Algorithms for the Enumeration Problem of Linear Congruence Modulo m as the Sum of Restricted Partition Numbers

Tian-Xiao He * and Peter J.-S. Shiue, †

Dedicated to Professor Harald Niederreiter for the occasion of his 70th birthday.

Abstract

We consider the congruence $x_1 + x_2 + \cdots + x_r \equiv c \bmod m$, where m and r are positive integers and $c \in Z_m := \{0, 1, ..., m-1\}$ $(m \geq 2)$. [3] deals with enumeration problems of this congruence, namely, the number of solutions with the restriction $x_1 \leq x_2 \leq \cdots \leq x_r$. Some properties and a neat formula of the solutions are presented in [3]. Due to the lack of a simple computational method for calculating the number of the solution of the congruence, we provide an algebraic and a recursive algorithms for those numbers. The former one can also give a new and simple approach to derive some properties of solution numbers.

AMS Subject Classification: 05A15, 05A17, 11P83, 11P81.

Key Words and Phrases: congruence, mutiset congruence solution, restricted integer partition.

*Department of Mathematics and Computer Science, Illinois Wesleyan University, Bloomington, Illinois 61702.

†Department of Mathematical Sciences, University of Nevada, Las Vegas, Las Vegas, Nevada, 89154-4020.

1 Introduction

Consider the congruence equation $x_1 + x_2 + \cdots + x_n \equiv 0 \mod n+1$, where n is a positive integer. It is well-known that the number of unordered solutions $x_1, x_2, \ldots, x_n$ in $Z_{n+1} = \{0, 1, \ldots, n\}$ with repetition allowed is $\frac{1}{n+1}\binom{2n}{n} = C_n$, the nth Catalan number (see Guy [5] and Stanley [9]). In [3], Chou and the authors studied an extension of the above problem, the enumeration problems for a linear equation of congruence modulo m, which has been found relates the restricted integer partition. More precisely, they consider the congruence solutions of equation

$$x_1 + x_2 + \cdots + x_r \equiv c \qquad \mod m, \tag{1}$$

where m and r are positive integers and $c \in Z_m = \{0, 1, \ldots, m-1\}$ ($m \geq 2$). Namely, [3] considers the solution $x_1 = a_1, \ldots, x_r = a_r$ of congruence (1) with $a_1, \ldots, a_r \in Z_m$. If $x_1 = a_1, \ldots, x_r = a_r$ is a solution of congruence equation (1), we form a multiset $\{a_1, \ldots, a_r\}$ and call it a multiset solution of congruence equation (1). Note that each multiset solution of (1) represents several solutions of (1) because all coefficients of (1) are the same. It is trivial that different multiset solutions represent different solutions. Two enumeration problems of the congruence solutions of (1) are dealt with in [3], namely, the numbers of solutions with the restrictions $x_1 \leq x_2 \leq \cdots \leq x_r$ and $x_1 < x_2 < \cdots < x_r$, respectively. Let $m, r \in \mathbb{N}$. Denote the number of the congruence solutions of Equation (1) with arbitrarily fixed $m, r \in \mathbb{N}$ by $|M_{m,r}(c)|$ ($c = 0, 1, \ldots, m-1$ $(mod\ m)$), which is used in [3]. If $gcd(m, r) = 1$, it is easy to see (also see [3])

$$|M_{m,r}(c)| = \frac{1}{m}\binom{m+r-1}{r}. \tag{2}$$

The lower bound and upper bound of $|M_{m,r}(c)|$ are also given for general (m, r) in [3]. In particular, for positive integers $m \geq r > 1$ and any integer c with $0 \leq c < m$, a neat formula of $|M_{m,r}(c)|$ is given. Since the quantities $|M_{m,r}(c)|$ and $|M_{m,k}(c-r)|$ are difficult to compute, we present two algorithms for evaluating $|M_{m,r}(c)|$ recursively. This is a motivation of this paper. Another motivation is based on the following consideration, which will be discussed in our forthcoming work.

The problem of solving the congruence equation (1) with the restrictions $x_1 \le x_2 \le \cdots \le x_r$ is equivalent to the following partition problem

$$\begin{aligned} & x_1 + x_2 + \cdots + x_r = km + c, \quad 0 \le k < r \\ & \textit{with the constraint } 0 \le x_1 \le x_2 \le \cdots \le x_r \le m-1, \end{aligned} \tag{3}$$

i.e., the problem of the restricted partition of $km + c$ $(0 \le k \le r-1)$ into at most r parts with each part $\le m-1$. Furthermore, [3] found the above problem and the two partition problems (4) and (5) shown below are equivalent. In fact, by using the linear and non-singular transform $y_r = x_1,\ y_{r-1} = x_2 - x_1, \ldots,\ y_1 = x_r - x_{r-1}$, we may change problem (3) to

$$\begin{aligned} & y_1 + 2y_2 + \cdots + ry_r = km + c, \quad 0 \le k < r \\ & \textit{with the constraints } y_1, \ldots, y_r \ge 0 \textit{ and} \\ & y_1 + y_2 + \cdots + y_r \le m-1, \end{aligned} \tag{4}$$

the problem of the restricted partition of $km + c$ $(0 \le k \le r-1)$ into at most $m-1$ parts with each part $\le r$.

By using the linear and non-singular transform $y_{r+1} = x_1,\ y_r = x_2 - x_1,\ y_{r-1} = x_3 - x_2, \ldots,\ y_1 = m - 1 - x_r$, we may change Problem (3) to

$$\begin{aligned} & y_1 + 2y_2 + \cdots + (r+1)y_{r+1} = km + c - 1, \quad 1 \le k < r+1 \\ & \textit{with the constraints } y_1, \ldots, y_{r+1} \ge 0 \textit{ and} \\ & y_1 + y_2 + \cdots + y_{r+1} = m-1, \end{aligned} \tag{5}$$

the problem of the restricted partition of $km + c - 1$ $(1 \le k \le r)$ into at most $m-1$ parts with each part $\le r+1$.

In [3], the restricted partition numbers as the solutions of Problem (4), denoted by $p_{r,\le m-1}(km + c)$, is given by (see also Theorem 3.1 in [1])

$$p_{r,\le m-1}(km + c) = \left[x^{km+c}\right] \frac{(1 - x^{m+r-1}) \cdots (1 - x^m)}{(1 - x^r) \cdots (1 - x)}, \tag{6}$$

which gives a presentation of $|M_{m,r}(c)|$ as

$$|M_{m,r}(c)| = \sum_{k=0}^{r-1} p_{r,\leq m-1}(km+c). \tag{7}$$

Following [3], the restricted partition numbers as the solutions of Problem (3), denoted by $p_{m-1,\leq r}(km+c)$, is given by

$$p_{m-1,\leq r}(km+c) = \left[x^{km+c}\right] \frac{(1-x^{m+r-1})\cdots(1-x^{r+1})}{(1-x^{m-1})\cdots(1-x)}, \tag{8}$$

which is equivalent to (6), hence, gives an alternative presentation of $|M_{m,r}(c)|$ as

$$|M_{m,r}(c)| = \sum_{k=0}^{r-1} p_{m-1,\leq r}(km+c). \tag{9}$$

[3] also presents another way to evaluate $|M_{m,r}(c)|$ using the number of solutions of Problem (5), denoted by $q_{r+1}(m, km+c-1)$ $(1 \leq k \leq r)$, which can be found as (also see (2.1.1) in [1])

$$q_{r+1}(m, km+c-1) = \left[y^{m-1}z^{km+c-1}\right] \Pi_{i=1}^{r+1} \frac{1}{1-yz^i}. \tag{10}$$

