Preprint, arXiv:1309.1679

SOME NEW PROBLEMS IN ADDITIVE COMBINATORICS

Zhi-Wei Sun

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

Abstract. In this paper we investigate some new problems in additive combinatorics. Our problems mainly involve permutations (or circular permutations) $a_1, \ldots, a_n$ of n distinct numbers or elements of an additive abelian group with adjacent sums $a_i + a_{i+1}$ (or differences $a_i - a_{i+1}$ or distances $|a_i - a_{i+1}|$) pairwise distinct. For any subset A of an additive torsion-free abelian group G with $|A| = n > 3$, we show that there is a numbering $a_1, \ldots, a_n$ of the elements of A such that

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

are pairwise distinct. We pose 18 open conjectures for further research; for example, we conjecture that the above assertion holds for any abelian group G.

1. Introduction

Additive combinatorics is an active field involving both number theory and combinatorics. For an excellent introduction to problems and results in this fascinating field, one may consult Tao and Vu [TV]. See also Alon [A] for a useful tool called Combinatorial Nullstellensatz. In this paper we study some new problems in additive combinatorics, they involve some special kinds of permutations or circular permutations.

Now we present our basic results.

Theorem 1.1. *Let $a_1, \ldots, a_n$ be a monotonic sequence of n distinct real numbers. Then there is a permutation $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$ with $b_1 = a_1$ such that*

$$|b_1 - b_2|,\ |b_2 - b_3|,\ \ldots,\ |b_{n-1} - b_n|$$

are pairwise distinct.

Remark 1.1. Theorem 1.1 is the starting point of our topics in this paper.

2000 *Mathematics Subject Classification.* Primary 11B13, 11P70; Secondary 05B10, 05D15, 05E15, 11A41, 11B75, 11T99, 20D60, 20K01.

Supported by the National Natural Science Foundation (grant 11171140) of China.

Corollary 1.1. *There is a circular permutation $q_1,\ldots,q_n$ of the first n primes $p_1,\ldots,p_n$ with $q_1=p_1=2$ and $q_n=p_n$ such that the n distances*

$$|q_1-q_2|,\ |q_2-q_3|,\ \ldots,\ |q_{n-1}-q_n|,\ |q_n-q_1|$$

are pairwise distinct.

Proof. This holds trivially in the case $n=1$. For $n>1$, by Theorem 1.1 there is a permutation $-q_n,-q_{n-1},\ldots,-q_2$ of $-p_n,-p_{n-1},\ldots,-p_2$ with $q_n=p_n$ such that $|-q_n+q_{n-1}|,\ldots,|-q_3+q_2|$ are pairwise distinct. Set $q_1=p_1=2$. Then $q_1,q_2,\ldots,q_n$ is a permutation of $p_1,p_2,\ldots,p_n$ and it meets our requirement since $q_1-q_2=2-q_2$ and $q_n-q_1=p_n-2$ are both odd while those q_i-q_{i+1} $(1<i<n)$ are even. □

Theorem 1.2. (i) *For any integer $n>3$, there is a circular permutation $i_0,\ldots,i_n$ of $0,\ldots,n$ with $i_0=0$ and $i_n=n$ such that all the $n+1$ adjacent differences $i_0-i_1,i_1-i_2,\ldots,i_{n-1}-i_n,i_n-i_0$ are pairwise distinct.*

(ii) *An integer $n>1$ is even if and only if there is a permutation $i_1,\ldots,i_n$ of $1,\ldots,n$ with*

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

pairwise distinct modulo n.

Remark 1.2. In contrast with Theorem 1.2(i), for any $n>2$ distinct integers $a_1<\ldots<a_n$ we clearly have

$$a_1+a_2<a_2+a_3<\ldots<a_{n-1}+a_n.$$

On Sept. 13, 2013 the author asked his students the following question: When $a_n+a_1=a_i+a_{i+1}$ for some $1\leqslant i<n$, how to construct a suitable permutation $b_1,\ldots,b_n$ of $a_1,\ldots,a_n$ such that $b_1+b_2,b_2+b_3,\ldots,b_{n-1}+b_n,b_n+b_1$ are pairwise distinct ? The author's PhD student Dianwang Hu suggested that it suffices to take $(b_1,\ldots,b_n)=(a_1,\ldots,a_i,a_{i+2},a_{i+1},a_{i+3},\ldots,a_n)$. But this does not work for $i=n-2$. If $i>2$, then the permutation $(b_1,\ldots,b_n)=(a_1,\ldots,a_{i-2},a_i,a_{i-1},a_{i+1},a_{i+2},\ldots,a_n)$ meets the requirement. The case $n=3$ is trivial. For $n=4$, the permutation (a_1,a_2,a_4,a_3) works for our purpose since $a_1+a_2<a_3+a_1<a_2+a_4<a_4+a_3$.

Theorem 1.3. *For any $n>3$ distinct elements $a_1,a_2,\ldots,a_n$ of a torsion-free abelian group G, there is a permutation $b_1,\ldots,b_n$ of $a_1,\ldots,a_n$ such that all the n sums*

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

are pairwise distinct.

