ARS MATHEMATICA CONTEMPORANEA

Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 8 (2015) 417–423

The multisubset sum problem for finite abelian groups

Amela Muratović-Ribić
University of Sarajevo, Department of Mathematics, Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina

Qiang Wang *
School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario, $K1S\ 5B6$, Canada

Received 28 October 2013, accepted 29 August 2014, published online 11 June 2015

Abstract

We use a similar techique as in [2] to derive a formula for the number of multisubsets of a finite abelian group G with any given size and any given multiplicity such that the sum is equal to a given element $g \in G$. This also gives the number of partitions of g into a given number of parts over a finite abelian group.

Keywords: Composition, partition, subset sum, polynomials, finite fields, character, finite abelian groups.

Math. Subj. Class.: 11B30, 05A15, 20K01, 11T06

1 Introduction

Let G be a finite abelian group of size n and D be a subset of G. The well known subset sum problem in combinatorics is to decide whether there exists a subset S of D which sums to a given element in G. This problem is an important problem in complexity theory and cryptography and it is NP-complete (see for example [3]). For any $g \in G$ and i a positive integer, we let the number of subsets S of D of size i which sum up to g be denoted by

$$N(D, i, g) = \#\{S \subseteq D : \#S = i, \sum_{s \in S} s = g\}.$$

*Research is partially supported by NSERC of Canada.
E-mail addresses: amela@pmf.unsa.ba (Amela Muratović-Ribić), wang@math.carleton.ca (Qiang Wang)

When D has more structure, Li and Wan made some important progress in counting these subset sums by a sieve technique [3, 4]. Recently Kosters [2] gives a shorter proof of the formula obtained by Li and Wan earlier, using character theory.

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

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

More generally, we consider a multisubset M of D. The number of times an element belongs to M is the *multiplicity* of that member. We define the *multiplicity* of a multisubset M is the largest multiplicity among all the members in M. We denote

$$M(D,i,j,g)=\#\{\text{multisubset } M \text{ of } D : \text{multiplicity}(M)\le j, \#M=i, \sum_{s\in M}s=g\}.$$

It is an interesting question by its own to count $M(D,i,j,g)$, the number of multisubsets of D of cardinality i which sum to g where every element is repeated at most j times. If $j=1$, then $M(D,i,j,g)=N(D,i,g)$. If $j\ge i$, this problem is also equivalent to counting partitions of g with at most i parts over D, which is $M(D,i,i,g)$. In this case we use a simpler notation $M(D,i,g)$ because the second i does not give any restriction.

Another motivation to study the enumeration of multisubset sums is due to a recent study of polynomials of prescribed ranges over a finite field. Indeed, through the study of enumeration of multisubset sums over finite fields [5], we were able to disprove a conjecture of polynomials of prescribed ranges ove a finite field proposed in [1]. Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q^*$ be the cyclic multiplicative group. When D is $\mathbb{F}_q$ (the additive group) or $\mathbb{F}_q^*$, counting the multisubset sum problem is the same as counting partitions over finite fields, which has been studied earlier in [6].

In this note, we use the similar method as in [2] to obtain $M(D,i,j,g)$ when $D=G$. However, we work in a power series ring instead of a polynomial ring.

Theorem 1. Let G be a finite abelian group of size n and let $g\in G$, $i,j\in\mathbb{Z}$ with $i\ge 0$ and $j\ge 1$. For any $s\mid n$, we define

$$C(n,i,j,s)=\sum_{\substack{k\ge 0, 0\le t\le \frac{n\gcd(s,j+1)}{s},\\ sk+t\cdot\mathrm{lcm}(s,j+1)=i}}(-1)^t\binom{n/s+k-1}{k}\binom{\frac{n\gcd(s,j+1)}{s}}{t}.$$

Then we have

$$M(G,i,j,g)=\frac{1}{n}\sum_{s|\gcd(exp(G),i)}C(n,i,j,s)\sum_{d|\gcd(s,e(g))}\mu(s/d)\#G[d].$$

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

As a corollary, we obtain the main theorem in [2] when $j=1$.