Hence,

$$|M_{m,r}(c)| = \sum_{k=1}^{r} q_{r+1}(m, km+c-1). \tag{11}$$

We can convert Problem (5) to Problem (4) by deleting part y_1 and subtracting 1 from each part. The resulting partitions of $km+c-1-(m-1)=(k-1)m+c$ have at most $m-1$ parts and each part is less than or equal to $r+1-1=r$. The revise process can convert Problem (4) to Problem (5). Hence, there holds a bijection between the partitions enumerated by $p_{\leq m-1,r}(km+c)$ for each $0 \leq k \leq r-1$ and those enumerated by $q_{r+1}(m, km+c-1)$ for the corresponding $1 \leq k \leq r$, i.e.,

$$q_{r+1}(m, km+c-1) = p_{r,\leq m-1}((k-1)m+c)), \quad 1 \leq k \leq r.$$

Thus, we see the equivalence between (9) and (11)

$$|M_{m,r}(c)| = \sum_{k=1}^{r} q_{r+1}(m, km + c - 1) = \sum_{k=0}^{r-1} p_{r,\leq m-1}(km + c).$$

Since it seems that there is no computationally closed form for $p_{r,\leq m-1}((k-1)m + c)$ or equivalent $q_{r+1}(m, km + c - 1)$ $(1 \leq k \leq r)$, [3] suggests to consider the algorithms shown in [6] and [8].

In next section, we will present an algorithm for the enumeration problem of linear congruence modulo m based on the nth root of unity, which can be applied to calculate $|M_{m,r}(c)|$ defined in (9) for individual parameter triple (m, r, c). We will also give recursive algorithms for the enumeration problem in Section 3, which can be applied to calculate $|M_{m,r}(c)|$ recursively that is typically suitable for coding.

In our forthcoming research, we will study how to use those algorithms to evaluate $p_{r,\leq m-1}((k-1)m+c)$, or equivalently, $q_{r+1}(m, km + c - 1)$ $(1 \leq k \leq r)$ based on an extension of the relationship shown in [3] between the restricted partitions of $km + c$ and the solutions of linear congruence modulo m.

2 An algebraic algorithm for the enumeration problem of linear congruence modulo m

ξ_m is said to be an mth root of unity of order m if $\xi_m^m = 1$. It is well known that for an mth root of unity, there holds

$$\sum_{k=0}^{m-1} \xi_m^{tk} = \begin{cases} m, & if\ m|t; \\ 0, & otherwise. \end{cases} \tag{12}$$

Denote by $f(x)$ the rational function on the right-hand side of (8), namely,

$$f(x) := \frac{(1 - x^{m+r-1}) \cdots (1 - x^{r+1})}{(1 - x^{m-1}) \cdots (1 - x)}. \tag{13}$$

Note that $f(x)$ is the Gaussian polynomial (see [7]) and has nonnegative coefficients. From (7) and (8) and using (12), we obtain

$$\sum_{k=0}^{m-1} f(\xi_m^k) = m|M_{m,r}(0)|,$$

where

$$f(\xi_m^k) := \lim_{x\to\xi_m^k} f(x).$$

Similarly,

$$\sum_{k=0}^{m-1} \xi_m^{-ck} f(\xi_m^k) = m|M_{m,r}(c)|$$

for $0 \leq c \leq m-1$. Hence, there holds

$$|M_{m,r}(c)| = \frac{1}{m}\sum_{k=0}^{m-1} \xi_m^{-ck} f(\xi_m^k), \tag{14}$$

with

$$f(\xi_m^k) := \lim_{x\to\xi_m^k} f(x),$$

where $0 \leq c \leq m-1$. Formula (14) provides an efficient calculation of the number of the congruence solutions of equation (1). For example, when $m = 6$ and $r = 3$, we have

$$f(x) = \frac{(1-x^8)\cdots(1-x^4)}{(1-x^5)\cdots(1-x)} = \frac{(1-x^8)(1-x^7)(1-x^6)}{(1-x^2)(1-x)(1-x^3)}.$$

Noticing that for $0 \leq k \leq m-1$,

$$\lim_{x\to\xi_m^k} \frac{(1-x^{m+s})}{(1-x^s)} = \begin{cases} \frac{m+s}{s}, & if\ ks \equiv 0\ (mod\, m); \\ 1, & if\ ks \not\equiv 0\ (mod\, m). \end{cases} \tag{15}$$

We obtain for $0 \leq c \leq 5\,(mod\ 6)$,

$$
\begin{aligned}
|M_{6,3}(c)| &= \frac{1}{6}\sum_{k=0}^{5}\xi_6^{-ck}f(\xi_6^k) \\
&= \frac{1}{6}\sum_{k=0}^{5}\lim_{x\to\xi_6^k}\left(x^{-c}\frac{1-x^8}{1-x^2}\,\frac{1-x^7}{1-x}\,(1+x^3)\right) \\
&= \frac{1}{6}\left(\lim_{x\to 1}\frac{1-x^8}{1-x^2}\,\frac{1-x^7}{1-x}(1+x^3)+\sum_{k=1}^{5}\lim_{x\to\xi_6^k}\left(x^{-c}\frac{1-x^8}{1-x^2}\,\frac{1-x^7}{1-x}\right)\right. \\
&\quad \left.\sum_{k=1}^{5}+\lim_{x\to\xi_6^k}\left(x^{3-c}\frac{1-x^8}{1-x^2}\,\frac{1-x^7}{1-x}\right)\right) \\
&= \frac{1}{6}\left(\frac{8}{2}\,\frac{7}{1}(2)+\sum_{k=1}^{5}\xi_6^{-ck}+\sum_{k=1}^{5}\xi_6^{(3-c)k}\right) \\
&= \frac{1}{6}\left(56+\sum_{k=0}^{5}\xi_6^{-ck}+(-1)+\sum_{k=0}^{5}\xi_6^{(3-c)k}-1\right) \\
&= \begin{cases} 10, & if\ c\equiv 0\ or\ 3\,(mod\ 6); \\ 9, & if\ c\equiv 1,\ 2,\ 4,\ or\ 5\,(mod\ 6). \end{cases}.
\end{aligned}
$$

Here, we use formula (12) to find

$$
\sum_{k=0}^{m-1}\xi_m^{tk}=\begin{cases} 6, & if\ t\equiv 0\ (mod\ 6); \\ 0, & if\ t\not\equiv 0\ (mod\ 6). \end{cases}
$$

Similarly, we may establish the following general result for calculating $|M_{m,r}(c)|$ for either m or r is a prime number. More precisely, we have

