COUNTING SUBSET SUMS OF FINITE ABELIAN GROUPS

JIYOU LI AND DAQING WAN

Abstract. In this paper, we obtain an explicit formula for the number of zero-sum k-element subsets in any finite abelian group.

1. Introduction

Let A be an abelian group. Let $D \subset A$ be a finite subset of n elements. For a positive integer $1 \leq k \leq n$ and an element $b \in A$, let $N_D(k,b)$ denote the number of k-element subsets $S \subseteq D$ such that $\sum_{a \in S} a = b$. The decision version of the subset sum problem over D is to determine if there is a non-empty subset $S \subseteq D$ such that $\sum_{a \in S} a = b$, that is, if $N_D(k,b) > 0$ for some $1 \leq k \leq n$. This problem naturally arises from a number of important applications in coding theory and cryptography. It is a well known NP-complete problem, even in the case when A is cyclic (finite or infinite), or the additive group of a finite field $\mathbb{F}_q$ or the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on an elliptic curve E defined over $\mathbb{F}_q$. The case that $A = \mathbb{Z}$ is the basis of the knapsack cryptosystem. The case $A = \mathbb{F}_q$ is related to the deep hole problem of extended Reed-Solomon codes, see [2]. The case $A = E(\mathbb{F}_q)$ is related to the minimal distance of extended elliptic codes, see [1].

The main combinatorial difficulty for the subset sum problem comes from the great flexibility in choosing the subset D which is in general either too small or far from any algebraic structure. Consequently, in order to say something significant about $N_D(k,b)$, it is necessary to put some restrictions on the subset D. From algorithmic point of view, the idea of dynamic algorithm [3] can be used to show that $N_D(k,b)$ can be computed in polynomial time if the set D is sufficiently large in the sense that $|D| = |A|^c$ for some positive constant c. From mathematical point of view, ideally, we would like to have an explicit formula or an asymptotic formula. This is apparently too much to hope for in general, even in the case that $|D| = |A|^c$ for some positive constant c. However, we expect the existence of an asymptotic formula for the number $N_D(k,b)$ for certain non-trivial values of k if D is close to a large subset with certain algebraic structure. For example, an old result of Ramanathan (1945) gives an explicit formula for $N_D(k,b)$ when $D = A$ is a finite cyclic group, obtained using Ramanujan's trigonometric sums. More recently, the authors [5] obtained an explicit formula for $N_D(k,b)$ in the case when $D = A$ is the additive group of a finite field $\mathbb{F}_q$ (which is an elementary abelian p-group) using entirely different arguments. In this paper, we present a general new approach which gives an explicit formula when $D = A$ is any finite abelian group. In particular, this generalizes and unifies previous formulas in this direction. Our main result is the following theorem.

Theorem 1.1. *Suppose we are given the isomorphism $A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ with $n = |A| = n_1 \cdots n_s$. Given $b \in A$, suppose $(b_1, b_2, \ldots, b_s)$ is the image of b in* *the isomorphism. Let $N(k,b)$ be the number of k-subsets of A whose elements sum to b. Then*

$$N(k,b) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \Phi(r,b),$$

where $\Phi(r,b) = \sum_{d|r,(n_i,d)|b_i} \mu(r/d) \prod_{i=1}^{s} (n_i, d)$ and μ is the usual Möbius function defined over the integers.

Remark. The average size of the number $N(k,b)$ is $\binom{n}{k}/n$. Thus, the total input and output size for the problem of computing $N(k,b)$ is roughly $sk \log n$. The above formula gives an algorithm for computing $N(k,b)$ in time which is polynomial in $sk \log n$. This is a deterministic polynomial time algorithm.

When A is cyclic one checks that in the above formula $\Phi(r,b)$ has a simple form $\Phi(r,b) = \sum_{d|(b,r)} \mu(r/d)d$ and thus we get the following formula, which was first found by Ramanathan [9] using the properties of the Ramanujan's trigonometrical sum. Some related results can be found in [7, 10].

Corollary 1.2. *Given $b \in \mathbb{Z}_n$. Let $N(k,b)$ be the number of k-subsets of $\mathbb{Z}_n$ whose elements sum to b. Then we have*

$$N(k,b) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} C_r(b) \binom{n/r}{k/r},$$

where $C_r(b) = \sum_{d|(r,b)} \mu(r/d)d$ is Ramanujan's trigonometrical sum, which can be also defined as

$$C_r(m) = \sum_{k,(k,r)=1} e^{2\pi i k m/r}.$$

In particular,

$$N(k,0) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \phi(r) \binom{n/r}{k/r},$$

where ϕ is the Euler totient function.

Corollary 1.3. *Let $N(b)$ be the number of subsets of A sum to b. For convenience we regard the empty set as a subset sum to 0. Then*

$$N(b) = \frac{1}{n} \sum_{r|n, r \text{ odd}} \Phi(r,b) 2^{n/r}.$$

In particular, when A is cyclic, we have

$$N(b) = \frac{1}{n} \sum_{r|n, r \text{ odd}} C_r(b) 2^{n/r}.$$

Furthermore, if $b = 0$ and n is odd then we get a classical formula [10]

$$N(0) = \frac{1}{n} \sum_{r|n} \phi(r) 2^{n/r}.$$

Remark. The average size of $N(b)$ is $2^n/n$, and thus the input and output size for computing $N(b)$ is roughly $O(sn)$. The formula in the above corollary gives an algorithm which computes the number $N(b)$ in time that is polynomial in sn. This is a deterministic polynomial time algorithm.

