SARAJEVO JOURNAL OF MATHEMATICS
Vol.20 (33), No.1 (2024), 95–101
DOI: 10.5644/SJM.20.01.09

APPLICATIONS OF THE MULTISUBSET SUM PROBLEM OVER FINITE ABELIAN GROUPS

AMELA MURATOVIĆ-RIBIĆ

Dedicated to acc. Mirjana Vuković on the occasion of her 75 th birthday

ABSTRACT. In the article, we use the subset sum formula over a finite abelian group on the product of finite groups to derive the number of restricted partitions of elements in the group and to count the number of compositions over finite abelian groups. Later, we apply the formula for the multisubset sum problem on a group $\mathbb{Z}_n$ to produce a new technique for studying restricted partitions of positive integers.

1. INTRODUCTION

The subset sum problem is important in cryptography, coding theory and theory of complexity. Let G be an abelian group and let $S \subseteq G$. Let i be a positive integer. The problem is to determine the number of subsets of S with i elements in which the elements sum up to the g. For general S it is known to be NP-complete. On the other hand, if $S = G$ the problem is solved first by Li and Wan in [4] by use of sieve technique and later by Kosters in [3] using character theory. A. Muratović-Ribić and Q. Wang extended this result to the multisubset sum problem where elements in the multisubsets can be repeated at most j times. In the first section, we consider formulas for the number of certain restriced partitions over direct products of the groups and the formula for the number of compositions of an element over finite abelian groups. In the second section, we apply the formula for the multisubset problem to provide a new formula for restricted partitions over integers and introduce a new technique in the study of partitions over integers.

1.1. **Partitions of finite abelian groups**

Let G be a finite abelian group of order n and $g \in G$ some fixed element. In [5] an exact formulais given for the multisubset sum problem in G of the element g with i parts where each part repeats at most j times. This number is denoted by $M(G,i,j,g)$. More precisely $M(G,i,j,g) = \#\{\{a_1,a_2,\ldots,a_i\}| \quad a_1,a_2,\ldots,a_i \in$

2020 *Mathematics Subject Classification.* 05A17, 11P81.
Key words and phrases. partitions of integers, subset sum problem, multisubset sum problem.

G, $a_1+a_2+\ldots+a_i=g$, each element a_t can be repeated at most j times$\}$. The special case when $j=1$ was denoted by $N(G,i,g)$ and it is known as the subset sum problem. We have (see [3])

$$N(G,i,g)=\frac{1}{n}\sum_{s|\,\gcd(exp(G),i)}(-1)^{i+i/s}\binom{n/s}{i/s}\sum_{d|\gcd(s,e(g))}\mu(s/d)\#G[d]$$

where $exp(G)$ is the exponent of G, $e(g)=\max\{d : d \mid exp(G), g\in dG\}$, μ is the Möbius inversion function, and $G[d]=\{h\in G : dh=0\}$ is d-torsion of G. On the other hand, taking $j\geq i$, we can dismiss the restriction on the number of repetitions of elements. Note that multisubset sum problem is actually the same problem of number of partitions of integers, i.e. we look for the number of sums $a_1+a_2\cdots+a_i=g$ where the order of sumands is not important. Thus we will call this sum a partition of the element g. In the following section, we will use the following results.

Corollary 1.1 (Corollary 2, [5].). *Let G be a finite abelian group of size n and let $g\in G$. Then the number of partitions of g over G with at most i parts is*

$$A(G,i,g)=\frac{1}{n}\sum_{s|\gcd(exp(G),i)}\binom{n/s+i/s-1}{i/s}\sum_{d|\gcd(s,e(g))}\mu(s/d)\#G[d]$$

where $\exp(G)$ *is the exponent of G, $e(G)=\max\{d : d\mid \exp(G), g\in dG\}$, μ is the Möbius inversion function, and $G[d]=\{h\in G : dh=0\}$ is d-torsion of G.*

Also, we use the result in [5] on page 422 for the explicit number of partitions without zero element with i parts of the element $g\in G$.

$$M(G\setminus\{0\},i,g)=\frac{1}{n}\sum_{s|\gcd(exp(G),i)}\binom{n/s+i/s-1}{i/s}\sum_{d|\gcd(s,e(g))}\mu(s/d)\#G[d]$$

$$-\sum_{s|\gcd(exp(G),i-1)}\binom{n/s+(i-1)/s-1}{(i-1)/s}\sum_{d|\gcd(s,e(g))}\mu(s/d)\#G[d]).$$

We will consider the product of the groups $G=G_1\times G_2\times\cdots\times G_k$ and restricted subset sums problem in G.

