A talk given at Zhejiang Univ. (Nov. 15, 2013)
and Frontiers in Combinatorics (Beijing, Dec. 15, 2013)
and Xiamen Univ. (Dec. 20, 2013)
and the 2nd Workshhop on Combinatorics and Graph Theory
(Changsha, June 2, 2014)
and Institute of Math., Academia Sinica (Taipei, July 24, 2014)
and Conf. on Combinatorics and its Appl. (Harbin, May 19, 2018)
and St. Petersburg Dept. of Steklov Math. Institute
of Russian Academy of Sci. (July 19, 2018)

Determinants, Permutations and Additive Combinatorics

Zhi-Wei Sun

Nanjing University, Nanjing 210093, P. R. China

Abstract

In this talk we will introduce some new problems and related progress on determinants involving Legendre symbols, circular permutations and additive combinatorics. For example, we conjecture that for any finite subset A of an additive cyclic group G with $|A| = n > 3$, there is a circular permutation $a_1, \ldots, a_n$ of 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. The speaker has proved this when G is the infinite cyclic group $\mathbb{Z}$.

Part I. Some new problems on determinants

Hankel-type determiants

For an $n \times n$ matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$ over the field of complex numbers, we often write $\det A$ in the form $|a_{ij}|_{1 \leqslant i,j \leqslant n}$.

For a sequence $a_0, a_1, a_2, \ldots$ of numbers, the determinants $|a_{i+j}|_{0 \leqslant i,j \leqslant n}$ are said to be of the Hankel type.

For $b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$ $(n = 0, 1, 2, \ldots)$, it is known that

$$|a_{i+j}|_{0 \leqslant i,j \leqslant n} = |b_{i+j}|_{0 \leqslant i,j \leqslant n}.$$

For Catalan numbers $C_n = \frac{1}{n+1}\binom{2n}{n}$ $(n = 0, 1, 2, \ldots)$, the Hankel-type determinant $|C_{i+j}|_{0 \leqslant i,j \leqslant n}$ takes the value 1.

Legendre symbols

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol $\left(\frac{a}{p}\right)$ is given by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for some } x \in \mathbb{Z}, \\ -1 & \text{if } p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ for no } x \in \mathbb{Z}. \end{cases}$$

It is well known that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any $a, b \in \mathbb{Z}$. Also,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv -1 \pmod{4}; \end{cases}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

The Law of Quadratic Reciprocity: If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Chapman's work on determinants with Legendre symbol entries

In 2004, R. Chapman [Acta Arith.] used quadratic Gauss sums to determine the values of

$$\left|\left(\frac{i+j-1}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2} \quad \text{and} \quad \left|\left(\frac{i+j-1}{p}\right)\right|_{1\leqslant i,j\leqslant (p+1)/2}.$$

Since $(p+1)/2-i+(p+1)/2-j-1\equiv -(i+j) \pmod p$, we see that

$$\left|\left(\frac{i+j-1}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2} = \left(\frac{-1}{p}\right)\left|\left(\frac{i+j}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2}$$

and

$$\left|\left(\frac{i+j-1}{p}\right)\right|_{1\leqslant i,j\leqslant (p+1)/2} = \left|\left(\frac{i+j}{p}\right)\right|_{0\leqslant i,j\leqslant (p-1)/2}.$$

Chapman's evil determinants

Conjecture (Chapman, 2003) Let p be an odd prime, and write

$$\varepsilon_p^{(2-(\frac{2}{p}))h(p)} = r_p + s_p\sqrt{p} \text{ with } r_p, s_p \in \mathbb{Z},$$

where ε_p and $h(p)$ denote the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively. Then

$$\left| \left(\frac{j-i}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2} = \begin{cases} -r_p & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

As Chapman could not solve this problem for several years, he called the determinant *evil*.

Chapman's conjecture on his "evil" determinant was recently confirmed by M. Vsemirnov [Linear Algebra Appl. 2012, and Acta Arith. 2013] via matrix decomposition and quadratic Gauss sums.