Another example is to take A to be an additive subgroup of a finite field $\mathbb{F}_q$ of characteristic p (or any finite dimensional vector space over $\mathbb{F}_p$). In this case, we obtain

Corollary 1.4. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let A be any additive subgroup of $\mathbb{F}_q$ and $|A| = n$. For any $b \in A$, let $N(k, b)$ be the number of k-subsets of A whose elements sum to b. Define $v(b) = -1$ if $b \neq 0$, and $v(b) = n - 1$ if $b = 0$. If $p \nmid k$, then*

$$N(k, b) = \frac{1}{n}\binom{n}{k}.$$

If $p \mid k$, then

$$N(k, b) = \frac{1}{n}\binom{n}{k} + (-1)^{k+\frac{k}{p}}\frac{v(b)}{n}\binom{n/p}{k/p}.$$

This generalizes the formula in [5] which works when $A = \mathbb{F}_q$.

The paper is organized as follows. We first present a sieve formula via the *Möbius* Inversion Formula in Section 2 and then prove Corollary 1.2 in Section 3. The proof of Theorem 1.1, Corollary 1.3 and Corollary 1.4 are given in Section 4.

2. A distinct coordinate sieving formula

The starting point of our approach is the new sieving formula discovered in [6], which significantly improves the classical inclusion-exclusion sieve in some interesting cases. In this section, we will give a reformulation and a new proof of this formula via the *Möbius* inversion on a suitable partially ordered set.

We recall some basic notations for our problem. Let D be a finite set, and let $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let X be a subset of D^k. In many situations we are interested in counting the number of elements in the set

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X \mid x_i \neq x_j, \forall i \neq j\}. \tag{2.1}$$

Let S_k be the symmetric group on $\{1, 2, \ldots, k\}$. Each permutation $\tau \in S_k$ factorizes uniquely (up to the order of the factors) as a product of disjoint cycles and each fixed point is viewed as a trivial cycle of length 1. For simplicity of the notation, we usually omit the 1-cycles. Two permutations in S_k are conjugate if and only if they have the same type of cycle structure (up to the order). Let C_k be the set of conjugacy classes of S_k and note that $|C_k| = p(k)$, the partition function. For a given $\tau \in S_k$, let $l(\tau)$ be the number of cycles of τ including the trivial cycles. Then $\operatorname{sign}(\tau) = (-1)^{k-l(\tau)}$. For a given permutation $\tau = (i_1 i_2 \cdots i_{a_1})(j_1 j_2 \cdots j_{a_2}) \cdots (l_1 l_2 \cdots l_{a_s})$ with $1 \leq a_i, 1 \leq i \leq s$, define

$$X_\tau = \left\{(x_1, \ldots, x_k) \in X, x_{i_1} = \cdots = x_{i_{a_1}}, \ldots, x_{l_1} = \cdots = x_{l_{a_s}}\right\}. \tag{2.2}$$

Each element of X_τ is said to be of type τ. Thus X_τ is the set of all elements in X of type τ.

A partially ordered set, also known as a poset, is a set P with a binary relation $\leq$ such that:

- for all a, b and c in P, we have that: $a \leq a$ (reflexivity);
- if $a \leq b$ and $b \leq a$ then $a = b$ (antisymmetry);
- if $a \leq b$ and $b \leq c$ then $a \leq c$ (transitivity).

We use the convenient notation $x < y$ to mean $x \leq y$ and $x \neq y$. We also use $y \geq x$ to denote $x \leq y$.

The incidence algebra $I(P, R)$[10] of a partially ordered set P over a commutative ring R with identity is the algebra of functions $f : P \times P \to R$ such that:

- $f(x, y) = 0$ unless $x \leq y$;
- $(f + g)(x, y) = f(x, y) + g(x, y)$ (addition);
- $(fg)(x, y) = \sum_{x \leq z \leq y} f(x, z)g(z, y)$ (convolution).

One checks that $I(P, R)$ is an associative R-algebra with identity $\delta(x, y)$, which is defined by $\delta(x, y) = 1$ if $x = y$ and $\delta(x, y) = 0$ otherwise.

The zeta function ζ is defined by $\zeta(x, y) = 1$ for all $x \leq y$ in P and $\zeta(x, y) = 0$ otherwise. It is easy to check that this function is invertible. Its inverse is called the *Möbius* function of P and is denoted by μ. We can define μ inductively. Namely, $\mu\zeta = \delta$ is equivalent to

- $\mu(x, x) = 1$, for all $x \in P$;
- $\mu(x, y) = -\sum_{x \leq z < y} \mu(x, z)$ for all $x < y$ in P.

The following inversion lemma is one of the most important tools in combinatorics. We omit the proof since it can be found in many combinatorial books.

