A talk given at *Number Theory in the Clouds* (April 17-18, 2020)

Proof of Some Conjectures involving Quadratic Residues

Zhi-Wei Sun

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

April 17, 2020

Part I. Backgrounds

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

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

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. 15, 2018 I found the pattern for $\mathrm{sign}(\pi_p)$ when $p \equiv 3 \pmod 4$, but I was not able to find a pattern for $\mathrm{sign}(\pi_p)$ when $p \equiv 1 \pmod 4$.

Theorem (Z.-W. Sun [Finite Fields Appl. Finite Fields Appl. 59 (2019), 246-283]). 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$=\begin{cases}\pm i^{(p-1)/4}p^{(p-3)/8}\varepsilon_p^{(\frac{a}{p})h(p)/2} & \text{if } p\equiv 1 \pmod 4,\\ (-p)^{(p-3)/8} & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(p+1)/8+(h(-p)-1)/2}(\frac{a}{p})p^{(p-3)/8}i & \text{if } p\equiv 7 \pmod 8,\end{cases}$$

For the case $p\equiv 3 \pmod 4$, we employ Galois theory in the proof.

It is difficult to recognize the sign in the case $p\equiv 1 \pmod 4$.

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

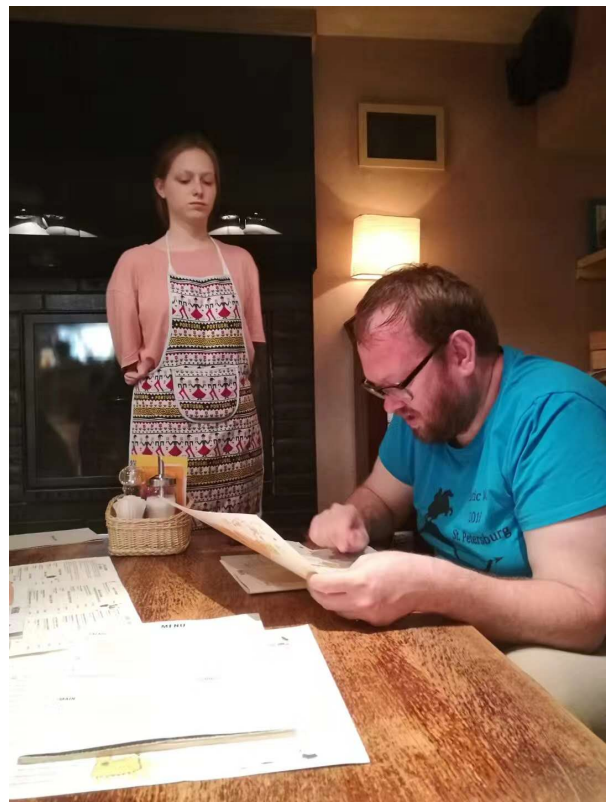
As $x+y=\frac{x^2-y^2}{x-y}$, from the above theorem we have the following result.

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

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

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

Part II. Joint Work with Fedor Petrov

Petrov.jpg 

Determine the product in the case $p \equiv 1 \pmod 4$

The following theorem confirms a conjecture of the speaker [Finite Fields Appl. 59(2019), 246-283].

Theorem 1 (F. 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

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

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

On the parity of $|\{1 \leqslant k < \frac{p}{4} : \ (\frac{k}{p}) = -1\}|$

Let p be a prime with $p \equiv 1 \pmod 4$. Then

$$\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod p$$

by Wilson's theorem. We may write $p = x^2 + y^2$ with $x, y \in \mathbb{Z}$,

$$x \equiv 1 \pmod 4 \ \text{ and } \ y \equiv \frac{p-1}{2}!x \pmod p.$$

As $y^2 \equiv p - 1 \pmod 8$, we see that $y \equiv (\frac{2}{p}) - 1 \pmod 4$. By a result of K. Burde [J. Number Theory 12(1980), 273-277], we have

$$\left|\left\{1 \leqslant k < \frac{p}{4} : \ \left(\frac{k}{p}\right) = 1\right\}\right| \equiv 0 \pmod 2$$

$$\iff y \equiv \left(\frac{2}{p}\right) - 1 \pmod 8.$$

Thus

$$(-1)^{|\{1 \leqslant k < \frac{p}{4} : \ (\frac{k}{p}) = -1\}|} = (-1)^{\frac{p-1}{4}} (-1)^{\frac{1}{4}(y - (\frac{2}{p}) + 1)} = (-1)^{\lfloor \frac{y}{4} \rfloor}.$$

Some Lemmas

Lemma 1 (see, e.g., K.S. Williams and J.D. Currie [Canad. J. Math. 34(1982)]). Let $p \equiv 1 \pmod 8$ be a prime. Then

$$2^{(p-1)/4} \equiv (-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} \pmod p.$$

Motivated by Zolotarev's Lemma, in 2006 Hao Pan obtained the following lemma.

Lemma 2. $(\mathrm{H.\ Pan,\ arXiv{:}0601026})$ Let $n > 1$ be an odd integer and let c be any integer relatively prime to n. For each $j = 1, \ldots, (n-1)/2$ let $\tau_c(j)$ be the unique $r \in \{1, \ldots, (n-1)/2\}$ with cj congruent to r or $-r$ modulo n. For the permutation τ_c on $\{1, \ldots, (n-1)/2\}$, its sign is given by

$$\mathrm{sign}(\tau_c) = \left(\frac{c}{n}\right)^{(n+1)/2},$$

where $(\frac{c}{n})$ is the Jacobi symbol.

