J. Algebraic Combin. 54 (2021), 893–912.

ON PERMUTATIONS OF $\{1,\ldots,n\}$ AND RELATED TOPICS

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

Abstract. In this paper we study combinatorial aspects of permutations of $\{1,\ldots,n\}$ and related topics. In particular, we prove that there is a unique permutation π of $\{1,\ldots,n\}$ such that all the numbers $k+\pi(k)$ $(k=1,\ldots,n)$ are powers of two. We also show that $n \mid \mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}$ for any integer $n>2$. We conjecture that if a group G contains no element of order among $2,\ldots,n+1$ then any $A\subseteq G$ with $|A|=n$ can be written as $\{a_1,\ldots,a_n\}$ with $a_1,a_2^2,\ldots,a_n^n$ pairwise distinct. This conjecture is confirmed when G is a torsion-free abelian group. We also prove that for any finite subset A of a torsion-free abelian group G with $|A|=n>3$, there is a numbering $a_1,\ldots,a_n$ of all the elements of A such that all the n sums

$$a_1+a_2+a_3,\ a_2+a_3+a_4,\ \ldots,\ a_{n-2}+a_{n-1}+a_n,\ a_{n-1}+a_n+a_1,\ a_n+a_1+a_2$$

are pairwise distinct, and conjecture that this remains valid if G is cyclic.

1. Introduction

As usual, for $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$ we let S_n denote the symmetric group of all the permutation of $\{1,\ldots,n\}$.

Let $A=[a_{ij}]_{1\leqslant i,j\leqslant n}$ be a $(0,1)$-matrix (i.e., $a_{ij}\in\{0,1\}$ for all $i,j=1,\ldots,n$). Then the permanent of A given by

$$\mathrm{per}(A)=\sum_{\pi\in S_n}a_{1\pi(1)}\cdots a_{n\pi(n)}$$

is just the number of permutations $\pi\in S_n$ with $a_{k\pi(k)}=1$ for all $k=1,\ldots,n$.

In 2002, B. Cloitre proposed the sequence [Cl, A073364] on OEIS whose n-th term $a(n)$ is the number of permutations $\pi\in S_n$ with $k+\pi(k)$ prime for all $k=1,\ldots,n$. Clearly, $a(n)=\mathrm{per}(A)$, where A is a matrix of order n whose

---

2020 *Mathematics Subject Classification.* Primary 05A05, 11B75; Secondary 11B13, 11B39, 20D60.

Keywords. Additive combinatorics, permutations, powers of two, permanents, groups.

Supported by the National Natural Science Foundation of China (grant no. 11971222).

(i,j)-entry $(1 \leqslant i,j \leqslant n)$ is 1 or 0 according as $i+j$ is prime or not. In 2018 P. Bradley [Br] proved that $a(n) > 0$ for all $n \in \mathbb{Z}^+$.

Our first theorem is an extension of Bradley's result.

Theorem 1.1. *Let $(a_1, a_2, \dots)$ be an integer sequence with $a_1 = 2$ and $a_k < a_{k+1} \leqslant 2a_k$ for all $k = 1, 2, 3 \dots$. Then, for any positive integer n, there exists a permutation $\pi \in S_n$ with $\pi^2 = I_n$ such that*

$$\{k + \pi(k) : \ k = 1, \dots, n\} \subseteq \{a_1, a_2, \dots\}, \tag{1.1}$$

where I_n is the identity of S_n with $I_n(k) = k$ for all $k = 1, \dots, n$.

Recall that the Fiboncci numbers $F_0, F_1, \dots$ and the Lucas numbers $L_0, L_1, \dots$ are defined by

$$F_0 = 0, \ F_1 = 1, \ \text{and} \ F_{n+1} = F_n + F_{n-1} \ (n = 1, 2, 3, \dots),$$

and

$$L_0 = 2, \ L_1 = 1, \ \text{and} \ L_{n+1} = L_n + L_{n-1} \ (n = 1, 2, 3, \dots).$$

If we apply Theorem 1.1 with the sequence $(a_1, a_2, \dots)$ equal to $(F_3, F_4, \dots)$ or $(L_0, L_2, L_3, \dots)$, then we immediately obtain the following consequence.

Corollary 1.1. *Let $n \in \mathbb{Z}^+$. Then there is a permutation $\sigma \in S_n$ with $\sigma^2 = I_n$ such that all the sums $k + \sigma(k)$ $(k = 1, \dots, n)$ are Fibonacci numbers. Also, there is a permutation $\tau \in S_n$ with $\tau^2 = I_n$ such that all the numbers $k + \tau(k)$ $(k = 1, \dots, n)$ are Lucas numbers.*

Remark 1.1. Let $f(n)$ be the number of permutations $\sigma \in S_n$ such that all the sums $k + \sigma(k)$ $(k = 1, \dots, n)$ are Fibonacci numbers. Via `Mathematica` we find that

$$(f(1), \dots, f(20)) = (1, 1, 1, 2, 1, 2, 4, 2, 1, 4, 4, 20, 4, 5, 1, 20, 24, 8, 96, 200).$$

For example, $\pi = (2,3)(4,9)(5,8)(6,7)$ is the unique permutation in S_9 such that all the numbers $k + \pi(k)$ $(k = 1, \dots, 9)$ are Fibonacci numbers.

Recall that those integers $T_n = n(n+1)/2$ $(n = 0, 1, 2, \dots)$ are called triangular numbers. Note that $T_n - T_{n-1} = n \leqslant T_{n-1}$ for every $n = 3, 4, \dots$. Applying Theorem 1.1 with $(a_1, a_2, a_3, \dots) = (2, T_2, T_3, \dots)$, we immediately get the following corollary.

Corollary 1.2. *For any $n \in \mathbb{Z}^+$, there is a permutation $\pi \in S_n$ with $\pi^2 = I_n$ such that each of the sums $k + \pi(k)$ $(k = 1, \dots, n)$ is either 2 or a triangular number.*

Remark 1.2. When $n = 4$, we may take $\pi = (2,4)$ to meet the requirement in Corollary 1.2. Note that $1 + 1 = 3 = T_2$ and $2 + 4 = 3 + 3 = T_3$.

Our next theorem focuses on permutations involving powers of two.

Theorem 1.2. *Let n be any positive integer. Then there is a unique permutation $\pi_n \in S_n$ such that all the numbers $k+\pi_n(k)$ $(k=1,\ldots,n)$ are powers of two. In other words, for the $n\times n$ matrix A whose (i,j)-entry is 1 or 0 according as $i+j$ is a power of two or not, we have* $\mathrm{per}(A)=1$.

Remark 1.3. Note that the number of 1's in the matrix A given in Theorem 1.2 coincides with

$$\sum_{k=0}^{\lfloor \log_2 n\rfloor+1}\sum_{\substack{1\leqslant i,j\leqslant n\\ i+j=2^k}}1=\sum_{k=0}^{\lfloor \log_2 n\rfloor}(2^k-1)+\sum_{i=2^{\lfloor \log_2 n\rfloor+1}-n}^{n}1=2n-\lfloor \log_2 n\rfloor-1.$$

Example 1.1. Here we list π_n in Theorem 1.2 for $n=1,\ldots,11$:

$$\pi_1=(1),\ \pi_2=(1),\ \pi_3=(1,3),\ \pi_4=(1,3),\ \pi_5=(3,5),\ \pi_6=(2,6)(3,5),$$
$$\pi_7=(1,7)(2,6)(3,5),\ \pi_8=(1,7)(2,6)(3,5),\ \pi_9=(2,6)(3,5)(7,9),$$
$$\pi_{10}=(3,5)(6,10)(7,9),\ \pi_{11}=(1,3)(5,11)(6,10)(7,9).$$

Theorem 1.2 has the following consequence.