Lemma 2.1 (*Möbius* Inversion Formula). *Let $(P, \leq)$ be a finite partially ordered set. Let $f, g : P \to \mathbb{C}$. Then*

$$g(x) = \sum_{x \leq y} f(y), \textit{for all } x \in P$$

if and only if

$$f(x) = \sum_{x \leq y} \mu(x, y)g(y), \textit{for all } x \in P$$

where $\mu(x, y)$ is the Möbius function as defined above.

Let $[k]$ be the set $\{1, 2, \ldots, k\}$. Let Π_k be the set of set partitions of $[k]$. Define a binary relation " $\leq$ " on Π_k as follows: $\tau \leq \delta$ if every block of τ is contained in a block of δ. For instance, $\{1, 2\}\{3, 4\}\{5, 6\} \leq \{1, 2, 3, 4\}\{5, 6\}$ and $\{1, 3\}\{2\}\{4\}\{5\}\{6\} \leq \{1, 2, 3\}\{4\}\{5, 6\}$. One checks that Π_k is indeed a partially ordered set.

To compute the values of the *Möbius* function μ in Π_k is a very nontrivial and important result in the theory of enumerative combinatorics. We cite it directly without proof. For details please refer to [10].

Lemma 2.2. *Denote 1 to be the smallest element in Π_k. For any $\tau \in \Pi_k$, let l be the number of blocks in τ and let $n_1, n_2, \ldots, n_l$ be the cardinality of each block of τ, then we have*

$$\mu(1, \tau) = \prod_{i=1}^{l} (-1)^{n_i - 1}(n_i - 1)!.$$

Now we will prove our new formula via this inversion formula.

Theorem 2.3. *Let $\overline{X}, X_\tau$ be defined as in (2.1) and (2.2). Then we have*

$$|\overline{X}| = \sum_{\tau \in S_k} \operatorname{sign}(\tau)|X_\tau|. \tag{2.3}$$

Furthermore,

$$|\overline{X}| = \sum_{\tau \in \Pi_k} \prod_{i=1}^{l} (-1)^{n_i - 1}(n_i - 1)!|X_\tau|,$$

where $(n_1, n_2, \ldots, n_l)$ *in the summation means the corresponding block sizes of* τ*.*

Proof. We note that for a set partition $\tau \in \Pi_k$ we can define X_τ similarly or even more naturally. For any $\tau \in \Pi_k$, define X_τ° to be the set of vectors $x \in X_\tau$ such that there does not exist $\delta \in \Pi_k$ satisfying $\tau < \delta$ and $x \in X_\delta$. Recall that $\tau < \delta$ if $\tau \leq \delta$ and $\tau \neq \delta$.

It is easy to check that

$$|X_\delta| = \sum_{\delta \leq \tau} |X_\tau^\circ|,$$

and thus by the *Möbius* Inversion Formula given in Lemma 2.1 we have

$$|X_\delta^\circ| = \sum_{\delta \leq \tau} \mu(\delta, \tau)|X_\tau|.$$

In particular, let $\delta = 1 = \{1\}\{2\}\cdots\{k\}$, then X_1° is just $\overline{X}$, which was defined as above to be the set of distinct coordinate vectors in X. Thus we have

$$\begin{aligned}
|\overline{X}| &= \sum_{1 \leq \tau} \mu(1, \tau)|X_\tau| \\
&= \sum_{\tau \in \Pi_k} \mu(1, \tau)|X_\tau| \\
&= \sum_{\tau \in \Pi_k : (n_1, n_2, \ldots, n_l)} \prod_{i=1}^{l} (-1)^{n_i - 1}(n_i - 1)!|X_\tau| \\
&= \sum_{\tau \in S_k} \operatorname{sign}(\tau)|X_\tau|.
\end{aligned}$$

The last equality comes from an elementary counting on the number of permutations for a given set partition of $[n]$. □

Remark: We remark that conversely we can prove Lemma 2.2 by our formula (2.3) in a very simple way.

Now the symmetric group S_k acts on D^k by permuting coordinates. That is, for given $\tau \in S_k$ and $x = (x_1, x_2, \ldots, x_k) \in D^k$, we have

$$\tau \circ x = (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)}).$$

Before stating a useful corollary, we first give a definition.

Definition 2.4. *Let* G *be a subgroup of* S_k*. A subset* $X \subset D^k$ *is said to be* G*-symmetric if for any* $x \in X$ *and any* $g \in G$*,* $g \circ x \in X$*. In particular, a* S_k*-symmetric* X *is simply called symmetric. Furthermore, if* X *satisfies the "strongly symmetric" condition, that is, for any* τ *and* τ' *in* S_k*, one has* $|X_\tau| = |X_{\tau'}|$ *provided* $l(\tau) = l(\tau')$*, then we call* X *a strongly symmetric set.*

The signless Stirling number of the first kind $c(k, i)$ is defined to be the number of permutations in S_k with exactly i cycles. Note that $c(k, 0) = 0$. It can also be defined by the following classic equality [10]:

$$\sum_{i=0}^{k}(-1)^{k-i}c(k,i)q^i = (q)_k, \tag{2.4}$$

where $(x)_k = x(x-1)\cdots(x-k+1)$ for $k \in \mathbb{Z}^+ = \{1,2,3,\dots\}$ and $(x)_0 = 1$.

