A talk given at *Int. Symp. on Wen-Tsun Wu's Academic Thought and Mathematical Mechanization* (Academy of Sciences, Beijing, May 12-17, 2019) and *the 10th Cross-strait Conf. on Graph Theory and Combin.* (Taichung, August 18-23, 2019)

Problems and Results on Permutations

Zhi-Wei Sun

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

August 19, 2019

Part I. On Signs of Permutations

Definition of signs of permutations

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

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

where

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

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 $\{1, \dots, n\}$. 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* $(\frac{a}{p})$ 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* $(\frac{a}{n})$ is given by

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

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

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

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

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.

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

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

On $\prod_{1\leqslant i<j\leqslant (p-1)/2}(j^2-i^2) \bmod p$

For an odd prime p, clearly $\mathrm{sign}(\pi_p)$ is the sign of the product

$$S_p := \prod_{1\leqslant i<j\leqslant (p-1)/2} (\{j^2\}_p - \{i^2\}_p).$$

It is relatively easy to determine S_p modulo p.

Theorem. Let $p = 2n+1$ be an odd prime. Then

$$\prod_{1\leqslant i<j\leqslant n}(j^2-i^2) \equiv \begin{cases} -n! \pmod p & \text{if } p \equiv 1 \pmod 4, \\ 1 \pmod p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Sketch of My Proof. This is because

$$\begin{aligned} &\prod_{1\leqslant i<j\leqslant n}(j-i) \times \prod_{1\leqslant i<j\leqslant n}(j+i) \\ =&\prod_{k=1}^{n} k^{n-k} \times \prod_{k=1}^{n} k^{\lfloor (k-1)/2 \rfloor}(p-k)^{\lfloor k/2 \rfloor} \\ \equiv&(-1)^{\sum_{k=0}^{n}\lfloor k/2 \rfloor}(n!)^{n-1} \pmod p \end{aligned}$$

and $(-1)^n(n!)^2 \equiv (p-1)! \equiv -1 \pmod p$ by Wilson's theorem.

Known results involving $\zeta = e^{2\pi i/p}$

Lemma. Let p be an odd prime, and let $\zeta = e^{2\pi i/p}$.
(i) For any $a \in \mathbb{Z}$ with $p \nmid a$, we have

$$\prod_{n=1}^{p-1}(1-\zeta^{an}) = p,$$

$$\sum_{x=0}^{p-1}\zeta^{ax^2} = \left(\frac{a}{p}\right)\sqrt{(-1)^{(p-1)/2}p} \ \text{(Gauss)}.$$

(ii) (Dirichlet's class number formula) If $p \equiv 1 \pmod 4$, then

$$\prod_{n=1}^{p-1}(1-\zeta^{n})^{(\frac{n}{p})} = \varepsilon_p^{-2h(p)},$$

where ε_p and $h(p)$ are the fundamental unit and the class number of the quadratic field $\mathbb{Q}(\sqrt{p})$ respectively. When $p \equiv 3 \pmod 4$, we have

$$ph(-p) = -\sum_{k=1}^{p-1}k\left(\frac{k}{p}\right).$$

On $\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})$

Theorem (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]).
Let $p>3$ be a prime and let $\zeta=e^{2\pi i/p}$. Let a be any integer not divisible by p.

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

$$\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})=\sqrt{p}\,\varepsilon_p^{-(\frac{a}{p})h(p)}.$$

(ii) If $p\equiv 3 \pmod 4$, then

$$\prod_{k=1}^{(p-1)/2}(1-\zeta^{ak^2})=(-1)^{(h(-p)+1)/2}\left(\frac{a}{p}\right)\sqrt{p}\,i.$$

On $\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}$ and $\prod_{k=1}^{(p-1)/2}\cos\pi\frac{ak^2}{p}$