Corollary 1.3. *For any $n\in\mathbb{Z}^+$, there is a unique permutation $\pi\in S_{2n}$ such that $k+\pi(k)\in\{2^a-1:\ a\in\mathbb{Z}^+\}$ for all $k=1,\ldots,2n$.*

Now we turn to our results of new types.

Theorem 1.3. (i) *Let p be any odd prime. Then there is no $\pi\in S_{p-1}$ such that all the $p-1$ numbers $k\pi(k)$ $(k=1,\ldots,p-1)$ are pairwise incongruent modulo p. Also,*

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1}\equiv 0 \pmod p. \tag{1.2}$$

(ii) *We have*

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}\equiv 0 \pmod n \quad \textit{for all } n=3,4,5,\ldots. \tag{1.3}$$

Remark 1.4. In contrast with Theorem 1.3, it is well-known that

$$\det[i^{j-1}]_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(j-i)=1!2!\ldots(n-1)!$$

and in particular

$$\det[i^{j-1}]_{1\leqslant i,j\leqslant p-1},\ \det[i^{j-1}]_{1\leqslant i,j\leqslant p}\not\equiv 0 \pmod p$$

for any odd prime p.

In additive combinatorics, there are some interesting topics involving both permutations and finite abelian groups, see. e.g., [FSX] and [GS]. Below we present two novel theorems on permutations involving groups.

Theorem 1.4. (i) *Let $a_1,\ldots,a_n$ be distinct elements of a torsion-free abelian group G. Then there is a permutation $\pi\in S_n$ such that all those $ka_{\pi(k)}$ ($k=1,\ldots,n$) are pairwise distinct.*

(ii) *Let a,b,c be three distinct elements of a group G such that none of them has order 2 or 3. Then $a^{\sigma(1)}$ and $b^{\sigma(2)}$ are distinct for some $\sigma\in S_2$. Also, $a^{\tau(1)},b^{\tau(2)},c^{\tau(3)}$ are pairwise distinct for some $\tau\in S_3$.*

Remark 1.5. On the basis of this theorem, we will formulate a general conjecture for groups in Section 4.

Theorem 1.5. *For any $n>3$ distinct elements $a_1,a_2,\ldots,a_n$ of a torsion-free abelian group G, there is a permutation $\pi\in S_n$ such that all the n sums*

$$b_1+b_2+b_3,\ b_2+b_3+b_4,\ \ldots,\ b_{n-2}+b_{n-1}+b_n,\ b_{n-1}+b_n+b_1,\ b_n+b_1+b_2$$

are pairwise distinct, where $b_k=a_{\pi(k)}$ for $k=1,\ldots,n$.

Remark 1.6. By Remark 1.2 of Sun [S19], for any finite subset A of a torsion-free abelian group with $|A|=n>2$ we may write A as $\{a_1,\ldots,a_n\}$ such that $a_1+a_2,\ldots,a_{n-1}+a_n,a_n+a_1$ are pairwise distinct.

We are going to prove Theorems 1.1-1.3 and Corollary 1.3 in the next section, and show Theorems 1.4-1.5 in Section 3. We will pose some conjectures in Section 4.

2. Proofs of Theorems 1.1-1.3 and Corollary 1.3

Proof of Theorem 1.1. For convenience, we set $a_0=1$ and $A=\{a_1,a_2,a_3,\ldots\}$. We use induction on $n\in\mathbb{Z}^+$ to show the desired result.

For $n=1$, we take $\pi(1)=1$ and note that $1+\pi(1)=2=a_1\in A$.

Now let $n\geqslant 2$ and assume the desired result for smaller values of n. Choose $k\in\mathbb{N}$ with $a_k\leqslant n<a_{k+1}$, and write $m=a_{k+1}-n$. Then $1\leqslant m\leqslant 2a_k-n\leqslant 2n-n=n$. Let $\pi(j)=a_{k+1}-j$ for $j=m,\ldots,n$. Then

$$\{\pi(j):\ j=m,\ldots,n\}=\{m,\ldots,n\},$$

and $\pi(\pi(j))=j$ for all $j=m,\ldots,n$.

Case 1. $m=1$.

In this case, $\pi\in S_n$ and $\pi^2=I_n$.

Case 2. $m=n$.

In this case, $a_{k+1}=2n\geqslant 2a_k$. On the other hand, $a_{k+1}\leqslant 2a_k$. So, $a_{k+1}=2a_k$ and $a_k=n$. Let $\pi(j)=n-j=a_k-j$ for all $0<j<n$. Then $\pi\in S_n$ and $j+\pi(j)\in\{a_k,a_{k+1}\}$ for all $j=1,\ldots,n$. Note that $\pi^2(k)=k$ for all $k=1,\ldots,n$.

Case 3. $1<m<n$.

In this case, by the induction hypothesis, for some $\sigma \in S_{m-1}$ with $\sigma^2 = I_{m-1}$, we have $i+\sigma(i) \in A$ for all $i = 1,\dots,m-1$. Let $\pi(i) = \sigma(i)$ for all $i = 1,\dots,m-1$. Then $\pi \in S_n$ and it meets our requirement.

In view of the above, we have completed the induction proof. $\Box$

Proof of Theorem 1.2. Applying Theorem 1.1 with $a_k = 2^k$ for all $k \in \mathbb{Z}^+$, we see that for some $\pi \in S_n$ with $\pi^2 = I_n$ all the numbers $k+\pi(k)$ $(k = 1,\dots,n)$ are powers of two.

Below we use induction on n to prove that the number of $\pi \in S_n$ with

$$\{k+\pi(k) :\ k = 1,\dots,n\} \subseteq \{2^a :\ a \in \mathbb{Z}^+\}$$

is exactly one.

The case $n = 1$ is trivial.

Now let $n > 1$ and assume that for each $m = 1,\dots,n-1$ there is a unique $\pi_m \in S_m$ such that all the numbers $k+\pi_m(k)$ $(k = 1,\dots,m)$ are powers of two. Choose $a \in \mathbb{Z}^+$ with $2^{a-1} \leqslant n < 2^a$, and write $m = 2^a - n$. Then $1 \leqslant m \leqslant n$.

Suppose that $\pi \in S_n$ and all the numbers $k+\pi(k)$ $(k = 1,\dots,n)$ are powers of two. If $2^{a-1} \leqslant k \leqslant n$, then

$$2^{a-1} < k+\pi(k) \leqslant k+n \leqslant 2n < 2^{a+1}$$

and hence $\pi(k) = 2^a - k$ since $k+\pi(k)$ is a power of two. Thus

$$\{\pi(k) :\ k = 2^{a-1},\dots,n\} = \{m,\dots,2^{a-1}\}.$$

If $k \in \{1,\dots,2^{a-1}-1\}$ and $2^{a-1} < \pi(k) \leqslant n$, then

$$2^{a-1} < k+\pi(k) \leqslant n+n < 2^{a+1},$$

hence $k+\pi(k) = 2^a = m+n$ and thus $m \leqslant k < 2^{a-1}$. So we have

$$\{\pi^{-1}(j) :\ 2^{a-1} < j \leqslant n\} = \{m,\dots,2^{a-1}-1\}.$$

(Note that $n - 2^{a-1} = 2^a - m - 2^{a-1} = 2^{a-1} - m$.)

By the above analysis, $\pi(k) = 2^a - k$ for all $k = m,\dots,n$, and

$$\{\pi(k) :\ k = m,\dots,n\} = \{m,\dots,n\}.$$

Thus π is uniquely determined if $m = 1$.