Corollary 1. (Theorem 1.1 in [2]) Let G be a finite abelian group of size n and let $g \in G$ and $i \in \mathbb{Z}$. Then we have

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

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

Moreover, when $j \geq i$, the formula gives the number of partitions of g with at most i parts over a finite abelian group. To avoid confusion the multiset consisting of $a_1, \ldots, a_n$ is denoted by $\{\{a_1, \ldots, a_n\}\}$, with possibly repeated elements, and by $\{a_1, \ldots, a_n\}$ the usual sets. We define a partition of the element $g \in G$ with exactly i parts in D as a multiset $\{\{a_1, a_2, \ldots, a_i\}\}$ such that all a_k's are nonzero elements in D and

$$a_1 + a_2 + \ldots + a_i = g.$$

Then the number of these partitions is denoted by $P_D(i,g)$, i.e.,

$$P_D(i,g) = \left|\left\{\{\{a_1, a_2, \ldots, a_i\}\} \subseteq D : a_1 + a_2 + \ldots + a_i = g, a_1, \ldots, a_i \neq 0\right\}\right|.$$

It turns out $M(D,i,g) = \sum_{k=0}^{i} P_D(k,g)$ is the number of partitions of $g \in G$ with at most i parts in D.

Corollary 2. 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

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

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

Proof. The number is $M(G,i,j,g)$ when $j \geq i \geq 0$. If $j \geq i$, then the linear Diophantine equation $sk + t \cdot \text{lcm}(s, j+1) = i$ reduces to $sk = i$ and $t = 0$. The rest of proof follows immediately. $\square$

In Section 2, we prove our main theorem and derive Corollary 1 as a consequence. In Section 3, we extend our study to a subset of a finite abelian group and make a few remarks on how to obtain the number of partitions over any subset of a finite abelian group.

2 Proof of Theorem 1

To make this paper self-contained, we recall the following lemmas (see Lemmas 2.1-2.4 in [2]). Let G be a finite abelian group of size n. Let $\mathbb{C}$ be the field of complex numbers and $\hat{G} = \text{Hom}(G, \mathbb{C}^*)$ be the group of characters of G. Let $\chi \in \hat{G}$ and $\bar{\chi}$ be the conjugate character which satisfies $\bar{\chi}(g) = \overline{\chi(g)} = \chi(-g)$ for all $g \in G$. We note that a character χ can be naturally extended to a $\mathbb{C}$-algebra morphism $\chi : \mathbb{C}[G] \to \mathbb{C}$ on the group ring $\mathbb{C}[G]$.

Lemma 1. Let $\alpha = \sum_{g \in G} \alpha_g g \in \mathbb{C}[G]$. Then we have $\alpha_g = \frac{1}{n} \sum_{\chi \in \hat{G}} \bar{\chi}(g)\chi(\alpha)$.

Lemma 2. Let m be a positive integer and $g \in G$. Then

$$\sum_{\chi \in \hat{G}, \chi^m = 1} \chi(g) = \delta_{g \in mG} \# G[m],$$

where $\delta_{g \in mG}$ is 1 if $g \in mG$ and it is zero otherwise.

Lemma 3. Let $\chi \in \hat{G}$ be a character and m be its order. Then we have

$$\prod_{\sigma \in G} (1 - \chi(\sigma) Y) = (1 - Y^m)^{n/m}.$$

Lemma 4. Let $g \in G$. The number $e(g)$ is equal to $lcm\{d : d \mid exp(G),\ g \in dG\}$. For $d \mid exp(G)$ we have $g \in dG$ if and only if $d \mid e(g)$.

Let us present the proof of Theorem 1. We use the multiplicative notation for the group.

Proof. Fix $j \geq 1$. Working in the power series ring $\mathbb{C}[G][[X]]$ over the group ring, the generating function of $\sum_{g \in G} M(G, i, j, g) g$ is

$$\sum_{i=0}^{\infty} \sum_{g \in G} M(G, i, j, g) g X^i = \prod_{\sigma \in G} (1 + \sigma X + \cdots + \sigma^j X^j) = \prod_{\sigma \in G} \frac{1 - \sigma^{j+1} X^{j+1}}{1 - \sigma X} \in \mathbb{C}[G][[X]].$$

Using Lemma 1, we write

$$\sum_{i=0}^{\infty} M(G, i, j, g) X^i = \frac{1}{n} \sum_{\chi \in \hat{G}} \bar{\chi}(g) \prod_{\sigma \in G} \frac{1 - \chi^{j+1}(\sigma) X^{j+1}}{1 - \chi(\sigma) X}.$$

