An on-line talk (June 26, 2020)

Introduction to Combinatorial Number Theory (VI)

– Permutations, Determinants and Permanants

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

June 26, 2020

Abstract

In this talk we introduce results and conjectures on permutations, determinants and permanants, most of them are related to Legendre symbols.

Part I. On Permutations

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.

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 involving circular permutations

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 G be an additive abelian group G of odd order. For any $A \subseteq G$ with $|A| = n > 2$, 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.

Remark. (i) In 2020, Mr. Yu-Xuan Ji at Nanjing Univ. verified this for $|G| < 30$.
(ii) If $G = \{a_1, \ldots, a_n\}$ is an additive abelian group with $|G| = n$ odd, then $a_1 + \ldots + a_n = 0$ since $a \neq -a$ for all $a \in G \setminus \{0\}$.

Another conjecture involving circular permutations

Conjecture (Sun, 2013-09-04). Let G be an additive abelian group with $\mathrm{Tor}(G)$ cyclic or odd. 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. The conjecture is even open for $G = \mathbb{Z}/p\mathbb{Z}$ with p an odd prime.

A conjecture for finite fields

Theorem (Sun [Nanjing Univ. Math. Biquarterly 36(2019)]). For any odd prime power $q = 2n + 1 > 13$ with $q \neq 25$, 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.

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 $q < 545$.

Definition of signs of permutations

Recall that for a permutation $a_{\sigma(1)}, \ldots, a_{\sigma(n)}$ of n distinct numbers $a_1, \ldots, a_n$, its *sign* (or *signature*) is given by

$$\operatorname{sign}(\sigma) := (-1)^{\mathsf{Inv}(\sigma)},$$

where

$$\mathsf{Inv}(\sigma) := |\{(i,j) : \ 1 \leqslant i < j \leqslant n \ \&\ \sigma(i) > \sigma(j)\}|$$

is the number of *inverse pairs* of σ. The permutation is said to be *odd* or *even* according as $\operatorname{sign}(\sigma)$ is -1 or 1.

Let S_n be the symmetric group of all the permutations on $\{1, \ldots, n\}$. It is well known that

$$\operatorname{sign}(\sigma\tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau) \ \text{ for all } \sigma, \tau \in S_n.$$

On the inverse of k modulo m

For a prime p and each $k = 1, \ldots, p-1$ let $\bar{k}$ be the inverse of k mod p (i.e., $1 \leqslant \bar{k} \leqslant p-1$ and $k\bar{k} \equiv 1 \pmod{p}$). Then the list $\bar{1}, \ldots, \overline{p-1}$ is a permutation of $1, \ldots, p-1$. What's the sign of this permutation?

Let $m > 1$ be a general odd integer, and let $a_1 < \ldots < a_{\varphi(m)}$ be all the numbers among $1, \ldots, m-1$ relatively prime to m. For each $k \in \{1, \ldots, m-1\}$ with $\gcd(k, m) = 1$, let $\sigma_m(k) = \bar{k}$ be the inverse of k modulo m, that is, $\bar{k} \in \{1, \ldots, m-1\}$ and $k\bar{k} \equiv 1 \pmod{m}$. Then σ_m is a permutation of $a_1, \ldots, a_{\varphi(m)}$.

Theorem (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]). For any odd integer $m > 1$, we have

$$\mathrm{sign}(\sigma_m) = -1 \iff m \text{ is a power of a prime } p \equiv 1 \pmod{4}.$$

In particular, $\mathrm{sign}(\sigma_p) = (-1)^{(p+1)/2}$ for each odd prime p.

Quadratic residues modulo primes

Let p be an odd prime. For $a \in \mathbb{Z}$ with $p \nmid a$, if $x^2 \equiv a \pmod{p}$ for some $x \in \mathbb{Z}$, then a is called a *quadratic residue* modulo p, otherwise a is called a quadratic nonresidue modulo p.

For example, $1, 2, 4$ are quadratic residues mod 7, and $3, 5, 6$ are quadratic nonresidue mod 7. (Note that $3^2 \equiv 2 \pmod{7}$.)

If $x = pq + r$ with $q, r \in \mathbb{Z}$ and $|r| \leqslant (p-1)/2$, then

$$x^2 \equiv r^2 = |r|^2 \pmod{p}.$$

If $0 \leqslant j < k \leqslant (p-1)/2$, then

$$k^2 - j^2 = (k-j)(k+j) \not\equiv 0 \pmod{p}.$$

Therefore

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

give all the $(p-1)/2$ quadratic residues modulo p.

Legendre symbols and Jacobi symbols

Let $a \in \mathbb{Z}$. For an odd prime p, the *Legendre symbol* $\left(\frac{a}{p}\right)$ is given by

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

Let n be a positive odd integer. Then the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is given by

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & \text{if } n = 1, \\ \prod_{i=1}^{r} \left(\frac{a}{p_i}\right) & \text{if } n = p_1 \dots p_r \text{ with } p_1, \dots, p_r \text{ prime.} \end{cases}$$

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

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

Zolotarev's Lemma

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, let $\{a\}_n$ denote the least nonnegative residue of a modulo n.

Zolotarev's Lemma (1872). Let p be any odd prime, and let $a \in \mathbb{Z}$ with $p \nmid a$. Then, the permutation $\{aj\}_p$ $(j = 1, \ldots, p-1)$ of $1, \ldots, p-1$ has the sign $(\frac{a}{p})$.

Frobenius' Extension. Let n be any positive odd integer relatively prime to $a \in \mathbb{Z}$. Then, the permutation $\{aj\}_n$ $(j = 0, \ldots, n-1)$ of $0, 1, \ldots, n-1$ has the sign $(\frac{a}{n})$.

Remark. Recently, I noted that Zolotarev's Lemma is actually equivalent to Gauss' Lemma and Frobenius' Extension is also equivalent to Jenkins' Extension of Gauss' Lemma.

