SOME NEW PROBLEMS IN ADDITIVE COMBINATORICS

ZHI-WEI SUN

ABSTRACT. In this paper we investigate some new problems in additive combinatorics. Our problems mainly involve permutations (or circular permutations) n distinct numbers (or elements of an additive abelian group) $a_1, \ldots, a_n$ with adjacent sums $a_i + a_{i+1}$ (or differences $a_i - a_{i+1}$) pairwise distinct. For an odd prime power $q = 2n + 1 > 13$ with $q \neq 25$, we show that there is a circular permutation $(a_1, \ldots, a_n)$ of the elements of $S = \{a^2 : a \in \mathbb{F}_q \setminus \{0\}\}$ such that $\{a_1 + a_2, \ldots, a_{n-1} + a_n, a_n + a_1\} = S$, where $\mathbb{F}_q$ denotes the field of order q. For any finite subset A of an additive torsion-free abelian group G with $|A| = n > 3$, we prove that there is a numbering $a_1, \ldots, a_n$ of the elements of A such that

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

are pairwise distinct. We also pose 30 open conjectures for further research.

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 [12]. See also Alon [1] 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 $n > 1$ 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.

Corollary 1.1. *There is a circular permutation* $(q_1, \ldots, q_n)$ *of the first* $n > 2$ *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. 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 the circular permutation $(q_1, q_2, \ldots, q_n)$ of $p_1, p_2, \ldots, p_n$ and meets our requirement since $|q_1 - q_2| = q_2 - 2$ and $|q_n - q_1| = p_n - 2$ are both odd while those $q_i - q_{i+1}$ $(1 < i < n)$ are even. $\square$

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 circular 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.

Remark 1.3. For any circular permutation (a_1, a_2, a_3) of $0, 1, 2$, the three numbers $a_1 + 2a_2, a_2 + 2a_3, a_3 + 2a_1$ cannot be pairwise distinct.

Theorem 1.4. *For any odd prime power $n > 2$, there are integers $a_1, a_2, \ldots, a_{\varphi(n)}$ such that both $\{a_1, \ldots, a_{\varphi(n)}\}$ and*

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

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

Remark 1.4. We conjecture that Theorem 1.4 remains valid if we just let $n > 2$ be odd.

Theorem 1.5. *Let $\mathbb{F}_q$ be a finite field with $q = 2n + 1 > 5$ an odd prime power, and set $S = \{a^2 : \ a \in \mathbb{F}_q \setminus \{0\}\}$.*

(i) *If $q \notin \{9, 25\}$, then there is a circular permutation $(a_1, \ldots, a_n)$ of all the n elements of S such that*

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

(ii) *Suppose that $q > 13$ and $q \neq 25$. Then there is a circular permutation $(b_1, \ldots, b_n)$ of all the n elements of S such that*

$$\{b_1 + b_2, \ b_2 + b_3, \ \ldots, \ b_{n-1} + b_n, \ b_n + b_1\} = S.$$

Remark 1.5. In the initial version of this paper posted to arXiv in 2013, the author posed the following conjecture weaker than Theorem 1.5 which was later confirmed by N. Alon and J. Bourgain [2]: For any prime $p = 2n + 1 > 5$, there is a circular permutation $(a_1, \ldots, a_n)$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent differences $a_1 - a_2, a_2 - a_3, \ldots, a_{n-1} - a_n, a_n - a_1$ are quadratic residues modulo p. Also, for any prime $p = 2n+1 > 13$, there is a circular permutation $(b_1, \ldots, b_n)$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent sums $b_1 + b_2, b_2 + b_3, \ldots, b_{n-1} + b_n, b_n + b_1$ are quadratic residues modulo p.

We are going to prove Theorems 1.1-1.5 in the next section, and pose sixteen conjectures concerning permutations in Section 3.

