On a permutation problem for finite abelian groups

Fan Ge

Department of Mathematics
University of Rochester
Rochester, NY-14627, USA

fange.math@gmail.com

Zhi-Wei Sun*

Department of Mathematics
Nanjing University
210093, People's Republic of China

zwsun@nju.edu.cn

Submitted: Feb 4, 2016; Accepted: Jan 19, 2017; Published: Feb 3, 2017
Mathematics Subject Classifications: 05E15, 11B75, 11A07, 11P70, 20K01.

Abstract

Let G be a finite additive abelian group with exponent $n > 1$, and let $a_1, \ldots, a_{n-1}$ be elements of G. We show that there is a permutation $\sigma \in S_{n-1}$ such that all the elements $sa_{\sigma(s)}$ $(s = 1, \ldots, n-1)$ are nonzero if and only if

$$\left|\left\{1 \leqslant s < n : \frac{n}{d}a_s \neq 0\right\}\right| \geqslant d - 1 \text{ for every positive divisor } d \text{ of } n.$$

When G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, this confirms a conjecture of Z.-W. Sun.

Keywords: combinatorial number theory; abelian group; permutation; subset sum.

1 Introduction

Let $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ and let S_n denote the symmetry group of all permutations on $\{1, \ldots, n\}$. A conjecture of G. Cramer stated that for any integers $m_1, \ldots, m_n$ with $\sum_{s=1}^n m_s \equiv 0 \pmod n$ there is a permutation $\sigma \in S_n$ such that $1+m_{\sigma(1)}, \ldots, n+m_{\sigma(n)}$ are pairwise distinct modulo n. In 1952 M. Hall [2] proved an extension of this conjecture.

In 1999 H. S. Snevily [4] conjectured that if $n > 1$ is an integer and $m_1, \ldots, m_k$ are integers with $k \leqslant n-1$ then there is a permutation $\sigma \in S_k$ such that $1+m_{\sigma(1)}, \ldots, k+m_{\sigma(k)}$ are pairwise distinct modulo n. This was confirmed by A. E. Kézdy and Snevily [3] in the case $k \leqslant (n+1)/2$, and an application to tree embeddings was also given in [3].

Let $n > 1$ and $m_1, \ldots, m_{n-1}$ be integers. When is there a permutation $\sigma \in S_{n-1}$ such that none of the $n-1$ numbers $sm_{\sigma(s)}$ $(s = 1, \ldots, n-1)$ is congruent to 0 modulo n? If there is such a permutation σ, then for each positive divisor d of n we have

$$|\{1 \leqslant c < d : d \nmid m_{\sigma(cn/d)}\}| \geqslant \left|\left\{1 \leqslant c < d : n \nmid \frac{cn}{d}m_{\sigma(cn/d)}\right\}\right| = d - 1,$$

*Supported by the National Natural Science Foundation (grant 11571162) of China.

and hence the sequence $\{m_s\}_{s=1}^{n-1}$ has the following property:

$$\left|\{1 \leqslant s < n : \ d \nmid m_s\}\right| \geqslant d-1 \ \text{ for any } d \in D(n), \tag{1}$$

where $D(n)$ denotes the set of all positive divisors of n.

In 2004 the second author (cf. [7]) made the following conjecture.

Conjecture 1. (Z.-W. Sun) Let $n > 1$ be an integer. If $m_1, m_2, \ldots, m_{n-1}$ are integers satisfying (1), then there exists a permutation σ on $\{1, \ldots, n-1\}$ such that $n \nmid sm_{\sigma(s)}$ for all $s = 1, \ldots, n-1$.

In this paper we aim to prove an extension of this conjecture for finite abelian groups.

For a finite multiplicative group G, its exponent $\exp(G)$ is defined to be the least positive integer such that $x^n = e$ for all $x \in G$, where e is the identity of G. For a finite abelian group G, $\exp(G)$ is known to be $\max\{o(x) : \ x \in G\}$, where $o(x)$ denotes the order of x. If G is an additive group, then for $k \in \mathbb{Z}^+$ and $a \in G$ we write ka for the sum $a_1 + \ldots + a_k$ with $a_1 = \cdots = a_k = a$.