Theorem 2.1 *Suppose $m=p$ is a prime number. Then for any positive number r, there holds*

$$
|M_{m,r}(c)|=\begin{cases} \frac{1}{m}\binom{m+r-1}{r}, & if\ gcd(m,r)=1; \\ \frac{1}{p}\left(\binom{(t+1)p-1}{p-1}+p-1\right), & if\ m=p,\ r=tp,\ and\ c\equiv 0\,(mod\ p); \\ \frac{1}{p}\left(\binom{(t+1)p-1}{p-1}-1\right), & if\ m=p,\ r=tp,\ and\ c\not\equiv 0\,(mod\ p). \end{cases} \tag{16}
$$

Proof. First, if $r < m$ or $t > m$ with $gcd(m,r) = 1$, then $|M_{m,r}(c)|$ is given in Theorem 4 of [3] as

$$|M_{m,r}(c)| = \frac{1}{m}\binom{m+r-1}{r}.$$

Hence, we only need to consider the case $r = tm$,where t are positive integers. From (14) with $r = tp$ and p is a prime,

$$\begin{aligned}
|M_{p,tp}(c)| &= \frac{1}{p}\sum_{k=0}^{p-1} \xi_p^{-ck} f(\xi_p^k) \\
&= \frac{1}{p}\sum_{k=0}^{p-1} \lim_{x\to\xi_p^k}\left(x^{-c}\frac{1-x^{(t+1)p-1}}{1-x^{p-1}}\,\frac{1-x^{(t+1)p-2}}{1-x^{p-2}}\cdots\frac{1-x^{tp+1}}{1-x}\right) \\
&= \frac{1}{p}\left(\binom{(t+1)p-1}{p-1} + \sum_{k=1}^{p-1}\xi_p^{-ck}\right) \\
&= \begin{cases} \frac{1}{p}\left(\binom{(t+1)p-1}{p-1} + p - 1\right), & if\ c \equiv 0\,(mod\ p); \\ \frac{1}{p}\left(\binom{(t+1)p-1}{p-1} - 1\right), & if\ c \not\equiv 0\,(mod\ p), \end{cases}
\end{aligned}$$

where the last step is due to $0 \le c \le m-1\,(mod\ m)$ and m is a prime. Lucas in his Theorie des Nombres proved that $(\binom{(t+1)p-1}{p-1} - 1)/p$ is a positive integer, i.e., $\binom{(t+1)p-1}{p-1} \equiv 1\,(mod\ p)$ when p is a prime number. The proof was simplified by Fine in [4] (also see in Cameron [2]).

■

Theorem 2.2 *Suppose $r = p$ is a prime number. Then for any positive number m, there holds*

$$|M_{m,r}(c)| = \begin{cases} \frac{1}{m}\binom{m+r-1}{r}, & if\ gcd(m,r) = 1; \\ \frac{1}{p}\left(\binom{(t+1)p-1}{p-1} + p - 1\right), & if\ m = tp,\ r = p,\ and\ c \equiv \ell p\,(mod\ tp); \\ \frac{1}{p}\left(\binom{(t+1)p-1}{p-1} - 1\right), & if\ m = tp,\ r = p,\ and\ c \not\equiv \ell p\,(mod\ tp), \end{cases} \tag{17}$$

where $\ell = 0, 1, \ldots, t-1$.

Proof. The case of $gcd(m,r)=1$ is treated as the same as Theorem 2.1. For $r=p$, a prime number, since $gcd(m,r)=gcd(m,p)\neq 1$ implies $gcd(m,p)=p$. Hence, we only need to consider the cases of $m=tp$ for $t=1,2,\ldots$. From (14) and noting

$$\frac{(1-x^{m+r-1})\cdots(1-x^{r+1})}{(1-x^{m-1})\cdots(1-x)}=\frac{(1-x^{m+r-1})\cdots(1-x^{m})}{(1-x^{r})\cdots(1-x)},$$

there holds

$$\begin{aligned}
|M_{tp,p}(c)| &= \frac{1}{tp}\sum_{k=0}^{tp-1}\xi_{tp}^{-ck}f(\xi_{tp}^{k})\\
&= \frac{1}{tp}\sum_{k=0}^{tp-1}\lim_{x\to\xi_{tp}^{k}}\left(x^{-c}\frac{1-x^{(t+1)p-1}}{1-x^{p-1}}\ \frac{1-x^{(t+1)p-2}}{1-x^{p-2}}\cdots\frac{1-x^{tp+1}}{1-x}\ \frac{1-x^{tp}}{1-x^{p}}\right)\\
&= \frac{1}{tp}\left(t\binom{(t+1)p-1}{p-1}+\sum_{k=1}^{tp-1}\xi_{tp}^{-ck}(1+\xi_{tp}^{kp}+\xi_{tp}^{2kp}+\cdots+\xi_{tp}^{(t-1)kp})\right)\\
&= \begin{cases}\frac{1}{tp}\left(t\binom{(t+1)p-1}{p-1}+tp-t\right), & if\ c\equiv 0,p,\ldots,(t-1)p\,(mod\ tp);\\ \frac{1}{tp}\left(t\binom{(t+1)p-1}{p-1}-t\right), & if\ c\not\equiv 0,p,\ldots,(t-1)p\,(mod\ tp),\end{cases}
\end{aligned}$$

which implies (17)

■

Remark 2.1 The numbers $|M_{m,r}(c)|$ in Theorems 2.1 and 2.2 were found in Theorems 7 and 8 with different forms by using different approach.

Our method is still applicable for other cases provided the limits $\lim_{x\to\xi_m^k}\frac{(1-x^{n+s})}{(1-x^{s})}$, that are similar to the ones shown in (15), could be well-treated in the case of $gcd(m,s)\neq 1$. As an example, we now calculate $|M_{4,6}(c)|$. From (14),

$$
\begin{aligned}
|M_{4.6}(c)| &= \frac{1}{4}\sum_{k=0}^{3}\xi_4^{-ck}\lim_{x\to\xi_4^k}\left(\frac{1-x^9}{1-x^3}\,\frac{1-x^8}{1-x^2}\,\frac{1-x^7}{1-x}\right)\\
= \quad & \frac{1}{4}\left(\frac{9\cdot 8\cdot 7}{3\cdot 2\cdot 1}+\sum_{k=0}^{3}\xi_4^{-ck}(1+\xi_4^{2k}+\xi_4^{4k}+\xi_4^{6k})\right)\\
= \quad & \begin{cases}\frac{1}{4}(84+2(4-1)-2)=22, & if\ c\equiv 0\, or\, 2\,(mod\, 4);\\ \frac{1}{4}(84-4)=20, & if\ c\equiv 1\, or\, 3\,(mod\, 4).\end{cases}
\end{aligned}
$$

Remark 2.2 To extend widely the application scope of our method, we modify formula (14) circumspectly by using primitive roots of unity. ξ_m is called a primitive mth root of unity if $\xi_m^n \neq 1$ for all $0<n<m$. For instance, if m is a prime, then ξ_m is a primitive mth root of unity. By means of primitive mth roots of unity, we may split the formula (14) into the following form:

$$
|M_{m,r}(c)| = \frac{1}{m}\sum_{d|m}\left(\sum_{o(\xi_m)=d}\xi_m^{-c}f(\xi_m)\right), \tag{18}
$$

where the inner summation is taken over all primitive dth roots of unity, and $f(\xi_m^k) := \lim_{x\to\xi_m^k} f(x)$.