It is immediate to get the following simpler formula in the symmetric case.

Corollary 2.5. *Let C_k be the set of conjugacy classes of S_k. If X is symmetric, then*

$$|\overline{X}| = \sum_{\tau \in C_k}(-1)^{k-l(\tau)}C(\tau)|X_\tau|, \tag{2.5}$$

where $C(\tau)$ is the number of permutations conjugate to τ. Furthermore, if X is strongly symmetric, then we have

$$|\overline{X}| = \sum_{i=1}^{k}(-1)^{k-i}c(k,i)|X_i|, \tag{2.6}$$

where X_i is defined as X_{τ_i} for some $\tau_i \in S_k$ with $l(\tau_i) = i$ and $c(k,i)$ is the signless Stirling number of the first kind.

3. Subset sums on cyclic groups

In this paper, we identify an element $b \in \mathbb{Z}_n$ with its least nonnegative integer representative.

Lemma 3.1. *Let $k_1, k_2, \dots, k_l, b$ be elements in $\mathbb{Z}_n$ and $(k_1, k_2, \dots, k_l, n) = d$. Let M be the number of solutions of the following congruence equation over $\mathbb{Z}_n$*

$$k_1x_1 + k_2x_2 + \cdots + k_lx_l \equiv b \mod n.$$

Then $M > 0$ if and only if $d \mid b$. Moreover, if $d \mid b$, then we have $M = dn^{l-1}$. In particular, if $(k_1, k_2, \dots, k_l, n) = 1$, then $M = n^{l-1}$.

Proof. As ideals in $\mathbb{Z}$, we have

$$k_1\mathbb{Z} + \cdots + k_l\mathbb{Z} + n\mathbb{Z} = (k_1, \dots, k_l, n)\mathbb{Z} = d\mathbb{Z}.$$

Thus, $M > 0$ if and only if $d|b$. Assume now that $d|b$. Then, M is the number of solutions of the linear equation

$$\frac{k_1}{d}x_1 + \cdots + \frac{k_l}{d}x_l \equiv \frac{b}{d} \mod \frac{n}{d}$$

in the ring $\mathbb{Z}_n$, which is $(\frac{n}{d})^{l-1}d^l = dn^{l-1}$. This is because each solution in $\mathbb{Z}_{\frac{n}{d}}$ lifts to exactly d^l solutions in $\mathbb{Z}_n$. □

Lemma 3.2. *Let $d \mid k$. Let $TP_k^d(j)$ be the number of permutations in S_k of j cycles with the length of its each cycle divisible by d. Then we have*

$$\sum_{j=1}^{k}(-1)^{k-j}TP_k^d(j)n^j = (-1)^{k+\frac{k}{d}}k!\binom{n/d}{k/d}. \tag{3.1}$$

Proof. A permutation $\tau \in S_k$ is said to be of type $(c_1, c_2, \cdots, c_k)$ if τ has exactly c_i cycles of length i. Let $N(c_1, c_2, \ldots, c_k)$ be the number of permutations in S_k which is of type $(c_1, c_2, \ldots, c_k)$. We have the following counting formula

$$N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1} c_1! 2^{c_2} c_2! \cdots k^{c_k} c_k!}. \tag{3.2}$$

Define the generating function

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum i c_i = k} N(c_1, c_2, \ldots, c_k) t_1^{c_1} t_2^{c_2} \cdots t_k^{c_k}. \tag{3.3}$$

From (3.2), we have

$$C_k(t_1, t_2, \ldots, t_k) = \sum_{\sum i c_i = k} \frac{k!}{c_1! c_2! \cdots c_k!} (\frac{t_1}{1})^{c_1} (\frac{t_2}{2})^{c_2} \cdots (\frac{t_k}{k})^{c_k}.$$

Thus we obtain the following exponential generating function

$$\sum_{k \geq 0} C_k(t_1, t_2, \ldots, t_k) \frac{u^k}{k!} = e^{u t_1 + u^2 \cdot \frac{t_2}{2} + u^3 \cdot \frac{t_3}{3} + \cdots}.$$

Now let $P_k^d(t) = \sum TP_k^d(j) t^j$. By (3.3) we have $P_k^d(t) = C_k(0, 0, \ldots, t, 0, \ldots)$, where t appears at the index divisible by d. For given generating function $f(x)$, we denote $[x^i] f(x)$ to be the coefficient of x^i in the formal power series expansion of $f(x)$. Then we have

$$\begin{aligned} P_k^d(t) &= \left[\frac{u^k}{k!}\right] e^{t\left(\frac{u^d}{d} + \frac{u^{2d}}{2d} + \cdots\right)} \\ &= \left[\frac{u^k}{k!}\right] e^{-\frac{t}{d} \log\left(1 - u^d\right)} \\ &= \left[\frac{u^k}{k!}\right] \frac{1}{(1 - u^d)^{t/d}} \\ &= \left[\frac{u^k}{k!}\right] \sum_{j \geq 0} \binom{j + t/d - 1}{j} (u^d)^j \\ &= k! \binom{k/d + t/d - 1}{k/d}. \end{aligned}$$

