ldots, a_{r,k}, n_k) = 1\}. \tag{9}$$

Denote this map by Chv.

Similarly, for $c \in [0, n^r - 1]$, let c_k be the unique number such that

$$c_k \in [0, n_k^r - 1] \text{ and } c \equiv c_k \pmod{n_k^r}, \tag{10}$$

where $1 \le k \le s$. Again, we have

$$\gcd(c, n^r) = \prod_{k=1}^{s} \gcd(c, n_k^r) = \prod_{k=1}^{s} \gcd(c_k, n_k^r).$$

Since $n_1^r, \ldots, n_s^r$ are pairwise coprime, we get

$$p^r \nmid \gcd(c, n^r) \iff p^r \nmid \gcd(c_k, n_k^r), \ \forall \, 1 \le k \le s \tag{11}$$

for any prime p. Using the Chinese remainder theorem and (11), there is a natural bijection between $\mathcal{C}$ and the set $\prod_{k=1}^{s} \mathcal{C}_{p_k}$ mapping

$$c \longmapsto (c_1, \ldots, c_k, \ldots, c_s),$$

where

$$\mathcal{C}_{p_k} = \{c_k | \, c_k \in [0, n_k^r - 1], \ p^r \nmid \gcd(c_k, n_k^r), \ \forall \text{ prime } p\}. \tag{12}$$

Denote this map by Ch. The inverse Ch^{-1} is explicitly given by

$$(c_1, \ldots, c_k, \ldots, c_s) \longmapsto c_1 e_1 + \cdots + c_k e_k + \cdots + c_s e_s \pmod{n^r}, \tag{13}$$

where $e_1, \ldots, e_s \in [0, n^r - 1]$ are the unique numbers such that

$$e_k \equiv 1 \pmod{n_k^r} \text{ and } e_k \equiv 0 \pmod{n_l^r}, \ \forall \, 1 \le l \ne k \le s. \tag{14}$$

Algorithmically, e_k can be computed by Euclidean division.

Finally, we obtain the following theorem.

Theorem 2.2. *Let n be a positive integer and $n = p_1^{m_1} \cdots p_s^{m_s}$ be its prime factorization. There is a natural bijection between the sets $\mathcal{A}$ and $\mathcal{C}$ (defined in* (4) and (5)*), explicitly given by*

$$\mathcal{A} \xrightarrow{Chv} \prod_{k=1}^{s} \mathcal{A}_{p_k} \xrightarrow{\prod_{k=1}^{s} E_{p_k}} \prod_{k=1}^{s} \mathcal{C}_{p_k} \xrightarrow{Ch^{-1}} \mathcal{C}, \tag{15}$$

where $\mathcal{A}_{p_k}$ and C_{p_k} $(1 \le k \le s)$ are sets defined by (9) and (12) *respectively and Chv, E_{p_k} and Ch^{-1} are maps defined by (8), (7) and (13) respectively.*

Proof. By Proposition 2.1, E_{p_k} is a bijection from $\mathcal{A}_{p_k}$ to $\mathcal{C}_{p_k}$. So, the product map $\prod_{k=1}^{s} E_{p_k}$ is a bijection between Cartesian product sets $\prod_{k=1}^{s} \mathcal{A}_{p_k}$ and $\prod_{k=1}^{s} \mathcal{C}_{p_k}$. We already showed that Chv and Ch are bijections by the Chinese remainder theorem. This concludes the proof. □

Remark. *By Theorem 2.2, it is easy to construct a natural correspondence between $\mathcal{B}$ and $\mathcal{D}$. For $n = 1$, both $\mathcal{B}$ and $\mathcal{D}$ have one element. So it is trivial. Now we assume $n > 1$. After modulo operation Chv, it is easy to see $\mathcal{A}$ and $\mathcal{B}$ have the same image. Clearly, for $n > 1$, $\mathcal{C}$ equals $\mathcal{D}$ by definition. Therefore, similar to (15), the following map*

$$\mathcal{B} \xrightarrow{Chv} \prod_{k=1}^{s} \mathcal{A}_{p_k} \xrightarrow{\prod_{k=1}^{s} E_{p_k}} \prod_{k=1}^{s} \mathcal{C}_{p_k} \xrightarrow{Ch^{-1}} \mathcal{D}, \tag{16}$$

gives a natural bijection between $\mathcal{B}$ and $\mathcal{D}$ for $n > 1$.