H. Pan (arXiv:0601026, 2006). Let $n > 1$ be an odd integer and let a be any integer relatively prime to n. For $j = 1, \ldots, (n-1)/2$ let $\tau_a(j)$ be the unique $r \in \{1, \ldots, (n-1)/2\}$ with aj congruent to r or $-r$ modulo n. For the permutation τ_a on $\{1, \ldots, (n-1)/2\}$, its sign is given by $(\frac{a}{n})^{(n+1)/2}$.

A basic result of Mordell

Wilson's Theorem. An integer $p > 1$ is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Let p be an odd prime. Then

$$-1 \equiv (p-1)! = \prod_{k=1}^{(p-1)/2} k(p-k) \equiv (-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} k^2 \pmod{p}$$

and thus

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

L. J. Mordell [Amer. Math. Monthly 68(1961)]: If $p > 3$ is a prime with $p \equiv 3 \pmod{4}$ then

$$\frac{p-1}{2}! \equiv (-1)^{(h(-p)+1)/2} \pmod{p},$$

where $h(-p)$ is the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$.

In the proof Mordell used Dirichlet's class number formula.

A mysterious discovery on Sept. 15, 2018

Let $p = 2n+1$ be an odd prime, and let $a_1 < \ldots < a_n$ be all the quadratic residues modulo p among $1, \ldots, p-1$. It is well known that $\{1^2\}_p, \ldots, \{n^2\}_p$ is a permutation of $a_1, \ldots, a_n$. Let π_p denote this permutation. *What's the sign of the permutation π_p?*

On Sept. 14, 2018, I made computation via Mathematica but could not see any pattern. Then I thought that perhaps $\mathrm{sign}(\pi_p)$ is distributed randomly.

After I waked up in the early morning of Sept. 15, 2018, I thought that it would be very interesting if $\mathrm{sign}(\pi_p)$ obeys certain pattern. Thus, I computed and analyzed $\mathrm{sign}(\pi_p)$ once again. This led to the following surprising discovery.

Conjecture (Z.-W. Sun, Sept. 15, 2018). Let $p \equiv 3 \pmod 4$ be a prime and let $h(-p)$ be the class number of $\mathbb{Q}(\sqrt{-p})$. Then

$$\mathrm{sign}(\pi_p) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

An example

For the prime $p = 11$,

$$(\{1^2\}_{11}, \ldots, \{5^2\}_{11}) = (1, 4, 9, 5, 3),$$

and

$$\begin{aligned}\{(j,k) :\ & 1 \leqslant j < k \leqslant 5 \ \&\ \{j^2\}_{11} > \{k^2\}_{11}\} \\ &= \{(2,5),\ (3,4),\ (3,5),\ (4,5)\}.\end{aligned}$$

Thus

$$\operatorname{sign}(\pi_{11}) = (-1)^4 = 1.$$

Determination of $\mathrm{sign}(\pi_p)$ for $p \equiv 3 \pmod 4$

Theorem (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]). Let p be a prime with $p \equiv 3 \pmod 4$. Then

$$\mathrm{sign}(\pi_p) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Moreover, for any $a \in \mathbb{Z}$ with $p \nmid a$, we have

$$\prod_{1 \leqslant j < k \leqslant (p-1)/2} \csc \pi \frac{a(k^2-j^2)}{p} = \prod_{1 \leqslant j < k \leqslant (p-1)/2} \left(\cot \pi \frac{aj^2}{p} - \cot \pi \frac{ak^2}{p} \right)$$

$$= \begin{cases} (2^{p-1}/p)^{(p-3)/8} & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} \left(\frac{a}{p}\right) (2^{p-1}/p)^{(p-3)/8} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

Remark. Note that for $1 \leqslant j < k \leqslant (p-1)/2$ we have

$$\{j^2\}_p > \{k^2\}_p \iff \cot \pi \frac{j^2}{p} < \cot \pi \frac{k^2}{p}.$$

An auxiliary theorem

Theorem (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]). Let p be an odd prime and let $\zeta = e^{2\pi i/p}$. Let $a \in \mathbb{Z}$ with $p \nmid a$.

(i) If $p \equiv 1 \pmod 4$, then

$$\prod_{1\leqslant j<k\leqslant (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})^2 = (-1)^{(p-1)/4} p^{(p-3)/4} \varepsilon_p^{(\frac{a}{p})h(p)},$$

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

(ii) When $p \equiv 3 \pmod 4$, we have

$$\prod_{1\leqslant j<k\leqslant (p-1)/2} (\zeta^{aj^2} - \zeta^{ak^2})$$

$$= \begin{cases} (-p)^{(p-3)/8} & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(p+1)/8+(h(-p)-1)/2}(\frac{a}{p})p^{(p-3)/8} i & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

To prove part (ii) of this theorem, I used Galois theory.

A theorem joint with Fedor Petrov

The following result was originally conjectured by the speaker in 2018.

Theorem (Fedor Petrov and Z.-W. Sun [Electron. Res. Arch. 28(2020)]). Let p be a prime with $p \equiv 1 \pmod 4$, and let $\zeta = e^{2\pi i/p}$. Let a be an integer not divisible by p. Then

$$(-1)^{|\{1\leqslant k<p/4:\ (\frac{k}{p})=-1\}|}\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})$$

$$=\begin{cases}1 & \text{if } p\equiv 1 \pmod 8,\\ (\frac{a}{p})\varepsilon_p^{-(\frac{a}{p})h(p)} & \text{if } p\equiv 5 \pmod 8.\end{cases}$$

Cloitre's problem and related results

For an $n \times n$ matrix $A = [a_{ij}]_{1 \leqslant i,j \leqslant n}$ with $a_{ij} \in \mathbb{C}$, its *permanent* is defined by

$$\mathrm{per}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Theorem (conjectured by B. Cloitre in 2002 and proved by P. Bradley [arXiv:1809.01012]). For any $n \in \mathbb{Z}^+$, there is a permutation $\pi \in S_n$ with $k + \pi(k)$ prime for all $k = 1, \ldots, n$.