Now assume that $m > 1$. As $\pi \in S_n$, we must have

$$\{\pi(k) :\ k = 1,\dots,m-1\} = \{1,\dots,m-1\}.$$

Since $k+\pi(k)$ is a power of two for every $k = 1,\dots,m-1$, by the induction hypothesis we have $\pi(k) = \pi_m(k)$ for all $k = 1,\dots,m-1$. Thus π is indeed uniquely determined.

In view of the above, the proof of Theorem 1.2 is now complete. $\Box$

Proof of Corollary 1.3. Clearly, $\pi \in S_{2n}$ and $k+\pi(k) \in \{2^a-1 :\ a \in \mathbb{Z}^+\}$ for all $k = 1,\dots,2n$, if and only if there are $\sigma,\tau \in S_n$ with $\pi(2k) = 2\sigma(k)-1$ and $\pi(2k-1) = 2\tau(k)$ for all $k = 1,\dots,n$ such that $k+\sigma(k), k+\tau(k) \in \{2^{a-1} :\ a \in \mathbb{Z}^+\}$ for all $k = 1,\dots,n$. Thus we get the desired result by applying Theorem 1.2. $\Box$

Lemma 2.1 (Alon's Combinatorial Nullstellensatz [A])**.** *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $|A_i|>k_i$ for $i=1,\ldots,n$ where $k_1,\ldots,k_n\in\{0,1,2,\ldots\}$. 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 $P(a_1,\ldots,a_n)\neq 0$.*

Lemma 2.2. *Let $a_1,\ldots,a_n$ be elements of a field F. Then the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ in the polynomial*

$$\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(a_jx_j-a_ix_i)\in F[x_1,\ldots,x_n]$$

is $(-1)^{n(n-1)/2}\mathrm{per}[a_i^{j-1}]_{1\leqslant i,j\leqslant n}$.

Proof. This is easy. In fact,

$$\begin{aligned}&\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(a_jx_j-a_ix_i)\\ =&(-1)^{\binom n2}\det[x_i^{n-j}]_{1\leqslant i,j\leqslant n}\times\det[a_i^{j-1}x_i^{j-1}]_{1\leqslant i,j\leqslant n}\\ =&(-1)^{\binom n2}\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)\prod_{i=1}^n x_i^{n-\sigma(i)}\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^n a_i^{\tau(i)-1}x_i^{\tau(i)-1}.\end{aligned}$$

Therefore the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ in this polynomial is

$$(-1)^{\binom n2}\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)^2\prod_{i=1}^n a_i^{\sigma(i)-1}=(-1)^{n(n-1)/2}\mathrm{per}[a_i^{j-1}]_{1\leqslant i,j\leqslant n}.$$

This concludes the proof. □

Remark 2.1. See [DKSS] and [S08, Lemma 2.2] for similar identities and arguments.

Proof of Theorem 1.3. (i) Let g be a primitive root modulo p. Then, there is a permutation $\pi\in S_{p-1}$ such that the numbers $k\pi(k)$ $(k=1,\ldots,p-1)$ are pairwise incongruent modulo p, if and only if there is a permutation $\rho\in S_{p-1}$ such that $g^{i+\rho(i)}$ $(i=1,\ldots,p-1)$ are pairwise incongruent modulo p (i.e., the numbers $i+\rho(i)$ $(i=1,\ldots,p-1)$ are pairwise incongruent modulo $p-1$).

Suppose that $\rho\in S_{p-1}$ and all the numbers $i+\rho(i)$ $(i=1,\ldots,p-1)$ are pairwise incongruent modulo $p-1$. Then

$$\sum_{i=1}^{p-1}(i+\rho(i))\equiv\sum_{j=1}^{p-1}j\pmod{p-1},$$

and hence $\sum_{i=1}^{p-1} i = p(p-1)/2 \equiv 0 \pmod{p-1}$ which is impossible. This contradiction proves the first assertion in Theorem 1.3(i).

Now we turn to prove the second assertion in Theorem 1.3(i). Suppose that $\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1} \not\equiv 0 \pmod p$. Then, by Lemma 2.2, the coefficient of $x_1^{p-2}\dots x_{p-1}^{p-2}$ in the polynomial

$$\prod_{1\leqslant i<j\leqslant p-1}(x_j-x_i)(jx_j-ix_i)$$

is not congruent to zero modulo p. Applying Lemma 2.1 with $F=\mathbb{Z}/p\mathbb{Z}$ and $A=\{k+p\mathbb{Z}:\ k=1,\dots,p-1\}$, we see that there is a permutation $\pi\in S_{p-1}$ such that all those $k\pi(k)$ $(k=1,\dots,p-1)$ are pairwise incongruent modulo p, which contradicts the first assertion of Theorem 1.3(i) we have just proved.

(ii) Let $n>2$ be an integer. Then

$$\begin{aligned}\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n} &= \sum_{\sigma\in S_n}\prod_{k=1}^{n}k^{\sigma(k)-1}\\ &\equiv \sum_{\substack{\sigma\in S_n\\ \sigma(n)=1}}(n-1)!\prod_{k=1}^{n-1}k^{\sigma(k)-2} = (n-1)!\sum_{\tau\in S_{n-1}}\prod_{k=1}^{n-1}k^{\tau(k)-1}\\ &=(n-1)!\,\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1} \pmod n.\end{aligned}$$

We want to prove that $n\mid \mathrm{per}[i^{j-1}]_{1\le i,j\le n}$. This holds when n is an odd prime p, because $p\mid \mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1}$ by Theorem 1.3(i). For $n=4$, we have

$$\begin{aligned}\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant 4} &\equiv 3!\sum_{\tau\in S_3}1^{\tau(1)-1}2^{\tau(2)-1}3^{\tau(3)-1}\\ &\equiv 6\left(1^{2-1}2^{1-1}3^{3-1}+1^{3-1}2^{1-1}3^{2-1}\right)\equiv 0 \pmod 4.\end{aligned}$$

Now assume that $n>4$ is composite. By the above, it suffices to show that $(n-1)!\equiv 0 \pmod n$. Let p be the smallest prime divisor of n. Then $n=pq$ for some integer $q\geqslant p$. If $p<q$, then $n=pq$ divides $(n-1)!$. If $q=p$, then $p^2=n>4$ and hence $2p<p^2$, thus $2n=p(2p)$ divides $(n-1)!$.

In view of the above, we have completed the proof of Theorem 1.3. □

3. Proofs of Theorems 1.4 and 1.5

Proof of Theorem 1.4. (i) The case $n=1$ is trivial. Below we let $n>1$. Note that the subgroup H of G generated by $a_1,\dots,a_n$ is infinite, finitely generated and torsion-free. Thus H is isomorphic to $\mathbb{Z}^r$ for some positive integer r. By algebraic number theory (cf. [He]), we may take an algebraic number field K with $[K:\mathbb{Q}]=r$ and hence H is isomorphic to the additive group O_K of algebraic integers in K. Thus, without any loss of generality, we may simply assume that G is the additive group $\mathbb{C}$ of all complex numbers.

By Lemma 2.2, the coefficient of $x_1^{n-1}\ldots x_n^{n-1}$ in the polynomial

$$P(x_1,\ldots,x_n):=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(jx_j-ix_i)\in\mathbb{C}[x_1,\ldots,x_n]$$

is $(-1)^{n(n-1)/2}\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}$, which is nonzero since $\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}>0$. Applying Lemma 2.1 we see that there are $x_1,\ldots,x_n\in A=\{a_1,\ldots,a_n\}$ with $P(x_1,\ldots,x_n)\neq 0$. Thus, for some $\pi\in S_n$ all the numbers $ka_{\sigma(k)}$ $(k=1,\ldots,n)$ are distinct. This ends the proof of part (i).