Theorem 2. *Let G be a finite additive abelian group with exponent $n > 1$. For any $a_1, \ldots, a_{n-1} \in G$, there is a permutation $\sigma \in S_{n-1}$ such that all the elements $sa_{\sigma(s)}$ ($s = 1, \ldots, n-1$) are nonzero if and only if*

$$\left|\left\{1 \leqslant s < n : \ \frac{n}{d}a_s \neq 0\right\}\right| \geqslant d-1 \ \ \textit{for all } d \in D(n). \tag{2}$$

Applying Theorem 2 to the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we immediately confirm Conjecture 1 of Sun. As an application, we obtain the following result.

Theorem 3. *Let $m_1, m_2, \ldots, m_{n-1}$ ($n > 1$) be integers satisfying* (1)*. Then the set*

$$\left\{\sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\}\right\}$$

contains a complete system of residues modulo n.

Obviously Theorem 3 extends the following result of the second author (cf. the paragraph following [6, Theorem 2.5]).

Corollary 4. *Let $n > 1$ be an integer and let $m_1, m_2, \ldots, m_{n-1}$ be integers all relatively prime to n. Then the set $\left\{\sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\}\right\}$ contains a complete system of residues modulo n.*

As usual, for any $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, we write (a, n) for the greatest common divisor of a and n.

Let $n > 1$ be an integer. If $m_s \in \mathbb{Z}$ and $(m_s, n) \leqslant s$ for all $s = 1, \ldots, n-1$, then for any $d \in D(n)$ we have

$$|\{1 \leqslant s < n : \ d \nmid m_s\}| \geqslant |\{1 \leqslant s < n : \ s < d\}| = d-1,$$

and hence by Theorem 2 for some $\sigma \in S_{n-1}$ we have $n \nmid \sigma(s)m_s$ for all $s = 1, \ldots, n-1$. This is equivalent to the following theorem in the case $a_1 = \cdots = a_{n-1}$.

Theorem 5. *Let $m_1, m_2, \ldots, m_{n-1}$ $(n > 1)$ be integers with $(m_s, n) \leqslant s$ for all $s = 1, \ldots, n-1$. For any $a_1, \ldots, a_{n-1} \in \mathbb{Z}$, there is a function $f : \{1, \ldots, n-1\} \to \{1, \ldots, n-1\}$ such that the sums*

$$f(1) + a_1,\ \ldots,\ f(n-1) + a_{n-1}$$

are pairwise distinct modulo n and also none of the numbers

$$f(1)m_1,\ \ldots,\ f(n-1)m_{n-1}$$

is divisible by n.

Motivated by Theorems 2 and 3, we pose the following conjecture.

Conjecture 6. Let G be a finite abelian group with exponent $n > 1$. If $a_1, \ldots, a_{n-1}$ are elements of G with $sa_s \neq 0$ for all $s = 1, \ldots, n-1$, then we have

$$\left| \left\{ \sum_{i \in I} a_i :\ I \subseteq \{1, \ldots, n-1\} \right\} \right| \geqslant n. \tag{3}$$

By Theorems 2 and 3, this conjecture holds for finite cyclic groups. For any finite abelian group G with exponent $n > 1$, it has a cyclic subgroup H of order n, and hence for $a_1, \ldots, a_{n-1} \in H$ the set $\{\sum_{i \in I} a_i :\ I \subseteq \{1, \ldots, n-1\}\}$ contains at most n elements of G.

We will prove Theorem 2 in the next section and Theorems 3 and 5 in Section 3.

2 Proof of Theorem 2

Proof of Necessity. If there is a permutation $\sigma \in S_{n-1}$ such that $sa_{\sigma(s)} \neq 0$ for all $s = 1, \ldots, n-1$, then for any $d \in D(n)$ we have

$$\left| \left\{ 1 \leqslant s < n :\ \frac{n}{d} a_s \neq 0 \right\} \right| \geqslant \left| \left\{ 1 \leqslant c < d :\ \frac{cn}{d} a_{\sigma(cn/d)} \neq 0 \right\} \right| = d - 1.$$

This concludes the proof of the necessity. □

Proof of Sufficiency. Suppose, to the contrary, that there are $a_1, \ldots, a_{n-1} \in G$ satisfying (2) such that the set

$$I(\sigma) := \{1 \leqslant i < n : ia_{\sigma(i)} = 0\} = \{1 \leqslant i < n : o(a_{\sigma(i)}) \mid i\}$$

is nonempty for any $\sigma \in S_{n-1}$. Take such $a_1, \ldots, a_{n-1} \in G$ with $\sum_{s=1}^{n-1} o(a_s)$ maximum, and choose $\sigma \in S_{n-1}$ with $|I(\sigma)|$ minimum.