Remark. Note that the number of the desired permutations $\pi \in S_n$ is just the permanent of the matrix A of order n whose (i,j)-entry $(1 \leqslant i, j \leqslant n)$ is 1 or 0 according as $i + j$ is prime or not.

Theorem (Z.-W. Sun, arXiv:1811.10503). For any $n \in \mathbb{Z}^+$, there is a *unique* permutation π of $\{1, \ldots, n\}$ such that all the numbers $k + \pi(k)$ $(k = 1, \ldots, n)$ are powers of two. In other words, for the $n \times n$ matrix A whose (i,j)-entry is 1 or 0 according as $i + j$ is a power of two or not, we have $\mathrm{per}(A) = 1$.

These theorems can be proved by induction on n.

Some conjectures on permutations of $\{1,\ldots,n\}$

Conjecture (Z.-W. Sun, arXiv:1811.10503). (i) For any $n \in \mathbb{Z}^+$, there is a permutation $\sigma_n \in S_n$ such that $k\sigma_n(k)+1$ is prime for every $k = 1,\ldots,n$.

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

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

Conjecture (Z.-W. Sun, 2018-11-17). For each integer $n > 3$, there is an odd permutation $\tau \in S_n$ such that $\sum_{k=1}^n k\tau(k)$ is an odd square.

Remark. This was posted to MathOverflow in 2018 and confirmed by the user `js21` who showed that τ can be a product of five disjoint transpositions when $n \geqslant 14$. See `http://mathoverflow.net/questions/315568`.

A conjecture involving unit fractions

Conjecture (Z.-W. Sun, arXiv:1811.10503).

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

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

For any integer $n > 7$, there exists a permutation $\pi \in S_n$ such that

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

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

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

Remark. G.-N. Han [Electron. Res. Arch. 28(2020)] confirmed three other conjectures of the speaker, e.g., for any integer $n > 5$ there is a permutation $\pi \in S_n$ with $\sum_{k=1}^{n-1} \frac{1}{\pi(k)\pi(k+1)} = 1$.

A conjecture on crossing numbers

For a permutation $\sigma \in S_n$, its crossing number $\mathrm{cr}(\sigma)$ is the number of pairs $\{i,j\}$ with $i,j \in \{1,\ldots,n\}$ such that

$$i < j \le \sigma(i) < \sigma(j) \quad \text{or} \quad \sigma(i) < \sigma(j) < i < j.$$

Crossing numbers play important roles in enumerative combinatorics.

Conjecture (Z.-W. Sun, 2019-08-20). Let $p > 5$ be a prime. For each $k = 1,\ldots,p-1$, let $\bar{k}$ be the inverse of k mod p, that is, $1 \le \bar{k} \le p-1$ and $k\bar{k} \equiv 1 \pmod{p}$. For the permutation $\sigma_p \in S_{p-1}$ with $\sigma_p(k) = \bar{k}$ $(k = 1,\ldots,p-1)$, we have

$$\mathrm{cr}(\sigma_p) \not\equiv 0 \pmod{p}.$$

Remark. I have verified that $p \nmid \mathrm{cr}(\sigma_p)$ for all primes $5 < p < 10640$.

A theorem on torsion-free abelian groups

For an element a of an additive group G, we let ka be the sum of k copies of a for all $k = 1, 2, 3, \ldots$.

Theorem (Z.-W. Sun, arXiv:1811.10503). Let $a_1, \ldots, a_n$ be distinct elements of a torsion-free abelian group G. Then there is a permutation $\pi \in S_n$ such that all those $ka_{\pi(k)}$ $(k = 1, \ldots, n)$ are pairwise distinct.

Proof. The subgroup H of G generated by $a_1, \ldots, a_n$ is finitely generated and torsion-free. As H is isomorphic to $\mathbb{Z}^r$ for some positive integer r, if we take an algebraic number field K with $[K : \mathbb{Q}] = n$ then H is isomorphic to the additive group O_K of algebraic integers in K. Thus, without any loss of generality, we may simply assume that G is the additive group $\mathbb{C}$ of all complex numbers.

Proof of the theorem (continued)

It is easy to see that the coefficient of $x_1^{n-1} \dots x_n^{n-1}$ in the polynomial

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

is $(-1)^{n(n-1)/2} \mathrm{per}[i^{j-1}]_{1 \leqslant i,j \leqslant n}$, which is nonzero since $\mathrm{per}[i^{j-1}]_{1 \leqslant i,j \leqslant n} > 0$. Applying Alon's Combinatorial Nullstellensatz, we see that there are

$$x_1, \dots, x_n \in A = \{a_1, \dots, a_n\}$$

with $P(x_1, \dots, x_n) \neq 0$. Thus, for some $\pi \in S_n$ all the numbers $ka_{\sigma(k)}$ $(k = 1, \dots, n)$ are distinct. This ends the proof.

A conjecture for general groups

Conjecture (Z.-W. Sun, arXiv:1811.10503). If a group G contains no element of order among $2, \ldots, n+1$, then any $A \subseteq G$ with $|A| = n$ can be written as $\{a_1, \ldots, a_n\}$ with $a_1, a_2^2, \ldots, a_n^n$ pairwise distinct.

Remark. We have proved this when $n \leqslant 3$ or G is a torsion-free abelian group. We even don't know how to prove the conjecture for $G = \mathbb{Z}/p\mathbb{Z}$ with p an odd prime.

Part II. Determinants and Permanents

On the permanent $\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}$

It is well-known that

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

and in particular

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

for any odd prime p.

Theorem (Z.-W. Sun, arXiv:1811.10503). (i) Let p be any odd prime. Then there is no $\pi\in S_{p-1}$ such that all the $p-1$ numbers $k\pi(k)$ $(k=1,\ldots,p-1)$ are pairwise incongruent modulo p.