Theorem 1.4. *For any $n > 3$ distinct elements $a_1, a_2, \dots, a_n$ of a torsion-free abelian group G, there is a permutation $b_1, \dots, b_n$ of $a_1, \dots, a_n$ such that all the n sums*

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

are pairwise distinct.

Theorem 1.5. *For any odd prime power $n > 1$, there are integers $a_1, a_2, \dots, a_{\varphi(n)}$ such that both $\{a_1, \dots, a_{\varphi(n)}\}$ and*

$$\{a_1 - a_2,\ a_2 - a_3,\ \dots,\ a_{\varphi(n)-1} - a_{\varphi(n)},\ a_{\varphi(n)} - a_1\}$$

are reduced systems of residues modulo n, where φ is Euler's totient function.

Remark 1.3. We conjecture that this holds for any odd number $n > 1$.

Theorem 1.6. *Let $\mathbb{F}_q$ be a finite field with $q = 2n + 1 > 2^{66}$. Set $S = \{a^2 : a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}\}$ and $T = \mathbb{F}_q^* \setminus S$. Then, there is a circular permutation $a_1, \dots, a_n$ of all the n elements of S such that*

$$\{a_1 + a_2,\ a_2 + a_3,\ \dots,\ a_{n-1} + a_n,\ a_n + a_1\} = S\ (or\ T).$$

Also, there is a circular permutation $b_1, \dots, b_n$ of all the n elements of S such that

$$\{b_1 - b_2,\ b_2 - b_3,\ \dots,\ b_{n-1} - b_n,\ b_n - b_1\} = S\ (or\ T).$$

Remark 1.4. Via a complicated reasoning, the number 2^{66} in Theorem 1.6 can be reduced to 13. In the initial version of this paper, the author posed the following conjecture weaker than Theorem 1.6 which was later confirmed by N. Alon and J. Bourgain [AB]: For any prime $p = 2n+1 > 13$, there is a circular permutation $a_1, \dots, a_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent sums $a_1 + a_2, a_2 + a_3, \dots, a_{n-1} + a_n, a_n + a_1$ are quadratic residues (or quadratic nonresidues) modulo p. Also, for any prime $p = 2n+1 > 5$, there is a circular permutation $b_1, \dots, b_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent differences $b_1 - b_2, b_2 - b_3, \dots, b_{n-1} - b_n, b_n - b_1$ are quadratic residues (or quadratic nonresidues) modulo p.

We are going to prove Theorem 1.1-1.6 in the next section, and pose some conjectures in Section 3 for further research. We have posted to OEIS some sequences (cf. [S13]) related to our conjectures.

2. Proofs of Theorems 1.1-1.4

Proof of Theorem 1.1. If $a_1 > a_2 > \ldots > a_n$, then $-a_1 < -a_2 < \ldots < -a_n$. So we may assume that $a_1 < a_2 < \ldots < a_n$ without loss of generality.

If $n = 2k$ is even, then the permutation

$$(b_1, \ldots, b_n) = (a_1, a_{2k}, a_2, a_{2k-1}, \ldots, a_{k-1}, a_{k+2}, a_k, a_{k+1})$$

meets our purpose since

$$a_{2k} - a_1 > a_{2k} - a_2 > a_{2k-1} - a_2 > \ldots > a_{k+2} - a_{k-1} > a_{k+2} - a_k > a_{k+1} - a_k.$$

When $n = 2k - 1$ is odd, the permutation

$$(b_1, \ldots, b_n) = (a_1, a_{2k-1}, a_2, a_{2k-2}, \ldots, a_{k-1}, a_{k+1}, a_k)$$

meets the requirement since

$$a_{2k-1} - a_1 > a_{2k-1} - a_2 > a_{2k-2} - a_2 > \ldots > a_{k+1} - a_{k-1} > a_{k+1} - a_k.$$

This concludes the proof. □

Proof of Theorem 1.2. (i) We first assume that $n = 2k$ is even. If k is even, then the circular permutation

$$(i_0, \ldots, i_n) = (0, 2k-1, 1, 2k-2, 2, \ldots, k+1, k-1, k, 2k)$$

meets the requirement since

$$-(2k-1),\ 2k-2,\ -(2k-3),\ 2k-4,\ \ldots,\ 2,\ -1,\ -k,\ 2k$$

are pairwise distinct. If k is odd, then it suffices to choose the circular permutation

$$(i_0, \ldots, i_n) = (0, 1, 2k-1, 2, 2k-2, \ldots, k-1, k+1, k, 2k)$$

since

$$-1,\ -(2k-2),\ 2k-3,\ -(2k-4),\ \ldots,\ -2,\ 1,\ -k,\ 2k$$

are pairwise distinct.

Now we handle the case $n = 2k + 1 \equiv 1 \pmod 2$. If k is even, then the circular permutation

$$(i_0, \ldots, i_n) = (0, 2k, 1, 2k-1, 2, 2k-2, \ldots, k-1, k+1, k, 2k+1)$$

meets the requirement since

$$-2k,\ 2k-1,\ -(2k-2),\ 2k-3,\ -(2k-4),\ \ldots,\ -2,\ 1,\ -(k+1),\ 2k+1$$

are pairwise distinct. If k is odd, then it suffices to choose the circular permutation

$$(i_0,\ldots,i_n)=(0,k,k{+}2,k{+}1,k{-}1,k{+}3,k{-}2,k{+}4,k{-}3,\ldots,2k{-}1,2,2k,1,2k{+}1)$$

since

$$-k,\ -2,\ 1,\ 2,\ -4,\ 5,\ \ldots,\ -(2k-2),\ 2k-1,\ -2k,\ 2k+1$$

are pairwise distinct.