Determining $\left|\left(\frac{i+dj}{p}\right)\right|_{0\leqslant i,j\leqslant (p-1)/2} \bmod p$

Theorem (Sun, 2013). Let p be an odd prime. For $d \in \mathbb{Z}$ define

$$R(d,p) := \left| \left(\frac{i+dj}{p}\right) \right|_{0\leqslant i,j\leqslant (p-1)/2}.$$

If $p \equiv 1 \pmod 4$, then

$$R(d,p) \equiv \left(\left(\frac{d}{p}\right) d\right)^{(p-1)/4} \frac{p-1}{2}! \pmod p.$$

When $p \equiv 3 \pmod 4$, we have

$$R(d,p) \equiv \begin{cases} \left(\frac{2}{p}\right) \pmod p & \text{if } \left(\frac{d}{p}\right) = 1, \\ 1 \pmod p & \text{if } \left(\frac{d}{p}\right) = -1. \end{cases}$$

Also,

$$R(-d,p) \equiv \left(\frac{2}{p}\right) R(d,p) \pmod p,$$

$$\left| \left(\frac{i+dj+c}{p}\right) \right|_{0\leqslant i,j\leqslant (p-1)/2} \equiv R(d,p) \pmod p \quad \text{for all } c \in \mathbb{Z}.$$

Determining $\left|\left(\frac{i^2+dj^2}{p}\right)\right|_{0\leqslant i,j\leqslant (p-1)/2} \bmod p$

Theorem (Sun, 2013) Let p be an odd prime and let $d \in \mathbb{Z}$. Define

$$T(d,p) := \left| \left(\frac{i^2+dj^2}{p}\right) \right|_{0\leqslant i,j\leqslant (p-1)/2}.$$

Then

$$\left(\frac{T(d,p)}{p}\right) = \begin{cases} \left(\frac{2}{p}\right) & \text{if } \left(\frac{d}{p}\right) = 1, \\ 1 & \text{if } \left(\frac{d}{p}\right) = -1. \end{cases}$$

Also,

$$T(-d,p) \equiv \left(\frac{2}{p}\right) T(d,p) \pmod{p}$$

and

$$\left| \left(\frac{i^2+dj^2+c}{p}\right) \right|_{0\leqslant i,j\leqslant (p-1)/2} \equiv T(d,p) \pmod{p} \quad \text{for all } c \in \mathbb{Z}.$$

Some auxiliary results

A Known Result. Let $P(z)=\sum_{k=0}^{n-1} a_k z^k$ be a polynomial with complex number coefficients. Then we have

$$|P(x_i+y_j)|_{1\leqslant i,j\leqslant n}=a_{n-1}^n\prod_{k=0}^{n-1}\binom{n-1}{k}\times\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)(y_j-y_i).$$

Zolotarev's Theorem (1872). Let p be any odd prime, and let $a\in\mathbb{Z}$ with $p\nmid a$. For $m\in\mathbb{Z}$ let $\{m\}_p$ denote the least nonnegative residue of an integer m modulo p. Then, the permutation $\{aj\}_p$ $(j=1,\ldots,p-1)$ of $1,\ldots,p-1$ has the sign $(\frac{a}{p})$.

Theorem (H. Pan, 2006) Let p be an odd prime, and let $a\in\mathbb{Z}$ with $p\nmid a$. For each $j=1,\ldots,(p-1)/2$ let $\sigma_a(j)$ be the unique $r\in\{1,\ldots,(p-1)/2\}$ such that $aj\equiv r$ or $-r\pmod p$. Then, the sign of the permutation σ_a equals $(\frac{a}{p})^{(p+1)/2}$.

Conjecture on $\left|\left(\frac{i^2+dj^2+c}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2}$

Conjecture→Theorem (Sun, July 2013) Let p be an odd prime, and define

$$S(d,p):=\left|\left(\frac{i^2+dj^2}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2}\quad\text{for } d\in\mathbb{Z}.$$

If $\left(\frac{d}{p}\right)=1$, then $\left(\frac{-S(d,p)}{p}\right)=1$. If $\left(\frac{d}{p}\right)=-1$, then $S(d,p)=0$.