The author [11] proved that for any integer $m > 4$ there is a number $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ such that $\pi(mn) = m + n$, where $\pi(x)$ denotes the number of primes not exceeding x. Sun (cf. [11, Conjecture 4.4] and [10, A247824]) also conjectured that for any $m \in \mathbb{Z}^+$ there is a positive integer n such that $m + n$ divides $p_m + p_n$, where p_k denotes the k-th prime. This has been verified for all $m = 1, \ldots, 10^5$. (The reader may consult [5] for basic knowledge about asymptotic behaviors of $\pi(x)$ and p_n.) With this background, we pose in Section 4 fourteen conjectures involving addition and divisibility.

We have posted to OEIS some sequences (cf. [10]) related to our conjectures in Sections 3 and 4.

2   Proofs of Theorems 1.1-1.5

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. $\qquad\square$

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 $n = 2m$ with $m \in \mathbb{Z}^+$. 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. $\square$

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

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

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

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

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

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

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

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

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

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

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

Proof of Theorem 1.4. Write $n = p^a$ with p an odd prime and a a positive integer. Take a primitive root g modulo n. Note that $g \not\equiv 1 \pmod{p}$ and $g^{\varphi(n)+1} \equiv g \pmod{n}$. 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. So it suffices to take $a_i = g^i$ for $i = 1, \ldots, \varphi(n)$. $\qquad\square$

Lemma 2.1. *Let q be an odd prime power and set $S = \{a^2 : a \in \mathbb{F}_q \setminus \{0\}\}$.*

(i) *The field $\mathbb{F}_q$ has a primitive element g with $g^2 - 1 \in S$ if and only if $q \notin \{3, 5, 9, 25\}$.*

(ii) *The field $\mathbb{F}_q$ has a primitive element g with $g^2 + 1 \in S$ if and only if $q \notin \{3, 5, 7, 9, 13, 25\}$.*

Proof. For an odd prime p let G_p be the set of those integers $g \in \{\pm 1, \ldots, \pm(p-1)/2\}$ which are primitive roots modulo p. Then

$$G_3 = \{-1\}, \ G_5 = \{\pm 1\}, \ G_7 = \{-2, 3\}, \ G_{13} = \{\pm 2, \pm 6\}$$

and

$$G_{61} = \{\pm 2, \pm 6, \pm 7, \pm 10, \pm 17, \pm 18, \pm 26, \pm 30\}.$$

Note that

$$\left(\frac{3^2 - 1}{7}\right) = 1, \ \left(\frac{2^2 - 1}{13}\right) = 1, \ \text{and} \ \left(\frac{2^2 + 1}{61}\right) = 1 = \left(\frac{7^2 - 1}{61}\right),$$

where $(-)$ denotes the Legendre symbol. Thus, it is easy to see that both parts of Lemma 2.1 hold for $q \in \{3, 5, 7, 13, 61\}$.

The field $\mathbb{F}_9$ can be viewed as

$$\mathbb{F}_3[x]/(x^2 + 1) = \{ax + b \bmod x^2 + 1 : a, b \in \mathbb{F}_3 = \{0, \pm 1\}\},$$

and it has four primitive elements: $\pm x \pm 1 \bmod x^2 + 1$. In the ring $\mathbb{F}_3[x]$ we have the congruence

$$(x \pm 1)^2 = x^2 \mp x + 1 \equiv \mp x \pmod{x^2 + 1}.$$

So, for any primitive element g of $\mathbb{F}_9$ neither $g^2 + 1$ nor $g^2 - 1$ belongs to $\{a^2 : a \in \mathbb{F}_9\}$.

Similarly, $\mathbb{F}_{25}$ can be viewed as

$$\mathbb{F}_5[x]/(x^2 - 2) = \{ax + b \bmod x^2 - 2 : a, b \in \mathbb{F}_5 = \{0, \pm 1, \pm 2\}\},$$

and it has eight primitive elements:

$$\pm x \pm 2 \bmod x^2 - 2, \ \text{and} \ \pm 2x \pm 1 \bmod x^2 - 2.$$

In the ring $\mathbb{F}_5[x]$ we have the congruences

$$(x \pm 2)^2 = x^2 \mp x - 1 \equiv 1 \mp x \pmod{x^2 - 2} \text{ and } (2x \pm 1)^2 = -x^2 \mp x + 1 \equiv -1 \mp x \pmod{x^2 - 2}.$$

So, for any primitive element g of $\mathbb{F}_{25}$ neither $g^2 + 1$ nor $g^2 - 1$ belongs to $\{a^2 : a \in \mathbb{F}_{25}\}$.