Corollary. Let $p>3$ be a prime and let $a\in\mathbb{Z}$ with $p\nmid a$. Then

$$\begin{aligned}&2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}\\ =&(-1)^{(a+1)\lfloor (p+1)/4\rfloor}\sqrt{p}\times\begin{cases}\varepsilon_p^{-(\frac{a}{p})h(p)} & \text{if } 4\mid p-1,\\ (-1)^{(h(-p)+1)/2}(\frac{a}{p}) & \text{if } 4\mid p-3,\end{cases}\end{aligned}$$

and

$$2^{(p-1)/2}\prod_{k=1}^{(p-1)/2}\cos\pi\frac{ak^2}{p}=\begin{cases}(-1)^{a(p-1)/4}\varepsilon_p^{(1-(\frac{2}{p}))(\frac{a}{p})h(p)} & \text{if } 4\mid p-1,\\ (-1)^{(a+1)(p+1)/4} & \text{if } 4\mid p-3.\end{cases}$$

More identities involving the sine and cosine functions

Theorem (Z.-W. Sun [Finite Fields Appl. 59(2019), 246-283]). Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\prod_{\substack{1\leqslant j<k\leqslant (p-1)/2\\ p\nmid j^2+k^2}} \sin \pi \frac{a(j^2+k^2)}{p}$$

$$= \left(\frac{p}{2^{p-1}}\right)^{(p-(\frac{-1}{p})-4)/8} \times \begin{cases} \varepsilon_p^{(\frac{a}{p})h(p)(1+(\frac{2}{p}))/2} & \text{if } 4 \mid p-1,\\ (-1)^{(p-3)/8} & \text{if } 8 \mid p-3,\\ (-1)^{(p+1)/8+(h(-p)+1)/2}(\frac{a}{p}) & \text{if } 8 \mid p-7,\end{cases}$$

and

$$\prod_{1\leqslant j<k\leqslant (p-1)/2} \cos \pi \frac{a(j^2+k^2)}{p} = (-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor} 2^{-\frac{p-1}{2}\lfloor\frac{p-3}{4}\rfloor}.$$

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

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

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

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

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

Reduction to $\prod_{1\leqslant j<k\leqslant (p-1)/2}\sin\pi\frac{a(k^2-j^2)}{p}$

For real numbers θ_1 and θ_2, clearly

$$\cot\pi\theta_1-\cot\pi\theta_2=\frac{\cos\pi\theta_1}{\sin\pi\theta_1}-\frac{\cos\pi\theta_2}{\sin\pi\theta_2}=\frac{\sin\pi(\theta_2-\theta_1)}{\sin\pi\theta_1\sin\pi\theta_2}.$$

Thus

$$\begin{aligned}&\prod_{1\leqslant j<k\leqslant(p-1)/2}\frac{\sin\pi a(k^2-j^2)/p}{\cot\pi aj^2/p-\cot\pi ak^2/p}\\ =&\prod_{1\leqslant j<k\leqslant(p-1)/2}\sin\pi\frac{aj^2}{p}\sin\pi\frac{ak^2}{p}\\ =&\prod_{k=1}^{(p-1)/2}\left(\sin\pi\frac{ak^2}{p}\right)^{|\{1\leqslant j\leqslant(p-1)/2:\ j\neq k\}|}.\end{aligned}$$

Recall that we have determined the value of $\prod_{k=1}^{(p-1)/2}\sin\pi\frac{ak^2}{p}$.