Conjecture (Sun, August 2013) Let p be an odd prime, and let $c,d\in\mathbb{Z}$ with $p\nmid cd$. Define

$$S_c(d,p)=\left|\left(\frac{i^2+dj^2+c}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2}.$$

Then

$$\left(\frac{S_c(d,p)}{p}\right)=\begin{cases}1 & \text{if } \left(\frac{c}{p}\right)=1\ \&\ \left(\frac{d}{p}\right)=-1,\\ \left(\frac{-1}{p}\right) & \text{if } \left(\frac{c}{p}\right)=\left(\frac{d}{p}\right)=-1,\\ \left(\frac{-2}{p}\right) & \text{if } \left(\frac{-c}{p}\right)=\left(\frac{d}{p}\right)=1,\\ \left(\frac{-6}{p}\right) & \text{if } \left(\frac{-c}{p}\right)=-1\ \&\ \left(\frac{d}{p}\right)=1.\end{cases}$$

Conjectures on $\left|\left(\frac{i^2+cij+dj^2}{n}\right)\right|_{1\leqslant i,j\leqslant n-1}$

For any odd integer $n>1$ and integers c and d, I introduced the notations

$$(c,d)_n:=\left|\left(\frac{i^2+cij+dj^2}{n}\right)\right|_{1\leqslant i,j\leqslant n-1}.$$

Conjecture (Sun, 2013). If d is nonzero, then there are infinitely many odd primes p with $(c,d)_p=0$. When $(c,d)_p$ is nonzero, its p-adic valuation (i.e., p-adic order) must be even.

Theorem (Sun). Let $c,d\in\mathbb{Z}$. Then $(c,d)_n=0$ for any positive odd integer n with $(\frac{d}{n})=-1$.

Conjecture (Sun). (i) For any odd integer $n>3$ we have $(2,3)_n\equiv 0\pmod{n^2}$.

(ii) For any odd integer $n>5$ we have $(6,15)_n\equiv 0\pmod{n^2}$.

Two more conjectures

Conjecture (Sun). (i) $(6,1)_n = (3,2)_n = (4,2)_n = 0$ for any positive integer $n \equiv 3 \pmod 4$.

(ii) $(3,3)_n = 0$ for any positive odd integer $n \not\equiv 1 \pmod{12}$.

Remark. This has just been confirmed by F. Petrov, Z.-W. Sun and M. Vsemirnov jointly.

Conjecture (Sun, 2013). Let $p = 2n+1$ be an odd prime. Then

$$\left| \left(\frac{i^2 - n!j}{p} \right) \right| = 0 \iff p \equiv 3 \pmod 4.$$

Remark. Fedor Petrov has solved the mod p version of this conjecture.

A curious conjecture

Theorem (Sun). (i) For any odd prime p, we have

$$\left|\frac{\left(\frac{i+j}{p}\right)}{i+j}\right|_{1\leqslant i,j\leqslant(p-1)/2}\equiv\begin{cases}\left(\frac{2}{p}\right)\pmod p & \text{if } p\equiv 1\pmod 4,\\ ((p-1)/2)!\pmod p & \text{if } p\equiv 3\pmod 4.\end{cases}$$

(ii) Let $p\equiv 3\pmod 4$ be a prime. Then

$$\left|\frac{1}{i^2+j^2}\right|_{1\leqslant i,j\leqslant(p-1)/2}\equiv\left(\frac{2}{p}\right)\pmod p.$$

Conjecture (Sun, August 2013). (i) For any prime $p>3$, we have

$$\left|(i^2+j^2)\left(\frac{i^2+j^2}{p}\right)\right|_{0\leqslant i,j\leqslant(p-1)/2}\equiv 0\pmod p.$$

(Confirmed by D. Grinberg, G.-N. Han, Z.-W. Sun and L.-L. Zhao.)
(ii) If $p>5$ and $p\equiv 1\pmod 4$, then

$$\left|(i+j)\left(\frac{i+j}{p}\right)\right|_{1\leqslant i,j\leqslant(p-1)/2}\text{ and }\left|(j-i)\left(\frac{j-i}{p}\right)\right|_{1\leqslant i,j\leqslant(p-1)/2}$$

are quadratic residues modulo p.