3 Recursive algorithms for the enumeration problem of linear congruence modulo m

We now try to find a recurrence formula to calculate $|M_{m,r}|$. There are three ways to enumerate $|M_{m,r}|$, namely, fixed arbitrarily m, r, and c, respectively. Let us consider the first case of fixing m. Since the sub-cases of $m=2$ and 3 have been considered in [3], we start from the case of $(m,r)=(4,r)$. If $r=2k+1$ ($k=0,1,\ldots$), then from (2) we have

$$
|M_{4,2k+1}| = \frac{1}{4}\binom{2k+4}{2k+1} = \frac{1}{4}\binom{2k+4}{3}. \tag{19}
$$

For $k \in \mathbb{N}$, denote

$$E_k = \{j : j = 6k - 2 \ (mod\ 4)\}, \tag{20}$$

and denote the characteristic function of E_k by $f_k = \chi_{E_k}$, i.e., $f_k(i) = 1$ if $i \in E_k$ and 0 otherwise. Thus, for $k \in \mathbb{N}$, $k \geq 2$, we have

$$\begin{aligned}
|M_{4,2k+2}(0)| &= \frac{3}{4}\binom{2k+4}{3} + \frac{1}{4}\binom{2k+2}{3} \\
&\quad - (|M_{4,2k}(1)| + |M_{4,2k}(2)| + |M_{4,2k}(3)|) + f_k(0), \\
|M_{4,2k+2}(1)| &= \frac{3}{4}\binom{2k+4}{3} + \frac{1}{4}\binom{2k+2}{3} \\
&\quad - (|M_{4,2k}(2)| + |M_{4,2k}(3)| + |M_{4,2k}(0)|) + f_k(1), \\
|M_{4,2k+2}(2)| &= \frac{3}{4}\binom{2k+4}{3} + \frac{1}{4}\binom{2k+2}{3} \\
&\quad - (|M_{4,2k}(3)| + |M_{4,2k}(0)| + |M_{4,2k}(1)|) + f_k(2), \\
|M_{4,2k+2}(3)| &= \frac{3}{4}\binom{2k+4}{3} + \frac{1}{4}\binom{2k+2}{3} \\
&\quad - (|M_{4,2k}(0)| + |M_{4,2k}(1)| + |M_{4,2k}(2)|) + f_k(3)(21)
\end{aligned}$$

Here, the initial conditions of the above recursive formula are

$$|M_{4,2}(0)| = |M_{4,2}(2)| = 3, \quad |M_{4,2}(1)| = |M_{4,2}(3)| = 2.$$

Noting $|M_{4,r}(i)| = |M_{4,r}(j)|$ when $i = j \ (mod\ 4)$, we may re-write formula (21) as the following unified form.

Proposition 3.1 *(19) and the following (22) give a method to count the numbers of mutiset congruence solutions of linear equations (1) for* $m = 4$*.*

$$|M_{4,2k+2}(i)| = \frac{3}{4}\binom{2k+4}{3} + \frac{1}{4}\binom{2k+2}{3} + f_k(i) - \sum_{j=i+1}^{i+3} |M_{4,2k}(j)|, \tag{22}$$

where $k \geq 1$, $i = 0, 1, 2,$ *and* 3, *and* $|M_{4,2}(0)| = |M_{4,2}(2)| = 3, |M_{4,2}(1)| = |M_{4,2}(3)| = 2.$

Proof. It is easy to check that $x_1 + x_2 \equiv 0 \ (mod\ 4)$ has only the congruence solutions $\{0, 0\}$, $\{1, 3\}$, and $\{2, 2\}$, $x_1 + x_2 \equiv 2 \ (mod\ 4)$ the solutions $\{0,2\}$, $\{1,1\}$, and $\{3,3\}$, $x_1+x_2 \equiv 1$ $(mod\ 4)$ the solutions $\{0,1\}$, $\{2,3\}$, and $x_1+x_2\equiv 3$ $(mod\ 4)$ the solutions $\{0,3\}$ and $\{1,2\}$. Thus, we have $|M_{4,2}(0)| = |M_{4,2}(2)| = 3$, and $|M_{4,2}(1)| = |M_{4,2}(3)| = 2$.

Denote by $(i,j)_\ell$ the multiset of congruence solutions of (1) with $m=4$ which satisfy $x_1 \equiv i$ $(mod\ 4)$ and $x_2+\cdots+x_\ell \equiv j$ $(mod\ 4)$, and $i \leq x_2$, where $i,j\in Z_m$. The cardinal number of set $(i,j)_\ell$ is denoted by $|(i,j)_\ell|$. Note that the set $(i,j)_\ell$ may be empty and, thus, $|(i,j)_\ell|$ may be zero.

Using the notation defined, the set of congruence solutions of equation (1) for $m=4$, $r=2k+2$, and $c=0$ consists of disjoint subsets $(0,0)_{2k+2}$, $(1,3)_{2k+2}$, $(2,2)_{2k+2}$, and $(3,1)_{2k+2}$. Therefore, the cardinal number of the set is the summation of the cardinal numbers of its four disjoint subsets. Obviously, for $k\geq 1$, the cardinal number of $(0,0)_{2k+2}$ is equal to the cardinal number of the congruence solution set of equation (1) for $m=4$, $r=2k+1$, and $c=0$. Thus,

$$|(0,0)_{2k+2}| = |M_{4,2k+1}(0)| = \frac{1}{4}\binom{2k+4}{3}. \tag{23}$$

Noting that the cardinal number of solution set of $x_2+\cdots+x_{2k+2}\equiv 3$ $(mod\ 4)$ (satisfying $x_2\geq 0$) is equal to the cardinal number of the solution set of $x_2+\cdots+x_{2k+2}\equiv 3$ $(mod\ 4)$ satisfying $x_2\geq 1$ plus the cardinal number of the solution set of $x_3+\cdots+x_{2k+2}\equiv 3$ $(mod\ 4)$ and $x_2\equiv 0$ $(mod\ 4)$ (with $x_3\geq 0$), i.e., the cardinal number of $(0,3)_{2k+2}$ is equal to the summation of the cardinal number of multiset $(1,3)_{2k+2}$ and the cardinal number of the multiset $(0,3)_{2k+1}$. Thus, we have

$$|(1,3)_{2k+2}| = |(0,3)_{2k+2}| - |(0,3)_{2k+1}| = |M_{4,2k+1}(3)| - |M_{4,2k}(3)|. \tag{24}$$