(ii) Suppose that $i_1,\ldots,i_n$ is a permutation of $1,\ldots,n$ with the $n{-}1$ integers i_k-i_{k+1} $(0<k<n)$ pairwise distinct modulo n. Then

$$\{i_k-i_{k+1} \bmod n:\ k=1,\ldots,n-1\}=\{r \bmod n:\ r=1,\ldots,n-1\}$$

and also

$$\{i_{k+1}-i_k \bmod n:\ k=1,\ldots,n-1\}=\{r \bmod n:\ r=1,\ldots,n-1\}.$$

Therefore

$$\sum_{k=1}^{n-1}(i_k-i_{k+1})\equiv\sum_{r=1}^{n-1}r\equiv\sum_{k=1}^{n-1}(i_{k+1}-i_k)\pmod n$$

and hence $n\mid 2(i_1-i_n)$ which implies that n is even.

Now assume that $n>1$ is even. Write $n=2m$. Then

$$(i_1,\ldots,i_n)=(m,m-1,m+1,m-2,m+2,\ldots,2,2m-2,1,2m-1,2m)$$

is a permutation of $1,\ldots,n$ with the required property.

In view of the above, we have completed the proof of Theorem 1.2. □

Proof of Theorem 1.3. 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 $a{+}c<b{+}c$. For convenience we suppose that $a_1<a_2<\ldots<a_n$ without any loss of generality.

Clearly $a_1+2a_2<a_2+2a_3<\ldots<a_{n-1}+2a_n$. Thus the permutation $(b_1,\ldots,b_n)=(a_1,\ldots,a_n)$ meets the requirement if $a_n+2a_1\neq a_i+2a_{i+1}$ for all $i=1,\ldots,n-1$.

Below we assume that $a_n+2a_1=a_i+2a_{i+1}$ for some $0<i<n$. Note that $1\leqslant i\leqslant n-2$ since $a_{n-1}+2a_n-(a_n+2a_1)=a_{n-1}+a_n-2a_1>0$.

Case 1. $i=1$.

In this case, $a_n + 2a_1 = a_1 + 2a_2$ and hence $a_1 + a_3 < a_1 + a_n = 2a_2$. The permutation $(b_1, \ldots, b_n) = (a_1, a_3, a_2, a_4, \ldots, a_n)$ meets our purpose since

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

Case 2. $i > 1$ and $n = 4$.

In this case, $a_4 + 2a_1 = a_2 + 2a_3$ and we may take the permutation $(b_1, b_2, b_3, b_4) = (a_2, a_1, a_3, a_4)$ since

$$a_2 + 2a_1 < a_1 + 2a_3 < a_2 + 2a_3 = a_4 + 2a_1 < a_4 + 2a_2 < a_3 + 2a_4.$$

Case 3. $i \geqslant 2$, $n \geqslant 5$, and a_{i-1}, a_i, a_{i+1} don't form an AP (arithmetic progression).

In this case, the permutation

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

works for our purpose since

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

Case 4. $2 \leqslant i < n - 2$ and $a_i - a_{i-1} = a_{i+1} - a_i \neq a_{i+2} - a_{i+1}$.

In this case, the permutation

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

works for our purpose since

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

Case 5. $2 \leqslant i < n - 2$, and $a_{i-1}, a_i, a_{i+1}, a_{i+2}$ form an AP.

In this case, the permutation

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

works for our purpose since

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

Case 6. $i = n-2 \geqslant 3$ and $a_{i+1}-a_i = a_i - a_{i-1} \neq a_{i-1}-a_{i-2}$.
In this case, the permutation

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

works for our purpose since

$$\begin{aligned}&\min\{a_{i-2}+2a_i, a_i+2a_{i-1}\}\\ <&\max\{a_{i-2}+2a_i, a_i+2a_{i-1}\} < a_{i-1}+2a_i\\ <&a_{i-1}+2a_{i+1} < a_i+2a_{i+1} = a_n+2a_1\\ <&a_{i+1}+2a_{i+2} = a_{n-1}+2a_n.\end{aligned}$$

Case 7. $i = n-2 \geqslant 3$, and $a_{i-2},a_{i-1},a_i,a_{i+1}$ form an AP.
In this case, the permutation

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

works for our purpose since

$$\begin{aligned}a_{i-2}+2a_{i-1} <&a_i+2a_{i-1}\\ <&a_{i-2}+2a_{i+1} \text{ (since } a_i-a_{i-2} = a_{i+1}-a_{i-1} < 2(a_{i+1}-a_{i-1}))\\ <&a_{i+1}+2a_i = a_{i-1}+2a_{i+1} < a_i+2a_{i+1} = a_n+2a_1\\ <&a_{i-1}+2a_{i+2} = a_{n-3}+2a_n.\end{aligned}$$

Combining the above we have finished the proof of Theorem 1.3. □

Proof of Theorem 1.4. As in the proof of Theorem 1.3, 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 $a+c < b+c$. For convenience we suppose that $a_1 < a_2 < \ldots < a_n$ without any loss of generality.