Theorem 1.1. *Let $G_1,G_2,\ldots,G_k$ be finite abelian groups and G its direct product, i.e. $G=G_1\times G_2\times\cdots\times G_k$ and let $g=(g_1,g_2,\ldots,g_k)\in G$. Let i be a positive integer. Consider subsets $a_1,a_2,\ldots,a_i$ in G of i elements where $a_t=(a_{t1},a_{t2},...,a_{tk})$, $a_{ts}\in G_s$ for $t=1,2,\ldots,i$ and $s=1,2,\ldots,k$, that sum to $g=(g_1,g_2,\ldots,g_k)$, i.e.,*

$$(g_1,g_2,\ldots,g_k)=(a_{11},\ldots,a_{1k})+(a_{21},\cdots,a_{2k})+\cdots+(a_{i1},\cdots,a_{ik})$$

such that in the partition of the s-th coordinate positions, $g_s=a_{1s}+a_{2s}+\cdots+a_{ks}$ and all elements $a_{1s},\ldots,a_{ks}$ are distinct. The number of such subsets is

$$N(G_1,i,g_1)\cdot N(G_2,i,g_2)\cdots N(G_k,i,g_k)\cdot(i!)^{k-1}.$$

Proof. Consider a partition of the element g with i parts $g = a_1 + a_2 + \ldots + a_i$ of the elements in G where all elements are distinct. It is easy to see that every partition of g uniquely determines partitions of $g_1, g_2, \ldots, g_k$ with

$$\begin{aligned} g &= (g_1, \ldots, g_k) = a_1 + a_2 + \cdots + a_i \\ &= (a_{11}, \ldots, a_{1k}) + \cdots + (a_{i1}, \ldots, a_{ik}) = (a_{11} + \ldots a_{i1}, \ldots, a_{1k} + \cdots + a_{ik}). \end{aligned}$$

Therefore, a partition of g produce unique set of partitions of $g_1, g_2, \ldots, g_k$. On the other hand, if we have given partitions of $g_1, g_2, \ldots, g_k$ say

$$g_s = a_{s1} + a_{s2} + \cdots + a_{si}$$

then we can obtain a partition of g with

$$\begin{aligned} g = (g_1, \ldots, g_k) &= (a_{11}, \ldots, a_{1k}) + \cdots + (a_{i1}, \ldots, a_{ik}) \\ &= (a_{11} + \ldots a_{i1}, \ldots, a_{1k} + \cdots + a_{ik}). \end{aligned}$$

If we keep the ordering in the partition of g_1 lfor instance $g_1 = a_{11} + a_{12} + \cdots + a_{1i}$ and permute the elements in the rest of the partitions of $g_2, \ldots, g_k$ we will obtain a set of ordered k-tuples

$$(a_{11}, a_{2\pi_2(1)}, \ldots, a_{i\pi_k(1)}), \qquad (a_{12}, a_{2\pi_2(2)}, \ldots, a_{i\pi_k(2)}), \quad \ldots \quad (a_{i1}, \ldots, a_{i\pi_k(i)})$$

which also sums to the element g and this is a different partition of g. Therefore, from the set of the partitions of the elements $g_1 \in G_1, g_2 \in G_2, \ldots, g_k \in G_k$ of i parts where all parts are distinct we can make $(i!)^{k-1}$ different partitions of the element $g = (g_1, g_2, \ldots, g_k) \in G$. Therefore there are

$$N(G_1, i, g_1) \cdot N(G_2, i, g_2) \cdots N(G_k, i, g_k) \cdot (i!)^{k-1}$$

partitions of g with distinct elements in each coordinate. □

Corollary 1.2. *Let $G = G_1 \times G_2 \times \cdots \times G_k$ and let $g = (g_1, g_2, \ldots, g_k) \in G$. Then*

$$N(G_1, i, g_1) \cdot N(G_2, i, g_2) \cdots N(G_k, i, g_k) \cdot (i!)^{k-1} \leq N(G, i, g).$$

Further, consider the problem of compositions over a finite abelian group G. A composition of an element is a solution of the equation $x_1 + x_2 + \cdots + x_i = g$. Note that order matters, and the number of compositions with all distinct parts (with possibly zero included) is $i!N(G, i, g)$.

To find the formula for the compositions with possible repetitions, in the equation $x_1 + x_2 + \cdots + x_i = g$, for any choice of $x_1, x_2, \ldots, x_{i-1}$ there is a unique x_i such that $\sum_{s=1}^{i} x_s = g$ so we can deduce that the number of compositions without restriction is $|G|^{i-1}$. To find the number of compositions without zero element consider the case when in $x_1 + x_2 + \ldots + x_i = g$ there are s nonzero elements and $i - s$ zero elements. Let $C(s, g)$ be the number of compositions of g with s nonzero parts. Choosing s positions for nonzero elements there are is $\binom{i}{s} C(s, g)$ compositions of g with s nonzero elements. Therefore

$$\sum_{s=0}^{i}\binom{i}{s}C(s,g)=|G|^{i-1}$$

which gives a recursive formula for $C(i,g)$.