The field $\mathbb{F}_{121}$ can be viewed as

$$\mathbb{F}_{11}[x]/(x^2 - 2) = \{ax + b \bmod x^2 - 2 : a, b \in \mathbb{F}_{11} = \{0, \pm 1, \ldots, \pm 5\}\},$$

and its primitive elements are the polynomials

$$\pm x \pm 2, \ \pm 2x \pm 2, \ \pm 2x \pm 4, \ \pm 3x \pm 3, \ \pm 3x \pm 5, \ \pm 4x \pm 4, \ \pm 5x \pm 1, \ \pm 5x \pm 5$$

modulo $x^2 - 2$. In the ring $\mathbb{F}_{11}[x]$ we have the congruences

$$(2x + 4)^2 + 1 \equiv (4x + 2)^2 \pmod{x^2 - 2} \text{ and } (x + 2)^2 - 1 \equiv (3x - 3)^2 \pmod{x^2 - 2}.$$

So, there are primitive elements g_1 and g_2 of $\mathbb{F}_{121}$ with $g_1^2 + 1, g_2^2 - 1 \in \{a^2 : a \in \mathbb{F}_{121} \setminus \{0\}\}$.

Now we consider the remaining case: $q > 13$ and $q \notin \{25, 61, 121\}$. Let $\varepsilon \in \{\pm 1\}$. By [4, Corollary 2], there exists a primitive element g of $\mathbb{F}_q$ with $g + \varepsilon g^{-1}$ also primitive. Let $n = (q - 1)/2$. As $g^n = -1 = (g + \varepsilon g^{-1})^n$, we have $(g^2 + \varepsilon)^n = g^n(g + \varepsilon g^{-1})^n = 1$ and hence $g^2 + \varepsilon \in S$.

In view of the above, we have completed the proof of Lemma 2.1. $\square$

Proof of Theorem 1.5. (i) As $q > 5$ and $q \notin \{9, 25\}$, by Lemma 2.1(i), there is a primitive element g_0 of $\mathbb{F}_q$ with $g_0^2 - 1 \in S$. Note that $g = g_0^{-1}$ is also a primitive element of $\mathbb{F}_q$ and $1 - g^2 \in S$. Clearly, $\{g^{2i} : i = 1, \ldots, n\} = S$ and $g^{2(n+1)} = g^2$. Observe that the n elements $g^{2i} - \varepsilon g^{2(i+1)} = g^{2i}(1 - g^2)$ $(i = 1, \ldots, n)$ are pairwise distinct and they all belong to S. This proves part (i) of Theorem 1.5.

(ii) As $q > 13$ and $q \neq 25$, by Lemma 2.1(ii), there is a primitive element g of $\mathbb{F}_q$ with $g^2 + 1 \in S$. Note that $g^2 = g^{2(n+1)}$ and

$$\{g^{2i} : i = 1, \ldots, n\} = S = \{g^{2i}(1 + g^2) = g^{2i} + g^{2(i+1)} : i = 1, \ldots, n\}.$$

So, part (ii) of Theorem 1.5 also holds. $\square$

3 Some Conjectures concerning Permutations

Conjecture 3.1. (2013-09-01) *Let $a_1, a_2, \ldots, a_n$ be $n > 1$ 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, Conjecture 3.1 holds when a_1 is the least element or the largest element of $\{a_1, \ldots, a_n\}$. After learning this conjecture from the initial version of this paper posted to arXiv in 2013, F. Monopoli [8] managed to prove that Conjecture 3.1 holds if the set $A = \{a_1, a_2, \ldots, a_n\}$ forms an arithmetic progression.

Conjecture 3.2. (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 3.2. By Theorem 1.2(ii), Conjecture 3.2 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 $a_1 - a_2 = a_3 - a_4$.

A subset A of a set S with $|A| = n \in \mathbb{Z}^+$ is called an n-subset of S.

