A talk given at *Number Theory and its Appl.*
(Yan'an, August 19-22, 2018)
and *Combin. and its Appl.* (Chongqing Univ., Sept. 21-23)
and Nankai Univ. (Oct. 1, 2018)
and *2019 Number Theory Workshop at Nanjing Normal Univ.*
(March 29–April 1, 2019)
and Capital Normal Univ. (April 12, 2019)
and Jiangsu Normal Univ. (Sept. 27, 2019)

On some determinants involving Legendre or Jacobi symbols

Zhi-Wei Sun

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

Abstract

Let p be an odd prime and let $n>1$ be an odd integer. In this talk we mainly introduce results and conjectures for the determinants

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

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

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

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

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

introduced by the speaker, where c and d are integers, $(\frac{\cdot}{p})$ is the Legendre symbol and $(\frac{\cdot}{n})$ is the Jacobi symbol.

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.

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

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

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

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

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 $b_{ij} = a_{ij} - a_{i0} - a_{0j} + a_{00}$.

By this lemma, $\left|x + \left(\frac{j-i}{n}\right)\right|_{1\leqslant i,j\leqslant (n-1)/2} = cx$, 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 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, 2018-09-12) Let $p > 3$ be an odd prime, and define

$$A_p^+ = [a_{ij}^+]_{1\le i,j\le (p-1)/2} \text{ with } a_{1j}^+ = \left(\frac{j}{p}\right) \text{ and } a_{ij}^+ = \left(\frac{i+j}{p}\right) \text{ for } i > 1,$$

and

$$A_p^- = [a_{ij}^-]_{1\le i,j\le (p-1)/2} \text{ with } a_{1j}^- = \left(\frac{j}{p}\right) \text{ and } a_{ij}^- = \left(\frac{i-j}{p}\right) \text{ for } i > 1.$$

If $p \equiv 3 \pmod 4$, then

$$\det A_p^+ = -2^{(p-3)/2} \text{ and } \det A_p^- = (-1)^{(p-3)/4}.$$

One week after my posting of this conjecture to `MathOverflow` (cf. `https://mathoverflow.net/questions/310381`), Gjergji Zaimi at UCLA proved it via **quadratic Gauss sums and Lagrange's interpolation formula**.

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. L. J. Mordell [Amer. Math. Monthly 68(1961)] showed that if $p>3$ is a prime with $p\equiv 3 \pmod 4$ then

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

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

$$\det M_p^+=2^{(p-1)/2}\det M_p$$

(conjectured by the speaker and confirmed by Li-Yuan Wang).

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

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

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

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

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

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

Let a_n denote the permanent in $(*)$. 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

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

More lemmas

Lemma. (i) (Gauss) For any prime $p \equiv 1 \pmod 4$ with $p = x^2 + y^2$ ($x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$), we have $\binom{(p-1)/2}{(p-1)/4} \equiv 2x \pmod p$.

(ii) (B. C. Berndt and S. Chowla, 1974) $\sum_{0<k<p/4}(\frac{k}{p}) = 0$ for any prime $p \equiv 3 \pmod 8$, and $\sum_{p/4<k<p/2}(\frac{k}{p}) = 0$ for any prime $p \equiv 7 \pmod 8$.

Lemma (Sun). Let p be an odd prime. If $p \equiv 1 \pmod 4$, then

$$\left(\frac{((p-3)/2)!!}{p}\right) = (-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}.$$

If $p \equiv 3 \pmod 4$, then

$$\left(\frac{((p-2+(\frac{2}{p}))/2)!!}{p}\right) = (-1)^{\lfloor (p+1)/8 \rfloor}.$$

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

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

Some lemmas

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ 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 $(\frac{a}{p})$.

Frenbinus' 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 $(\frac{a}{n})$.

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

Using Zolotarev's Lemma we can easily show that $S(d, p) = 0$ for any odd prime p and integer d with $(\frac{d}{p}) = -1$.

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).
(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

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

(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, 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, arXiv:1812.08080). (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 due to a discussion with Maxim Vsemirnov.)

(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

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

(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.