To enumerate the cardinal number of the set $(2,2)_{2k+2}$, we find this number plus the cardinal number of solution set $(1,1)_{2k+1}$ is equal to the cardinal number of the solution set $(1,2)_{2k+2}$, which can be verified as follows. First, we notice the fact that any element in the set $(1,2)_{2k+2}$ satisfies $x_1\equiv 1$ $(mod\ 4)$, $x_2+\cdots+x_{2k+2}\equiv 2$ $(mod\ 4)$, and $x_2\geq 1$ belongs either the case of $(mod\ 4)$ $x_1\equiv 1\equiv x_2\leq x_3\leq\cdots x_{2k+2}$ or the case $x_1\equiv 1$ $(mod\ 4)$, $(mod\ 4)$ $2\equiv x_2\leq x_3\leq\cdots\leq x_{2k+2}$. Secondly, a solution satisfying the first case is also a solution of $x_2\equiv 1$ $(mod\ 4)$, $x_3+\cdots+x_{2k+2}\equiv 1$ $(mod\ 4)$, and therefore it is an element of set $(1,1)_{2k+1}$. Thirdly, the number of solutions in $(1,2)_{2k+2}$ that belong to the second case is equal to the number of the solutions satisfying $x_1 \equiv 2$ $(mod\ 4)$, $x_2 + \cdots + x_{2k+2} \equiv 2$ $(mod\ 4)$, and $x_2 \geq 2$, i.e., the cardinal number of the solution set $(2,2)_{2k+2}$. Thus, by using the above fact and a similar proof as we carried off (24), there hold

$$\begin{aligned} |(2,2)_{2k+2}| &= |(1,2)_{2k+2}| - |(1,1)_{2k+1}| \\ &= |(0,2)_{2k+2}| - |(0,2)_{2k+1}| - [|(0,1)_{2k+1}| - |(0,1)_{2k}|] \\ &= |M_{4,2k+1}(2)| + |M_{4,2k-1}(1)| - [|M_{4,2k}(1)| + |M_{4,2k}(2)|]. \end{aligned} \tag{25}$$

We may use a similar process to count the cardinal number of set $(3,1)_{2k+2}$. However, by noting the fact that an element in $(3,1)_{2k+2}$ must be of the form $(mod\ 4)$ $3 \equiv x_1 = x_2 = \cdots = x_{2k+2}$ if the set $(3.1)_{2k+2} \neq \phi$. Therefore, $x_2 + \cdots + x_{2k+2} = 6k+3$. If $6k+3 \equiv 1$ $(mod\ 4)$, then $|(3,1)_{2k+2}| = 1$, otherwise, $|(3,1)_{2k+2}| = 0$, or equivalently, the characteristic function $f_k = \chi_{E_k}$ of the set E_k $(k \in \mathbb{N})$ defined by (20) takes value 1 at 0, i.e., $0 \equiv 6k-2$ $(mod\ 4)$ or $1 \equiv 6k+3$ $(mod\ 4)$, then $|(3,1)_{2k+2}| = 1$, otherwise, $|(3,1)_{2k+1}| = 0$. Therefore, we have proved the first recursive formula of (21). Similarly, we obtain the other three formulas of (21). The equivalence between (21) and (22) is obvious, which completes the proof of the proposition.

■

Example 1 Using (21) or (22) for $k = 1$, we may obtain

$$|M_{4,4}(0)| = 10, |M_{4,4}(1)| = 8, |M_{4,4}(2)| = 9, \textit{ and } |M_{4,4}(3)| = 8.$$

For $k = 2$, we have

$$|M_{4,6}(0)| = 22, |M_{4,6}(1)| = 20, |M_{4,6}(2)| = 22, \textit{ and } |M_{4,6}(3)| = 20.$$

From Proposition 3.1, we may present an algorithm based on the following two propositions.

Proposition 3.2 *Denote by $(i,j)_{m,\ell}$ the multiset of congruence solutions of $x_1 \equiv i$ $(mod\ m)$ and $x_2 + \cdots + x_\ell \equiv j$ $(mod\ m)$, which satisfy $x_2 \geq x_1$, where $i, j \in Z_m$. The cardinal number of set $(i,j)_{m,\ell}$ is denoted by $|(i,j)_{m,\ell}|$. Then the cardinal number of the congruence solution multiset of (1) with $m \in \mathbb{N}$ and $r = \ell + 1$ can be written as*

$$|M_{m,\ell}| = \sum_{i+j\equiv c\ (mod\ m)} |(i,j)_{m,\ell}|, \tag{26}$$

where i runs all distinct values in Z_m.

Proof. Denote the set of congruence solutions of (1) with $m \in \mathbb{N}$, $r = \ell$, and $c \in Z_m$ by $S_{m,\ell}(c)$, which cardinal number is $|M_{m,\ell}(c)|$. Since an element of $S_{m,\ell}(c)$, i.e., a congruence solution of (1) with $m \in \mathbb{N}$, $r = \ell$, and $c \in Z_m$ must be a solution of $x_1 \equiv i\ (mod\ m)$ and $x_2 + \cdots + x_\ell \equiv c - i\ (mod\ m)$ that satisfies $x_2 \geq x_1$ for some $i \in Z_m$, we have

$$S_{m,\ell}(c) \subset \cup_{i+j\equiv c\ (mod\ m)}(i,j)_{m,\ell}.$$

It is easy to see every element in $(i,j)_\ell$ $(i+j \equiv c\ (mod\ m))$ is in $S_{m,\ell}(c)$, we have

$$\cup_{i+j\equiv c\ (mod\ m)}(i,j)_{m,\ell} \subset S_{m,\ell}(c).$$

Noting $\{(i,j)_{m,\ell} : i,j \in Z_m, i+j \equiv c\ (mod\ m)\}$ is a pair disjoint set, i.e., $(i,j)_{m,\ell} \cap (u,v)_{m,\ell} = \phi$ when $i \neq u$, with $i+j$ and $u+v \equiv c\ (mod\ m)$, we immediately obtain (26).

∎

Proposition 3.3 *Let $(i,j)_{m,\ell}$ and $|(i,j)_{m,\ell}|$ be defined as in Proposition 3.2. Then we have recursive relation formula*

$$|(i,j)_{m,\ell}| = |(i-1,j)_{m,\ell}| - |(i-1,j-i+1)_{m,\ell-1}| \tag{27}$$

for any $m \in \mathbb{N}$, $\ell \geq 1$, and $i,j \in Z_m$, with initial conditions $|(i,j)_{m,2}| = 1$ if $i \leq j$ and 0 otherwise, where $(i-1,j-i+1)_{m,k} = (i-1,m+j-i+1)_{m,k}$ if $j-i+1$ becomes negative.

Proof. The initial conditions are clearly true due to the definition of $(i,j)_{m,\ell}$. Using the notation defined, any element in the set $(i-1,j)_{m,\ell}$ satisfies either the case of $x_1 \equiv i-1\ (mod\ m)$, $x_2+\cdots+x_\ell \equiv j\ (mod\ m)$, and $x_2 \equiv i-1\ (mod\ m)$ or the case of $x_1 \equiv i-1\ (mod\ m)$, $x_2 + \cdots + x_\ell \equiv j\ (mod\ m)$, and $x_2 \geq i$. The number of the solutions in the set $(i-1,j)_{m,\ell}$ satisfying the first case is obviously equal to the number of solutions of the equations $x_2 \equiv i-1\ (mod\ m)$ and $x_3 + \cdots + x_\ell \equiv j-i+1\ (mod\ m)$ with $x_3 \geq i-1$, which can be written as

$|(i-1, j-i+1)_{m,\ell-1}|$. The number of the solutions in the set $(i-1, j)_{m,\ell}$ satisfying the second case is equal to the number of the solutions of equations $x_2 \equiv i\ (mod\ m)$ and $x_2 + \cdots x_\ell \equiv j\ (mod\ m)$ with codition $x_2 \geq x_1$, which can be written as $|(i,j)_{m,\ell}|$ from the definition. Thus we obtain $|(i-1,j)_{m,\ell}| = |(i-1, j-i+1)_{m,\ell-1}| + |(i,j)_{m,\ell}|$, which implies (27).