Conjecture 3.3. (2013-09-03) *Let $n > 2$ be an integer, and let A be an n-subset of a finite additive abelian group G with $|G|$ odd.*

(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) *If $n = |G| - 1$, then 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 3.3. A conjecture of H. S. Snevily [9] states that for any two n-subsets A and B of an additive abelian group of odd order, we may write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ so that the n sums $a_1 + b_1, \ldots, a_n + b_n$ are pairwise distinct. This was proved by Arsovski [1] in 2009. Note that Conjecture 3.3(i) is stronger than Snevily's conjecture in the case $A = B$. In the spirit of Remark 1.2, the assertion in Conjecture 3.3(i) holds if A is an n-subset of a torsion-free abelian group with $n > 2$. See [10, A228762] for some data related to Conjecture 3.3(ii).

Conjecture 3.4. *Let A be a finite subset of an additive abelian group G with $|A| = n > 3$.*

(i) (2013-09-20) *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) (2017-12-11) *Let B be any n-subset of G. Then we can write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ so that either 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, or the n sums

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

are pairwise distinct.

Remark 3.4. (i) When $A = \{a_1, \ldots, a_n\}$ forms an abelian group G 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 (otherwise $0 \notin \{a_1 - a_2, a_2 - a_3, \ldots, a_n - a_1\} = G$).

(ii) The author has proved part (ii) in the case $A = B$ for $n = 4$. When G is an abelian group of odd order, Conjecture 3.4(ii) is equivalent to Snevily's conjecture confirmed by Arsovski [1] since $a = 2(\frac{|G|+1}{2}a)$ for all $a \in G$.

Conjecture 3.5. (joint with Qing-Hu Hou) (i) (2013-09-05) *For any finite field $\mathbb{F}_q$ with $q > 7$, there is a numbering $a_1, \ldots, a_q$ of all 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 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 3.5. (a) We have verified part (i) for primes q below 545, and part (ii) for primes p below 545. For the field

$$\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1) = \{\overline{ax + b} : \ a, b \in \mathbb{F}_3 = \{0, \pm 1\}\}$$

with $\overline{ax + b}$ the residue class of $ax + b$ modulo $x^2 + 1$, the four primitive elements are $\overline{\pm x \pm 1}$. For the circular permutation

$$(\bar{0}, \overline{-x + 1}, \bar{1}, \overline{-x}, \overline{-x - 1}, \overline{-1}, \overline{x - 1}, \overline{x}, \overline{x + 1})$$

of all the elements of $\mathbb{F}_9$, all the 9 adjacent sums are primitive elements of $\mathbb{F}_9$. 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 element of the field $\mathbb{F}_q$ with $q > 3$ 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 3.6. (2013-09-11) *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 3.6. Compare this conjecture with Theorem 1.5 and Conjecture 3.5(ii).

Conjecture 3.7. (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 $1, \ldots, n$ 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 $1, \ldots, n$ 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 $1, \ldots, n$ 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 3.7. 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. See also [10, A229141] for related data.

Conjecture 3.8. (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 $a_0 + a_1 a_2, a_0 + a_2 a_3, \ldots, a_0 + a_{q-2} a_{q-1}, a_0 + a_{q-1} a_1$ are primitive elements of the field $\mathbb{F}_q$.

Remark 3.8. 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 $i_1 i_2 - 1, i_2 i_3 - 1, \ldots, i_9 i_{10} - 1, i_{10} i_1 - 1$ are primitive roots modulo 11.

Conjecture 3.9. (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 3.9. (i) See [10, A228886] for related data. 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 3.9 can be replaced by $2n \pm 1$.

(ii) Now we explain why Conjecture 3.9 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 3.10. (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 $a_1 a_2, a_2 a_3, ..., a_{n-1} a_n, a_n a_1$ 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* $a_1 a_2, a_2 a_3, ..., a_{n-1} a_n, a_n a_1$ *are also pairwise distinct, unless* $|A| = 4$ *and* A *has the form* $\{\pm s, \pm t\}$.

Remark 3.10. For the set $A = \{1, 2, \ldots, n\}$ with $n \in \{3, 5, 7, \ldots\}$, 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 odd.