(ii) We have

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

Proof of the First Part of the Theorem

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

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

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

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

Two Lemmas

To prove the second part of the Theorem, we need some lemmas.

Lemma 1. (Alon's Combinatorial Nullstellensatz) Let $A_1, \ldots, A_n$ be finite subsets of a field F with $|A_i| > k_i$ for $i = 1, \ldots, n$ where $k_1, \ldots, k_n \in \{0, 1, 2, \ldots\}$. If the coefficient of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ in $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ is nonzero and $k_1 + \cdots + k_n$ is the total degree of P, then there are $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.

Lemma 2. Let $a_1, \ldots, a_n$ be elements of a field F. Then the coefficient of $x_1^{n-1} \ldots x_n^{n-1}$ in the polynomial

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

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

Remark. Lemma 2 can be easily proved by using Vandermonde determinants.

Proof of the Second Part of the Theorem

Let $n > 2$ be an integer. Then

$$\operatorname{per}[i^{j-1}]_{1\leqslant i,j\leq n} = \sum_{\sigma\in S_n}\prod_{k=1}^{n} k^{\sigma(k)-1}$$

$$\equiv \sum_{\substack{\sigma\in S(n)\\ \sigma(n)=1}} (n-1)!\prod_{k=1}^{n-1} k^{\sigma(k)-2} = (n-1)!\sum_{\tau\in S_{n-1}}\prod_{k=1}^{n-1} k^{\tau(k)-1}$$

$$=(n-1)!\operatorname{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1} \pmod n.$$

For $n = 4$, it is easy to check that $\operatorname{per}[i^{j-1}]_{1\leqslant i,j\leq 4} \equiv 0 \pmod 4$

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

In view of the above, it remains to show $p \mid \operatorname{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1}$ for any odd prime p.

Proof of the Second Part of the Theorem (continued)

Suppose that $\operatorname{per}[i^{j-1}]_{1\le i,j\le p-1} \not\equiv 0 \pmod p$ for some odd prime p. Then, by Lemma 2, the coefficient of $x_1^{p-2}\dots x_{p-1}^{p-2}$ in the polynomial

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

is not congruent to zero modulo p.

Applying Lemma 1 with $F=\mathbb{Z}/p\mathbb{Z}$ and

$$A=\{k+p\mathbb{Z}:\ k=1,\dots,p-1\},$$

we see that there are $a_1,\dots,a_{p-1}\in A$ such that

$$\prod_{1\leqslant i<j\leqslant p-1}(a_j-a_i)(ja_j-ia_i)\not\equiv 0 \pmod p.$$

So, there is a permutation $\pi\in S_{p-1}$ such that all those $k\pi(k)$ $(k=1,\dots,p-1)$ are pairwise incongruent modulo p, which contradicts the first part of the Theorem.

A conjecture on $\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1}$

Conjecture (Z.-W. Sun, arXiv:1811.10503). (i) For any $n\in\mathbb{Z}^+$, we have

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n-1}\not\equiv 0\pmod n\iff n\equiv 2\pmod 4.$$

(ii) If p is a Fermat prime (i.e., a prime of the form 2^k+1), then

$$\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1}\equiv p\times\frac{p-1}{2}!\pmod{p^2}.$$

If a positive integer $n\not\equiv 2\pmod 4$ is not a Fermat prime, then

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

Remark. The sequence $a_n=\mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant n}$ $(n=1,2,3,\ldots)$ is available from `http://oeis.org/A322363`.

A conjecture involving Domb numbers

A determinant of the form $|a_{i+j}|_{0\leqslant i,j\leqslant n-1}$ is called a *Hankel-type determinant*.

Conjecture (Sun, August 2013). Define the 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

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

Conjecture (Sun, 2013-08-24). Let $a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k+1}$ for $n \in \mathbb{N}$. Then, for any prime $p > 3$ we have

$$|a_{i+j}|_{0\leqslant i,j\leqslant p-1} \equiv 0 \pmod{p^2}.$$

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. In 2013 C. Krattenthaler confirmed that $W_n = 0$ for any $n \equiv 1 \pmod 3$.

Skew-symmetric determinants

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

If the transpose A^T of A equals $-A$ (i.e., $a_{ji} = -a_{ij}$ for all $i, j = 1, \ldots, n$), then the matrix A (as well as $\det A$) is said to be *skew-symmetric*. If $A = [a_{ij}]_{1 \leqslant i,j \leqslant n}$ is skew-symmetric, then

$$\det A = \det A^T = \det(-A) = (-1)^n \det A$$

and this $\det A = 0$ if n is odd.

Cayley's Theorem (1849). Let $A = [a_{ij}]$ be a skew-symmetric matrix of order $2n$ with $a_{ij} \in \mathbb{Z}$ for all $i, j = 1, \ldots, n$. Then $\det A$ is an integer square. Moreover, $\det A = \mathrm{pf}(A)^2$, where $\mathrm{pf}(A)$ is the Pfaffian of A defined by

$$\mathrm{pf}(A) = \frac{1}{n! 2^n} \sum_{\sigma \in S_{2n}} \mathrm{sgn}(\sigma) \prod_{i=1}^{n} a_{\sigma(2i-1),\sigma(2i)}$$

with $\mathrm{sgn}(\sigma)$ the sign of σ.

An example involving Jacobi symbols

Let $n \equiv 3 \pmod 4$ be a positive integer. Then

$$\left(\frac{j-i}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{i-j}{n}\right) = -\left(\frac{i-j}{n}\right)$$

and hence

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

Lemma (Sun). For any matrix $A = [a_{ij}]_{0\leqslant i,j\leqslant n}$ with $a_{ij} \in \mathbb{C}$,

$$|x + a_{ij}|_{0\leqslant i,j\leqslant n} = |A| + x|B|,$$

where $B = |b_{ij}|_{1\leqslant i,j\leqslant n}$ with $b_{ij} = a_{ij} - a_{i0} - a_{0j} + a_{00}$.