It is direct to check that

$$(-1)^k P_k^d(-n) = (-1)^{k + \frac{k}{d}} k! \binom{n/d}{k/d},$$

by the following equality for all integers k

$$\binom{r}{k} = (-1)^k \binom{k - r - 1}{k}.$$

Thus (3.1) follows from

$$\sum_{j=1}^{k} (-1)^{k-j} TP_k^d(j) n^j = (-1)^k P_k^d(-n)$$

and the proof is complete. □

Lemma 3.3. *Let d, r, n, b be nonnegative integers. If $r \nmid n$ then we have*

$$\sum_{d|r,(n,d)|b} (n,d)\mu(r/d) = 0.$$

Proof. Since $r \nmid n$, there is a prime p such that $\mathrm{ord}_p r = s > 0$ and $\mathrm{ord}_p n = t < s$. By the definition of the *Möbius* function, if $\mathrm{ord}_p(r/d) > 1$ then $\mu(r/d) = 0$. Thus we have

$$\begin{aligned}\sum_{d|r,(n,d)|b} (n,d)\mu(r/d) &= \sum_{\substack{d|r,(n,d)|b \\ \mathrm{ord}_p d = s}} (n,d)\mu(r/d) + \sum_{\substack{d|r,(n,d)|b \\ \mathrm{ord}_p d = s-1}} (n,d)\mu(r/d) \\ &= \sum_{\substack{d|r,(n,dp)|b \\ \mathrm{ord}_p d = s-1}} (n,dp)\mu(r/dp) + \sum_{\substack{d|r,(n,d)|b \\ \mathrm{ord}_p d = s-1}} (n,d)\mu(r/d) \\ &= -\sum_{\substack{d|r,(n,d)|b \\ \mathrm{ord}_p d = s-1}} (n,d)\mu(r/d) + \sum_{\substack{d|r,(n,d)|b \\ \mathrm{ord}_p d = s-1}} (n,d)\mu(r/d) \\ &= 0.\end{aligned}$$

□

First we prove our main result in the cyclic case.

Theorem 3.4. *Given $b \in \mathbb{Z}_n$ and $1 \leq k \leq n$. Let $N(k,b)$ be the number of k-subsets of $\mathbb{Z}_n$ whose elements sum to b. Then we have*

$$N(k,b) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d|(r,b)} \mu(r/d)d.$$

In particular,

$$N(k,0) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \phi(r) \binom{n/r}{k/r},$$

where ϕ is the Euler totient function.

Proof. Let X be the number of solutions of the equation $x_1 + x_2 + \cdots + x_k = b$ in $\mathbb{Z}_n$. Since X is symmetric, by applying Corollary 2.5 we have

$$k! \cdot N(k,b) = |\overline{X}| = \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau)|X_\tau|, \tag{3.4}$$

where X_τ is defined as in (2.2).

Since $x_1 + x_2 + \cdots + x_k = b$ is linear, by Lemma 3.1 it is easy to check that when $(n,k) = 1$ we always have $|X_\tau| = n^{l(\tau)-1}$, where $l(\tau)$ is the number of cycles of τ. Thus, when $(n,k) = 1$, X is strongly symmetric and we conclude

$$\begin{aligned}N(k,b) &= \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i)|X_i| = \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i) n^{i-1} \\ &= \frac{1}{n}\frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k,i) n^i = \frac{1}{n}\frac{1}{k!}(n)_k = \frac{1}{n}\binom{n}{k}.\end{aligned}$$

Now, we consider the general case. For each $d \mid k$ we denote TP_k^d to be the conjugacy classes in C_k whose each cycle length is divisible by d. Let CP_k^d to be the conjugacy classes in C_k such that the greatest common divisor of the cycle length equals d. Since $TP_k^d = \sum_{d|r} CP_k^r$. By the *Möbius* Inversion Formula we have

$$CP_k^d = \sum_{d|r} \mu(r/d) TP_k^r = \sum_{d|r|k} \mu(r/d) TP_k^r,$$

where μ is the usual *Möbius* function defined over the integers. Note that for given $\tau \in CP_k^d$, if $(n,d) \nmid b$ then $|X_\tau| = 0$ and otherwise by Lemma 3.1 we have $|X_\tau| = (n,d) n^{l(\tau)-1}$, where (n,d) is the greatest common divisor of n and d. Thus by (3.4) we have

$$\begin{aligned} k! \cdot N(k,b) &= \sum_{\tau \in C_k} (-1)^{k-l(\tau)} C(\tau) |X_\tau| \\ &= \sum_{d|k} \sum_{\tau \in CP_k^d} (-1)^{k-l(\tau)} C(\tau) |X_\tau| \\ &= \sum_{d|k,(n,d)|b} \sum_{\tau \in CP_k^d} (-1)^{k-l(\tau)} C(\tau)(n,d) n^{l(\tau)-1}. \end{aligned}$$