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

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

For convenience we set

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

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 the permutation $(b_1,\ldots,b_n) = (a_1,\ldots,a_n)$ meets the requirement. Obviously

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

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

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 $(b_1,\ldots,b_5) = (a_1,a_2,a_3,a_5,a_4)$ 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 number $a_5+a_6+a_1$ 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 $(b_1,\ldots,b_6) = (a_1,a_2,a_5,a_3,a_4,a_6)$ 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 $(b_1,\ldots,b_6) = (a_1,a_2,a_3,a_4,a_6,a_5)$ 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 number $a_6+a_7+a_1$ 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 $(b_1, \dots, b_7) = (a_1, a_2, a_3, a_4, a_7, a_5, a_6)$ 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 $(b_1, \dots, b_7) = (a_1, a_2, a_3, a_4, a_6, a_5, a_7)$ 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

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

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

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

because

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

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

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

because

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

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 the permutation $(b_1,\ldots,b_n)$ given by

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

meets the requirement since

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

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

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

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

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

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 the permutation

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

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 the permutation $(b_1,\ldots,b_n)$ given by

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

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 the permutation $(b_1,\ldots,b_n)$ given by

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

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 the permutation

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

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 the permutation

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

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 the the permutation

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

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 the the permutation

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

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 1.4. □

Proof of Theorem 1.5. When $n>1$ is an odd prime power p^a with p prime and a a positive integer, we take a primitive root g modulo n. Clearly, both $\{g^i:\ i=1,\ldots,\varphi(n)\}$ and

$$\{g^i-g^{i+1}=g^i(1-g):\ i=1,\ldots,\varphi(n)\}$$

are reduced systems of residues modulo n. (Note that $g^{\varphi(n)+1}=g$ and $g\not\equiv 1 \pmod p$.) So it suffices to take $a_i=g^i$ for $i=1,\ldots,\varphi(n)$. □

Proof of Theorem 1.6. Let $\varepsilon\in\{\pm1\}$, and let $R=S$ or T. Choose $a\in T$. By [H, Corollary 3], there exists a primitive root g of $\mathbb{F}_q$ with $1+\varepsilon g^2$ (or $a+\varepsilon a g^2$) also a primitive root of $\mathbb{F}_q$. Note that T contains all the primitive roots of $\mathbb{F}_q$. So there is a primitive root g of $\mathbb{F}_q$ with $1+\varepsilon g^2\in R$. Clearly, $\{g^{2i}:\ i=1,\ldots,n\}=S$ and $g^{2i}+\varepsilon g^{2(i+1)}=g^{2i}(1+\varepsilon g^2)\in R$ for all $i=1,\ldots,n$. Therefore

$$\{g^2-g^4,\ g^4-g^6,\ \ldots,\ g^{2n-2}-g^{2n},\ g^{2n}-g^2=g^{2n}-g^{2(n+1)}\}=R.$$

This concludes the proof. □

3. Some open conjectures

Conjecture 3.1 (2013-09-01). *Let $a_1,a_2,\ldots,a_n$ be n distinct real numbers. Then there is a permutation $b_1,\ldots,b_n$ of $a_1,\ldots,a_n$ with $b_1=a_1$ such that the $n-1$ numbers*

$$|b_1-b_2|,\ |b_2-b_3|,\ \ldots,\ |b_{n-1}-b_n|$$

are pairwise distinct.

Remark 3.1. By Theorem 1.1, this conjecture holds when a_1 is the least element or the largest element of $\{a_1,\ldots,a_n\}$.

Conjecture 3.2 (2013-08-31). *Let $a_1 < a_2 < \ldots < a_n$ be n distinct real numbers. If there is a circular permutation $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$ with the n adjacent distances*

$$|b_1 - b_2|,\ |b_2 - b_3|,\ \ldots,\ |b_{n-1} - b_n|,\ |b_n - b_1|$$

pairwise distinct, then there is such a circular permutation $b_1, \ldots, b_n$ with a_1 and a_n adjacent (i.e, we may require additionally that $b_1 = a_1$ and $b_n = a_n$).

Remark 3.2. For the 6 consecutive primes $11, 13, 17, 19, 23, 29$, the circular permutation $(11, 13, 29, 17, 23, 19)$ has distinct adjacent distances but the least element 11 and the largest element 29 are not adjacent on the circle. However, the circular permutation $(11, 19, 17, 13, 23, 29)$ with 11 and 29 adjacent on the circle also has distinct adjacent distances.