Thus, if $n \equiv 3 \pmod 4$ then $\left|x + \left(\frac{j-i}{n}\right)\right|_{1\leqslant i,j\leqslant (n-1)/2} = cx$, where $c := \left|\left(\frac{j-i}{n}\right) + \left(\frac{i}{n}\right) - \left(\frac{j}{n}\right)\right|_{1\leqslant i,j\leqslant (n-3)/2}$ is a square by Cayley's theorem.

Conjecture (Sun). For any prime $p \equiv 3 \pmod 4$, we have $\left|x + \left(\frac{j-i}{p}\right)\right|_{1\leqslant i,j\leqslant (p-1)/2} = x$.

Chapman's work on determinants with Legendre symbol entries

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

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

and

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

(Note that $(\frac{p+1}{2}-i)+(\frac{p+1}{2}-j)-1\equiv -(i+j) \pmod p$.)

Quadratic Gauss Sums: If p is an odd prime and a is an integer with $p\nmid a$, then

$$\sum_{x=0}^{p-1} e^{2\pi i a x^2/p} = \sum_{r=0}^{p-1}\left(\frac{r}{p}\right)e^{2\pi i a r/p} = \left(\frac{a}{p}\right)\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Chapman's evil determinants

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

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

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 finally confirmed by M. Vsemirnov [Linear Algebra Appl. 2012, and Acta Arith. 2013] via matrix decomposition and quadratic Gauss sums.

Some variants

Conjecture (Z.-W. Sun, 2018-09-13) Let $p > 3$ be a prime and let $h(-p)$ be the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Define M_p as the matrix obtaining from $[(\frac{i-j}{p})]_{0\leqslant i,j\leqslant (p-1)/2}$ via replacing all the entries in the first row by 1. Then

$$\det M_p = \begin{cases} (-1)^{(p-1)/4} & \text{if } p\equiv 1 \pmod 4, \\ (-1)^{(h(-p)-1)/2} & \text{if } p\equiv 3 \pmod 4. \end{cases}$$

Remark. Li-Yuan Wang has proved that the two sides of the last equality are congruent modulo p. If we define M_p^+ as the matrix obtaining from $[(\frac{i+j}{p})]_{0\leq i,j\leq (p-1)/2}$ via replacing all the entries in the first row by 1, then $\det M_p^+$ can be determined explicitly (conjectured by the speaker and confirmed by Li-Yuan Wang).

On the permanent $\mathrm{per}[(\frac{i+j}{2n+1})]_{0\leqslant i,j\leqslant n}$

Conjecture (Z.-W. Sun, 2018). For each $n = 0, 1, 2, \ldots$ we have

$$\mathrm{per}\left[\left(\frac{i+j}{2n+1}\right)\right]_{0\leqslant i,j\leqslant n} > 0,$$

where $(\frac{\cdot}{2n+1})$ is the Jacobi symbol.

Let a_n denote the permanent in the conjecture. Via Mathematica I find that

$$a_0 = a_1 = 1,\ a_2 = a_3 = 2,\ a_4 = 20,\ a_5 = 16,\ a_6 = 48,\ a_7 = 55,$$
$$a_8 = 128,\ a_9 = 320,\ a_{10} = 1206,\ a_{11} = 768,\ a_{12} = 406446336,$$
$$a_{13} = 43545600,\ a_{14} = 141312,\ a_{15} = 2267136,\ a_{16} = 389112,$$
$$a_{17} = 1624232,\ a_{18} = 138739712,\ a_{19} = 122605392,\ a_{20} = 2262695936,$$
$$a_{21} = 20313407488,\ a_{22} = 17060393728,\ a_{23} = 189261676544,$$
$$a_{24} = 374345132371011500507136,\ a_{25} = 669835780976.$$

On $W_p=|(\frac{i^2-((p-1)/2)!j}{p})|_{0\leqslant i,j\leqslant (p-1)/2}$

Theorem (Sun [Finite Fields Appl. 56(2019), 285-307]). Let $p=2n+1$ be an odd prime and let

$$W_p:=\left|\left(\frac{i^2-n!j}{p}\right)\right|_{0\leqslant i,j\leqslant n}.$$

Then

$$\left(\frac{W_p}{p}\right)=\begin{cases}(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{\lfloor (p+1)/8\rfloor} & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

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

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

Two further conjectures

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

$$\left| \left(\frac{i^2 - n!j}{p} \right) \right|_{1 \leqslant i,j \leqslant n} = 0 \iff p \equiv 3 \pmod 4.$$

Remark. In 2018, F. Petrov confirmed the mod p version of this conjecture.

Conjecture (Sun, 2018). For any prime $p \equiv 3 \pmod 4$, both

$$(-1)^{\lfloor (p+1)/8 \rfloor} \left| x + \left(\frac{i^2 - n!j}{p} \right) \right|_{0 \leqslant i,j \leqslant n}$$

and

$$\frac{(-1)^{\lfloor (p+1)/8 \rfloor}}{x} \left| x + \left(\frac{i^2 - n!j}{p} \right) \right|_{1 \leqslant i,j \leqslant n}$$

are positive squares not depending on x, where $n = (p-1)/2$.

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

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

Introduce $S(d,n)$ and $T(d,n)$

It is well known that for any odd prime p the $(p-1)/2$ squares

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

give all the $(p-1)/2$ quadratic residues modulo p. So we think that it's natural to consider some determinants with Legendre symbol (or Jacobi symbol) entries related to binary quadratic forms.

For any integer d and odd integer $n > 1$, I introduced in 2013

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

and

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

where $(\frac{\cdot}{n})$ is the Jacobi symbol. It is easy to show that $S(d,n) = T(d,n) = 0$ if n is composite.