For given d, denote by $TP_k^d(j)$ and $CP_k^d(j)$, the number of permutations in TP_k^d and CP_k^d respectively with j cycles. If $d \mid k$ and $(n,d) \mid b$, then

$$\begin{aligned} \sum_{\tau \in CP_k^d} (-1)^{k-l(\tau)} C(\tau)(n,d) n^{l(\tau)-1} &= \sum_{j=1}^{k} (-1)^{k-j} CP_k^d(j)(n,d) n^{j-1} \\ &= \frac{(n,d)}{n} \sum_{j=1}^{k} (-1)^{k-j} \sum_{d|r|k} \mu(r/d) TP_k^r(j) n^j \\ &= \frac{(n,d)}{n} \sum_{d|r|k} \mu(r/d) \sum_{j=1}^{k} (-1)^{k-j} TP_k^r(j) n^j \\ &= \frac{(n,d)}{n} \sum_{d|r|k} \mu(r/d)(-1)^{k+\frac{k}{r}} k! \binom{n/r}{k/r}. \end{aligned}$$

The last equality comes from Lemma 3.2. Thus we have

$$\begin{aligned} N(k,b) &= \frac{1}{n} \sum_{d|k,(n,d)|b} (n,d) \sum_{d|r|k} \mu(r/d)(-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \\ &= \frac{1}{n} \sum_{r|k} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d|r,(n,d)|b} (n,d) \mu(r/d). \end{aligned}$$

By Lemma 3.3, if $r \nmid n$, then $\sum_{d|r,(n,d)|b} (n,d)\mu(r/d) = 0$. Thus by a substitution d of (n,d) we have

$$N(k,b) = \frac{1}{n} \sum_{r|(n,k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d|(r,b)} \mu(r/d) d$$

We notice that the last summation is exactly the famous Ramanujan's trigonometrical sum $C_r(b)$, which can be also defined as

$$C_r(m) = \sum_{k,(k,r)=1} e^{2\pi ikm/r},$$

and satisfies the equality [9]

$$C_r(m) = \mu(r/(r,m))\frac{\phi(r)}{\phi(r/(r,m))}.$$

Thus we may write the above formula as

$$N(k,b) = \frac{1}{n}\sum_{r|(n,k)} (-1)^{k+\frac{k}{r}}\binom{n/r}{k/r}C_r(b).$$

In particular, when $b = 0$ we have

$$N(k,0) = \frac{1}{n}\sum_{r|(n,k)} (-1)^{k+\frac{k}{r}}\binom{n/r}{k/r}\phi(r). \qquad \square$$

Now let us consider the subset sum problem over $\mathbb{Z}_n$.

Corollary 3.5. *Let $N(b)$ be the number of subsets of $\mathbb{Z}_n$ sum to b. For convenience we regard the empty set as a subset sum to 0. Then we have*

$$N(b) = \frac{1}{n}\sum_{r|n, r \text{ odd}} C_r(b)2^{n/r}.$$

Proof. One checks that the formula for $N(k,b)$ holds when $k = 0$, i.e., corresponding to the empty set. Thus we have

$$\begin{aligned} N(b) = \sum_{k=0}^{n} N(k,b) &= \sum_{k=0}^{n}\frac{1}{n}\sum_{r|(n,k)} (-1)^{k+\frac{k}{r}}\binom{n/r}{k/r}C_r(b) \\ &= \frac{1}{n}\sum_{r|n} C_r(b)\sum_{k=0,r|k}^{n} (-1)^{k+\frac{k}{r}}\binom{n/r}{k/r}. \end{aligned}$$

Note that the last summation vanishes if r is even and otherwise we have

$$\sum_{k=0,r|k}^{n} (-1)^{k+\frac{k}{r}}\binom{n/r}{k/r} = \sum_{l=0}^{n/r}\binom{n/r}{l} = 2^{n/r}.$$

Thus

$$N(b) = \frac{1}{n}\sum_{r|n, r \text{ odd}} C_r(b)2^{n/r}. \quad \square$$

4. Subset sums on finite abelian groups

Now we turn to prove Theorem 1.1. The method is very similar to the proof of the cyclic case.

Proof. Let A be an abelian group of order n. By the structure theory of finite abelian groups we may suppose that $A \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$ with $n_1 \mid n_2 \mid \cdots \mid n_s$ and $n = n_1 n_2 \cdots n_s$. Given $b \in A$ and suppose $b = (b_1, b_2, \ldots, b_s)$. Let $N(k, b)$ be the number of k-subsets of A whose elements sum to b. Let X be the set of solutions of the equation $x_1 + x_2 + \cdots + x_k = b$ in A. Since X is symmetric, by applying Corollary 2.5 we have

$$k! \cdot N(k, b) = \sum_{\tau \in C_k} (-1)^{k - l(\tau)} C(\tau) |X_\tau|, \tag{4.1}$$

where X_τ is defined as in (2.2). Now we turn to computing $|X_\tau|$.