Conjecture 3.11. (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* $i_0 + i_1$, $i_1 + i_2$, $\ldots$, $i_{n-1} + i_n$, $i_n + i_0$ *belong to the set* $\{k \in \mathbb{Z}^+ : 6k - 1 \text{ and } 6k + 1 \text{ are twin primes}\}$.

Remark 3.11. 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. [10, A228917]). In 1982 A. Filz [6] (see also [7, 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 3.12. (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 3.12. Recall that 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 3.13. (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 3.13. See [10, A228956 and A229005] for related data. 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 3.14. (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 3.14. See [10, A229082] for related data. 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 3.15. (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 3.15. See [10, A227456] for related data. 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 3.15, we give two desired permutations for $n = 9$:

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

Conjecture 3.16. (2013-09-17) *For any 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 3.16. See [10, A229232] for related data. 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 $i_1i_2 - 1, i_2i_3 - 1, \ldots, i_{22}i_{23} - 1, i_{23}i_1 - 1$ are primes.

4   Conjectures involving Addition and Divisibility

Conjecture 4.1. *Let m be any positive integer.*

(i) (2014-09-29) $m + n$ *divides* $p_m^2 + p_n^2$ *for some* $n \in \mathbb{Z}^+$.

(ii) (2014-09-30) $m + n$ *divides* $p_{m^2} + p_{n^2}$ *for some* $n \in \mathbb{Z}^+$. *Moreover, for $m > 1$ we may require that* $n \leqslant m(m - 1)/2$.

Remark 4.1. See [10, A247975 and A248354] for related data. For $m = 4703$, the least $n \in \mathbb{Z}^+$ with $m + n$ dividing $p_m^2 + p_n^2$ is 760027770. Note also that $2 + 3$ divides $p_{2^2} + p_{3^2} = 7 + 23 = 30$.

Conjecture 4.2. (2014-09-29) *Let $m \in \mathbb{Z}^+$ and $\varepsilon \in \{\pm 1\}$. Then, there is a positive integer n such that*
$$p_{mn} \equiv \varepsilon \pmod{m + n};$$
moreover, we may require $n \leqslant m(m - 1)/2$ if $m > 2$.

Remark 4.2. For example, $p_{2 \times 4} = 19 \equiv 1 \pmod{2 + 4}$. See [10, A248004] for related data.

Conjecture 4.3. (2014-09-30) *Let $m \in \mathbb{Z}^+$. Then $m + n$ divides $\pi(m)^2 + \pi(n)^2$ for some $n \in \mathbb{Z}^+$. Also, $m + n$ divides $\pi(m^2) + \pi(n^2)$ for some $n \in \mathbb{Z}^+$.*

Remark 4.3. See [10, A248044 and A248052] for related data. For example,
$$\pi(5)^2 + \pi(12)^2 = 3^2 + 5^2 = 34 \equiv 0 \pmod{5 + 12}$$
and
$$\pi(4^2) + \pi(8^2) = 6 + 18 = 24 \equiv 0 \pmod{4 + 8}.$$

Conjecture 4.4. (2014-09-27) *Let a be any integer with $a \not\equiv 3 \pmod{6}$. Define the Lucas sequences $(u_n(a))_{n \geqslant 0}$ and $(v_n(a))_{n \geqslant 0}$ by*
$$u_0(a) = 0, \ u_1(a) = 1, \ u_{n+1}(a) = au_n(a) + u_{n-1}(a) \ (n = 1, 2, 3, \ldots),$$
and
$$v_0(a) = 2, \ v_1(a) = a, \ v_{n+1}(a) = av_n(a) + v_{n-1}(a) \ (n = 1, 2, 3, \ldots).$$
Let $m \in \mathbb{Z}^+$. Then there are infinitely many $n \in \mathbb{Z}^+$ with $m + n$ dividing $u_m(a) + u_n(a)$. Also, there are infinitely many $n \in \mathbb{Z}^+$ with $m + n$ dividing $v_m(a) + v_n(a)$.