Separating the first sum on the right hand side, we obtain

$$\sum_{i=0}^{\infty} M(G, i, j, g) X^i = \frac{1}{n} \sum_{s \mid exp(G)} \sum_{\chi \in \hat{G}, ord(\chi) = s} \bar{\chi}(g) \prod_{\sigma \in G} \frac{1 - \chi^{j+1}(\sigma) X^{j+1}}{1 - \chi(\sigma) X}.$$

For each fixed χ of the order s, we know that χ^{j+1} has the order $\frac{s}{\gcd(s, j+1)}$. Therefore by Lemma 3, we simplify the above as follows:

$$\sum_{i=0}^{\infty} M(G, i, j, g) X^i = \frac{1}{n} \sum_{s \mid exp(G)} \sum_{\chi \in \hat{G}, ord(\chi) = s} \bar{\chi}(g) \frac{\left(1 - X^{\operatorname{lcm}(s, j+1)}\right)^{\frac{n \gcd(s, j+1)}{s}}}{(1 - X^s)^{n/s}}. \quad (2.1)$$

Note that

$$\sum_{\chi \in \hat{G}, \chi^s = 1} \bar{\chi}(g) = \sum_{d \mid s} \sum_{\chi \in \hat{G}, ord(\chi) = d} \bar{\chi}(g).$$

By Lemma 2 and the Möbius inversion formula, we obtain

$$\sum_{\chi \in \hat{G}, ord(\chi) = s} \bar{\chi}(g) = \sum_{d \mid s} \mu(s/d) \sum_{\chi \in \hat{G}, \bar{\chi}^d = 1} \bar{\chi}(g) = \sum_{d \mid s} \mu(s/d) \delta_{g \in dG} \# G[d].$$

Because $d \mid s \mid exp(G)$, by Lemma 4, $g \in dG$ if and only if $d \mid e(g)$. Hence

$$\sum_{\chi \in \hat{G}, ord(\chi)=s} \bar{\chi}(g) = \sum_{d|s} \mu(s/d)\delta_{g\in dG}\#G[d] = \sum_{d|\gcd(s,e(g))} \mu(s/d)\#G[d].$$

Plugging this into Equation (2.1), we get

$$\sum_{i=0}^{\infty} M(G,i,j,g)X^i = \frac{1}{n}\sum_{s|exp(G)}\sum_{d|gcd(s,e(g))} \mu(s/d)\#G[d]\frac{\left(1-X^{\mathrm{lcm}(s,j+1)}\right)^{\frac{n\gcd(s,j+1)}{s}}}{(1-X^s)^{n/s}}.$$

By applying the binomial theorem to the right hand side and comparing coefficients of X^i in both sides, we single out $M(G,i,j,g)$ and obtain

$$M(G,i,j,g) = \frac{1}{n}\sum_{s|exp(G)}\sum_{d|gcd(s,e(g))} \mu(s/d)\#G[d]C(n,i,j,s).$$

After bringing $C(n,i,j,s)$ out of the inner sum we complete the proof. $\square$

Finally we remark that we can derive Corollary 1 using $N(G,i,g) = M(G,i,1,g)$. When $j=1$, let us consider $sk + t\cdot \mathrm{lcm}(s,j+1) = sk + t\cdot \mathrm{lcm}(s,2) = i$. If s is even, we obtain $sk+st=i$ and thus $k+t=i/s$. Note that we have the following power series expansions

$$\frac{1}{(1-x)^{n/s}} = \sum_{k=0}^{\infty}\binom{n/s+k-1}{k}x^k,$$

$$(1-x)^{2n/s} = \sum_{t=0}^{2n/s}(-1)^t\binom{2n/s}{t}x^t,$$

and

$$(1-x)^{n/s} = \sum_{j=0}^{n/s}\binom{n/s}{j}(-1)^j x^j.$$

Now we compare the coefficients of the term $x^{i/s}$ in both sides of

$$\frac{1}{(1-x^s)^{n/s}}(1-x^s)^{2n/s} = (1-x^s)^{n/s},$$

after expanding these power series. Hence we obtain

$$C(n,i,1,s) = \sum_{\substack{k+t=i/s\\ k\geq 0, 0\leq t\leq 2n/s}} (-1)^t\binom{n/s+k-1}{k}\binom{2n/s}{t} = (-1)^{i/s}\binom{n/s}{i/s}.$$

Moreover, $C(n,i,1,s) = (-1)^{i+i/s}\binom{n/s}{i/s}$ because i is even.