Conjecture 3.3 (2013-09-02). *Let $a_1, \ldots, a_n$ be n distinct elements of a finite additive abelian group G. Suppose that $n \nmid |G|$, or n is even and the Sylow 2-subgroup of G is cyclic. Then there exists a permutation $b_1, \ldots, b_n$ of $a_1, \ldots, a_n$ with $b_1 = a_1$ such that the $n - 1$ elements $b_i - b_{i+1}$ $(0 < i < n)$ are pairwise distinct.*

Remark 3.3. By Theorem 1.2(ii), this holds when $\{a_1, \ldots, a_n\} = G = \mathbb{Z}/n\mathbb{Z}$ with n even. For the Klein quaternion group

$$G = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \{(0, 0), (0, 1), (1, 0), (1, 1)\},$$

if $\{a_1, a_2, a_3, a_4\} = G$ then we have $a_1 - a_2 = a_3 - a_4$.

Conjecture 3.4 (2013-09-03). *Let A be an n-subset of a finite additive abelian group G with $2 \nmid n$ or $n \nmid |G|$.*

(i) *There always exists a numbering $a_1, a_2, \ldots, a_n$ of all the n elements of A such that the n sums*

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

are pairwise distinct.

(ii) *In the case $3 < n < |G|$, there is a numbering $a_1, a_2, \ldots, a_n$ of all the n elements of A such that the n differences*

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

are pairwise distinct.

Remark 3.4. A conjecture of Snevily [Sn] states that for any two n-subsets A and B of an additive abelian group of odd order there is a numbering $a_1, \ldots, a_n$ of the elements of A and a numbering $b_1, \ldots, b_n$ of the elements of B such that the n sums $a_1 + b_1, \ldots, a_n + b_n$ are pairwise distinct. This was proved by Arsovski [A] in 2009. Note that part (i) of Conjecture 3.4 is stronger than Snevily's conjecture in the case $A = B$.

Conjecture 3.5 (2013-09-20). *Let A be a finite subset of an additive abelian group G with $|A| = n > 3$.*

(i) *If G is finite with $|G| \not\equiv 0 \pmod 3$, then there is a numbering $a_1, \ldots, a_n$ of all the elements of A such that the n sums*

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

are pairwise distinct.

(ii) *There always exist two numberings $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ of all the elements of A such that the n sums*

$$a_1 + 2b_1,\ a_2 + 2b_2,\ \ldots,\ a_{n-1} + 2b_{n-1},\ a_n + 2b_n$$

are pairwise distinct.

Remark 3.5. (i) When $A = \{a_1, \ldots, a_n\}$ forms an abelian group of the form $(\mathbb{Z}/3\mathbb{Z})^r$, the n elements

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

cannot be pairwise distinct.

(ii) The author has proved part (ii) for $n \leqslant 4$.

Conjecture 3.6 (2013-09-04). *Let A be a finite subset of an additive abelian group G with $|A| = n > 3$. Then there is a numbering $a_1, \ldots, a_n$ of all the elements of A such that the n sums*

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

are pairwise distinct.

Remark 3.6. By Theorem 1.4, Conjecture 3.6 holds for any torsion-free abelian group G. In 2008 the author [S08] proved that for any three n-subsets A, B, C of an additive abelian group with cyclic torsion subgroup, there is a numbering $a_1, \ldots, a_n$ of the elements of A, a numbering $b_1, \ldots, b_n$ of the elements of B and a numbering $c_1, \ldots, c_n$ of the elements of C such that the n sums $a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n$ are pairwise distinct. Note that Conjecture 3.6 holds in the case $A = G = \mathbb{Z}/n\mathbb{Z}$ with $3 \nmid n$ since the natural circular permutation $(0, 1, \ldots, n-1)$ of the elements of $\mathbb{Z}/n\mathbb{Z}$ meets the requirement. We even think that Conjectures 3.5 and 3.6 might hold for any group G.

Conjecture 3.7 (joint with Qing-Hu Hou). (i) (2013-09-05) *Let $\mathbb{F}_q$ be the finite field with $q > 7$ elements. Then there is a numbering $a_1, \ldots, a_q$ of the elements of $\mathbb{F}_q$ such that all the q sums*

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{q-1} + a_q,\ a_q + a_1$$

are generators of the cyclic group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ (i.e., primitive elements of $\mathbb{F}_q$).

(ii) (2013-09-07) *Let $p = 2n + 1$ be an odd prime. If $p > 19$, then 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 primitive roots modulo p. When $p > 13$, there is a circular permutation $i_1, \ldots, i_n$ of $1, \ldots, n$ such that all the n adjacent differences $i_1 - i_2, i_2 - i_3, \ldots, i_{n-1} - i_n, i_n - i_1$ are primitive roots modulo p.*

Remark 3.7. (a) We have verified part (i) for all primes $q < 545$, and part (ii) for all primes $p < 545$. For the circular permutation

$$(a_1, a_2, \ldots, a_{11}) = (0, 6, 7, 1, 5, 3, 10, 8, 9, 4, 2)$$

of $0, 1, \ldots, 10$, the 11 sums $a_1 + a_2, a_2 + a_3, \ldots, a_{10} + a_{11}, a_{11} + a_1$ are all primitive roots modulo the prime 11.

(b) If g is a primitive root of the field $\mathbb{F}_q$ with $q > 2$ and $a_i = g^{i-1}$ for all $i = 1, \ldots, q-1$, then it is easy to see that $a_1-a_2, a_2-a_3, \ldots, a_{q-2}-a_{q-1}, a_{q-1}-a_1$ are pairwise distinct and that $a_1 + a_2, a_2 + a_3, \ldots, a_{q-2} + a_{q-1}, a_{q-1} + a_1$ are also pairwise distinct.