For given $\tau \in S_k$, suppose τ factors into l cycles with lengths $a_1, a_2, \ldots, a_l$ respectively. Then $|X_\tau|$ equals the number of solutions of the linear equation $a_1 x_1 + a_2 x_2 + \cdots + a_l x_l = b$ over A. For any $1 \leq i \leq l$ we write $x_i = (x_{i1}, x_{i2}, \ldots, x_{is})$ and $b = (b_1, b_2, \ldots, b_s)$ where $x_{ij}, b_i \in \mathbb{Z}_{n_i} \forall 1 \leq j \leq s$. Thus for computing $|X_\tau|$ it suffices to consider the system of equations over $\mathbb{Z}_{n_1}, \mathbb{Z}_{n_2}, \ldots, \mathbb{Z}_{n_s}$:

$$a_1 x_{1i} + a_2 x_{2i} + \cdots + a_l x_{li} = b_1 \in \mathbb{Z}_{n_i}, \quad \text{for } i = 1, \ldots, s.$$

Note that we have $\sum_{i=1}^{l} a_i = k$. When $(n, k) = 1$, then $(a_1, \ldots, a_l, n) = 1$ and by Lemma 3.1 we always have

$$|X_\tau| = \prod_{i=1}^{s} (n_i)^{l(\tau) - 1} = n^{l(\tau) - 1},$$

where $l(\tau)$ is the number of cycles of τ. Thus, in the case $(n, k) = 1$, we conclude

$$\begin{aligned} N(k, b) &= \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k, i) |X_i| = \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k, i) n^{i-1} \\ &= \frac{1}{n} \frac{1}{k!} \sum_{i=1}^{k} (-1)^{k-i} c(k, i) n^{i} = \frac{1}{n} \frac{1}{k!} (n)_k = \frac{1}{n} \binom{n}{k}. \end{aligned}$$

For each $d \mid k$ we denote TP_k^d to be the conjugacy classes in C_k whose each cycle length is divisible by d. Let CP_k^d to be the conjugacy classes in C_k such that the greatest common divisor of the cycle length equals d. Let (n, d) be the greatest common divisor of n and d. One checks that

$$CP_k^d = \sum_{d \mid r \mid k} \mu(r/d) TP_k^r,$$

where μ is the usual *Möbius* function. Note that for given $\tau \in CP_k^d$, if there exists i such that $(n_i, d) \nmid b_i$ then $|X_\tau| = 0$ and otherwise we have $|X_\tau| = \prod_{i=1}^{s} (n_i, d) n_i^{l(\tau) - 1}$ by Lemma 3.1. Thus by (4.1) we have

$$\begin{aligned} k! \cdot N(k, b) &= \sum_{\tau \in C_k} (-1)^{k - l(\tau)} C(\tau) |X_\tau| \\ &= \sum_{d \mid k} \sum_{\tau \in CP_k^d} (-1)^{k - l(\tau)} C(\tau) |X_\tau| \\ &= \sum_{d \mid k, (n_i, d) \mid b_i} \sum_{\tau \in CP_k^d} (-1)^{k - l(\tau)} C(\tau) \prod_{i=1}^{s} (n_i, d) n_i^{l(\tau) - 1}. \end{aligned}$$

For given j, denote by $TP_k^d(j)$ and $CP_k^d(j)$, the number of permutations in TP_k^d and CP_k^d respectively with j cycles. If $d \mid k, (n_i, d) \mid b_i$ for any $1 \leq i \leq s$, then we have

$$\begin{aligned}
\sum_{\tau \in CP_k^d} (-1)^{k-l(\tau)} C(\tau) \prod_{i=1}^{s} (n_i, d) n_i^{l(\tau)-1} &= \prod_{i=1}^{s} (n_i, d) \sum_{j=1}^{k} (-1)^{k-j} CP_k^d(j) n^{j-1} \\
&= \frac{\prod_{i=1}^{s} (n_i, d)}{n} \sum_{j=1}^{k} (-1)^{k-j} \sum_{d \mid r \mid k} \mu(r/d) TP_k^r(j) n^{j-1} \\
&= \frac{\prod_{i=1}^{s} (n_i, d)}{n} \sum_{d \mid r \mid k} \mu(r/d) \sum_{j=1}^{k} (-1)^{k-j} TP_k^r(j) n^{j} \\
&= \frac{\prod_{i=1}^{s} (n_i, d)}{n} \sum_{d \mid r \mid k} \mu(r/d) (-1)^{k+\frac{k}{r}} k! \binom{n/r}{k/r}.
\end{aligned}$$

The last equality follows from Lemma 3.2. Thus we have

$$\begin{aligned}
N(k, b) &= \frac{1}{n} \sum_{d \mid k, (n_i, d) \mid b_i} \prod_{i=1}^{s} (n_i, d) \sum_{d \mid r \mid k} \mu(r/d) (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \\
&= \frac{1}{n} \sum_{r \mid k} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d \mid r, (n_i, d) \mid b_i} \mu(r/d) \prod_{i=1}^{s} (n_i, d) \\
&= \frac{1}{n} \sum_{r \mid (n, k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d \mid r, (n_i, d) \mid b_i} \mu(r/d) \prod_{i=1}^{s} (n_i, d)
\end{aligned}$$

The last equality follows by that when $r \nmid n$ we still have

$$\sum_{d \mid r, (n, d) \mid b} \prod_{i=1}^{s} (n_i, d) \mu(r/d) = 0$$

from the proof of Lemma 3.3.