2. New approach to study restricted partitions over integers

2.1. **Introduction**

A partition of a positive integer n is a way of writing of n as a sum of positive integers, where the order of integers is irrelevant. In number theory and combinatorics, besides constructing partitions, it is important to determine their number. They occur in the study of the symmetric polynomials and of the symmetric groups and in group representation theory in general.

The number of partitions of a given integer n is denoted by $p(n)$. Partitions are defined for non-negative integers where the only partition of the zero is the empty set. The generating function of $p(n)$ is

$$\sum_{n=0}^{\infty}p(n)x^n=\sum_{j=0}^{\infty}(1+x^j+x^{2j}+\ldots+x^{kj}+\ldots)=\prod_{j=0}^{\infty}(1-x^j)^{-1}.$$

Using the expansion of the generating function the first approximation of $p(n)$ was given by Hardy and Ramanujan $p(n)\sim\frac{1}{4n\sqrt{3}}\exp\left(\pi\sqrt{\frac{2n}{3}}\right),\qquad n\to\infty.$

Restricted partitions are partitions with a fixed number of summands or with a given bound on summands. Thus we can consider the partitions of an integer n with k parts. Its number is denoted by $p_k(n)$.

One can recover the function $p(n)$ by $p(n)=\sum_{k=0}^{n}p_k(n)$. The generating function for such partitions is $\sum_{n\geq 0}p_k(n)x^n=x^k\prod_{i=1}^{k}\frac{1}{(1-x^k)}$. More generally, for a given subset t of positive integers, the generating function of the $p(n)$ whose parts belong to T is $\prod_{t\in T}(1-x^t)^{-1}$. Using this result, Hardy in [2] used the expansion of $\prod_{i=1}^{3}(1-x^i)^{-1}=\frac{1}{6(1-x)^3}+\frac{4}{(1-x)^2}+\frac{17}{72(1-x)}+\cdots$ and found that the number of partitions $r(n)$ of n whose parts are $1,2$ or 3 is

$$r(n)=\frac{(n+3)^2}{12}-\frac{7}{72}+\frac{(-1)^n}{8}+\frac{2}{8}\cos\frac{2n\pi}{3}. \tag{2.1}$$

It is easy to verify that the sum ofthe last three numbers is less than $\frac{1}{2}$ and thus $r(n)$ is the integer closest to $\frac{(n+3)^2}{12}$.

To every partition we can adjoin its Young table. It is common that summands in the partitions are written in nondecreasing order. If the partition is $a_1+a_2+\ldots+a_k=n$ then $a_1\leq a_2\leq\cdots\leq a_k$. We draw rectangulars of the dimensions $1\times a_k$, $1\times a_{k-1},\ldots,1\times a_1$ one below the other to obtain a Young table. A Young table flipped across the diagonal forms a Young table of the conjugate partition. We can conclude that the number of partitions whose parts are 1, 2 or 3 is equivalent to the number of partitions of n with at most three parts. Note that the number of rows in a Young table is the number of parts.

We can simultaneously limit the number and size of parts. If the partition n is having at most M parts and all summands are less than or equal to N then its Young table fits in a $M \times N$ rectangle. The number of such partitions we denote by $p(N,M;n)$. Then it satisfies a recursive formula $p(N,M;n) = p(N,M-1;n) + p(N-1,M;n-M)$. Note that the number of partitions of n into exactly M parts whose sumanads are less or equal to the N is given by $p(N,M;n) - p(N,M-1;n)$.

2.2. Application of the multisubset sum problem to partitions of integers

Consider now some positive integer g and let $n > g$. Identify notation for $\bar{g} = g((\text{mod}\, n)) \in \mathbb{Z}_n$ with g. Using the fact that $g = g + jn \pmod{n}$ we can conclude that the following holds.

Theorem 2.1.

$$A(\mathbb{Z}_n, i, g) = p(n-1,i;g) + p(n-1,i;g+n) + \cdots p(n-1,i;g+(i-1)n).$$

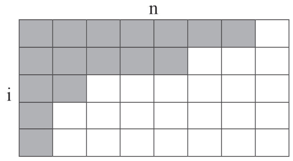
A similar formula holds if we use partitions with exactly i parts instead lessthan or equal to i.