Conjecture 3.8. *Let $p = 2n + 1$ be an odd prime. If $p > 19$, then there is a circular permutation $a_1, \ldots, a_n$ of all the $(p - 1)/2 = n$ quadratic residues modulo p such that all the n adjacent sums $a_1+a_2, a_2+a_3, \ldots, a_{n-1}+a_n, a_n+a_1$ are primitive roots modulo p. If $p > 13$, then there is a circular permutation $b_1, \ldots, b_n$ of all the $(p-1)/2 = n$ quadratic residues modulo p such that all the n differences $b_1 - b_2, b_2 - b_3, \ldots, b_{n-1} - b_n, b_n - b_1$ are primitive roots modulo p.*

Remark 3.8. Compare this conjecture with Theorem 1.6.

Conjecture 3.9 (2013-09-15)**.** *Let $p = 2n + 1 > 11$ be a prime.*

(i) *There is a circular permutation $i_1, \ldots, i_n$ of $1, \ldots, n$ such that all the n numbers $i_1^2 + i_2,\ i_2^2 + i_3,\ \ldots,\ i_{n-1}^2 + i_n,\ i_n^2 + i_1$ are quadratic residues modulo p. Also, there is a circular permutation $j_1, \ldots, j_n$ of the $1, \ldots, n$ such that all the n numbers $j_1^2 - j_2,\ j_2^2 - j_3,\ \ldots,\ j_{n-1}^2 - j_n,\ j_n^2 - j_1$ are quadratic residues modulo p.*

(ii) *If $p > 13$, then there is a circular permutation $i_1, \ldots, i_n$ of the $1, \ldots, n$ such that all the n numbers*

$$i_1^2 + i_2,\ i_2^2 + i_3,\ \ldots,\ i_{n-1}^2 + i_n,\ i_n^2 + i_1$$

are primitive roots modulo p. Also, there is a circular permutation $j_1, \ldots, j_n$ of the $1, \ldots, n$ such that all the n numbers

$$j_1^2 - j_2,\ j_2^2 - j_3,\ \ldots,\ j_{n-1}^2 - j_n,\ j_n^2 - j_1$$

are primitive roots modulo p.

Remark 3.9. For example, $(i_1,\ldots,i_{11})=(1,6,7,11,4,5,3,8,10,9,2)$ is a circular permutation of $1,\ldots,11$ for which all the sums $i_1^2+i_2,i_2^2+i_3,\ldots,i_{10}^2+i_{11},i_{11}^2+i_1$ are primitive roots modulo 23. Also,

$$(j_1,\ldots,j_{11})=(1,9,7,5,11,10,3,2,6,8,4)$$

is a circular permutation of $1,\ldots,11$ for which all the sums $j_1^2-i_2,j_2^2-i_3,\ldots,j_{10}^2-j_{11},j_{11}^2-i_1$ are primitive roots modulo 23.

Conjecture 3.10 (2013-09-17). *Let $\mathbb{F}_q$ be a finite field with $q>7$ elements and let a_0 be any element of $\mathbb{F}_q$. Then there is a circular permutation $a_1,\ldots,a_{q-1}$ of all the nonzero elements of $\mathbb{F}_q$ such that all the $q-1$ elements $a_0+a_1a_2,a_0+a_2a_3,\ldots,a_0+a_{q-2}a_{q-1},a_0+a_{q-1}a_1$ are primitive roots of the filed $\mathbb{F}_q$.*

Remark 3.10. For the circular permutation $(i_1,\ldots,i_{10})=(1,9,2,4,5,8,10,3,6,7)$ of $1,\ldots,10$, all the 10 integers $i_1i_2-1,i_2i_3-1,\ldots,i_9i_{10}-1,i_{10}i_1-1$ are primitive roots modulo 11.

Conjecture 3.11 (2013-09-07). *For any positive integer $n\neq 2,4$, there exists a permutation $i_0,i_1,\ldots,i_n$ of $0,1,\ldots,n$ with $i_0=0$ and $i_n=n$ such that all the $n+1$ adjacent sums*

$$i_0+i_1,\ i_1+i_2,\ \ldots,\ i_{n-1}+i_n,\ i_n+i_0$$

are coprime to both $n-1$ and $n+1$.

Remark 3.11. (i) Note that there is no circular permutation $i_0,\ldots,i_7$ of $0,\ldots,7$ with $i_0+i_1,i_1+i_2,\ldots,i_6+i_7,i_7+i_0$ all relatively prime to $7\times 13-1=90$. We also guess that $n\pm 1$ in Conjecture 3.11 can be replaced by $2n\pm 1$.

(ii) Now we explain why Conjecture 3.11 holds for any positive odd integer n. If $n\equiv 1,3 \pmod 6$, then $n-2$ and $2n-1$ are relatively prime to both $n-1$ and $n+1$, and hence the circular permutation

$$(i_0,\ldots,i_n)=(0,n-2,2,n-4,4,\ldots,1,n-1,n)$$

meets the requirement. If $n\equiv 3,5 \pmod 6$, then $n+2$ is relatively prime to both $n-1$ and $n+1$, and hence the circular permutation

$$(i_0,\ldots,i_n)=(0,1,n-1,3,n-3,\ldots,n-2,2,n)$$

suffices for our purpose.