On $T(d,p)$ modulo p

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

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

Sketch of the Proof. Set $n = (p-1)/2$. Then

$$\begin{aligned} &|(i^2+dj^2)^n|_{0\leqslant i,j\leqslant n} = |((i-1)^2+d(j-1)^2)^n|_{1\leqslant i,j\leqslant n+1} \\ =&\prod_{k=0}^{n}\binom{n}{k}\prod_{1\leqslant i<j\leqslant n+1}((i-1)^2-(j-1)^2)(d(j-1)^2-d(i-1)^2) \\ =&\frac{(n!)^{n+1}}{\prod_{k=0}^{n}k!(n-k)!}(-d)^{n(n+1)/2}\prod_{0\leqslant i<j\leqslant n}(j-i)^2(j+i)^2 \\ =&(-d)^{n(n+1)/2}(n!)^{n+1}\prod_{0\leqslant i<j\leqslant n}(i+j)^2. \end{aligned}$$

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

Theorem (Z.-W. Sun) (conjectured in 2013 and proved in 2018). Let $p = 2n+1$ be an odd prime and let $d \in \mathbb{Z}$ with $p \nmid d$. If $(\frac{d}{p}) = 1$, then $(\frac{-S(d,p)}{p}) = 1$.

Proof. The sum of entries in each column of the determinant $S(d,p) = |(\frac{i^2+dj^2}{p})|_{1\leqslant i,j\leqslant n}$ actually equals $-(1+(\frac{d}{p}))/2$.

Suppose that $(\frac{d}{p}) = 1$. By adding the last n rows of $T(d,p) = |(\frac{i^2+dj^2}{p})|_{0\leqslant i,j\leqslant n}$ to the first row we see that the initial term in the first row becomes n while all the other terms in the first row turn out to be zero. It follows that

$$T(d,p) = nS(d,p) \equiv -\frac{1}{2}S(d,p) \pmod{p}.$$

Thus $\left(\frac{-S(d,p)}{p}\right) = \left(\frac{2T(d,p)}{p}\right) = 1$.

A further observation

Conjecture (Sun, Sept. 2018) (cf. `https://mathoverflow.net/questions/A310192`). Let $p \equiv 3 \pmod 4$ be a prime. Then $-S(1,p) = -|(\frac{i^2+j^2}{p})|_{1\leqslant i,j\leqslant (p-1)/2}$ is a square. (Confirmed by Max Alekseyev and Dmitry Krachun)

Max Alekseyev's Idea. Let $p = 2n+1 \equiv 3 \pmod 4$ be a prime and set $\zeta_p := e^{2\pi i/p}$. For $j,k = 1,\ldots,n$ we have

$$\left(\frac{j^2+k^2}{p}\right)\sqrt{-p} = \sum_{r=0}^{p-1} \zeta_p^{(j^2+k^2)r^2} = 1 + 2\sum_{r=1}^{n} \zeta_p^{j^2r^2}\zeta_p^{r^2j^2}.$$

Clearly, $\alpha := 1/(p^{1/4}-1))(1+p^{1/4}i)$ satisfies the quadratic equation $(p-1)\alpha^2 + 2(\sqrt{-p}-1)\alpha - 1 = 0$. So,

$$\left(\frac{j^2+k^2}{p}\right)\sqrt{-p} = 1+2\sum_{r=1}^{n} \zeta_p^{j^2r^2}\zeta_p^{r^2j^2} = 2\sum_{r=1}^{n}(\zeta_p^{j^2r^2}+\alpha)(\zeta_p^{r^2k^2}+\alpha)$$

and hence $S(1,p) = \det\left(\frac{2}{\sqrt{-p}}A^2\right)$ where $A = [\zeta_p^{j^2k^2}+\alpha]_{1\leqslant j,k\leqslant n}$.

D. Krachun's solution

Dmitry Krachun's Solution. As $\sum_{j=0}^{p-1}\zeta_p^{j^2}=\sqrt{-p}$, we have $\sqrt{-p}\in\mathbb{Q}[\zeta_p]$. Let $\lambda_p=-2\sqrt{-p}$. Then

$$\alpha=(1-\sqrt{-p}\pm\sqrt{\lambda_p})/(p-1)\in\mathbb{Q}[\zeta_p][\sqrt{\lambda_p}].$$

As $S(1,p)=\det\left(\frac{2}{\sqrt{-p}}A^2\right)$, we see that $-S(1,p)$ is a square in $\mathbb{Q}[\zeta_p][\sqrt{\lambda_p}]$. Write $-S(1,p)=(a\sqrt{\lambda_p}+b)^2$ with $a,b\in\mathbb{Q}[\zeta_p]$. As $S(1,p)\in\mathbb{Z}\subseteq\mathbb{Q}[\zeta_p]$ but $\sqrt{\lambda_p}\notin\mathbb{Q}[\zeta_p]$, we have $ab=0$. If $b=0$, then $-S(1,p)=a^2\lambda_p$ and hence $S(1,p)^2=a^4(-4p)$ which contradicts Sun's result that $(\frac{-S(1,p)}{p})=1$. So, $-S(1,p)=b^2$ with $b\in\mathbb{Q}[\zeta_p]$ and hence $-S(1,p)$ is an integer square since $p\nmid S(1,p)$.

Two conjectures for primes $p \equiv 1 \pmod 4$

Conjecture 1 (Sun, 2018). Let $p \equiv 1 \pmod 4$ be a prime, and let A_p denote the matrix $[a_{ij}]_{1\leq i,j\leq (p-1)/2}$, where

$$a_{1j} = \left(\frac{j}{p}\right), \quad \text{and} \quad a_{ij} = \left(\frac{i^2+j^2}{p}\right) \text{ for } i > 1.$$

Then $-\det A_p$ is always an odd square.

Conjecture 2 (Sun, 2018). Let $p \equiv 1 \pmod 4$ be a prime and write $p = x^2 + 4y^2$ with $x, y \in \mathbb{Z}$. Then, for any $d \in \mathbb{Z}$ with $(\frac{d}{p}) = -1$, we have

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

for some positive integer z not depending on d.

Joint work with D. Grinberg and L.-L. Zhao

The following theorem was originally conjectured by Z.-W. Sun in 2013.