Claim 1: $|I(\sigma)| = 1$.

As $n = \exp(G)$, there is an element x of G with $o(x) = n$. Let $j \in I(\sigma)$, and for $s = 1, \ldots, n-1$ define

$$a_s^* = \begin{cases} x & \text{if } s = \sigma(j), \\ a_s & \text{otherwise.} \end{cases}$$

If $(n/d)a_{\sigma(j)} \neq 0$ with $d \in D(n)$, then $d > 1$ and $(n/d)x \neq 0$. As $o(a_{\sigma(j)}) \mid j$, we have $o(a_{\sigma(j)}) \leqslant j < n = o(x)$. Since $\sum_{s=1}^{n-1} o(a_s^*) > \sum_{s=1}^{n-1} o(a_s)$, by our choice of $a_1, \ldots, a_{n-1}$, for some $\tau \in S_{n-1}$ we have $sa^*_{\tau(s)} \neq 0$ for all $s = 1, \ldots, n-1$. For any $1 \leqslant s < n$ with $\tau(s) \neq \sigma(j)$, we have $sa_{\tau(s)} = sa^*_{\tau(s)} \neq 0$. Thus $|I(\tau)| \leqslant 1 \leqslant |I(\sigma)|$. Combining this with the choice of σ, we have proved Claim 1.

For $\pi \in S_{n-1}$ with $|I(\pi)| = 1$, by i_π we denote the unique element of $I(\pi)$. Without loss of generality, below we assume that

$$i_\sigma = \min\{i_\pi : \ \pi \in S_{n-1} \text{ and } |I(\pi)| = 1\}. \tag{4}$$

For simplicity, now we just write i for i_σ. As $o(a_{\sigma(i)})$ divides both i and $n = \exp(G)$, we have $o(a_{\sigma(i)}) \mid i_n$, where $i_n = (i, n)$.

Claim 2: $i \mid n$.

Suppose that $i \nmid n$. Then $i_n \neq i$, $i_n \notin I(\sigma)$ and hence $0 \neq i_n a_{\sigma(i_n)}$. Thus $o(a_{\sigma(i_n)}) \nmid i_n$ and hence $o(a_{\sigma(i_n)}) \nmid i$. Therefore

$$ia_{\sigma*(ii_n)(i)} = ia_{\sigma(i_n)} \neq 0 \ \text{ and } \ i_n a_{\sigma*(ii_n)(i_n)} = i_n a_{\sigma(i)} = 0,$$

where $*$ is the multiplication in S_{n-1} and thus $\sigma * (ii_n)$ is the product of σ and the cyclic permutation (ii_n). So we get $|I(\sigma * (ii_n))| = 1$ and $i_{\sigma*(ii_n)} = i_n < i = i_\sigma$, which contradicts (4). This proves Claim 2.

Claim 3: If $1 \leqslant j < n$ and $o(a_{\sigma(j)}) \nmid i$, then $i < j$ and $i \mid j$.

Assume that $1 \leqslant j < n$ and $o(a_{\sigma(j)}) \nmid i$. Then $j \neq i$ since $o(a_{\sigma(i)}) \mid i$. For any $s = 1, \ldots, n-1$ with $s \neq i, j$, we have

$$sa_{\sigma*(ij)(s)} = sa_{\sigma(s)} \neq 0.$$

Also, $ia_{\sigma*(ij)(i)} = ia_{\sigma(j)} \neq 0$ since $o(a_{\sigma(j)}) \nmid i$. As $|I(\sigma * (ij))| \geqslant |I(\sigma)| = 1$, we must have $0 = ja_{\sigma*(ij)(j)} = ja_{\sigma(i)}$, i.e., $o(a_{\sigma(i)}) \mid j$. Since $I(\sigma*(ij)) = \{j\}$, we have $j = i_{\sigma*(ij)} > i = i_\sigma$.