Conjecture 3.12 (2013-09-22). (i) *Let A be a set of $n>2$ distinct nonzero real numbers. Then there is a circular permutation $a_1,a_2,...,a_n$ of all the elements of A such that the n adjacent sums $a_1+a_2,a_2+a_3,...,a_{n-1}+a_n,a_n+a_1$ are* *pairwise distinct, and that the n adjacent products $a_1a_2, a_2a_3, ..., a_{n-1}a_n, a_na_1$ are also pairwise distinct, except for the following three cases:*

(a) $|A| = 4$ *and A has the form* $\{\pm s, \pm t\}$.

(b) $|A| = 5$ *and A has the form* $\{r, \pm s, \pm t\}$.

(c) $|A| = 6$ *and A has the form* $\{\pm r, \pm s, \pm t\}$.

(ii) *For any set A of $n > 3$ distinct nonzero real numbers, there is a circular permutation $a_1, a_2, ..., a_n$ of all the elements of A such that the n adjacent differences $a_1 - a_2, a_2 - a_3, ..., a_{n-1} - a_n, a_n - a_1$ are pairwise distinct, and that the n adjacent products $a_1a_2, a_2a_3, ..., a_{n-1}a_n, a_na_1$ are also pairwise distinct, except for the case where $|A| = 4$ and A has the form $\{\pm s, \pm t\}$.*

Remark 3.12. For the set $A = \{1, 2, \ldots, n\}$ with n an odd prime power, obviously $1+2, 2+3, \ldots, (n-1)+n, n+1$ are pairwise distinct since $n+1$ is even, and $1 \times 2, 2 \times 3, \ldots, (n-1)n, n \times 1$ are also pairwise distinct since n is an odd prime power.

Conjecture 3.13 (2013-09-08). *For any positive integer n, there is a circular permutation $i_0, i_1, \ldots, i_n$ of $0, 1, \ldots, n$ such that all the $n+1$ adjacent sums $i_0 + i_1,\ i_1 + i_2,\ \ldots,\ i_{n-1} + i_n,\ i_n + i_0$ are among those integers k with $6k - 1$ and $6k + 1$ twin primes.*

Remark 3.13. Clearly this conjecture implies the twin prime conjecture. Qing-Hu Hou has verified this conjecture for all $n \leqslant 100$. We also have similar conjectures for cousin primes, sexy primes, and primes of the form $4k - 1$ or $4k + 1$ or $6k + 1$ (cf. [S13, A228917]). In 1982 A. Filz [F] (see also [G, p. 160]) 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.

Conjecture 3.14 (2013-09-08). *For any integer $n > 2$, there exists a circular permutation $i_0, i_1, \ldots, i_n$ of $0, 1, \ldots, n$ such that all the $n+1$ adjacent sums $i_0 + i_1,\ i_1 + i_2,\ \ldots,\ i_{n-1} + i_n,\ i_n + i_0$ are of the form $(p+1)/6$, where p is a Sophie Germain prime.*

Remark 3.14. A prime p with $2p + 1$ also prime is called a Sophie Germain prime. It is conjectured that there are infinitely many Sophie Germain primes.

Conjecture 3.15. (i) (2013-09-09) *For any positive integer n, there exists a circular permutation $i_0, i_1, \ldots, i_n$ of $0, 1, \ldots, n$ such that all the $2n+2$ numbers*

$$|i_0 \pm i_1|,\ |i_1 \pm i_2|,\ \ldots,\ |i_{n-1} \pm i_n|,\ |i_n \pm i_0|$$

are of the form $(p-1)/2$, where p is an odd prime.

(ii) (2013-09-10) *For any positive integer $n \neq 2, 4$, there exists a circular permutation $i_0, i_1, \ldots, i_n$ of $0, 1, \ldots, n$ such that all the $n+1$ numbers*

$$|i_0^2 - i_1^2|,\ |i_1^2 - i_2^2|,\ \ldots,\ |i_{n-1}^2 - i_n^2|,\ |i_n^2 - i_0^2|$$

are of the form $(p-1)/2$, where p is an odd prime.

Remark 3.15. Here are two suitable circular permutations: $(0,1,2,3,5,4,7,8,6,9)$ for $n=9$ in part (i), and $(i_0,\ldots,i_5)=(0,1,4,5,2,3)$ for $n=5$ in part (ii).

Conjecture 3.16 (2013-09-13). *For any positive integer $n \neq 4$, there exists a circular permutation $i_0, i_1, \ldots, i_n$ of $0,1,\ldots,n$ with $i_0=0$ and $i_n=1$ such that all the $n+1$ numbers*

$$i_0^2+i_1,\ i_1^2+i_2,\ \ldots,\ i_{n-1}^2+i_n,\ i_n^2+i_0$$

are of the form $(p-1)/2$, where p is an odd prime.