We give an example to illustrate (16), the bijection between $\mathcal{B}$ and $\mathcal{D}$.

Example: Take $n = 12$, $r = 2$. Both sets $\mathcal{B}$ and $\mathcal{D}$ have cardinality $\varphi_2(12) = 12^2(1 - 1/2^2)(1 - 1/3^2) = 96$. In this case $n_1 = 4, n_2 = 3$. Clearly, $e_1 = 81, e_2 = 64$ since $81 \equiv 1 \pmod{16}$, $81 \equiv 0 \pmod 9$, $64 \equiv 0 \pmod{16}$, $64 \equiv 1 \pmod 9$.

Compute the image of $(7,8)$ concretely.

$$\begin{aligned}
(7,8) &\longmapsto ((3,0),(1,2)) \quad (\text{mod } 4,\ \text{mod } 3)\\
&\longmapsto ((1,1,0,0),(1,2)) \quad (\text{2-adic expansion},\ \text{3-adic expansion})\\
&\longmapsto ((1,0,1,0),(1,2)) \quad \text{rearranging digits}\\
&\longmapsto (1+0\times 2+1\times 2^2+0\times 2^3,\ 1+2\times 3)=(5,7)\\
&\qquad (\text{2-adic expansion},\ \text{3-adic expansion})\\
&\longmapsto (81\times 5+64\times 7) \quad \text{Chinese remainder theorem}\\
&\longmapsto 133 \pmod{144}.
\end{aligned}$$

Compute other cases by Mathematica 11.2. Then, we get the following table.

elements of $\mathcal{B}$	mod 4, mod 3	2-adic, 3-adic	mod 16, mod 9	elements of $\mathcal{D}$
(1,1)	((1,1),(1,1))	((1,0,1,0),(1,1))	(3,4)	67
(1,2)	((1,2),(1,2))	((1,0,0,1),(1,2))	(9,7)	25
(1,3)	((1,3),(1,0))	((1,0,1,1),(1,0))	(11,1)	91
(1,4)	((1,0),(1,1))	((1,0,0,0),(1,1))	(1,4)	49
(1,5)	((1,1),(1,2))	((1,0,1,0),(1,2))	(3,7)	115
(1,6)	((1,2),(1,0))	((1,0,0,1),(1,0))	(9,1)	73
(1,7)	((1,3),(1,1))	((1,0,1,1),(1,1))	(11,4)	139
(1,8)	((1,0),(1,2))	((1,0,0,0),(1,2))	(1,7)	97
(1,9)	((1,1),(1,0))	((1,0,1,0),(1,0))	(3,1)	19
(1,10)	((1,2),(1,1))	((1,0,0,1),(1,1))	(9,4)	121
(1,11)	((1,3),(1,2))	((1,0,1,1),(1,2))	(11,7)	43
(1,12)	((1,0),(1,0))	((1,0,0,0),(1,0))	(1,1)	1
(2,1)	((2,1),(2,1))	((0,1,1,0),(2,1))	(6,5)	86
(2,3)	((2,3),(2,0))	((0,1,1,1),(2,0))	(14,2)	110
(2,5)	((2,1),(2,2))	((0,1,1,0),(2,2))	(6,8)	134
(2,7)	((2,3),(2,1))	((0,1,1,1),(2,1))	(14,5)	14
(2,9)	((2,1),(2,0))	((0,1,1,0),(2,0))	(6,2)	38
(2,11)	((2,3),(2,2))	((0,1,1,1),(2,2))	(14,8)	62
(3,1)	((3,1),(0,1))	((1,1,1,0),(0,1))	(7,3)	39
(3,2)	((3,2),(0,2))	((1,1,0,1),(0,2))	(13,6)	141
(3,4)	((3,0),(0,1))	((1,1,0,0),(0,1))	(5,3)	21
(3,5)	((3,1),(0,2))	((1,1,1,0),(0,2))	(7,6)	87
(3,7)	((3,3),(0,1))	((1,1,1,1),(0,1))	(15,3)	111
(3,8)	((3,0),(0,2))	((1,1,0,0),(0,2))	(5,6)	69
(3,10)	((3,2),(0,1))	((1,1,0,1),(0,1))	(13,3)	93
(3,11)	((3,3),(0,2))	((1,1,1,1),(0,2))	(15,6)	15
(4,1)	((0,1),(1,1))	((0,0,1,0),(1,1))	(2,4)	130
(4,3)	((0,3),(1,0))	((0,0,1,1),(1,0))	(10,1)	10
(4,5)	((0,1),(1,2))	((0,0,1,0),(1,2))	(2,7)	34
(4,7)	((0,3),(1,1))	((0,0,1,1),(1,1))	(10,4)	58
(4,9)	((0,1),(1,0))	((0,0,1,0),(1,0))	(2,1)	82
(4,11)	((0,3),(1,2))	((0,0,1,1),(1,2))	(10,7)	106
(5,1)	((1,1),(2,1))	((1,0,1,0),(2,1))	(3,5)	131
(5,2)	((1,2),(2,2))	((1,0,0,1),(2,2))	(9,8)	89
(5,3)	((1,3),(2,0))	((1,0,1,1),(2,0))	(11,2)	11
(5,4)	((1,0),(2,1))	((1,0,0,0),(2,1))	(1,5)	113
(5,5)	((1,1),(2,2))	((1,0,1,0),(2,2))	(3,8)	35
(5,6)	((1,2),(2,0))	((1,0,0,1),(2,0))	(9,2)	137
(5,7)	((1,3),(2,1))	((1,0,1,1),(2,1))	(11,5)	59
(5,8)	((1,0),(2,2))	((1,0,0,0),(2,2))	(1,8)	17
(5,9)	((1,1),(2,0))	((1,0,1,0),(2,0))	(3,2)	83
(5,10)	((1,2),(2,1))	((1,0,0,1),(2,1))	(9,5)	41
(5,11)	((1,3),(2,2))	((1,0,1,1),(2,2))	(11,8)	107
(5,12)	((1,0),(2,0))	((1,0,0,0),(2,0))	(1,2)	65