Suppose that j is not divisible by i. Then $k := (i, j) < i$ and hence $ka_{\sigma(k)} \neq 0$ as $I(\sigma) = \{i\}$. By the last paragraph, we must have $o(a_{\sigma(k)}) \mid i$ since $k \not> i$. For any $s = 1, \ldots, n-1$ with $s \neq i, j, k$, we have $sa_{\sigma*(kij)(s)} = sa_{\sigma(s)} \neq 0$. Note that $ia_{\sigma*(kij)(i)} = ia_{\sigma(j)} \neq 0$. If $0 \neq ja_{\sigma(k)} = ja_{\sigma*(kij)(j)}$, then we must have $I(\sigma * (kij)) = \{k\}$ and hence $i_{\sigma*(kij)} = k < i = i_\sigma$ which leads to a contradiction. Therefore, $0 = ja_{\sigma(k)}$, i.e., $o(a_{\sigma(k)}) \mid j$. Since $o(a_{\sigma(k)})$ also divides i, the number $o(a_{\sigma(k)})$ must divide $(i, j) = k$, which contradicts the fact that $ka_{\sigma(k)} \neq 0$. This proves Claim 3.

In light of Claims 2 and 3, we have $i \in D(n)$ and

$$\begin{aligned} |\{1 \leqslant s < n : \ o(a_s) \nmid i\}| =& |\{1 \leqslant j < n : \ o(a_{\sigma(j)}) \nmid i\}| \\ \leqslant& |\{i < j < n : \ i \mid j\}| = \frac{n}{i} - 2. \end{aligned}$$

Hence, for $d = n/i \in D(n)$, we have

$$\left|\left\{1 \leqslant s < n : \ \frac{n}{d} a_s \neq 0\right\}\right| < d - 1,$$

which contradicts our condition (2). This proves the sufficiency. $\square$

3 Proofs of Theorems 3 and 5

For a real number x, we let $\{x\} = x - \lfloor x \rfloor$ be its fractional part. For any real numbers α and β, we set $\alpha + \beta\mathbb{Z} = \{\alpha + \beta q : \ q \in \mathbb{Z}\}$.

We need the following result of the second author [5, Theorem 1].

Lemma 7. *Let $\alpha_1, \ldots, \alpha_k$ be real numbers and let $\beta_1, \ldots, \beta_k$ be positive reals. If $A = \{\alpha_s + \beta_s\mathbb{Z}\}_{s=1}^k$ covers consecutive*

$$\left|\left\{\left\{\sum_{s\in I}\frac{1}{\beta_s}\right\} : \ I \subseteq \{1, \ldots, k\}\right\}\right|$$

integers, then it covers all the integers.

Proof of Theorem 3. Without loss of generality, we simply assume that $m_1, \ldots, m_{n-1} \in \{1, \ldots, n\}$. Because Conjecture 1 follows from Theorem 2, for some $\sigma \in S_{n-1}$ we have $n \nmid sm_{\sigma(s)}$ for all $s = 1, \ldots, n-1$. Note that $A = \{s + (n/m_{\sigma(s)})\mathbb{Z}\}_{s=1}^{n-1}$ covers $1, \ldots, n-1$ but it does not cover 0. By Lemma 7, the fractional parts

$$\left\{\sum_{s\in I}\frac{1}{n/m_{\sigma(s)}}\right\} \quad (I \subseteq \{1, \ldots, n-1\})$$

must have more than $n-1$ distinct values. Thus, the set

$$\left\{\sum_{i\in I} m_i : \ I \subseteq \{1, \ldots, n-1\}\right\} = \left\{\sum_{s\in I} m_{\sigma(s)} : \ I \subseteq \{1, \ldots, n-1\}\right\}$$

contains a complete system of residues modulo n. This concludes our proof. $\square$

To prove Theorem 5, we need the following lemma.