(ii) Let e be the identity of the group G. Suppose that $a=b^2$ and also $a^2=b$. Then $a=(a^2)^2=a^4$, and hence $a^3=e$. As the order of a is not three, we have $a=e$ and hence $b=a^2=e$, which leads to a contradiction since $a\neq b$. Therefore $a^{\sigma(1)}$ and $b^{\sigma(2)}$ are distinct for some $\sigma\in S_2$.

To prove the second assertion in Theorem 1.4(ii), we distinguish two cases.

Case 1. One of a,b,c is the square of another element among a,b,c.

Without loss of generality, we simply assume that $a=b^2$. As $a\neq b$ we have $b\neq e$. As b is not of order two, we also have $a\neq e$. Note that $b^2=a\neq c$. If $b^2=a^3$, then $a=a^3$ which is impossible since the order of a is not two. If $a^3\neq c$, then c,b^2,a^3 are pairwise distinct.

Now assume that $a^3=c$. As a is not of order three, we have $b\neq a^2$ and $c\neq e$. Note that $a^3=c\neq b$ and also $a^3=c\neq c^2$. If $b\neq c^2$, then b,c^2,a^3 are pairwise distinct. If $b=c^2$, then $a=b^2=c^4=(a^3)^4$ and hence the order of a is 11, thus $a^2\neq(a^3)^3=c^3$ and hence b,a^2,c^3 are pairwise distinct.

Case 2. None of a,b,c is the square of another one among a,b,c.

Suppose that there is no $\tau\in S_3$ with $a^{\tau(1)},b^{\tau(2)},c^{\tau(3)}$ pairwise distinct. Then $c^3\in\{a,b^2\}\cap\{a^2,b\}$. If $c^3=a$, then $c^3\neq b$ and hence $a=c^3=a^2$, thus $a=e=c$ which leads to a contradiction. (Recall that none of a,b,c is of order 3.) Therefore $c^3=b^2$. As c is not of order three, if $b=e$ then we have $c=e=b$ which is impossible. So $c^3=b^2\neq b$ and hence $b^2=c^3=a^2$. Similarly, $a^3=b^2=c^2$. Thus $a^3=b^2=a^2$, hence $a=e$ and $b^2=a^2=e$, which contradicts $b\neq a$ since b is not of order two.

In view of the above, we have finished the proof of Theorem 1.4. $\square$

Proof of Theorem 1.5. The subgroup of G generated by $a_1,\ldots,a_n$ is a finitely generated torsion-free abelian group. So we may simply assume that $G=\mathbb{Z}^r$ for some positive integer r without any loss of generality. It is well known that there is a linear ordering $\leqslant$ on $G=\mathbb{Z}^r$ such that for any $a,b,c\in G$ if $a<b$ then $-b<-a$ and $a+c<b+c$ (cf. [L]). For convenience, we suppose $a_1<a_2<\ldots<a_n$ without any loss of generality.

If $n=4$, then $(b_1,b_2,b_3,b_4)=(a_1,a_2,a_3,a_4)$ meets the requirement since

$$a_1+a_2+a_3<a_4+a_1+a_2<a_3+a_4+a_1<a_2+a_3+a_4.$$

Below we assume $n \geqslant 5$.

Clearly

$$a_1+a_2+a_3 < a_2+a_3+a_4 < \dots < a_{n-2}+a_{n-1}+a_n.$$

For convenience we set

$$S := \{a_{i-1}+a_i+a_{i+1}:\ i=2,\dots,n-1\},$$

and let $\min S$ and $\max S$ denote the least element and the largest element of S respectively. Note that

$$\min S = a_1+a_2+a_3 < a_n+a_1+a_2 < a_{n-1}+a_n+a_1 < \max S = a_{n-2}+a_{n-1}+a_n.$$

If $\{a_n+a_1+a_2,\ a_{n-1}+a_n+a_1\} \cap S = \emptyset$, then $(b_1,\dots,b_n)=(a_1,\dots,a_n)$ meets the requirement. Obviously

$$-a_n < -a_{n-1} < \dots < -a_2 < -a_1 \text{ and } (-a_2)+(-a_1)+(-a_n) = -(a_1+a_2+a_n).$$

So, it suffices to find a desired permutation $b_1,\dots,b_n$ of $a_1,\dots,a_n$ under the condition $a_{n-1}+a_n+a_1 \in S$.

Case 1. $n=5$.

As $a_4+a_5+a_1 \in S$, we have $a_4+a_5+a_1 = a_2+a_3+a_4$ and we may take $(b_1,\dots,b_5)=(a_1,a_2,a_3,a_5,a_4)$ since

$$a_1+a_2+a_3 < a_4+a_1+a_2 < a_2+a_3+a_4 = a_5+a_4+a_1 < a_2+a_3+a_5 < a_3+a_5+a_4.$$

Case 2. $n=6$.

As $a_5+a_6+a_1 \in S$, the sum $a_5+a_6+a_1$ is equal to $a_2+a_3+a_4$ or $a_3+a_4+a_5$. If $a_5+a_6+a_1 = a_2+a_3+a_4$, then we may take $(b_1,\dots,b_6)=(a_1,a_2,a_5,a_3,a_4,a_6)$ since

$$\begin{aligned} a_1+a_2+a_5 <& a_6+a_1+a_2 < a_4+a_6+a_1 < a_5+a_6+a_1 = a_2+a_3+a_4 \\ <& a_2+a_5+a_3 < a_5+a_3+a_4 < a_3+a_4+a_6. \end{aligned}$$

If $a_5+a_6+a_1 = a_3+a_4+a_5$, then $a_6+a_1 = a_3+a_4$ and we may take $(b_1,\dots,b_6)=(a_1,a_2,a_3,a_4,a_6,a_5)$ since

$$\begin{aligned} a_1+a_2+a_3 <& a_5+a_1+a_2 < a_6+a_1+a_2 = a_2+a_3+a_4 \\ <& a_3+a_4+a_5 = a_6+a_5+a_1 < a_3+a_4+a_6 < a_4+a_6+a_5. \end{aligned}$$

Case 3. $n=7$.

As $a_6+a_7+a_1 \in S$, the sum $a_6+a_7+a_1$ is equal to $a_2+a_3+a_4$ or $a_3+a_4+a_5$ or $a_4+a_5+a_6$. If $a_6+a_7+a_1 = a_4+a_5+a_6$, then $a_7+a_1 = a_4+a_5$ and we may take $(b_1, \ldots, b_7) = (a_2, a_1, a_4, a_5, a_3, a_6, a_7)$ since

$$\begin{aligned} a_2+a_1+a_4 <& a_1+a_4+a_5 = a_1+a_1+a_7 < a_7+a_2+a_1 \\ <& a_7+a_1+a_3 = a_4+a_5+a_3 < a_5+a_3+a_6 \\ <& a_4+a_5+a_6 = a_1+a_6+a_7 < a_2+a_6+a_7 < a_3+a_6+a_7. \end{aligned}$$

If $a_6+a_7+a_1 = a_2+a_3+a_4$, then we may take $(b_1, \ldots, b_7) = (a_1, a_2, a_3, a_5, a_4, a_6, a_7)$ since

$$\begin{aligned} a_1+a_2+a_3 <& a_7+a_1+a_2 < a_5+a_7+a_1 < a_6+a_7+a_1 = a_2+a_3+a_4 \\ <& a_2+a_3+a_5 < a_3+a_5+a_4 < a_5+a_4+a_6 < a_4+a_6+a_7. \end{aligned}$$