A conjecture involving Domb numbers

Conjecture (Sun, August 2013). Define Domb numbers by

$$D_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k} \binom{2(n-k)}{n-k} \ (n = 0, 1, \ldots),$$

Then, for any prime p, we have

$$|D_{i+j}|_{0 \leqslant i,j \leqslant p-1} \equiv \begin{cases} (\frac{-1}{p})(4x^2 - 2p) \pmod{p^2} & \text{if } p = x^2 + 3y^2, \\ 0 \pmod{p^2} & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

We also have some other similar conjectures.

Another conjecture involving binary quadratic forms

Conjecture (Sun, August 2013). For $n = 0, 1, 2, \ldots$ let

$$h_n = \sum_{k=0}^{n} \binom{n}{k}^2 C_k \quad \text{with } C_k = \frac{\binom{2k}{k}}{k+1} \text{ (the } k\text{-th Catalan number).}$$

Let p be any odd prime. If $p \equiv 1 \pmod 3$ and $p = x^2 + 3y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 3$, then

$$|h_{i+j}|_{0 \leqslant i,j \leqslant p-1} \equiv (-1)^{(p-1)/2} \left(2x - \frac{p}{2x}\right) \pmod{p^2}.$$

If $p \equiv 2 \pmod 3$ then

$$|h_{i+j}|_{0 \leqslant i,j \leqslant p-1} \equiv (-1)^{(p+1)/2} \frac{3p}{\binom{(p+1)/2}{(p+1)/6}} \pmod{p^2}.$$

One more conjecture involving binary quadratic forms

Conjecture (Sun, August 2013). For $n = 0, 1, 2, \ldots$ let

$$w_n = \sum_{k=0}^{\lfloor n/3 \rfloor} (-1)^k 3^{n-3k} \binom{n}{3k} \binom{2k}{k} \binom{3k}{k} \quad \text{and} \quad W_n = |w_{i+j}|_{0 \leqslant i,j \leqslant n}.$$

(i) For any prime $p \equiv 1 \pmod 3$, write $4p = x^2 + 27y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 3$, then

$$W_{p-1} \equiv (-1)^{(p+1)/2} \left(x - \frac{p}{x}\right) \pmod{p^2}.$$

(ii) $W_n = 0$ if and only if $n \equiv 1 \pmod 3$.

Remark. C. Krattenthaler has confirmed that $W_n = 0$ for any $n \equiv 1 \pmod 3$.

Joint work with Bao-Xuan Zhu [Int. J. Number Theory, 14(2018), 1265-1277]

`From the abstract`: In this paper we confirm several conjectures of Z.-W. Sun on Hankel-type determinants for some combinatorial sequences including Franel numbers, Domb numbers and Apéry numbers. For any nonnegative integer n, define

$$f_n := \sum_{k=0}^{n} \binom{n}{k}^3,\ D_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k} \binom{2(n-k)}{n-k},$$

$$b_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k},\ A_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2.$$

For $n = 0, 1, 2, \ldots$, we show that $6^{-n}|f_{i+j}|_{0\le i,j\le n}$ and $12^{-n}|D_{i+j}|_{0\le i,j\le n}$ are positive odd integers, and $10^{-n}|b_{i+j}|_{0\le i,j\le n}$ and $24^{-n}|A_{i+j}|_{0\le i,j\le n}$ are always integers.

Some open conjectures on Hankel-type determinants

Recall the two kinds of Apéry numbers

$$b_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k} \text{ and } A_n := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \ (n = 0, 1, \ldots).$$

Conjecture 1 (Sun, August 14, 2013). We have $|b_{i+j}|_{0\leqslant i,j\leqslant n} > 0$ and $|A_{i+j}|_{0\leqslant i,j\leqslant n} > 0$ for all $n = 0, 1, 2, \ldots$.