Theorem (D. Grinberg, Z.-W. Sun and L.-L. Zhao, June 2018; arXiv:2007.06453). (i) For any odd integer $n > 3$, we have

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

(iii) Let $n > 2$ be an integer, and set

$$a_n = |(i+j)^n|_{0\leqslant i,j\leqslant n-1} \quad \text{and} \quad b_n = \left|(i^2+j^2)^n\right|_{0\leqslant i,j\leqslant n-1}.$$

Then $n^2 \mid a_n$ and $(2n)! \mid b_n$. Moreover,

$$a'_n = \frac{(-1)^{n(n-1)/2} a_n}{(n-2)!\, n \prod_{k=1}^{n} k!} \text{ and } b'_n = \frac{(-1)^{n(n-1)/2} b_n}{2\prod_{k=1}^{n}(k!(2k-1)!)}$$

are positive integers.

More conjectures

Conjecture (Sun, 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

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

Conjecture (Sun, 2018). Let $p > 3$ be a prime and let $d \in \mathbb{Z}$ with $p \nmid d$. For the determinant

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

we have

$$\left(\frac{D}{p}\right) = \begin{cases} (\frac{d}{p})^{(p-1)/4} & \text{if } p \equiv 1 \pmod 4, \\ (\frac{d}{p})^{(p+1)/4}(-1)^{(h(-p)-1)/2} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

A theorem and a related conjecture

Theorem (Sun, 2013). (i) For any odd prime p, we have

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

(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, 2013). Let $p\equiv 5\pmod 6$ be a prime. Then $2\left|\frac{1}{i^2-ij+j^2}\right|_{1\leq i,j\leq p-1}$ is a quadratic residue modulo p and the p-adic order (or valuation) of $\left|\frac{1}{i^2-ij+j^2}\right|_{1\leqslant i,j\leqslant(p-1)/2}$ is $(p+1)/6$.

On $(c,d)_n$ and $[c,d]_n$

For any odd integer $n>1$ and integers c and d, in 2013 I introduced the notations

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

and

$$[c,d]_n := \left|\left(\frac{i^2+cij+dj^2}{n}\right)\right|_{0\leqslant i,j\leqslant n-1}.$$

Theorem (Z.-W. Sun, 2018). Let $c,d\in\mathbb{Z}$.

(i) $(c,d)_n=0$ for any positive odd integer n with $(\frac{d}{n})=-1$.

(ii) If p is an odd prime with $(\frac{d}{p})=1$, then

$$[c,d]_p=\begin{cases}\frac{p-1}{2}(c,d)_p & \text{if } p\nmid c^2-4d,\\ \frac{1-p}{p-2}(c,d)_p & \text{if } p\mid c^2-4d.\end{cases}$$

$(c,d)_n = 0$ if $(\frac{d}{n}) = -1$

Let n be any positive odd integer relatively prime to d. For $j = 0, \ldots, n-1$ let $\sigma_d(j)$ be the least nonnegative residue of dj modulo n. Then σ_d is a permutation on $\{0, \ldots, n-1\}$ with $\sigma_d(0) = 0$. By Frobenius' extension of the Zolotarev lemma, $\operatorname{sign}(\sigma_d) = (\frac{d}{n})$.

Now suppose that $(\frac{d}{n}) = -1$. Then $\operatorname{sign}(\sigma_d) = -1$ and hence

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

$$= \left| \left(\frac{di^2 + ci\sigma_d(j) + \sigma_d(j)^2}{n} \right) \right|_{1 \leqslant i,j \leqslant n-1}$$

$$= \sum_{\pi \in S_{n-1}} \operatorname{sign}(\pi) \prod_{i=1}^{n} \left(\frac{di^2 + ci\sigma_d(\pi(i)) + \sigma_d(\pi(i))^2}{n} \right)$$

$$= \operatorname{sign}(\sigma_d) \sum_{\tau \in S_{n-1}} \operatorname{sign}(\tau) \prod_{i=1}^{n} \left(\frac{di^2 + ci\tau(i) + \tau(i)^2}{n} \right) = -(c,d)_n.$$

The relation between $(c,d)_p$ and $[c,d]_p$ when $(\frac{d}{p}) = 1$

Let p be an odd prime. For any $a, b \in \mathbb{Z}$, it is known that

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + ax + b}{p} \right) = \begin{cases} -1 & \text{if } p \nmid a^2 - 4b, \\ p-1 & \text{if } p \mid a^2 - 4b. \end{cases}$$

So, for each $j = 1, \ldots, p-1$, we have

$$\sum_{i=1}^{p-1} \left(\frac{i^2 + cij + dj^2}{p} \right) = \begin{cases} -1 - (\frac{d}{p}) & \text{if } p \nmid c^2 - 4d, \\ p-1-(\frac{d}{p}) & \text{if } p \mid c^2 - 4d. \end{cases}$$

Now assume that $(\frac{d}{p}) = 1$. Let $\lambda = 1/2$ if $p \nmid c^2 - 4d$, and $\lambda = 1/(2-p)$ otherwise. Then $\lambda \sum_{i=1}^{p-1} (\frac{i^2+cij+dj^2}{p}) = -1$. By adding the last $p-1$ rows multiplied by λ to the first row of $[c,d]_p$, the initial term of the resulting determinant becomes $(p-1)\lambda$ while all other terms in the first row vanish. Thus

$$[c,d]_p = (p-1)\lambda (c,d)_p.$$

On $(c,d)_n$ and $[c,d]_n$

Conjecture (Sun, Jan. 2019). Let n be a positive odd integer. If $c, d \in \mathbb{Z}$ and $(\frac{d}{n}) = -1$, then $\varphi(n)^2 \mid [c,d]_n$.

The following result was first conjectured by Z.-W. Sun in 2013.

Theorem (D. Krachun, F. Petrove, Z.-W. Sun and M. Vsemirnov [Finite Fields Appl. 64(2020), 101672]).