If $a_6+a_7+a_1 = a_3+a_4+a_5$ and $a_5+a_6+a_1 \neq a_2+a_3+a_4$, then $a_6+a_1 < a_3+a_4$ and we may take $(b_1, \ldots, b_7) = (a_1, a_2, a_3, a_4, a_7, a_5, a_6)$ since

$$\begin{aligned} a_1+a_2+a_3 <& a_6+a_1+a_2 < \min\{a_5+a_6+a_1, a_2+a_3+a_4\} \\ <& \max\{a_5+a_6+a_1, a_2+a_3+a_4\} < a_1+a_6+a_7 = a_3+a_4+a_5 \\ <& a_3+a_4+a_7 < a_4+a_7+a_5 < a_7+a_5+a_6. \end{aligned}$$

If $a_6+a_7+a_1 = a_3+a_4+a_5$ and $a_5+a_6+a_1 = a_2+a_3+a_4$, then $a_7+a_1 < a_3+a_4$ and we may take $(b_1, \ldots, b_7) = (a_1, a_2, a_3, a_4, a_6, a_5, a_7)$ since

$$\begin{aligned} a_1+a_2+a_3 <& a_7+a_1+a_2 < a_5+a_6+a_1 = a_2+a_3+a_4 \\ <& a_5+a_7+a_1 < a_3+a_4+a_5 = a_6+a_7+a_1 \\ <& a_3+a_4+a_6 < a_4+a_6+a_5 < a_6+a_5+a_7. \end{aligned}$$

Case 4. $n > 7$ and $a_n+a_1+a_2 \notin S$.

In this case, there is a unique $2 < i < n-1$ with $a_{i-1}+a_i+a_{i+1} = a_{n-1}+a_n+a_1$. If $i < n-3$, then we may take

$$(b_1, \ldots, b_n) = (a_1, \ldots, a_{i-2}, a_{i-1}, a_i, a_{i+2}, a_{i+1}, a_{i+3}, \ldots, a_n)$$

because

$$\begin{aligned} a_{i-2}+a_{i-1}+a_i <& a_{i-1}+a_i+a_{i+1} = a_{n-1}+a_n+a_1 < a_{i-1}+a_i+a_{i+2} \\ <& a_i+a_{i+2}+a_{i+1} < a_{i+2}+a_{i+1}+a_{i+3} \\ <& a_{i+1}+a_{i+3}+a_{i+4} < \ldots < a_{n-2}+a_{n-1}+a_n. \end{aligned}$$

When $i \in \{n-2, n-3\}$, we have $i \geqslant n-3 > 4$, and hence in the case $a_1+a_2+a_n \neq a_{i-4}+a_{i-3}+a_{i-1}$ we may take

$$(b_1, \ldots, b_n) = (a_1, \ldots, a_{i-4}, a_{i-3}, a_{i-1}, a_{i-2}, a_i, a_{i+1}, a_{i+2}, \ldots, a_n)$$

because

$$\begin{aligned}a_{i-4}+a_{i-3}+a_{i-2} <&a_{i-4}+a_{i-3}+a_{i-1} < a_{i-3}+a_{i-1}+a_{i-2}\\ <&a_{i-1}+a_{i-2}+a_i < a_{i-2}+a_i+a_{i+1}\\ <&a_{i-1}+a_i+a_{i+1} = a_{n-1}+a_n+a_1\\ <&a_i+a_{i+1}+a_{i+2} < \dots < a_{n-2}+a_{n-1}+a_n\end{aligned}$$

and

$$\begin{aligned}a_n+a_1+a_2 <&(a_{i-2}+a_{n-1}-a_{i+1})+a_n+a_1\\ =& a_{i-2}-a_{i+1}+(a_{i-1}+a_i+a_{i+1}) = a_{i-1}+a_{i-2}+a_i.\end{aligned}$$

If $i \in \{n-2, n-3\}$ and $a_1+a_2+a_n = a_{i-4}+a_{i-3}+a_{i-1}$, then we may take

$$(b_1,\dots,b_n) = (a_1,\dots,a_{i-4},a_{i-3},a_i,a_{i-2},a_{i-1},a_{i+1},a_{i+2},\dots,a_n)$$

because

$$\begin{aligned}a_n+a_1+a_2 =&a_{i-4}+a_{i-3}+a_{i-1}\\ <&a_{i-4}+a_{i-3}+a_i < a_{i-3}+a_i+a_{i-2} < a_i+a_{i-2}+a_{i-1}\\ <&a_{i-2}+a_{i-1}+a_{i+1} < a_{i-1}+a_i+a_{i+1} = a_{n-1}+a_n+a_1\\ <&a_{i-1}+a_{i+1}+a_{i+2} < \dots < a_{n-2}+a_{n-1}+a_n.\end{aligned}$$

Case 5. $n > 7$ and $a_n+a_1+a_2 \in S$.

In this case, for some $2 < j < i \leqslant n-2$ we have

$$a_{n-1}+a_n+a_1 = a_{i-1}+a_i+a_{i+1} > a_{j-1}+a_j+a_{j+1} = a_n+a_1+a_2.$$

If $j+1 = i$, then

$$\begin{aligned}a_{n-1}-a_2 =&(a_{n-1}+a_n+a_1)-(a_n+a_1+a_2)\\ =&a_{i-1}+a_i+a_{i+1}-(a_i+a_{i-1}+a_{i-2}) = a_{i+1}-a_{i-2}\end{aligned}$$

which is impossible since $i \geqslant 4$ and $n > 6$.

If $i-j > 5$, then

$$(b_1,\dots,b_n) = (a_1,\dots,a_{j-1},a_j,a_{j+2},a_{j+1},a_{j+3},\dots,a_{i-3},a_{i-1},a_{i-2},a_i,a_{i+1},\dots,a_n)$$

meets the requirement since

$$\begin{aligned}a_{j-1}+a_j+a_{j+1} = a_n+a_1+a_2 &< a_{j-1}+a_j+a_{j+2}\\ &< a_j+a_{j+2}+a_{j+1} < a_{j+2}+a_{j+1}+a_{j+3}\\ &< \dots < a_{i-3}+a_{i-1}+a_{i-2} < a_{i-1}+a_{i-2}+a_i\\ &< a_{i-2}+a_i+a_{i+1} < a_{i-1}+a_i+a_{i+1} = a_{n-1}+a_n+a_1\\ &< a_i+a_{i+1}+a_{i+2} < \dots < a_{n-2}+a_{n-1}+a_n.\end{aligned}$$

If $i-j=5$, then $j+4=i-1$ and

$$(b_1,\ldots,b_n)=(a_1,\ldots,a_{j-1},a_j,a_{j+2},a_{j+1},a_{i-1},a_{i-2},a_i,a_{i+1},\ldots,a_n)$$

meets the requirement. If $i-j=4$, then

$$(b_1,\ldots,b_n)=(a_1,\ldots,a_{j-1},a_j,a_{j+2},a_{j+3},a_{j+1},a_i,a_{i+1},\ldots,a_n)$$

meets the requirement since

$$\begin{aligned}a_{j-1}+a_j+a_{j+1}=&a_n+a_1+a_2\\<&a_{j-1}+a_j+a_{j+2}<a_j+a_{j+2}+a_{j+3}\\<&a_{j+2}+a_{j+3}+a_{j+1}<a_{j+3}+a_{j+1}+a_i\\<&a_{j+1}+a_i+a_{i+1}<a_{i-1}+a_i+a_{i+1}=a_{n-1}+a_n+a_1\\<&a_i+a_{i+1}+a_{i+2}<\ldots<a_{n-2}+a_{n-1}+a_n.\end{aligned}$$

If $i-j=3$, then

$$(b_1,\ldots,b_n)=(a_1,\ldots,a_{j-1},a_j,a_{j+2},a_{j+1},a_i,a_{i+1},\ldots,a_n)$$

meets the requirement since

$$\begin{aligned}a_{j-1}+a_j+a_{j+1}=&a_n+a_1+a_2\\<&a_{j-1}+a_j+a_{j+2}<a_j+a_{j+2}+a_{j+1}\\<&a_{j+2}+a_{j+1}+a_i=a_{i-1}+a_{i-2}+a_i<a_{i-2}+a_i+a_{i+1}\\<&a_{i-1}+a_i+a_{i+1}=a_{n-1}+a_n+a_1\\<&a_i+a_{i+1}+a_{i+2}<\ldots<a_{n-2}+a_{n-1}+a_n.\end{aligned}$$