When $b = 0$, that is $b_i = 0$ for all $1 \leq i \leq s$, we always have $(n_i, d) \mid b_i$ and thus

$$N(k, 0) = \frac{1}{n} \sum_{r \mid (n, k)} (-1)^{k+\frac{k}{r}} \binom{n/r}{k/r} \sum_{d \mid r} \mu(r/d) \prod_{i=1}^{s} (n_i, d). \quad \square$$

Corollary 4.1. *Let $N(b)$ be the number of subsets of A sum to b. For convenience we consider the empty set as a subset sum to 0. Let*

$$\Phi(r, b) = \sum_{d \mid r, (n_i, d) \mid b_i} \mu(r/d) \prod_{i=1}^{s} (n_i, d).$$

Then we have

$$N(b) = \frac{1}{n} \sum_{r \mid n, r \text{ odd}} \Phi(r, b) 2^{n/r}.$$

Proof. The proof is similar to that of Corollary 3.5. □

When A is an elementary abelian p-group we have the following simpler formula.

Corollary 4.2. *Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let A be any additive subgroup of $\mathbb{F}_q$ and $|A| = n$. For any $b \in A$, denote $N(k,b)$ to be the number of k-subsets of A whose elements sum to b. Define $v(b) = -1$ if $b \neq 0$, and $v(b) = n-1$ if $b = 0$. If $p \nmid k$, then*

$$N(k,b) = \frac{1}{n}\binom{n}{k}.$$

If $p \mid k$, then

$$N(k,b) = \frac{1}{n}\binom{n}{k} + (-1)^{k+\frac{k}{p}}\frac{v(b)}{n}\binom{n/p}{k/p}.$$

Proof. Since in this case we have $n = p^t$ and $n_i = p$, $b = (b_1, b_2, \dots, b_t)$. It follows from the formula given by Theorem 1.1 that when $p \nmid k$, then $(n,k) = 1$ and

$$N(k,b) = \frac{1}{n}\binom{n}{k}\sum_{d|1,(p,d)|b_i}\mu(1/d)\prod_{i=1}^{s}(p,d) = \frac{1}{n}\binom{n}{k}.$$

When $p \mid k$, assuming that $k = k_0 p^{t_0}$ and $(p, k_0) = 1$ we have

$$\begin{aligned} N(k,b) &= \frac{1}{n}\sum_{r|p^{t_0}}(-1)^{k+\frac{k}{r}}\binom{n/r}{k/r}\sum_{d|r,(p,d)|b_i}\mu(r/d)\prod_{i=1}^{s}(p,d) \\ &= \frac{1}{n}\binom{n}{k} + (-1)^{k+\frac{k}{p}}\frac{1}{n}\binom{n/p}{k/p}\sum_{d|p,(p,d)|b_i}\mu(p/d)\prod_{i=1}^{s}(p,d). \end{aligned}$$

If $b = 0$ then $b_i = 0$ for $1 \leq i \leq t$ then

$$N(k,0) = \frac{1}{n}\binom{n}{k} + (-1)^{k+\frac{k}{p}}\frac{1}{n}\binom{n/p}{k/p}(n-1).$$

If $b \neq 0$ then there is some i such that $b_i \neq 0$ and since $(b_i, p) = 1$ we can only take $d = 1$ in the summation. Thus

$$N(k,b) = \frac{1}{n}\binom{n}{k} - (-1)^{k+\frac{k}{p}}\frac{1}{n}\binom{n/p}{k/p}.$$ □

When $A = \mathbb{F}_q$, the formula was first found by the authors in [5].

References

[1] Q. Cheng, *Hard problems of algebraic geometry codes*, IEEE Trans. & Inform Theory, 2008, 54(1), 402–406.

[2] Q. Cheng and E. Murray, *On deciding deep holes of Reed-Solomon codes*, In: TAMS 2007, Lecture Notes in Computer Science, Vol. 4484, Springer, 2007.

[3] T.H. Cormen, C.E. Leiserson, R.L. Rivest and C. Stein, *Introduction to Algorithms*, MIT Press and McGraw-Hill, 2001.

[4] R.L. Graham, D.E. Knuth and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed. Reading, MA: Addison-Wesley, 1994.

[5] Jiyou Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields & Applications, 14 (2008), 911–929.

[6] Jiyou Li and D. Wan, *A new sieve for distinct coordinate counting*, Science in China Series A, 53 (2010), 2351–2362.

[7] Nicol C. A., *Linear congruences and the Von Stemeck function*, Duke Math. J., 26 (1959), 193–197.

[8] A.M. Odlyzko and R.P. Stanley, *Enumeration of power sums modulo a prime*, J. Number Theory, 10 (1978), no. 2, 263–272.

[9] Ramanathan K. G., *Some applications of Ramanujan's trigonometrical sum $C_m(n)$*, Proceedings of the Indian Academy of Sciences, vol. 20 (1945), 62–69.

[10] R.P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge University Press, Cambridge, 1997.

Department of Mathematics, Shanghai Jiao Tong University, Shanghai, P.R. China
E-mail address: lijiyou@sjtu.edu.cn

Department of Mathematics, University of California, Irvine, CA 92697-3875, USA
E-mail address: dwan@math.uci.edu