■

Proposition 3.4 *Let $|M_{m,\ell}(c)|$ and $(i,j)_{m,\ell}$ be defined as before. There hold some initial cardinal numbers of congruence solution sets of equations with form (1): For $m, \ell \in \mathbb{N}$ and $c \in Z_m$,*

$$|M_{m,\ell}(c)| = |(0, c)_{m,\ell+1}|, \tag{28}$$

$$|M_{m,1}(c)| = 1, \tag{29}$$

and

$$|M_{2k-1,2}(c)| = k \tag{30}$$

and

$$|M_{2k,2}(c)| = \begin{cases} k+1 & if\ c = 0, 2, \ldots, 2k-2 \\ k & if\ c = 1, 3, \ldots, 2k-1, \end{cases} \tag{31}$$

for all $k \geq 1$.

Algorithm 1 To evaluate $|M_{m,\ell+1}(c)|$, we use Proposition 3.2 to write

$$|M_{m,\ell+1}(c)| = \sum_{i=0}^{c-1} |(i, c-i)_{m,\ell+1}|$$

and use Proposition 3.3 to reduce i on the right-hand side of the above equation one-by-one till $i = 0$, which generates each $|(i,j)_{\ell+1}|$ to be a linear combination of $|(0,u)_{\ell+1-v}|$ for some $u \in Z_m$ and $v \leq \ell + 1$. Then, we apply (28) to converse $|(0,u)_{\ell+1-v}|$ to $|M_{m,\ell-v}(u)|$ and use initial cardinal numbers (29)-(31) to find the values of $|M_{m,\ell-v}(u)|$ and $|M_{m,\ell+1}(c)|$ eventually. The example for the case of $m = 4$ was shown in Proposition 3.1.

Example 2 As another example, we now see the case of $m = 6$, $\ell = 3$, and $c = 0$. From Proposition 3.2, we have

$$|M_{6,3}(0)| = |(0,0)_{6,3}| + |(1,5)_{6,3}| + |(2,4)_{6,3}| + |(3,3)_{6,3}| + |(4,2)_{6,3}| + |(5,1)_{6,3}|,$$

where each term on the right-hand side can be calculated by using Propositions 3.3 and 3.4 as follows.

$$\begin{aligned}
|(0,0)_{6,3}| &= |M_{6,2}(0)| = 4,\\
|(1,5)_{6,3}| &= |(0,5)_{6,3}| - |(0,5)_{6,2}| = |M_{6,2}(5)| - 1 = 2,\\
|(2,4)_{6,3}| &= |(0,4)_{6,3}| - |(0,4)_{6,2}| - |(1,3)_{6,2}| = |M_{6,2}(4)| - 1 - 1 = 2,\\
|(3,3)_{6,3}| &= |(0,3)_{6,3}| - |(0,3)_{6,2}| - |(1,2)_{6,2}| - |(2,1)_{6,2}|\\
&= |M_{6,2}(3)| - 1 - 1 - 0 = 1,\\
|(4,2)_{6,3}| &= |(0,2)_{6,3}| - |(0,2)_{6,2}| - |(1,1)_{6,2}| - |(2,0)_{6,2}| - |(3,5)_{6,2}|\\
&= |M_{6,2}(2)| - 3 = 1,\\
|(5,1)_{6,3}| &= |(0,1)_{6,3}| - |(0,1)_{6,2}| - |(1,0)_{6,2}| - |(2,5)_{6,2}| - |(3,4)_{6,2}|\\
&\quad - |(4,3)_{6,2}| = |M_{6,2}(1)| - 3 = 0.
\end{aligned}$$

Thus, $|M_{6.3}(0)| = 4 + 2 + 2 + 1 + 1 = 10$.

Similarly, using Propositions 3.3 and 3.4 we have

$$\begin{aligned}
&|(0,1)_{6,3}| = 3,\ |(1,0)_{6,3}| = 3,\ |(2,5)_{6.3}| = 1,\\
&|(3,4)_{6,3}| = 1,\ |(4,3)_{6,3}| = 1,\ |(5,2)_{6,3}| = 0, \qquad (32)\\
&|(0,2)_{6,3}| = 4,\ |(1,1)_{6,3}| = 2,\ |(2,0)_{6.3}| = 2,\\
&|(3,5)_{6,3}| = 0,\ |(4,4)_{6,3}| = 1,\ |(5,3)_{6,3}| = 0, \qquad (33)\\
&|(0,3)_{6,3}| = 3,\ |(1,2)_{6,3}| = 3,\ |(2,1)_{6.3}| = 2,\\
&|(3,0)_{6,3}| = 1,\ |(4,5)_{6,3}| = 0,\ |(5,4)_{6,3}| = 1, \qquad (34)\\
&|(0,4)_{6,3}| = 4,\ |(1,3)_{6,3}| = 2,\ |(2,2)_{6.3}| = 2,\\
&|(3,1)_{6,3}| = 1,\ |(4,0)_{6,3}| = 0,\ |(5,5)_{6,3}| = 0, \qquad (35)\\
&|(0,5)_{6,3}| = 3,\ |(1,4)_{6,3}| = 3,\ |(2,3)_{6.3}| = 1,\\
&|(3,2)_{6,3}| = 2,\ |(4,1)_{6,3}| = 0,\ |(5,0)_{6,3}| = 0, \qquad (36)
\end{aligned}$$

which yield

$$\begin{aligned}
& |M_{6,3}(1)| \\
= \ & |(0,1)_{6,3}| + |(1,0)_{6,3}| + |(2,5)_{6.3}| + |(3,4)_{6,3}| + |(4,3)_{6,3}| + |(5,2)_{6,3}| \\
= \ & 9; && (37) \\
& |M_{6,3}(2)| \\
= \ & |(0,2)_{6,3}| + |(1,1)_{6,3}| + |(2,0)_{6.3}| + |(3,5)_{6,3}| + |(4,4)_{6,3}| + |(5,3)_{6,3}| \\
= \ & 9; && (38) \\
& |M_{6,3}(3)| \\
= \ & |(0,3)_{6,3}| + |(1,2)_{6,3}| + |(2,1)_{6.3}| + |(3,0)_{6,3}| + |(4,5)_{6,3}| + |(5,4)_{6,3}| \\
= \ & 10; && (39) \\
& |M_{6,3}(4)| \\
= \ & |(0,4)_{6,3}| + |(1,3)_{6,3}| + |(2,2)_{6.3}| + |(3,1)_{6,3}| + |(4,0)_{6,3}| + |(5,5)_{6,3}| \\
= \ & 9; && (40)
\end{aligned}$$

and

$$\begin{aligned}
& |M_{6,3}(5)| \\
= \ & |(0,5)_{6,3}| + |(1,4)_{6,3}| + |(2,3)_{6.3}| + |(3,2)_{6,3}| + |(4,1)_{6,3}| + |(5,0)_{6,3}| \\
= \ & 9, && (41)
\end{aligned}$$

respectively, by using Proposition 3.2.