If $j>4$ and $i=j+2$, then

$$(b_1,\ldots,b_n)=(a_1,\ldots,a_{j-3},a_{j-1},a_{j-2},a_{j+1},a_j,a_i,a_{i+1},a_{i+2},\ldots,a_n)$$

meets the requirement since

$$\begin{aligned}a_{j-4}+a_{j-3}+a_{j-1}&<a_{j-3}+a_{j-1}+a_{j-2}<a_{j-1}+a_{j-2}+a_{j+1}\\&<a_{j-2}+a_{j+1}+a_j<a_{j-1}+a_j+a_{j+1}=a_n+a_1+a_2\\&<a_{j+1}+a_j+a_i<a_j+a_i+a_{i+1}\\&<a_{i-1}+a_i+a_{i+1}=a_{n-1}+a_n+a_1<a_i+a_{i+1}+a_{i+2}.\end{aligned}$$

If $i=j+2\leqslant n-4$, then

$$(b_1,\ldots,b_n)=(a_1,\ldots,a_{j-2},a_{j-1},a_j,a_i,a_{i-1},a_{i+2},a_{i+1},a_{i+3},a_{i+4},\ldots,a_n)$$

meets the requirement since

$$\begin{aligned}a_{j-2}+a_{j-1}+a_j &< a_{j-1}+a_j+a_{j+1}=a_n+a_1+a_2\\ &< a_{j-1}+a_j+a_i < a_j+a_i+a_{i-1}\\ &< a_{i-1}+a_i+a_{i+1}=a_{n-1}+a_n+a_1\\ &< a_i+a_{i-1}+a_{i+2} < a_{i-1}+a_{i+2}+a_{i+1}\\ &< a_{i+2}+a_{i+1}+a_{i+3} < a_{i+1}+a_{i+3}+a_{i+4}\\ &< \ldots < a_{n-2}+a_{n-1}+a_n.\end{aligned}$$

If $i\geqslant n-3$, $j\leqslant 4$ and $i-j=2$, then $2=i-j\geqslant n-3-4$ and hence $n\in\{8,9\}$.

For $n=8$, we need to consider the case $i=6$ and $j=4$. As $a_8+a_1+a_2=a_3+a_4+a_5$ and $a_7+a_8+a_1=a_5+a_6+a_7$, we have $a_8+a_1=a_5+a_6=a_3+a_4+a_5-a_2$. If $2a_5\neq a_4+a_7$, then $a_5+a_8+a_1=2a_5+a_6\neq a_4+a_6+a_7$ and hence we may take

$$(b_1,\ldots,b_8)=(a_1,a_2,a_3,a_4,a_6,a_7,a_5,a_8)$$

since

$$\begin{aligned}a_1+a_2+a_3 &< a_2+a_3+a_4 < a_3+a_4+a_5=a_8+a_1+a_2 < a_3+a_4+a_6\\ &< \min\{a_4+a_6+a_7,a_5+a_8+a_1\} < \max\{a_4+a_6+a_7,a_5+a_8+a_1\}\\ &< a_6+a_7+a_5=a_7+a_8+a_1 < a_7+a_5+a_8.\end{aligned}$$

If $2a_5=a_4+a_7$, then $a_6+a_8+a_1=a_5+2a_6>a_4+a_5+a_7$ and we may take

$$(b_1,\ldots,b_8)=(a_1,a_2,a_3,a_4,a_5,a_7,a_8,a_6)$$

since

$$\begin{aligned}a_1+a_2+a_3 &< a_1+a_3+a_4=a_1+a_2+a_6 < a_2+a_3+a_4\\ &< a_3+a_4+a_5=a_8+a_1+a_2 < a_4+a_5+a_7 < a_6+a_8+a_1\\ &< a_5+a_7+a_8 < a_7+a_8+a_6.\end{aligned}$$

When $n=8$, $i=5$ and $j=3$, it suffices to apply the result for $i=6$ and $j=4$ to the sequence

$$\begin{aligned}a'_1=-a_8 &< a'_2=-a_7 < a'_3=-a_6 < a'_4=-a_5\\ &< a'_5=-a_4 < a'_6=-a_3 < a'_7=-a_2 < a'_8=-a_1\end{aligned}$$

since $a'_7+a'_8+a'_1=-(a_1+a_2+a_8)=-(a_2+a_3+a_4)=a'_5+a'_6+a'_7$ and $a'_8+a'_1+a'_2=-(a_1+a_7+a_8)=-(a_4+a_5+a_6)=a'_3+a'_4+a'_5$.

Now it remains to consider the last case where $n = 9$, $i = 6$ and $j = 4$. As $a_3 + a_4 + a_5 = a_9 + a_1 + a_2$ and $a_5 + a_6 + a_7 = a_8 + a_9 + a_1$, we have $a_3 + a_4 < a_9 + a_1$ and hence $a_3 + a_4 + a_6 < a_3 + a_4 + a_7 < a_7 + a_9 + a_1$. If $a_7 + a_9 + a_1 = a_4 + a_5 + a_6$, then

$$a_8 - a_7 = (a_8 + a_9 + a_1) - (a_7 + a_9 + a_1) = a_5 + a_6 + a_7 - (a_4 + a_5 + a_6) = a_7 - a_4.$$

When $2a_7 \neq a_8 + a_4$, we have $a_7 + a_9 + a_1 \neq a_4 + a_5 + a_6$ and hence we may take

$$(b_1, \ldots, b_9) = (a_1, a_2, a_3, a_4, a_6, a_5, a_8, a_7, a_9)$$

since

$$\begin{aligned} a_1 + a_2 + a_3 &< a_2 + a_3 + a_4 < a_3 + a_4 + a_5 = a_9 + a_1 + a_2 < a_3 + a_4 + a_6 \\ &< \min\{a_4 + a_5 + a_6, a_7 + a_9 + a_1\} < \max\{a_4 + a_5 + a_6, a_7 + a_9 + a_1\} \\ &< a_6 + a_5 + a_7 = a_8 + a_9 + a_1 < a_6 + a_5 + a_8 \\ &< a_5 + a_8 + a_7 < a_8 + a_7 + a_9. \end{aligned}$$

If $2a_7 = a_8 + a_4$, then $a_5 + a_6 + a_7 < 2a_7 + a_6 = a_4 + a_6 + a_8$ and hence we may take

$$(b_1, \ldots, b_9) = (a_1, a_2, a_3, a_4, a_6, a_8, a_5, a_7, a_9)$$

since

$$\begin{aligned} a_1 + a_2 + a_3 &< a_2 + a_3 + a_4 < a_3 + a_4 + a_5 = a_9 + a_1 + a_2 < a_3 + a_4 + a_6 \\ &< a_9 + a_1 + a_6 < a_7 + a_9 + a_1 < a_8 + a_9 + a_1 = a_5 + a_6 + a_7 \\ &< a_4 + a_6 + a_8 < a_6 + a_8 + a_5 < a_8 + a_5 + a_7 < a_5 + a_7 + a_9. \end{aligned}$$

In view of the above, we have completed the proof of Theorem 1.5. $\square$

4. Some conjectures

Motivated by Theorem 1.3(i) and Theorem 1.4, we pose the following conjecture for finite groups.