Remark 3.16. For $i,j \in \{0,\ldots,n\}$ with $i+j>1$, if j is a multiple of 3 and $2(i^2+j)+1$ is a prime then $2i^2+1 \not\equiv 0 \pmod 3$ and hence $3 \mid i$. So, if $i_0, i_1, \ldots, i_n$ is a permutation of $0,1,\ldots,n$ with $i_0=0$ such that all the $n+1$ numbers $i_0^2+i_1$, $i_1^2+i_2$, $\ldots$, $i_{n-1}^2+i_n$, $i_n^2+i_0$ are of the form $(p-1)/2$ with p an odd prime, then we must have $i_n=1$ (otherwise, $i_n, i_{n-1}, \ldots, i_1$ are all divisible by 3 which is impossible). To illustrate Conjecture 3.16, we give a desired permutation for $n=20$:

$$(i_0,\ldots,i_{20})=(0,3,12,9,15,18,6,20,19,14,13,4,2,7,16,17,11,10,5,8,1).$$

Conjecture 3.17 (2013-09-16). *Let n by any positive integer. Then there exists a circular permutation $i_0, i_1, \ldots, i_n$ of $0,1,\ldots,n$ such that all the $n+1$ numbers*

$$i_0^2+i_1,\ i_1^2+i_2,\ \ldots,\ i_{n-1}^2+i_n,\ i_n^2+i_0$$

are of the form $(p-1)/4$ with p a prime congruent to 1 modulo 4. Also, there is a circular permutation $j_0, j_1, \ldots, j_n$ of $0,1,\ldots,n$ with $j_0=0$ and $j_n=1$ such that all the $n+1$ numbers

$$j_0^2+j_1,\ j_1^2+j_2,\ \ldots,\ j_{n-1}^2+j_n,\ j_n^2+j_0$$

are of the form $(p+1)/4$ with p a prime congruent to 3 modulo 4.

Remark 3.17. For $i,j \in \{0,\ldots,n\}$ with $i+j>1$, if j is a multiple of 3 and $4(i^2+j)-1$ is a prime then $4i^2-1 \not\equiv 0 \pmod 3$ and hence $3 \mid i$. So, if $j_0, j_1, \ldots, j_n$ is a permutation of $0,1,\ldots,n$ with $j_0=0$ such that all the $n+1$ numbers $j_0^2+j_1$, $j_1^2+j_2$, $\ldots$, $j_{n-1}^2+j_n$, $j_n^2+j_0$ are of the form $(p+1)/4$ with p a prime congruent to 3 modulo 4, then we must have $j_n=1$ (otherwise, $j_n, j_{n-1}, \ldots, j_1$ are all divisible by 3 which is impossible). To illustrate Conjecture 3.17, we give two desired permutations for $n=9$:

$$(i_0,\ldots,i_9)=(0,1,2,3,4,6,9,7,8,5) \text{ and } (j_0,\ldots,j_9)=(0,3,6,9,2,4,5,8,7,1).$$

Conjecture 3.18 (2013-09-17). *For any positive integer $n > 5$ with $n \neq 13$, there is a circular permutation $i_1, i_2, \ldots, i_n$ of $1, \ldots, n$ such that $i_1 i_2 - 1, i_2 i_3 - 1, \ldots, i_{n-1} i_n - 1, i_n i_1 - 1$ are all prime. Also, for any positive integer $n > 1$ (resp. $n \neq 4$), there is a circular permutation $i_1, i_2, \ldots, i_n$ of $1, \ldots, n$ such that $2i_1 i_2 - 1, 2i_2 i_3 - 1, \ldots, 2i_{n-1} i_n - 1, 2i_n i_1 - 1$ (resp. $2i_1 i_2 + 1, 2i_2 i_3 + 1, \ldots, 2i_{n-1} i_n + 1, 2i_n i_1 + 1$) are all prime.*

Remark 3.18. For the circular permutation

$$(i_1, \ldots, i_{23}) = (1, 6, 23, 10, 9, 22, 11, 18, 13, 14, 21, 2, 15, 4, 17, 16, 5, 12, 7, 20, 19, 8, 3),$$

all the 23 numbers $i_1 i_2 - 1, i_2 i_3 - 1, \ldots, i_{22} i_{23} - 1, i_{23} i_1 - 1$ are primes.

Acknowledgments. The initial version of this paper was posted to arXiv in Sept. 2013 with the ID `arXiv:1309.1679`. The author would like to thank Prof. Noga Alon for helpful comments, and Prof. Qing-Hu Hou for checking many of the author's conjectures via a computer.

References

[A] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29.

[AB] N. Alon and J. Bourgain, *Additive patterns in multiplicative subgroups*, preprint, 2013.

[Ar] B. Arsovski, *A proof of Snevily's conjecture*, Israel J. Math. **182** (2011), 505–508.

[F] A. Filz, *Problem 1046*, J. Recreational Math., **14**(1982), 64; **15**(1983), 71.

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

[H] W. B. Han, *Polynomials and primitive roots over finite fields*, Acta Math. Sinica **32** (1989), no. 1, 110–117.

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

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

[S13] Z.-W. Sun, Sequences A185645, A227456, A228728, A228762, A228766, A228772, A228886, A228917, A228956, A229005, A229038, A229082, A229130, A229141, A229232 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://oeis.org`.

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.