elements of $\mathcal{B}$	mod 4, mod 3	2-adic, 3-adic	mod 16, mod 9	elements of $\mathcal{D}$
(6,1)	((2,1),(0,1))	((0,1,1,0),(0,1))	(6,3)	102
(6,5)	((2,1),(0,2))	((0,1,1,0),(0,2))	(6,6)	6
(6,7)	((2,3),(0,1))	((0,1,1,1),(0,1))	(14,3)	30
(6,11)	((2,3),(0,2))	((0,1,1,1),(0,2))	(14,6)	78
(7,1)	((3,1),(1,1))	((1,1,1,0),(1,1))	(7,4)	103
(7,2)	((3,2),(1,2))	((1,1,0,1),(1,2))	(13,7)	61
(7,3)	((3,3),(1,0))	((1,1,1,1),(1,0))	(15,1)	127
(7,4)	((3,0),(1,1))	((1,1,0,0),(1,1))	(5,4)	85
(7,5)	((3,1),(1,2))	((1,1,1,0),(1,2))	(7,7)	7
(7,6)	((3,2),(1,0))	((1,1,0,1),(1,0))	(13,1)	109
(7,7)	((3,3),(1,1))	((1,1,1,1),(1,1))	(15,4)	31
(7,8)	((3,0),(1,2))	((1,1,0,0),(1,2))	(5,7)	133
(7,9)	((3,1),(1,0))	((1,1,1,0),(1,0))	(7,1)	55
(7,10)	((3,2),(1,1))	((1,1,0,1),(1,1))	(13,4)	13
(7,11)	((3,3),(1,2))	((1,1,1,1),(1,2))	(15,7)	79
(7,12)	((3,0),(1,0))	((1,1,0,0),(1,0))	(5,1)	37
(8,1)	((0,1),(2,1))	((0,0,1,0),(2,1))	(2,5)	50
(8,3)	((0,3),(2,0))	((0,0,1,1),(2,0))	(10,2)	74
(8,5)	((0,1),(2,2))	((0,0,1,0),(2,2))	(2,8)	98
(8,7)	((0,3),(2,1))	((0,0,1,1),(2,1))	(10,5)	122
(8,9)	((0,1),(2,0))	((0,0,1,0),(2,0))	(2,2)	2
(8,11)	((0,3),(2,2))	((0,0,1,1),(2,2))	(10,8)	26
(9,1)	((1,1),(0,1))	((1,0,1,0),(0,1))	(3,3)	3
(9,2)	((1,2),(0,2))	((1,0,0,1),(0,2))	(9,6)	105
(9,4)	((1,0),(0,1))	((1,0,0,0),(0,1))	(1,3)	129
(9,5)	((1,1),(0,2))	((1,0,1,0),(0,2))	(3,6)	51
(9,7)	((1,3),(0,1))	((1,0,1,1),(0,1))	(11,3)	75
(9,8)	((1,0),(0,2))	((1,0,0,0),(0,2))	(1,6)	33
(9,10)	((1,2),(0,1))	((1,0,0,1),(0,1))	(9,3)	57
(9,11)	((1,3),(0,2))	((1,0,1,1),(0,2))	(11,6)	123
(10,1)	((2,1),(1,1))	((0,1,1,0),(1,1))	(6,4)	22
(10,3)	((2,3),(1,0))	((0,1,1,1),(1,0))	(14,1)	46
(10,5)	((2,1),(1,2))	((0,1,1,0),(1,2))	(6,7)	70
(10,7)	((2,3),(1,1))	((0,1,1,1),(1,1))	(14,4)	94
(10,9)	((2,1),(1,0))	((0,1,1,0),(1,0))	(6,1)	118
(10,11)	((2,3),(1,2))	((0,1,1,1),(1,2))	(14,7)	142
(11,1)	((3,1),(2,1))	((1,1,1,0),(2,1))	(7,5)	23
(11,2)	((3,2),(2,2))	((1,1,0,1),(2,2))	(13,8)	125
(11,3)	((3,3),(2,0))	((1,1,1,1),(2,0))	(15,2)	47
(11,4)	((3,0),(2,1))	((1,1,0,0),(2,1))	(5,5)	5
(11,5)	((3,1),(2,2))	((1,1,1,0),(2,2))	(7,8)	71
(11,6)	((3,2),(2,0))	((1,1,0,1),(2,0))	(13,2)	29
(11,7)	((3,3),(2,1))	((1,1,1,1),(2,1))	(15,5)	95
(11,8)	((3,0),(2,2))	((1,1,0,0),(2,2))	(5,8)	53
(11,9)	((3,1),(2,0))	((1,1,1,0),(2,0))	(7,2)	119
(11,10)	((3,2),(2,1))	((1,1,0,1),(2,1))	(13,5)	77
(11,11)	((3,3),(2,2))	((1,1,1,1),(2,2))	(15,8)	143
(11,12)	((3,0),(2,0))	((1,1,0,0),(2,0))	(5,2)	101
(12,1)	((0,1),(0,1))	((0,0,1,0),(0,1))	(2,3)	66
(12,5)	((0,1),(0,2))	((0,0,1,0),(0,2))	(2,6)	114
(12,7)	((0,3),(0,1))	((0,0,1,1),(0,1))	(10,3)	138
(12,11)	((0,3),(0,2))	((0,0,1,1),(0,2))	(10,6)	42