Conjecture 4.1. *Let n be a positive integer, and let G be a group containing no element of order among $2, \ldots, n+1$. Then, for any $A \subseteq G$ with $|A| = n$, we may write $A = \{a_1, \ldots, a_n\}$ with $a_1, a_2^2, \ldots, a_n^n$ pairwise distinct.*

Remark 4.1. (a) Theorem 1.4 shows that this conjecture holds when $n \leqslant 3$ or G is a torsion-free abelian group.

(b) For $n = 4, 5, 6, 7, 8, 9$ we have verified the conjecture for cyclic groups $G = \mathbb{Z}/m\mathbb{Z}$ with $|G| = m$ not exceeding 100, 100, 70, 60, 30, 30 respectively.

(c) If G is a finite group with $|G| > 1$, then the least order of a non-identity element of G is $p(G)$, the smallest prime divisor of $|G|$.

Inspired by Theorem 1.3, we formulate the following conjecture.

Conjecture 4.2. *Let $n>1$ be an integer with $n\not\equiv 2 \pmod 4$.*

(i) *We have*

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1}\equiv 0 \pmod n. \tag{4.1}$$

(ii) *If $n\equiv 1 \pmod 3$, then*

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1}\equiv 0 \pmod {n^2}. \tag{4.2}$$

Remark 4.2. We have checked this conjecture via computing $\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1}$ modulo n^2 for $n\leqslant 17$. The sequence $a_n=\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}$ $(n=1,2,3,\ldots)$ is available from [S18, A322363].

Conjecture 4.3. (i) *For any $n\in\mathbb{Z}^+$, there is a permutation $\sigma_n\in S_n$ such that $k\sigma_n(k)+1$ is prime for every $k=1,\ldots,n$.*

(ii) *For any integer $n>2$, there is a permutation $\tau_n\in S_n$ such that $k\tau_n(k)-1$ is prime for every $k=1,\ldots,n$.*

Remark 4.3. See [S18, A321597] for related data and examples.

Conjecture 4.4. (i) *For each $n\in\mathbb{Z}^+$, there is a permutation π_n of $\{1,\ldots,n\}$ such that $k^2+k\pi_n(k)+\pi_n(k)^2$ is prime for every $k=1,\ldots,n$.*

(ii) *For any positive integer $n\neq 7$, there is a permutation π_n of $\{1,\ldots,n\}$ such that $k^2+\pi_n(k)^2$ is prime for every $k=1,\ldots,n$.*

Remark 4.4. See [S18, A321610] for related data and examples.

As usual, for $k=1,2,3,\ldots$ we let p_k denote the k-th prime.

Conjecture 4.5. *For any $n\in\mathbb{Z}^+$, there is a permutation $\pi\in S_n$ such that $p_k+p_{\pi(k)}+1$ is prime for every $k=1,\ldots,n$.*

Remark 4.5. See [S18, A321727] for related data and examples.

In 1973 J.-R. Chen [Ch] proved that there are infinitely many primes p with $p+2$ a product of at most two primes; nowadays such primes p are called Chen primes.

Conjecture 4.6. *Let $n\in\mathbb{Z}^+$. Then, there is an even permutation $\sigma\in S_n$ with $p_kp_{\sigma(k)}-2$ prime for all $k=1,\ldots,n$. If $n>2$, then there is an odd permutation $\tau\in S_n$ with $p_kp_{\tau(k)}-2$ prime for all $k=1,\ldots,n$.*

Remark 4.6. See [S18, A321855] for related data and examples. If we let $b(n)$ denote the number of even permutations $\sigma\in S_n$ with $p_kp_{\sigma(k)}-2$ prime for all $k=1,\ldots,n$, then

$$(b(1),\ldots,b(11))=(1,1,1,1,3,6,1,1,33,125,226).$$

Conjecture 2.17(ii) of Sun [S15] implies that for any odd integer $n > 1$ there is a prime $p \leqslant n$ such that $pn - 2$ is prime.

In 2002, Cloitre [Cl, A073112] created the sequence A073112 on OEIS whose n-th term is the number of permutations $\pi \in S_n$ with $\sum_{k=1}^n \frac{1}{k+\pi(k)} \in \mathbb{Z}$. Recently Sun [S18a] conjectured that for any integer $n > 5$ there is a permutation $\pi \in S_n$ satisfying

$$\sum_{k=1}^n \frac{1}{k+\pi(k)} = 1,$$

and this was later confirmed by the user Zhao Shen at Mathoverflow via clever induction arguments.

In 1982 A. Filz (cf. [G, pp. 160-162]) conjectured that for any $n = 2, 4, 6, \ldots$ there is a circular permutation $(i_1, \ldots, i_n)$ of $1, \ldots, n$ such that all the n adjacent sums

$$i_1 + i_2,\ i_2 + i_3,\ \ldots,\ i_{n-1} + i_n,\ i_n + i_1$$

are prime.

Motivated by this, we pose the following conjecture.

Conjecture 4.7. (i) *For any integer $n > 6$, there is a permutation $\pi \in S_n$ such that*

$$\sum_{k=1}^{n-1} \frac{1}{\pi(k)+\pi(k+1)} = 1. \tag{4.3}$$

Also, for any integer $n > 7$, there is a permutation $\pi \in S_n$ such that

$$\frac{1}{\pi(1)+\pi(2)} + \frac{1}{\pi(2)+\pi(3)} + \ldots + \frac{1}{\pi(n-1)+\pi(n)} + \frac{1}{\pi(n)+\pi(1)} = 1. \tag{4.4}$$

(ii) *For any integer $n > 7$, there is a permutation $\pi \in S_n$ such that*

$$\sum_{k=1}^{n-1} \frac{1}{\pi(k)^2 - \pi(k+1)^2} = 0. \tag{4.5}$$

Remark 4.7. See [S18, A322070 and A322099] for related data and examples. For the latter assertion in Conjecture 4.7(i), the equality (4.4) with $n = 8$ holds if we take $(\pi(1), \ldots, \pi(8)) = (6, 1, 5, 2, 4, 3, 7, 8)$. In a previous version of this paper posted to arXiv, the author also conjectured that for any integer $n > 5$ there is a permutation $\pi \in S_n$ with $\sum_{k=1}^{n-1} \frac{1}{\pi(k)\pi(k+1)} = 1$; this, together with two other conjectures of the author, was confirmed by G.-N. Han [H].

Conjecture 4.8. (i) *For any integer $n>1$, there is a permutation $\pi\in S_n$ such that*

$$\sum_{0<k<n}\pi(k)\pi(k+1)\in\{2^m+1:\ m=0,1,2,\dots\}. \tag{4.6}$$

(ii) *For any integer $n>4$, there is a unique power of two which can be written as $\sum_{k=1}^{n-1}\pi(k)\pi(k+1)$ with $\pi\in S_n$ and $\pi(n)=n$.*

Remark 4.8. Concerning part (i) of Conjecture 4.8, when $n=4$ we may choose $(\pi(1),\dots,\pi(4))=(1,3,2,4)$ so that

$$\sum_{k=1}^{3}\pi(k)\pi(k+1)=1\times3+3\times2+2\times4=2^4+1.$$

For any $\pi\in S_n$, if for each $k=1,\dots,n$ we let

$$\pi'(k)=\begin{cases}\pi(\pi^{-1}(k)+1) & \text{if } \pi^{-1}(k)\neq n,\\ \pi(1) & \text{if } \pi^{-1}(k)=n,\end{cases}$$

then $\pi'\in S_n$ and

$$\pi(1)\pi(2)+\dots+\pi(n-1)\pi(n)+\pi(n)\pi(1)=\sum_{k=1}^{n}k\pi'(k).$$

By the Cauchy-Schwarz inequality (cf. [N, p. 178]), for any $\pi\in S_n$ we have

$$\left(\sum_{k=1}^{n}k\pi(k)\right)^2\leqslant\left(\sum_{k=1}^{n}k^2\right)\left(\sum_{k=1}^{n}\pi(k)^2\right)$$

and hence

$$\sum_{k=1}^{n}k\pi(k)\leqslant\sum_{k=1}^{n}k^2=\frac{n(n+1)(2n+1)}{6}.$$

If we let $\sigma(k)=n+1-\pi(k)$ for all $k=1,\dots,n$, then $\sigma\in S_n$ and

$$\begin{aligned}\sum_{k=1}^{n}k\pi(k)=&\sum_{k=1}^{n}k(n+1-\sigma(k))=(n+1)\sum_{k=1}^{n}k-\sum_{k=1}^{n}k\sigma(k)\\ \geqslant&\frac{n(n+1)^2}{2}-\frac{n(n+1)(2n+1)}{6}=\frac{n(n+1)(n+2)}{6}.\end{aligned}$$