Conjecture 2 (Sun, August 2013). For any positive integer n, we have

$$|B_{i+j}^2|_{0\leqslant i,j\leqslant n} < 0 \quad \text{and} \quad |E_{i+j}^2|_{0\leqslant i,j\leqslant n} > 0,$$

where the Bernoulli numbers $B_0, B_1, B_2, \ldots$ and the Euler numbers $E_0, E_1, E_2, \ldots$ are given by

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} \quad \text{and} \quad \frac{2}{e^x + e^{-x}} = \sum_{n=0}^{\infty} E_n \frac{x^n}{n!}.$$

A conjecture involving the Möbius function

Möbius function:

$$\mu(n)=\begin{cases}1 & \text{if } n=1,\\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes},\\ 0 & \text{if } n \text{ is not squarefree.}\end{cases}$$

Conjecture (Sun, August 2013). For any positive integer n, we have

$$|\mu(i+j-1)|_{1\leqslant i,j\leqslant n}\neq 0 \quad \text{and} \quad |\mu^2(i+j)|_{1\leqslant i,j\leqslant n}\neq 0.$$

Conjecture (Sun, August 2013). Let $f(p)$ take 1 or 0 according as p is prime or not. Then, for any integer $n>15$ we have

$$|f(i+j)|_{1\leqslant i,j\leqslant n}\neq 0.$$

Part II. Some open problems in additive combinatorics

Filz's Prime Circle Problem

Filz's Conjecture (1982). 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.

Filz's Conjecture in Graph-Theoretic Language. Let n be a positive even integer. Construct a simple graph G with vertices $1, \ldots, n$ such that the vertices i and j are adjacent if and only of $i + j$ is prime. Then G is a Hamiltonian graph.

A Similar Observation (conjectured by Sun and proved by Y.-G. Chen). For any integer $n > 4$, there is a circular permutation $i_1, \ldots, i_n$ of $1, \ldots, n$ such that

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

are prime.

Two conjectures involving $|i \pm j|$ and $|i^2 - j^2|$

Conjecture (Sun, 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.

Conjecture (Sun, 2013-09-10). For any positive integer $n \neq 2, 4$, there is a circular permutation $i_0, i_1, \ldots, i_n$ of $0, \ldots, n$ 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.

Circular permutations related to twin primes

Conjecture (Sun, 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. This conjecture implies the twin prime conjecture. Qing-Hu Hou has verified it for all $n \leqslant 100$. For $n = 10$ we may take the circular permutation $(0, 5, 2, 3, 9, 1, 6, 4, 8, 10, 7)$.

Let $a(n)$ denote the number of undirected circular permutation $i_0, i_1, \ldots, i_n$ of $0, 1, \ldots, n$ meeting the requirement. I found the values of $a(1), \ldots, a(9)$: 1, 1, 1, 2, 2, 2, 5, 2, 12. Later Max Alekseyev computed $a(n)$ for $n = 10, \ldots, 25$.

$$39,\ 98,\ 526,\ 2117,\ 6663,\ 15043, 68403,\ 791581,\ 4826577,$$
$$19592777,\ 102551299,\ 739788968,\ 4449585790,$$
$$36547266589,\ 324446266072,\ 2743681178070.$$

Theorem (Sun, 2013-08) 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.

Proof. 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

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

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

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

Corollary. 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.

Conjecture (Sun, 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.

Francesco Monopoli [Electron. J. Combin. 22(2015), no. 3, #P3.20]: The conjecture holds if the set $A = \{a_1, a_2, \ldots, a_n\}$ forms an arithmetic progression.

Circular permutations of quadratic residues (I)

Conjecture (Sun, 2013-09). For any prime $p = 2n + 1 > 13$, 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 sums

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

are quadratic residues (or quadratic nonresidues) modulo p. Also, for any prime $p = 2n + 1 > 5$, there is a circular permutation $b_1, \ldots, b_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent differences

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

are quadratic residues (or quadratic nonresidues) modulo p.

Circular permutations of quadratic residues (I)

Conjecture (Sun, 2013-09). For any prime $p = 2n + 1 > 13$, 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 sums

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

are quadratic residues (or quadratic nonresidues) modulo p. Also, for any prime $p = 2n + 1 > 5$, there is a circular permutation $b_1, \ldots, b_n$ of the $(p-1)/2 = n$ quadratic residues modulo p such that all the n adjacent differences

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

are quadratic residues (or quadratic nonresidues) modulo p.

Later this was confirmed by **N. Alon and J. Bourgain** [Geom. Funct. Anal. 24(2014), 721-739]. Below is a lemma.