(i) For any positive integer $n \equiv 3 \pmod 4$, we have

$$(6,1)_n = [6,1]_n = (3,2)_n = [3,2]_n = 0$$

and

$$(4,2)_n = (8,8)_n = (3,3)_n = (21,112)_n = 0.$$

(ii) $(10,9)_p = 0$ for any prime $p \equiv 5 \pmod{12}$.

(iii) $[5,5]_p = 0$ for any prime $p \equiv 13, 17 \pmod{20}$.

Few words about the proofs

The proof of part (i) is related to elliptic curves over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and combinatorial congruences. The proofs of parts (ii) and (iii) are more sophisticated, and they involve character sums and permutation polynomials over finite fields.

For primes $p \equiv 5 \pmod{12}$ we actually show that

$$\sum_{\substack{0<i<p \\ (\frac{i}{p})=1}} \left(\frac{\sqrt{i}}{p}\right)\left(\frac{i^2+10ij+9j^2}{p}\right) = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x(x^4+10x^2j+9j^2)}{p}\right)$$

vanishes for each $j = 1, \ldots, p-1$, where $\sqrt{i}$ with $(\frac{i}{p}) = 1$ denotes the unique $x \in \{1, \ldots, (p-1)/2\}$ with $x^2 \equiv i \pmod{p}$.

For primes $p \equiv 13, 17 \pmod{12}$ we actually show that

$$\sum_{\substack{0<i<p \\ (\frac{i}{p})=1}} \left(\frac{\sqrt{i}}{p}\right)\left(\frac{i^2+5ij+5j^2}{p}\right) = \frac{1}{2}\sum_{x=0}^{p-1}\left(\frac{x(x^4+5x^2j+5j^2)}{p}\right)$$

vanishes for each $j = 0, \ldots, p-1$.

On the sum $\sum_{x=0}^{p-1}\left(\frac{x^5+cx^3+dx}{p}\right)$ (I)

Conjecture (Sun, 2018). Let $p \equiv 1 \pmod 4$ be a prime, and let $c, d \in \mathbb{Z}$ and

$$S_p(c,d) := \sum_{x=0}^{p-1}\left(\frac{x^5+cx^3+dx}{p}\right).$$

(i) If $d^{(p-1)/4} \equiv -1 \pmod p$ (i.e., d is a quadratic residue and a quartic nonresidue mod p), then $S_p(c,d) = 0$. (This was recently proved by D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov [Finite Fields Appl 64(2020)].)

(ii) If $S_p(c,d) = 0$ but $d^{(p-1)/4} \not\equiv -1 \pmod p$, then

$$\left(\frac{c^2-4d}{p}\right) = \left(\frac{d}{p}\right).$$

On the sum $\sum_{x=0}^{p-1}\left(\frac{x^5+cx^3+dx}{p}\right)$ (II)

Conjecture (Sun, 2018). Let $p \equiv 1 \pmod{12}$ be a prime and write $p = a^2 + 3b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 3$. Suppose that $d \in \mathbb{Z}$ is a quadratic residue mod p. Then

$$S_p(10d, 9d^2) = \begin{cases} -4a & \text{if } 3d \text{ is a quartic residue mod } p, \\ 4a & \text{otherwise.} \end{cases}$$

Conjecture (Sun, 2018). Let $p \equiv 1, 9 \pmod{20}$ be a prime and write $p = a^2 + 5b^2$ with $a, b \in \mathbb{Z}$. If $d \in \mathbb{Z}$ and $(\frac{d}{p}) \equiv 5^{(p-1)/4} \pmod p$, then $S_p(5d, 5d^2) = \pm 4a$.

On the sum $\sum_{x=0}^{p-1}\left(\frac{x^5+cx^3+dx}{p}\right)$ (III)

Conjecture (Sun, 2018). (i) $S_p(8d,18d^2)=0$ for any prime $p\equiv 13,17 \pmod{24}$ and integer d. (This implies $[8,18]_p=0$ for any prime $p\equiv 13,17 \pmod{24}$.)

(ii) Suppose that $p\equiv 1 \pmod{24}$ is a prime and $p=a^2+6b^2$ with $a,b\in\mathbb{Z}$ and $a\equiv 1 \pmod 3$. Then, for any $d\in\mathbb{Z}$ we have

$$S_p(8d,18d^2)=\begin{cases}-4a & \text{if } 2^{(p-1)/8}\equiv (3d)^{(p-1)/4} \pmod p,\\ 4a & \text{if } 2^{(p-1)/8}\equiv -(3d)^{(p-1)/4} \pmod p\\ 0 & \text{if } 2^{(p-1)/4}\not\equiv (\frac{d}{p}) \pmod p.\end{cases}$$

(iii) If $p\equiv 5 \pmod{24}$ and $p=2a^2+3b^2$ with $a,b\in\mathbb{Z}$, then $S_p(8d,18d^2)=\pm 4a$ for any integer $d\not\equiv 0 \pmod p$.

After I posted this conjecture to `MathOverflow`, Michael Stoll proved part (i) by using **advanced tools** such as elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-6}]$ and ℓ-adic Tate module.

Main References:

1. Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. 56 (2019), 285-307.

2. Z.-W. Sun, *Quadratic residues and related permutations*, Finite Fields Appl. **59** (2019), 246–283.

3. Z.-W. Sun, *Some new problems in additive combinatorics*, Nanjing Univ. J. Math. Biquarterly **36** (2019), 134–155.

4. Z.-W. Sun, *On permutations of* $\{1,\ldots,n\}$ *and related topics*, `http://arxiv.org/abs/1811.10503`.

5. D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, *On some determinants involving Jacobi symbols*, Finite Fields Appl. **64** (2020), Article ID 101672.

6. F. Petrov and Z.-W. Sun, *Proof of some conjectures involving quadratic residues*, Electron. Res. Arch. **28** (2020), 589-597.

Thank you!