Thus

$$\left\{\sum_{k=1}^{n}k\pi(k):\ \pi\in S_n\right\}\subseteq T(n):=\left\{\frac{n(n+1)(n+2)}{6},\dots,\frac{n(n+1)(2n+1)}{6}\right\}. \tag{4.7}$$

Actually equality in (4.7) holds when $n\neq3$, which was first realized by M. Aleksevev (cf. the comments in [B]). Note that $|T(n)|=n(n^2-1)/6+1$.

Inspired by the above analysis, here we pose the following conjecture in additive combinatorics.

Conjecture 4.9. *Let $n \in \mathbb{Z}^+$ and let F be a field with $p(F) > n+1$, where $p(F) = p$ if the characteristic of F is a prime p, and $p(F) = +\infty$ if the characteristic of F is zero. Let A be any finite subset of F with $|A| \geqslant n + \delta_{n,3}$, where $\delta_{n,3}$ is 1 or 0 according as $n = 3$ or not. Then, for the set*

$$S(A) := \left\{ \sum_{k=1}^{n} ka_k : \ a_1, \dots, a_n \text{ are distinct elements of } A \right\}, \tag{4.8}$$

we have

$$|S(A)| \geqslant \min\left\{ p(F), \ (|A| - n)\frac{n(n+1)}{2} + \frac{n(n^2-1)}{6} + 1 \right\}. \tag{4.9}$$

Remark 4.9. One may compare this conjecture with the author's conjectural linear extension of the Erdős-Heilbronn conjecture (cf. [SZ]). Perhaps, Conjecture 4.9 remains valid if we replace the field F by any finite additive group G with $|G| > 1$ and use $p(G)$ (the least prime factor of $|G|$) instead of $p(F)$.

Recall that the torsion subgroup of a group G is given by

$$\mathrm{Tor}(G) = \{g \in G : \ g \text{ is of finite order}\}.$$

Conjecture 3.3(i) of the author [S19] states that if A is an n-subset (with $|A| = n > 2$) of an additive abelian group G of odd order then there is a numbering $a_1, \dots, a_n$ of all the elements of A such that $a_1 + a_2, \dots, a_{n-1} + a_n, a_n + a_1$ are pairwise distinct, this was verified by Yu-Xuan Ji (a student at Nanjing Univ.) for $|G| < 30$ in 2020. Motivated by this and Theorem 1.5, we formulate the following conjecture.

Conjecture 4.10. *Let G be an additive abelian group with $\mathrm{Tor}(G)$ cyclic or $|\mathrm{Tor}(G)|$ odd. For any finite subset A of G with $|A| = n > 3$, there is a numbering $a_1, \dots, a_n$ of all the elements of A such that the n sums*

$$a_1+a_2+a_3, \ a_2+a_3+a_4, \ \dots, \ a_{n-2}+a_{n-1}+a_n, \ a_{n-1}+a_n+a_1, \ a_n+a_1+a_2$$

are pairwise distinct.

Remark 4.10. (a) Conjecture 4.10 holds in the case $A = G = \mathbb{Z}/n\mathbb{Z} = \{\bar{a} = a + n\mathbb{Z} : \ a \in \mathbb{Z}\}$ with $n > 3$ and $3 \nmid n$ since the natural list $\bar{0}, \bar{1}, \dots, \overline{n-1}$ of the elements of $\mathbb{Z}/n\mathbb{Z}$ meets the requirement.

(b) In 2008 the author [S08] proved that for any three n-subsets A, B, C of an additive abelian group G with $\mathrm{Tor}(G)$ cyclic, there is a numbering $a_1, \dots, a_n$ of the elements of A, a numbering $b_1, \dots, b_n$ of the elements of B and a numbering $c_1, \dots, c_n$ of the elements of C such that the n sums $a_1+b_1+c_1, \dots, a_n+b_n+c_n$ are pairwise distinct.

References

[A] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. (1999), 7–29.

[B] J. Boscole, Sequence A126972 in OEIS, 2007, Website: `http://oeis.org/A126972`.

[Br] P. Bradley, *Prime number sums*, preprint, arXiv:1809.01012 (2018).

[Ch] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica 16 (1973), 157–176.

[Cl] B. Cloitre, Sequences A073112 and A073364 in OEIS (2002), `http://oeis.org`.

[DKSS] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126** (2001), 17C28.

[FSX] T. Feng, Z.-W. Sun and Q. Xiang, *Exterior algebras and two conjectures on finite abelian groups*, Israel J. Math. **182** (2011), 425–437.

[GS] F. Ge and Z.-W. Sun, *On a permutation problem for finite abelian groups*, Electron. J. Combin. **24** (2017), no. 1, #P1.17, 1–6.

[G] R. K. Guy, Unsolved Problems in Number Theory, 3rd Edition, Springer, 2004.

[H] G.-N. Han, *On the existence of permutations conditioned by certain rational functions*, Electron. Res. Arch. **28** (2020), 149–156.

[He] E. Hecke, *Lectures on the Theory of Algebraic Numbers, Grad. Texts in Math., 77, Springer, New York, 1981, pp. 108C116.*.

[L] F. W. Levi, *Ordered groups*, Proc. Indian Acad. Sci. Sect. A **16** (1942), 256–263.

[N] M. B. Nathanson, Additive Number Theory: The Classical Bases, Grad. Texts in Math., Vol. 164, Springer, New York, 1996.

[S08] Z.-W. Sun, *An additive theorem and restricted sumsets*, Math. Res. Lett. **15** (2008), 1263–1276.

[S15] Z.-W. Sun, *Problems on combinatorial properties of primes*, in: M. Kaneko, S. Kanemitsu and J. Liu (eds.), Number Theory: Plowing and Starring through High Wave Forms, Proc. 7th China-Japan Seminar (Fukuoka, Oct. 28–Nov. 1, 2013), Ser. Number Theory Appl., Vol. 11, World Sci., Singapore, 2015, pp. 169–187.

[S18] Z.-W. Sun, Sequences A321597, A321610, A321611, A321727, A321855, A322070, A322099, A322363 in OEIS (2018), `http://oeis.org`.

[S18a] Z.-W. Sun, *Permutations* $\pi\in S_n$ *with* $\sum_{k=1}^n\frac{1}{k+\pi(k)}=1$, Question 315648 on Mathoverflow, Nov. 19, 2018. Website: `https://mathoverflow.net/questions/315648`.

[S19] Z.-W. Sun, *Some new problems in additive combinatorics*, Nanjing Univ. J. Math. Biquarterly **36** (2019), 134–155. `http://maths.nju.edu.cn/~zwsun/196a.pdf`.

[SZ] Z.-W. Sun and L.-L. Zhao, *Linear extension of the Erdős-Heilbronn conjecture*, J. Combin. Theory Ser. A **119** (2012), 364–381.