B. Jacobson (JCTB 1980): For each $k > 1$, any 2-connected k-regular graph with at most $3k$ vertices is Hamiltonian.

Alon and Bourgain's general result

Theorem (Alon & Bourgain). There exists a constant $c > 0$ such that for any prime power q and For any multiplicative subgroup A of the finite field $\mathbb{F}_q$ with

$$|A| = d \geq cq^{3/4} \frac{\sqrt{(\log q)(\log\log\log q)}}{\log\log q},$$

there is a numbering $a_1, a_2, \ldots, a_d$ of the elements of A such that

$$a_1 + a_2,\ a_2 + a_3,\ \ldots,\ a_{d-1} + a_d,\ a_d + a_1$$

all belong to A.

Their tools include algebraic graph theory and probability method.

A Key Lemma (Krivelevich & Sudakov). Let G be a d-regular graph with n vertices. If n is large enough, and the absolute value of each nontrivial eigenvalue of the adjacency matrix of G is smaller than $d(\log\log n)^2/(1000(\log n)\log\log\log n)$, then G is a Hamiltonian graph.

Circular permutations of quadratic residues (II)

Theorem (Sun, Oct. 2013). Let $\mathbb{F}_q$ be a finite field with $q = 2n+1 > 2^{66}$ elements. Set

$$S = \{a^2 : \ a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}\} \ \text{ and } \ T = F_q^* \setminus S.$$

Then, there is a circular permutation $a_1, \ldots, a_n$ of all the elements of S such that

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

Also, there is a circular permutation $a_1, \ldots, a_n$ of all the elements of S such that

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

Circular permutations of quadratic residues (II)

Proof. Let $\varepsilon \in \{\pm 1\}$, and $R = S$ or T. Choose an element $a \in T$. By a result of Wenbao Han [Acta Math. Sinica 32(1989)], there exists a primitive root g of $\mathbb{F}_q$ such that $1 + \varepsilon g^2$ (or $a + \varepsilon a g^2$) is also a primitive root and hence an element of T. So there is a primitive root g with $1 + \varepsilon g^2 \in R$. Set $a_i = g^{2i}$ for $i = 1, \ldots, n$. Then

$$\{a_1, a_2, \ldots, a_n\} = S \quad \text{and} \quad \{a_1 + \varepsilon a_2, \ldots, a_n + \varepsilon a_1\} = R.$$

Note that

$$g^{2i} + \varepsilon g^{2(i+1)} = g^{2i}(1 + \varepsilon g^2) \in R \quad \text{for all } i = 1, \ldots, n.$$

Remark. 2^{66} in the theorem can be reduced to 13 via a complicated analysis.

A conjecture on primitive roots

Conjecture (joint with Q.-H. Hou, 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 $\mathbb{F}_q$).

Remark. We have verified this for all primes $q < 545$.

Two more conjectures on primitive roots

Conjecture (Sun, 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 roots of the filed $\mathbb{F}_q$.

Conjecture (Sun, 2013-04-24) For any prime q, there is a partition number $p(n) < q$ which is a primitive root modulo q, where $p(n)$ denotes the number of ways to write n as a sum of positive integers with the order of addends ignored.

Two conjectures related to coprime properties

Conjecture (Sun, 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. I have proved this for any positive odd integer n.

Conjecture (Sun, 2013-10-04). Let $n > 1$ be odd. Then there is a reduced system $\{a_1, \ldots, a_{\varphi(n)}\}$ of residues modulo n such that

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

is also a reduced system of residues modulo n.

Remark. I have proved this for any odd prime power n.

A conjecture on n real numbers

Conjecture (Sun, 2013-09-22) 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 $\{\pm r, \pm s, \pm t\}$.

Remark. For the set $A = \{1, 2, \ldots, n\}$ with n an odd prime power, the natural order of the elements of A meets the requirement. We also have a similar conjecture involving differences and products.

On polynomials over finite fields

It is known that $\sum_{a\in\mathbb{F}_q} a^k = 0$ for all $k = 0, 1, \ldots, q-2$, where $\mathbb{F}_q$ denotes the finite field of q elements.