Remark 4.4. Note that those $F_n = u_n(1)$ $(n = 0, 1, 2, \ldots)$ are the Fibonacci numbers and those $L_n = v_n(1)$ $(n = 0, 1, 2, \ldots)$ are the Lucas numbers. For $m \in \mathbb{Z}^+$, see [10, A247937 and A247940] for the least $n > m$ with $m + n$ dividing $F_m + F_n$ (or $L_m + L_n$). See also [10, A248133, A248136, A248137, A248139, A248142] for similar conjectures.

Conjecture 4.5. *Let m be a positive integer.*

(i) (2014-09-29) $m + n$ *divides* $\binom{2m}{m} + \binom{2n}{n}$ *for some* $n \in \mathbb{Z}^+$.

(ii) (2014-09-29) *If* $m \neq 3$, *then* $m + n$ *divides* $C_m + C_n$ *for some* $n \in \mathbb{Z}^+$ *with* $\gcd(m, n) = 1$, *where* C_k *refers to the Catalan number* $\binom{2k}{k}/(k+1) = \binom{2k}{k} - \binom{2k}{k+1}$.

(iii) (2014-10-01) *For each* $m = 1, 2, 3, \ldots$, *there is a positive integer* n *such that* $\gcd(m, n) = 1$ *and* $mn \mid C_{m+n}$.

Remark 4.5. See [10, A248125, A248124 and A248123] for related data. For example, the least $n \in \mathbb{Z}^+$ with $\gcd(9, n) = 1$ and $(9 + n) \mid (C_9 + C_n)$ is 95; also, $\gcd(4, 21) = 1$, and 4×21 divides $C_{4 \times 21} = 4861946401452$.

Conjecture 4.6. (2014-09-29) *For any integer* $m > 6$, *there is a positive integer* n *with* $\varphi(m)\varphi(n) \equiv 0 \pmod{m + n}$.

Remark 4.6. See [10, A248007] for related data. For example, $\varphi(10)\varphi(14) = 4 \times 6 \equiv 0 \pmod{10 + 14}$.

Conjecture 4.7. (2014-09-29) *Let m be any positive integer. Then $m + n$ divides $\sigma(mn)$ for some $n \in \mathbb{Z}^+$, where $\sigma(k)$ refers to the sum of all positive divisors of k.*

Remark 4.7. See [10, A248008] for related data. For example, $4 + 6$ divides $\sigma(4 \times 6) = 60$.

Conjecture 4.8. (2014-09-29) *Let m be a positive integer.*

(i) *If* $m > 1$, *then* $(m + n) \mid \sigma(m)\varphi(n)$ *for some* $n = 1, \ldots, m$.

(ii) *There is a positive integer* n *such that* $(m + n) \mid \varphi(m)\sigma(n)$. *Moreover, we may require* $n < 2m$ *if* $m > 2$.

Remark 4.8. See [10, A248029 and A248030] for related data. For example,

$$\sigma(8)\varphi(7) = 15 \times 6 = 90 \equiv 0 \pmod{8 + 7}$$

and

$$\varphi(2)\sigma(12) = 28 \equiv 0 \pmod{2 + 12}.$$

Conjecture 4.9. (2014-09-29) *Let m be any positive integer. Then $m + n$ divides $\varphi(m)^2 + \varphi(n)^2$ for some $n \in \mathbb{Z}^+$. Moreover, we may require $n \leqslant m^2$ except for $m = 33$.*

Remark 4.9. See [10, A248035] for related data. For example,

$$\varphi(33)^2 + \varphi(1523)^2 = 20^2 + 1522^2 = 2316884 \equiv 0 \pmod{33 + 1523}.$$

Conjecture 4.10. (i) (2014-09-29) *For any $m \in \mathbb{Z}^+$, we have $(m+n) \mid (\sigma(m)^2 + \sigma(n)^2)$ for some $n \in \mathbb{Z}^+$.*

(ii) (2014-09-30) *For any $m \in \mathbb{Z}^+$, we have $(m+n) \mid (\sigma(m^2) + \sigma(n^2))$ for some $n \in \mathbb{Z}^+$.*