Similarly, if s is odd, we obtain $sk+2st=i$ and thus $k+2t=i/s$. Moreover, $i+i/s$ is even. Using

$$(1-x^{2s})^{n/s}\frac{1}{(1-x^s)^{n/s}} = (1+x^s)^{n/s},$$

we obtain

$$C(n,i,1,s)=\sum_{\substack{k+2t=i/s\\ k\geq 0,0\leq t\leq n/s}}(-1)^t\binom{n/s+k-1}{k}\binom{n/s}{t}=(-1)^{i+i/s}\binom{n/s}{i/s}.$$

3 A few remarks

In this section we study $M(D,i,j,g)$ where $j\geq i$ and D is a subset of G. We recall that in this case we use the notation $M(D,i,g)$ because j does not really put any restriction. First of all, we note that

$$\sum_{i=0}^{\infty}\sum_{g\in G}M(G\setminus\{0\},i,g)gX^i=\prod_{\sigma\in G,\sigma\neq 0}\frac{1}{1-\sigma X}=(1-X)\sum_{i=0}^{\infty}\sum_{g\in G}M(G,i,g)gX^i.$$

By Corollary 2, we obtain

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

We note $M(G\setminus\{0\},i,g)=P_G(i,g)$. Therefore we obtain an explicit formula for the number of partitions of g into i parts over G. More generally, let $D=G\setminus S$, where $S=\{u_1,u_2,\ldots,u_{|S|}\}\neq\emptyset$. Denote by $M_S(G,i,g)$ the number of multisubsets of G of sizes i that contain at least one element from S. Then the number of multisubsets of $D=G\setminus S$ with i parts which sum up to g is equal to

$$M(G\setminus S,i,g)=M(G,i,g)-M_S(G,i,g).$$

Note that $M(G,0,0)=1$ and $M(G,0,s)=0$ for any $s\in G\setminus\{0\}$. The principle of inclusion-exclusion immediately implies that $M_S(G,i,g)$ is given in the following formula. We note that the formula is quite useful when the size of S is small in order to compute $M(G\setminus S,i,g)$.

Proposition 1. For all $i=1,2,\ldots$ and $g\in G$ we have

$$\begin{aligned}M_S(G,i,g)&=\sum_{u\in S}M(G,i-1,g-u)-\ldots\\ &+(-1)^{t-1}\sum_{\{u_1,u_2,\ldots,u_t\}\subseteq S}M(G,i-t,g-(u_1+u_2+\ldots+u_t))+\ldots\\ &+(-1)^{i-2}\sum_{\{u_1,u_2,\ldots,u_{i-1}\}\subseteq S}M(G,1,g-(u_1+u_2+\ldots+u_{i-1}))+\\ &(-1)^{i-1}\sum_{\{u_1,u_2,\ldots,u_i\}\subseteq S}M(G,1,g-(u_1+u_2+\ldots+u_i)).\end{aligned}$$

Proof. Fix an element $g \in G$. Denote by $\mathcal{A}_u$ the family of all the multisubsets of G with i parts which sum up to g and each multisubset also contains the element u. The principle of the inclusion-exclusion implies that

$$|\cup_{u\in S}\mathcal{A}_u| = \sum_{u\in S}|\mathcal{A}_u| - \sum_{\{u_1,u_2\}\subseteq S}|\mathcal{A}_{u_1}\cap\mathcal{A}_{u_2}| + \dots \tag{3.1}$$

It is obvious to see $|\mathcal{A}_{u_1}\cap\mathcal{A}_{u_2}| = M(G, i-2, g-(u_1+u_2))$ etc. by definition and the result follows directly. □

Acknowledgements

We thank anonymous referees for their helpful suggestions.

References

[1] A. Gács, T. Héger, Z. L. Nagy, D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, *Finite Field Appl.* **16** (2010), 301-314.

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

[3] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Field Appl.* **14** (2008), 911-929.

[4] J. Li and D. Wan, Counting subset sums of finite abelian groups, *J. Combin. Theory Ser. A* **119** (2012), no. 1, 170-182.

[5] A. Muratović-Ribić and Q. Wang, On a conjecture of polynomials with prescribed range, *Finite Field Appl.* **18** (2012), no. 4, 728-737.

[6] A. Muratović-Ribić and Q. Wang, Partitions and compositions over finite fields, *Electron. J. Combin.* **20** (2013), no. 1, P34, 1-14.