Reduction to $\prod_{1\leqslant j<k\leqslant(p-1)/2}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p})$

For $1\leqslant j<k\leqslant(p-1)/2$, clearly

$$\sin\pi\frac{a(k^2-j^2)}{p} = \frac{e^{i\pi a(k^2-j^2)/p}-e^{-i\pi a(k^2-j^2)/p}}{2i}$$
$$= \frac{i}{2}e^{-i\pi a(k^2+j^2)/p}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p}).$$

It is easy to show that

$$\sum_{1\leqslant j<k\leqslant(p-1)/2}(j^2+k^2)=\frac{p-3}{2}\sum_{k=1}^{(p-1)/2}k^2=\frac{p-3}{2}\cdot\frac{p^2-1}{24}p.$$

Determine $\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2$ with $\zeta=e^{2\pi i/p}$

$$\begin{aligned}
&\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2\\
=&(-1)^{\binom{(p-1)/2}{2}}\prod_{1\leqslant j<k\leqslant (p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})(\zeta^{ak^2}-\zeta^{aj^2})\\
=&(-1)^{\binom{(p-1)/2}{2}}\prod_{k=1}^{(p-1)/2}\prod_{\substack{j=1\\ j\neq k}}^{(p-1)/2}(\zeta^{ak^2}-\zeta^{aj^2})\\
=&(-1)^{(p-1)(p-3)/8}\prod_{n=1}^{p-1}(1-\zeta^{an})^{r(n)},
\end{aligned}$$

where

$$\begin{aligned}
r(n)=&|\{(j,k):\ 1\leqslant j,k<p/2\ \&\ j^2-k^2\equiv n \pmod p\}|\\
=&\sum_{\substack{0<x<p\\ p\nmid n+x}}\frac{(\frac{x}{p})+1}{2}\cdot\frac{(\frac{n+x}{p})+1}{2}=\left\lfloor\frac{p-1}{4}\right\rfloor-\frac{1+(\frac{-1}{p})}{2}\cdot\frac{1+(\frac{n}{p})}{2}.
\end{aligned}$$

The value of $\prod_{1\leqslant j<k\leqslant(p-1)/2}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p})^2$

When $p\equiv 1 \pmod 4$, we get

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

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

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})^2=(-p)^{(p-3)/4}.$$

How to determine the value of $\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})$ *in the case* $p\equiv 3 \pmod 4$*?*

We need Galois theory!

The cyclotomic field $\mathbb{Q}(e^{2\pi i/n})$

Let $n > 1$ be an integer and let $\zeta_n = e^{2\pi i/n}$. The minimal polynomial of ζ_n over $\mathbb{Q}$ is the cyclotomic polynomial

$$\Phi_n(x) = \prod_{\substack{a=1 \\ (a,n)=1}}^{n} (x - \zeta_n^a) \in \mathbb{Z}[x].$$

It is known that the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(\mathbb{Q}(\zeta_n)) : \ \sigma(r) = r \text{ for all } r \in \mathbb{Q}\}$$

has exactly $\varphi(n)$ elements, and they are

$$\varphi_a \ (1 \leqslant a \leqslant n \ \& \ (a,n) = 1) \ \text{ with } \varphi_a(\zeta_n) = \zeta_n^a.$$

The value of $\prod_{1\leqslant j<k\leqslant(p-1)/2}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p})^2$

Let p be an odd prime let $\zeta = e^{2\pi i/p}$. Let $a \in \mathbb{Z}$ with $p \nmid a$, and let $\varphi_a \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\varphi_a(\zeta) = \zeta^a$. Then

$$\begin{aligned}\varphi_a\left(\sqrt{(-1)^{(p-1)/2}p}\right) &= \varphi_a\left(\sum_{x=0}^{p-1}\zeta^{x^2}\right)\\ &= \sum_{x=0}^{p-1}\zeta^{ax^2} = \left(\frac{a}{p}\right)\sqrt{(-1)^{(p-1)/2}p}.\end{aligned}$$

Now assume that $p \equiv 3 \pmod 4$. Recall that

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{j^2}-\zeta^{k^2})^2 = (-p)^{(p-3)/4}.$$

So, for some $\varepsilon \in \{\pm 1\}$, we have

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{j^2}-\zeta^{k^2}) = \varepsilon(\sqrt{p}\, i)^{(p-3)/4}.$$