Lemma 8. (Alon's Combinatorial Nullstellensatz [1]) *Let $A_1, \ldots, A_n$ be finite subsets of a field F with $|A_i| > k_i$ for $i = 1, \ldots, n$ where $k_1, \ldots, k_n$ are nonnegative integers. If the coefficient of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ in $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ is nonzero and $k_1 + \cdots + k_n$ is the total degree of P, then there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.*

Proof of Theorem 5. Let p be the smallest prime not dividing n. By Euler's theorem, $p^{\varphi(n)} \equiv 1 \pmod{n}$, where φ denotes Euler's totient function. Let us consider the finite field $\mathbb{F}_q$ with $q = p^{\varphi(n)}$. As $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$, and n is a divisor of $q-1$, there is an element $g \in \mathbb{F}_q^*$ of order n. For $i = 1, \ldots, n-1$ define

$$A_i := \{g^k : \ 1 \leqslant k \leqslant n-1 \text{ and } (g^k)^{m_i} \neq 1\}.$$

Then $|A_i| = n - (m_i, n) \geqslant n - i$ for all $i = 1, \ldots, n-1$. For the polynomial

$$P(x_1, \ldots, x_{n-1}) := \prod_{1\leqslant i<j\leqslant n-1} (g^{a_i}x_i - g^{a_j}x_j),$$

we clearly have

$$\begin{aligned} P(x_1,\dots,x_{n-1}) &= \det\left|(g^{a_i}x_i)^{j-1}\right|_{1\leqslant i,j\leqslant n-1} \\ &= \sum_{\sigma\in S_{n-1}} \operatorname{sign}(\sigma)\prod_{i=1}^{n-1}(g^{a_i}x_i)^{\sigma(i)-1}, \end{aligned}$$

where $\operatorname{sign}(\sigma)$, the sign of σ, takes 1 or -1 according as the permutation σ is even or odd. Choose $\sigma_0\in S_{n-1}$ with $\sigma_0(i)=n-i$ for all $i=1,\dots,n-1$. Then the coefficient of the monomial $\prod_{i=1}^{n-1}x_i^{n-1-i}$ in $P(x_1,\dots,x_{n-1})$ coincides with

$$\operatorname{sign}(\sigma_0)\prod_{i=1}^{n-1}(g^{a_i})^{n-i-1}\neq 0,$$

and $\deg P=\binom{n-1}{2}=\sum_{i=1}^{n-1}(n-1-i)$. In view of Lemma 8, there are $x_1\in A_1,\dots,x_{n-1}\in A_{n-1}$ such that $P(x_1,\dots,x_{n-1})\neq 0$.

Write $x_i=g^{f(i)}$ for all $i=1,\dots,n-1$, where $f(i)\in\{1,\dots,n-1\}$. If $1\leqslant i<j\leqslant n-1$, then $g^{a_i+f(i)}=g^{a_i}x_i\neq g^{a_j}x_j=g^{a_j+f(j)}$ and hence

$$f(i)+a_i\not\equiv f(j)+a_j \pmod n.$$

For each $i=1,\dots,n-1$, as $(g^{f(i)})^{m_i}\neq 1$ we have $n\nmid f(i)m_i$. This completes the proof of Theorem 5. $\square$

Acknowledgement

The authors would like to thank the referee for helpful comments.

References

[1] N. Alon. Combinatorial Nullstellensatz. *Combin. Probab. Comput.*, 8:7–29, 1999.

[2] M. Hall. A combinatorial problem on abelian groups. *Proc. Amer. Math. Soc.*, 3:584–587. 1952.

[3] A. E. Kézdy, and H. S. Snevily. Distinct sums modulo n and tree embeddings. *Combin. Probab. Comput.*, 11:35–42, 2002.

[4] H. S. Snevily. The Cayley addition table of $\mathbb{Z}_n$. *Amer. Math. Monthly*, 106:584–585, 1999.

[5] Z.-W. Sun. Covering the integers by arithmetic sequences. *Acta Arith.*, 72:109–129, 1995.

[6] Z.-W. Sun. Unification of zero-sum problems, subset sums and covers of $\mathbb{Z}$. *Electron. Res. Announc. Amer. Math. Soc.*, 9:51–60, 2003.

[7] Z.-W. Sun. A new conjecture in combinatorial number theory. *Message to Number Theory Mailing List*, November 9, 2009. Available from the website http://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;3c0f47f6.0911