Remark 4.10. See [10, A248036 and A248054] for related data. For example,

$$\sigma(1024)^2 + \sigma(2098177)^2 = 4423875080209 \equiv 0 \pmod{1024 + 2098177}$$

and

$$\sigma(4^2) + \sigma(7^2) = 31 + 57 = 88 \equiv 0 \pmod{4 + 7}.$$

Conjecture 4.11. (2014-10-02) *For $k \in \mathbb{Z}^+$ let $p(k)$ be the number of partitions of k (i.e., unordered ways to write k as a sum of some positive integers with repetitions allowed).*

(i) *For any $m \in \mathbb{Z}^+$, there is a positive integer n such that $m + n$ divides $p(m) + p(n)$.*

(ii) *For any $m \in \mathbb{Z}^+$, there is a positive integer n such that $(m + n) \mid p(mn)$.*

Remark 4.11. See [10, A248143 and A248144] for related data. For example,

$$p(5) + p(13) = 7 + 101 = 108 \equiv 0 \pmod{5 + 13}$$

and

$$p(6 \times 14) = 26543660 \equiv 0 \pmod{6 + 14}.$$

Conjecture 4.12. (2014-09-30) *Let m be any positive integer. Then mn divides $\varphi(m^2 + n^2)$ for some $n \in \mathbb{Z}^+$.*

Remark 4.12. We have verified this for all $m = 1, \ldots, 1242$, see [10, A248058] for related data. For example, for $m = 1093$ the least $n \in \mathbb{Z}^+$ with $mn \mid \varphi(m^2 + n^2)$ is 57343152. In fact,

$$\varphi(1093^2 + 57343152^2) = \varphi(3288237082489753) = 3285228630168576$$
$$= 52416 \times 1093 \times 57343152.$$

If $(mq)^2 + 1$ is prime for some $q \in \mathbb{Z}^+$, then for $n = m^2 q$ we have

$$\varphi(m^2 + n^2) = \varphi(m^2)\varphi(1 + m^2 q^2) = \varphi(m^2)m^2 q^2 \equiv 0 \pmod{mn}.$$

Conjecture 4.13. (2014-10-08) *For any $m \in \mathbb{Z}^+$, there is a positive integer n such that $\varphi(m+n) \mid n$. Moreover, we may require $n \leqslant m(m-1)$ for $m > 1$.*

Remark 4.13. See [10, A248568] for related data. For example, $\varphi(10+40) = 20$ divides 40.

Conjecture 4.14. (2014-10-05) *Let m be any positive integer. Then $p_{m+n} - p_n$ divides $m+n$ for some $n \in \mathbb{Z}^+$. Also, $p_{m+n} - p_n$ divides n for some $n \in \mathbb{Z}^+$.*

Remark 4.14. See [10, A248366 and A248369] for related data. For example, $p_{5+175} - p_{175} = 1069 - 1039 = 30$ divides $5 + 175 = 180$ and $p_{7+80} - p_{80} = 449 - 409 = 40$ divides 80.

References

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

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

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

[4] S. D. Cohen, T. Oliveira e Silva and N. Sutherland, *Linear combinations of primitive elements of a finite field*, Finite Fields Appl. **51** (2018), 388–406.

[5] R. Crandall and C. Pomerance, Prime Numbers: A Computational Perspective, Springer, New York, 2001.

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

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

[8] F. Monopoli, *Absolute differences along Hamiltonian paths*, Electron. J. Combin. **22** (2015), no. 3, #P3.20, 1–8.

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

[10] Z.-W. Sun, Sequences A227456, A228762, A228886, A228917, A228956, A229005, A229038, A229082, A229141, A229232, A247824, A247937, A247940, A247975, A248004, A248007, A248008, A248029, A248030, A248035, A248036, A248044, A248052, A248054, A248058, A248123, A248124, A248125, A248133, A248136, A248137, A248139, A248142, A248143, A248144, A248354, A248366, A248369, A248568 in OEIS (On-Line Encyclopedia of Integer Sequences), `http://oeis.org`

[11] Z.-W. Sun, *A new theorem on the prime-counting function*, Ramanujan J. **42** (2017), 59–67.

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

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

E-mail address: zwsun@nju.edu.cn