On $\prod_{1\leqslant j<k\leqslant(p-1)/2}(e^{2\pi iaj^2/p}-e^{2\pi iak^2/p})$

Applying the automorphism φ_a of the cyclotomic field $\mathbb{Q}(\zeta)$, we get

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})=\varepsilon\varphi_a(\sqrt{p}\,i)^{(p-3)/4}=\varepsilon\left(\left(\frac{a}{p}\right)\sqrt{p}\,i\right)^{(p-3)/4}.$$

Thus, for any $r=1,\ldots,(p-1)/2$ we have

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\zeta^{r^2j^2}-\zeta^{r^2k^2}\right)=\varepsilon(\sqrt{p}\,i)^{(p-3)/4};$$

on the other hand,

$$\prod_{1\leqslant j<k\leqslant(p-1)/2}\left(\zeta^{r^2j^2}-\zeta^{r^2k^2}\right)=\prod_{1\leqslant j<k\leqslant(p-1)/2}(1-\zeta^{r^2(k^2-j^2)}).$$

Determine ε

Therefore

$$
\begin{aligned}
&\left(\varepsilon(\sqrt{p}\, i)^{(p-3)/4}\right)^{(p-1)/2}\\
=&\prod_{1\leqslant j<k\leqslant (p-1)/2}\ \prod_{r=1}^{(p-1)/2}(1-\zeta^{(k^2-j^2)r^2})\\
=&\prod_{1\leqslant j<k\leqslant (p-1)/2}\left((-1)^{(h(-p)+1)/2}\left(\frac{k^2-j^2}{p}\right)\sqrt{p}\, i\right).
\end{aligned}
$$

and hence

$$
\begin{aligned}
\varepsilon =&\varepsilon^{(p-1)/2}=(-1)^{\frac{h(-p)+1}{2}\cdot\frac{(p-1)(p-3)}{8}}\prod_{1\leqslant j<k\leqslant (p-1)/2}\left(\frac{k^2-j^2}{p}\right)\\
=&(-1)^{\frac{h(-p)+1}{2}\cdot\frac{p-3}{4}}.
\end{aligned}
$$

Two related theorems

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 $p \nmid a$. Then

$$(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor} 2^{(p-1)(p-3)/8} \prod_{1\leqslant j<k\leqslant(p-1)/2} \cos\pi\frac{a(k^2-j^2)}{p}$$

$$= \prod_{1\leqslant j<k\leqslant(p-1)/2} (\zeta^{aj^2}+\zeta^{ak^2}) = \begin{cases} 1 & \text{if } p\equiv 3 \pmod 4, \\ \pm\varepsilon_p^{(\frac{a}{p})h(p)((\frac{2}{p})-1)/2} & \text{if } p\equiv 1 \pmod 4. \end{cases}$$

Theorem (Fedor Petrov and Z.-W. Sun [arXiv:1907.12981]). 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

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

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

Part II. Permutations related to Permanents or Groups

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.

Note that

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

Conjecture (Z.-W. Sun, arXiv:1811.10503). (i) For any integer $n > 5$, there is a permutation $\pi \in S_n$ with $\sum_{k=1}^{n-1} \frac{1}{\pi(k)\pi(k+1)} = 1$.

(ii) 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 $n > 5$, there exists a permutation $\pi \in S_n$ such that $\sum_{k=1}^{n-1} \frac{1}{\pi(k)-\pi(k+1)} = 0$.

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 $\rho \in S_n$ 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

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

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

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

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

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 $p \mid \mathrm{per}[i^{j-1}]_{1\leqslant i,j\leqslant p-1}$ for any odd prime p.

Proof of the Second Part of the Theorem (continued)

Suppose that $\mathrm{per}[i^{j-1}]_{1\le i,j\le p-1} \not\equiv 0 \pmod{p}$ 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 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)

As mentioned before, 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.

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

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

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

Let a_n denote the permanent in $(*)$. Via Mathematica I find that

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

Main References:

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

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

Thank you!