On the determinant $|\cot \pi jk/p|_{1\leqslant j,k\leqslant (p-1)/2}$

Theorem (Sun, 2019). For any odd prime p, we have

$$D_p := \det\left[\cot \pi\frac{jk}{p}\right]_{1\leqslant j,k\leqslant (p-1)/2} \in \begin{cases} \mathbb{Q} & \text{if } p\equiv 1 \pmod 4,\\ \sqrt{p}\,\mathbb{Q} & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Proof. The Galois group

$$\mathrm{Gal}(\mathbb{Q}(e^{2\pi i/p})/\mathbb{Q}) = \{\sigma\in \mathrm{Aut}(\mathbb{Q}(e^{2\pi i/p})):\ \sigma(r)=r \text{ for all } r\in\mathbb{Q}\}$$

consists of those automorphisms σ_a $(1\le a\le p-1)$ with $\sigma_a(e^{2\pi i/p}) = e^{2\pi ia/p}$. By Gauss' Lemma,

$$\left(\frac{a}{p}\right) = (-1)^{|\{1\le j\le (p-1)/2:\ \{aj/p\}>1/2\}|}.$$

For $j=1,\ldots,(p-1)/2$ let $\pi_a(j)$ be the unique $r\in\{1,\ldots,(p-1)/2\}$ with $aj\equiv \pm r \pmod p$. Then $\mathrm{sign}(\pi_a) = (\frac{a}{p})^{(p+1)/2}$ (by a result of Pan).

On the determinant $\left|\cot \pi jk/p\right|_{1\leqslant j,k\leqslant (p-1)/2}$

Using pth roots of unity, we get

$$\begin{aligned}\sigma_a\left(\frac{D_p}{i^{(p-1)/2}}\right) &= \frac{1}{i^{(p-1)/2}} \det\left[\cot \pi \frac{ajk}{p}\right]_{1\leq j,k\leq (p-1)/2} \\ &= \frac{\left(\frac{a}{p}\right)}{i^{(p-1)/2}} \det\left[\cot \pi \frac{\pi_a(j)k}{p}\right]_{1\leq j,k\leq (p-1)/2} \\ &= \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)^{(p+1)/2} \frac{D_p}{i^{(p-1)/2}} = \left(\frac{a}{p}\right)^{(p-1)/2} \frac{D_p}{i^{(p-1)/2}}.\end{aligned}$$

Thus, if $p \equiv 1 \pmod 4$ then $\sigma_a(D_p) = D_p$ for all $a = 1, \ldots, p-1$ and hence $D_p \in \mathbb{Q}$.

On the determinant $|\cot \pi jk/p|_{1\leqslant j,k\leqslant (p-1)/2}$

In the case $p \equiv 3 \pmod 4$, we have

$$\sigma_a\left(\frac{D_p}{\sqrt{p}}\right) = \sigma_a\left(\frac{iD_p}{\sqrt{-p}}\right) = \left(\frac{a}{p}\right)\frac{iD_p}{\sigma_a(\sqrt{-p})}.$$

Using quadratic Gauss sums we see that

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

Therefore $\sigma_a(D_p/\sqrt{p}) = D_p/\sqrt{p}$ for all $a = 1, \ldots, p-1$, and hence $D_p/\sqrt{p} \in \mathbb{Q}$.

A conjecture related to the class number of $\mathbb{Q}(\sqrt{-p})$

Conjecture (Z.-W. Sun, Jan. 2019). For any prime $p \equiv 3 \pmod 4$, the number

$$\left(\frac{-2}{p}\right)\frac{\det\left[\cot \pi jk/p\right]_{1\leqslant j,k\leqslant (p-1)/2}}{2^{(p-3)/2}p^{(p-5)/4}}$$

is a positive integer divisible by $h(-p)$.

Remark. I verified this for all primes $p < 30$ with $p \equiv 3 \pmod 4$. Later, Francois Brunault extended the verification for all primes $p < 50$ with $p \equiv 3 \pmod 4$. Note that $h(-23) = h(-31) = 3$, $h(-43) = 1$ and $h(-47) = 5$.

For any positive integer n, we have

$$\frac{1}{2n}\left|\cos \pi\frac{jk}{n}\right|_{0\leqslant j,k\leqslant n} = \left|\cos \pi\frac{jk}{n}\right|_{1\leqslant j,k\leqslant n} = (-1)^{\lfloor \frac{n+1}{2}\rfloor}\frac{n^{(n-1)/2}}{2^{(n-1)/2}}.$$

This was first conjectured by Z.-W. Sun and later confirmed by F. Petrov.

Main References:

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

2. D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, *On some determinants involving Jacobi symbols*, arXiv:1812.08080, `http://arxiv.org/abs/1812.08080`

3. Various questions of Z.-W. Sun posted to MathOverflow available from `https://mathoverflow.net`.

Thank you!