Example 3 Using Propositions 3.2-3.4 and the values of $|(i,j)_{6,3}|$ and the values of $|M_{6,}(i)|$, $i = 0,1,2,\ldots,5$, we can find $|M_{6,4}(i)|$, $i = 0,1,2,\ldots,5$, recursively. For instance, using the values $|(i,j)_{6,3}|$ shown in (32)-(36) and the values of $|M_{6,3}(i)|$ shown in (37)-(41) and $|M_{6,3}(0)| = 10$, we obtain

$$\begin{aligned}
& |(0,0)_{6,4}| = |M_{6,3}(0)| = 10, \\
& |(1,5)_{6,4}| = |(0,5)_{6,4}| - |(0,5)_{6,3}| = |M_{6,3}(5)| - |M_{6,2}(5)| = 9 - 3 = 6, \\
& |(2,4)_{6,4}| = |(1,4)_{6,4}| - |(1,3)_{6,3}| = |(0,4)_{6,4}| - |(0,4)_{6,3}| - |(1,3)_{6,3}| \\
& \qquad = |M_{6,3}(4)| - 4 - 2 = 3,
\end{aligned}$$

$$
\begin{aligned}
|(3,3)_{6,4}| &= |(2,3)_{6,4}| - |(2,1)_{6,3}| = |(1,3)_{6,4}| - |(1,2)_{6,3}| - |(2,1)_{6,3}| \\
&= |(0,3)_{6,4}| - |(0,3)_{6,3}| - |(1,2)_{6,3}| - |(2,1)_{6,3}| \\
&= |M_{6,3}(3)| - 3 - 3 - 2 = 2, \\
|(4,2)_{6,4}| &= |(3,2)_{6,4}| - |(3,5)_{6,3}| = |(2,2)_{6,4}| - |(2,0)_{6,3}| - |(3,5)_{6,3}| \\
&= |(1,2)_{6,4}| - |(1,1)_{6,3}| - |(2,0)_{6,3}| - |(3,5)_{6,3}| \\
&= |(0,2)_{6,4}| - |(0,2)_{6,3}| - |(1,1)_{6,3}| - |(2,0)_{6,3}| - |(3,5)_{6,3}| \\
&= |M_{6,4}(2)| - 4 - 2 - 3 - 0 = 1, \\
|(5,1)_{6,4}| &= |(4,1)_{6,4}| - |(4,3)_{6,3}| = |(3,1)_{6,4}| - |(3,4)_{6,3}| - |(4,3)_{6,3}| \\
&= |(2,1)_{6,4}| - |(2,5)_{6,3}| - |(3,4)_{6,3}| - |(4,3)_{6,3}| \\
&= |(1,1)_{6,4}| - |(1,0)_{6,3}| - |(2,5)_{6,3}| - |(3,4)_{6,3}| - |(4,3)_{6,3}| \\
&= |(0,1)_{6,4}| - |(0,1)_{6,3}| - |(1,0)_{6,3}| - |(2,5)_{6,3}| - |(3,4)_{6,3}| - |(4,3)_{6,3}| \\
&= |M_{6,3}(1)| - 3 - 3 - 1 - 1 - 1 = 0.
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
& |M_{6,4}(0)| \\
= \; & |(0,0)_{6,4}| + |(1,5)_{6,4}| + |(2,4)_{6,4}| + |(3,3)_{6,4}| + |(4,2)_{6,4}| + |(5,1)_{6,4}| \\
= \; & 22.
\end{aligned}
$$

We now give a recursive algorithm to enumerate the congruence solutions of Equation (1) with the restriction $x_1 \leq x_2 \leq \cdots \leq x_r$ with a matrix formulation.

From Propositions 3.2-3.4 we can establish

Theorem 3.5 *Let $(i,j)_{m,\ell}$ and $|(i,j)_{m,\ell}|$ be defined as in Proposition 3.2. Then*

$$
|(i,j)_{m,\ell}| = \sum_{k=i}^{m-1} |(k, j-k)_{m,\ell-1}| \tag{42}
$$

and

$$
|M_{m,\ell}(j)| = \sum_{i=0}^{m-1} |(i, j-i)_{m,\ell}| = \sum_{i=0}^{m-1} \sum_{k=i}^{m-1} |(k, j-i-k)_{m,\ell-1}| \tag{43}
$$

Proof. Using formula (27) repeatedly, we may find

$$|(i,j)_{m,\ell}| = |(0,j)_{m,\ell}| - \sum_{k=0}^{i-1} |(k, j-k)_{m,\ell-1}|.$$

From formulas (26) and (28) presented in Propositions 3.2 and 3.4, respectively, we further have

$$\begin{aligned} |(i,j)_{m,\ell}| &= |M_{m,\ell-1}(j)| - \sum_{k=0}^{i-1} |(k, j-k)_{m,\ell-1}| \\ &= \sum_{k=i}^{m-1} |(k, j-k)_{m,\ell-1}|. \end{aligned}$$

Therefore, formula (26) yields

$$|M_{m,\ell}(j)| = \sum_{i=0}^{m-1} |(i, j-i)_{m,\ell}| = \sum_{i=0}^{m-1}\sum_{k=i}^{m-1} |(k, j-i-k)_{m,\ell-1}|,$$

which completes the proof.

■

Theorem 3.5 suggests the following algorithm with a matrix formulation.

Algorithm 2 Consider the $\ell-1$st matrix

$$\begin{pmatrix} |(0,j)_{m,\ell-1}| & |(1,j-1)_{m,\ell-1}| & \cdots & |(m-1,j-m+1)_{m,\ell-1}| \\ |(0,j-1)_{m,\ell-1}| & |(1,j-2)_{m,\ell-1}| & \cdots & |(m-1,j-m)_{m,\ell}| \\ \vdots & \vdots & \cdots & \vdots \\ |(0,j-m+1)_{m,\ell-1}| & |(1,j-m)_{m,\ell-1}| & \cdots & |(m-1,j-2m+2)_{m,\ell-1}| \end{pmatrix} \tag{44}$$

From (42), the sum of the first row of matrix (44) is equal to $|(0,j)_{m,\ell}|$, the sum of all the entries in the second row except the first one is equal to $|(1,j-1)_{m,\ell}|$, and so forth, finally, the last entry in the last row is equal to $|(m-1,j-m+1)_{m,\ell}|$. From (43), the sum of all the values found, $|(0,j)_{m,\ell}|$, $|(1,j-1)_{m,\ell}|$, …, $|(m-1,j-m+1)_{m,\ell}|$, gives $|M_{m,\ell}(j)|$. In addition, those values, $|(0,j)_{m,\ell}|$, $|(1,j-1)_{m,\ell}|$, $\ldots$, $|(m-1,j-m+1)_{m,\ell}|$, for $j=0,1,\ldots,m-1$, form a new matrix, the ℓth matrix, which can be used to evaluate cardinal number of the solution sets, $|M_{m,\ell+1}(j)|$, $j=0,1,\ldots,m-1$. Repeating the process, until we obtain $|M_{m,r}(j)|$, $j=0,1,\ldots,m-1$, the number of the the congruence solutions of Equation (1) with the restriction $x_1\leq x_2\leq\cdots\leq x_r$.