Denote by $p^e(i,n-1;k)$ the number of partitions of an integer k with exactly i parts where the summands are less than or equal to $n-1$.

Theorem 2.2. *Let n be a positive integer and $1 \leq j < i \leq n$. Then*

$$p^e(i,n-1;jn) = p^e(i,n-1;(i-j)n).$$

Proof. Put the Young table Y of the partition α of a number jn in $i \times (n-1)$ grid. Add a column at the end of the grid to obtain $i \times n$ grid T. Note that $T \setminus Y$ has a $(i-j)n$ squares and it is the Young table of the partition of $(i-j)n$ rotated for 180° with exactly i parts where each summand is less than n.



Since $T \setminus Y$ is uniquely determined by Y, there is a one to one correspondence between the partitions on jn and partitions of $(i-j)n$ with i parts whose summands are less than n. □

Corollary 2.1. *Note that if the number of parts in the partitions is at most i then $p(i,n-1;jn) = p(i,n-1;(i-j)n)$.*

Proof. Indeed,

$$p(i,n-1;jn) = p^e(i,n-1;jn) + p^e(i-1,n-1;jn) + \ldots p^e(1,n-1;jn) =$$

$$p^e(i,n-1;(i-j)n)+p^e(i-1,n-1;(i-j)n)+\cdots+p^e(1,n-1;(i-j)n)=$$
$$=p(i,n-1;(i-j)n). \qquad \square$$

If we apply the equation in Theorem 2.1 for $g=0$ we obtain that

$$A(n,i;0)=1+p(i,n-1;n)+p(i,n-1;2n)+\cdots+p(i,n-1;(i-1)n), \quad (2.2)$$

where the Corollary 2.1. implies the simmetry of summands.

3. Special cases

Consider the case $i=2$. Thus we consider a partition with at most two parts. Apply the equation (2.2) to $G=\mathbb{Z}_n$

$$1+p(2,n-1;n)=A(n,2,0).$$

We have $exp(G)=n$, $g=0$, $e(g)=n$. If n is odd number then

$$A(G,2,0)=\frac{1}{n}\binom{n+1}{2}=\frac{n+1}{2},$$

and thus $p(2,n-1;n)=\frac{n-1}{2}$. If n is even then

$$A(G,2,0)=\frac{1}{n}\left(\frac{(n+1)n}{2}+\frac{n}{2}(-1+2)\right)=\frac{n+2}{2},$$

so we have $p(2,n-1;n)=\lfloor\frac{n}{2}\rfloor$. These results can be obtained directly and they are well known.

Now consider the case $i=3$. Here we will rather use a formula for the number of partitions with exactly 3 parts.

Then we have

$$M(\mathbb{Z}_n\setminus\{0\},3,0)=p^e(n-1,3,0)+p^e(n-1,3,n)+p^e(n-1,3;2n).$$

Using Theorem 2.2. we have that $p^e(n-1,3,n)=p^e(n-1,3;2n)$. Further, evaluating $M(\mathbb{Z}_n\setminus\{0\},3;0)$ we have that

$$p^e(n-1,3,n)=\begin{cases}\frac{n^2}{12}, & n\equiv 0 \mod 6\\ \frac{(3n+5)(n+1)}{12}, & n\equiv 1 \mod 6 \quad \text{or} \quad n\equiv 5 \mod 6,\\ \frac{n^2-4}{12}, & n\equiv 2 \mod 6 \quad \text{or} \quad n\equiv 4 \mod 6,\\ \frac{n^2}{12}, & n\equiv 3 \mod 6\end{cases}$$

which is a more precise result than given in the equation (2.1).

Open problem: Apply this approach to obtain more interesting results on the problem of determining the number of restricted partitions of integers.

REFERENCES

[1] Andrews, George E., *The Theory of Partitions*, Cambridge University Press, 1976.

[2] G.H. Hardy, E.M. Wright *An Introduction to the Theory of Numbers*, Oxford at the Clerendon Press, 4th edition United Kingdom, 1960.

[3] M. Kosters, The subset problem for finite abelian groups, *J. Combin. Thery Ser. A* 120(2013), 527-530.

[4] Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Thery Ser. A* 199 (2012), no. 1, 170-182.

[5] Amela Muratović-Ribić, Qiang Wang, The multisubset sum problem for finite abelian groups, *Ars Mathematica Contemporanea* 8 (2015), 417-423.

(Received: January 11, 2024)
(Revised: April 24, 2024)

Amela Muratović-Ribić
University of Sarajevo
Faculty of Science and Mathematics
Department of Mathematical and Computer Sciences
Zmaja od Bosne 33-35
71 000 Sarajevo
Bosnia and Herzegovina
e-mail: *amela@pmf.unsa.ba*