Conjecture (Sun, 2013-09-30). (i) For any finite field $\mathbb{F}_q$ and a polynomial $P(x) \in \mathbb{F}_q[x]$ of degree smaller than $q-1$, if $P(x)$ is not of the form $c - x$, then there is a circular permutation $a_1, \ldots, a_q$ of all the elements of $\mathbb{F}_q$ with

$$\{P(a_1) + a_2,\ P(a_2) + a_3,\ \ldots,\ P(a_{q-1}) + a_q,\ P(a_q) + a_1\} = \mathbb{F}_q.$$

(ii) Let F be any field with $|F| > 7$, and let A be a finite subset of F with $|A| = n > 2$. Let $P(x) \in F[x]$ with $\deg(P) < p-1$ if F is of prime characteristic p. If $P(x)$ is not of the form $c - x$, then there is a circular permutation $a_1, \ldots, a_n$ of all the elements of A such that the n sums

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

are pairwise distinct.

A conjecture related to Snevily's conjecture

Snevily's Conjecture (proved by Arsovski in 2011). Let G be any abelian group of odd order, and let A and B be finite subsets of G with $|A| = |B| = n$. Then there is a numbering $a_1, \ldots, a_n$ of the n elements of A and a numbering $b_1, \ldots, b_n$ of the n elements of B such that $a_1 + b_1,\ a_2 + b_2,\ \ldots,\ a_n + b_n$ are pairwise distinct.

Conjecture (Sun, 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.

A conjecture involving $a_i + 2a_{i+1}$

Conjecture $(2013\text{-}09\text{-}20)$ Let G be an additive abelian group.

(i) If G is finite with $|G| \not\equiv 0 \pmod 3$, then for any finite subset A of G with $|A| = n > 3$, 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) Let A and B be finite subsets of G with $|A| = |B| = n$. Then we can write $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ so that either

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

are pairwise distinct, or

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

are pairwise distinct.

Remark. When $A = \{a_1, \ldots, a_n\}$ is an abelian group of the form $(\mathbb{Z}/3\mathbb{Z})^r$, $a_1 + 2a_2 = a_1 - a_2$, ..., $a_n + 2a_1 = a_n - a_1$ cannot be pairwise distinct. Part (i) holds with G torsion-free.

A theorem involving three subsets

Motivated by Snevily's conjecture, we obtained the following result involving three subsets.

Theorem (Sun, [Math. Res. Lett. 15(2008)]). Let G be an abelian group with cyclic torsion group, and let A, B, C be subsets of G with $|A| = |B| = |C| = n$. Then, there is a numbering $a_1, \ldots, a_n$ of the n 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 $a_1 + b_1 + c_1, \ldots, a_n + b_n + c_n$ are pairwise distinct.

Corollary. Let N be any positive integer. For the $N \times N \times N$ Latin cube over Z/NZ formed by the Cayley addition table, each $n \times n \times n$ subcube with $n \leqslant N$ contains a Latin transversal.

Conjecture (Sun, [Math. Res. Lett. 15(2008)]). Every $n \times n \times n$ Latin cube contains a Latin transversal.

Remark. In 1967 Ryser conjectured that every Latin square of odd order has a Latin transversal.

A conjecture for abelian groups with no involution

An element of a group is called an *involution* if its order is two.

Conjecture (Sun, 2013-09-04). Let G be an additive abelian group. If G is cyclic or G contains no involution, then for any finite subset A of G with $|A| = n > 3$, there is a numbering $a_1, \ldots, a_n$ of all the n 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.

Remark. For a finite abelian group $G = \{a_1, a_2, \ldots, a_n\}$, it is easy to see that $2(a_1 + \cdots + a_n) = 0$.

Theorem (Sun, 2013-09-19). The conjecture holds for any *torsion-free* abelian group G.

Remark. (1) I became too tired and ill immediately after I spent the whole day to finish the proof of this theorem.
(2) The conjecture is even open for cyclic groups of odd prime orders.

For sources of my conjectures, you may visit

http://math.nju.edu.cn/∼zwsun
http://arxiv.org/abs/1308.2900
http://arxiv.org/abs/1309.1678.
http://arxiv.org/abs/1405.0290.

You are welcome to solve my conjectures!

Thank you!