Example 4 Let us use Algorithm 2 to evaluate $|M_{6,4}(j)|$, $j=0,1,\ldots,5$. First, we find $|M_{6,3}(j)|$, $j=0,1,\ldots,5$ using the 2nd matrices as follows.

$$
\begin{array}{cccccc|l}
1 & 1 & 1 & 1 & 0 & 0 & 4\\
1 & 1 & 1 & 0 & 0 & 0 & 2\\
1 & 1 & 1 & 0 & 0 & 1 & 2\\
1 & 1 & 0 & 0 & 1 & 0 & 1\\
1 & 1 & 0 & 1 & 1 & 0 & 1\\
1 & 0 & 1 & 1 & 0 & 0 & 0\\
\hline
 & & & & & & 10=|M_{6,3}(0)|
\end{array}
$$

$$
\begin{array}{cccccc|l}
1 & 1 & 1 & 0 & 0 & 0 & 3\\
1 & 1 & 1 & 0 & 0 & 1 & 3\\
1 & 1 & 0 & 0 & 1 & 0 & 1\\
1 & 1 & 0 & 1 & 1 & 0 & 2\\
1 & 0 & 1 & 1 & 0 & 0 & 0\\
1 & 1 & 1 & 1 & 0 & 0 & 0\\
\hline
 & & & & & & 9=|M_{6,3}(5)|
\end{array}
$$

1	1	1	0	0	1	4
1	1	0	0	1	0	2
1	1	0	1	1	0	2
1	0	1	1	0	0	1
1	1	1	1	0	0	0
1	1	1	0	0	0	0
						$9 = \lvert M_{6,3}(4)\rvert$

1	1	0	0	1	0	3
1	1	0	1	1	0	3
1	0	1	1	0	0	2
1	1	1	1	0	0	1
1	1	1	0	0	0	0
1	1	1	0	0	1	1
						$10 = \lvert M_{6,3}(3)\rvert$

1	1	0	1	1	0	4
1	0	1	1	0	0	2
1	1	1	1	0	0	2
1	1	1	0	0	0	0
1	1	1	0	0	1	1
1	1	0	0	1	0	0
						$9 = \lvert M_{6,3}(2)\rvert$

$$
\begin{array}{cccccc|l}
1 & 0 & 1 & 1 & 0 & 0 & 3 \\
1 & 1 & 1 & 1 & 0 & 0 & 3 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 \\
\hline
 & & & & & & 9 = |M_{6,3}(1)|
\end{array}
$$

Second, we find $|M_{6,4}(j)|$, $j = 0, 1, \ldots, 5$ using the 3rd matrices as follows. To save the space, we combine six matrices together.

$$
\begin{array}{cccccc|cccccc}
4 & 2 & 2 & 1 & 1 & 0 & 10 & & & & & \\
3 & 3 & 1 & 2 & 0 & 0 & 6 & 9 & & & & \\
4 & 2 & 2 & 1 & 0 & 0 & 3 & 5 & 9 & & & \\
3 & 3 & 2 & 1 & 0 & 1 & 2 & 4 & 7 & 10 & & \\
4 & 2 & 2 & 0 & 1 & 0 & 1 & 1 & 3 & 5 & 9 & \\
3 & 3 & 1 & 1 & 1 & 0 & 0 & 1 & 2 & 3 & 6 & 9 \\
4 & 2 & 2 & 1 & 1 & 0 & & 0 & 1 & 2 & 4 & 6 \\
3 & 3 & 1 & 2 & 0 & 0 & & & 0 & 0 & 2 & 3 \\
4 & 2 & 2 & 1 & 0 & 0 & & & & 0 & 0 & 1 \\
3 & 3 & 2 & 1 & 0 & 1 & & & & & 1 & 1 \\
4 & 2 & 2 & 0 & 1 & 0 & & & & & & 0 \\
\hline
 & & & & & & 22 & 20 & 22 & 20 & 22 & 20
\end{array}
$$

Thus, $|M_{6,4}(0)| = |M_{6,4}(4)| = |M_{6,4}(2)| = 22$ and $|M_{6,4}(5)| = |M_{6,4}(3)| = |M_{6,4}(1)| = 20$. Although we may use (2) to obtain $|M_{6,5}(i)| = 42$ for $i = 0, 1, \ldots, 5$, we can also use Algorithm 2 to evaluate the values.

10	6	3	2	1	0	22					
9	5	4	1	1	0	11	20				
9	7	3	2	1	0	6	13	22			
10	5	3	2	0	0	2	5	10	20		
9	6	4	2	0	1	1	3	7	13	22	
9	6	3	1	1	0	0	1	2	5	11	20
10	6	3	2	1	0		0	1	3	6	12
9	5	4	1	1	0			0	1	2	6
9	7	3	2	1	0				0	1	3
10	5	3	2	0	0					0	0
9	6	4	2	0	1						1
						42	42	42	42	42	42

Acknowledgments

Authors would like to express their gratitude to the anonymous referees for their helpful comments and suggestions.

References

[1] G. E. Andrews, The Theory of Partitions, Encyclo. Math. Appls. Vol. 2, Addison-Wesley, London, 1976.

[2] P. J. Cameron, Combinatorics: topics, techniques, algorithms. Cambridge University Press, Cambridge, 1994.

[3] W.-S. Chou, T. X. He, and Peter J.-S. Shiue, Enumeration problems for a linear congruence modulo m, Taiwanese Journal of Mathematics, 18 (2014), No.1, 265-275.

[4] N. J. Fine, Binomial coefficients modulo a prime. Amer. Math. Monthly 54, (1947). 589-592.

[5] R. K. Guy, Parker's permutation problem involves the Catalan numbers, Amer. Math. Monthly **100** (March, 1993), 287-289.

[6] J. D. Opdyke, A unified approach to algorithms generating unrestricted and restricted integer compositions and integer partitions, J. Math. Model Algor., 9 (2010), 53-97.

[7] H. Rademacher, Topics in analytic number theory. Edited by E. Grosswald, J. Lehner and M. Newman. Die Grundlehren der mathematischen Wissenschaften, Band 169. Springer-Verlag, New York-Heidelberg, 1973.

[8] L. A. Sanchis and M. B. Squire, Parallel algorithms for counting and randomly generating integer partitions, J. Paral. Diatrb. Computing, 34 (1996), 29-35.

[9] R. P. Stanley, Enumerative Combinatorics, vol. 2, Cambridge Stud. Adv. Math. vol. 62, Cambridge Univ. Press, Camabridge, 1998.

[10] R. P. Stanley, Catalan Addendum,
http://www.math.mit.edu/rstan/ec/catadd.pdf.