Acknowledgments

We are indeed grateful to the anonymous referees, who carefully read the paper and gave many valuable suggestions, which made the paper more elegant and interesting. This research is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07041132).

References

[1] E. Cohen, Theorie des nombres, Herman, Paris, 1914.
[2] E. Cohen, An extension of Ramanujan's sum, Duke Math. J 16 (1949) 85–90, Also see the paper.
[3] E. Cohen, Generalizations of the Euler ϕ-function, Scr. Math. 23 (1958) 157–161.
[4] L. Dickson, History of the Theory of Numbers, in: Divisibility and Primality, vol. I, Chelsea Publishing Co, New York, 1966.
[5] P. Haukkanen, Menon's identity with respect to a generalized divisibility relation, Aequationes Math. 70 (3) (2005) 240–246.
[6] C. Jordan, Traitee. Substitutions Et Des Equations Algebriques, Gauthier-Yillars, Paris, 1957.
[7] Y. Li, D. Kim, Menon-type identities derived from actions of subgroups of general linear groups, J. Number Theory 179 (2017) 97–112.
[8] P.K. Menon, On the sum $\sum(a-1, n)[(a, n)=1]$, J. Indian Math. Soc. 29 (1965) 155–163.
[9] B. Sury, Some number-theoretic identities from group actions, Rend. Circ. Mat. Palermo (2) 58 (2009) 99–108.
[10] L. Tóth, Menon's identity and arithmetical sums representing functions of several variables, Rend. Semin. Mat. Univ. Politec. Torino 69 (1) (2011) 97–110.
[11] M. Tărnăuceanu, A generalization of menon's identity, J. Number Theory 132 (2012) 2568–2573.
[12] X.-P. Zhao, Z.-F. Cao, Another generalization of menon's identity, Int. J Number Theory 13 (2017) 2373–2379.