Proof of Theorem 1 in the case $p \equiv 1 \pmod 8$

As $p \equiv 1 \pmod 8$, there is an integer c with $c^2 \equiv 2 \pmod p$. For $j = 1, \ldots, (p-1)/2$ let $\tau_c(j)$ be the unique $r \in \{1, \ldots, (p-1)/2\}$ with cj congruent to r or $-r$ modulo p. Then τ_c is a permutation on $\{1, \ldots, (p-1)/2\}$, and

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

$$= (-1)^{|\{(j,k):\ 1 \leqslant j < k \leqslant (p-1)/2\ \&\ \tau_c(j) > \tau_c(k)\}|} = \operatorname{sign}(\tau_c) = \left(\frac{c}{p}\right)$$

with the aid of Pan's Lemma. Note that

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

So the desired result follows.

Proof of Theorem 1 in the case $p \equiv 5 \pmod 8$

We first prove the desired result for $a = 1$.

In view of Sun's result, we only need to prove that

$$(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} \prod_{1\leqslant j<k\leqslant (p-1)/2} (\zeta^{j^2}+\zeta^{k^2}) > 0.$$

As $(\frac{-1}{p}) = 1$, for each $1 \leqslant j \leqslant (p-1)/2$ there is a unique integer $j_* \in \{1, \ldots, (p-1)/2\}$ such that $p - j^2 \equiv j_*^2 \pmod p$. As $(\frac{2}{p}) = -1$, we have $j \neq j_*$.

Proof of Theorem 1 in the case $p \equiv 5 \pmod 8$

For any distinct $j, k \in \{1, \ldots, (p-1)/2\}$, we have $\zeta^{j^2} + \zeta^{k^2} \neq 0$ (since $\zeta^{2j^2} \neq \zeta^{2k^2}$) and

$$(\zeta^{j^2} + \zeta^{k^2})(\zeta^{j_*^2} + \zeta^{k_*^2}) = (\zeta^{j^2} + \zeta^{k^2})(\zeta^{-j^2} + \zeta^{-k^2}) = |\zeta^{j^2} + \zeta^{k^2}|^2 > 0;$$

also,

$$\{j, k\} = \{j_*, k_*\} \iff j_* = k \text{ and } k_* = j \iff j_* = k.$$

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

$$\zeta^{j^2} + \zeta^{j_*^2} = \zeta^{j^2} + \zeta^{-j^2} = 2\cos 2\pi \frac{j^2}{p} = 2\cos 2\pi \frac{j_*^2}{p}$$

and hence

$$\zeta^{j^2} + \zeta^{j_*^2} > 0 \iff \cos 2\pi \frac{j^2}{p} > 0 \iff \{j^2\}_p < \frac{p}{4} \text{ or } \{j_*^2\}_p < \frac{p}{4}.$$

Complete the proof for the case $\left(\frac{a}{p}\right) = 1$

Thus the sign of the product

$$\prod_{\substack{1 \leqslant j < k \leqslant (p-1)/2 \\ p \mid j^2 + k^2}} (\zeta^{j^2} + \zeta^{k^2}) = (-1)^{(p-1)/4} \prod_{1 \leqslant j < j_* \leqslant (p-1)/2} (-\zeta^{j^2} - \zeta^{j_*^2})$$

is

$$(-1)^{(p-1)/4 - |\{1 \leqslant k < \frac{p}{4} : \, (\frac{k}{p}) = 1\}|} = (-1)^{|\{1 \leqslant k < \frac{p}{4} : \, (\frac{k}{p}) = -1\}|}.$$

This proves the desired result for $a = 1$.

In the case $\left(\frac{a}{p}\right) = 1$, we have

$$\left\{ \{aj^2\}_p : \; 1 \leqslant j \leqslant \frac{p-1}{2} \right\} = \left\{ \{k^2\}_p : \; 1 \leqslant k \leqslant \frac{p-1}{2} \right\}$$

and so the desired result reduces to the case $a = 1$.

Handle the case $\left(\frac{a}{p}\right) = -1$

By the above, we have

$$(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} \prod_{1\leqslant j<k\leqslant (p-1)/2} (\zeta^{j^2} + \zeta^{k^2}) = \varepsilon_p^{-h(p)}. \qquad (*)$$

Let φ_a be the element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\varphi_a(\zeta) = \zeta^a$. Then

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

by the evaluation of quadratic Gauss sums. Hence

$$\varphi_a(\varepsilon_p^{-h(p)}) = \left(\frac{N(\varepsilon_p)}{\varepsilon_p}\right)^{-h(p)} = -\varepsilon_p^{h(p)}$$

where $N(\varepsilon_p)$ is the norm of ε_p with respect to the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, and we have used the known results $N(\varepsilon_p) = -1$ and $2 \nmid h(p)$.

Complete the proof for the case $\left(\frac{a}{p}\right) = -1$

Thus, by applying the automorphism φ_a to the identity $(*)$, we get

$$(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} \prod_{1\leqslant j<k\leqslant (p-1)/2} (\zeta^{aj^2} + \zeta^{ak^2})$$

$$= \varphi_a\left(\varepsilon_p^{-h(p)}\right) = -\varepsilon_p^{h(p)} = \left(\frac{a}{p}\right) \varepsilon_p^{-(\frac{a}{p})h(p)}.$$

Triangular numbers modulo primes

The *triangular numbers* are those

$$T_n = \frac{n(n+1)}{2} \quad (n \in \mathbb{N} = \{0, 1, 2, \ldots\}).$$

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

$$T_k - T_j = \frac{(k-j)(k+j+1)}{2} \not\equiv 0 \pmod{p}.$$

So, the triangular numbers

$$T_0, T_1, \ldots, T_{(p-1)/2}$$

are pairwise distinct modulo p.

A theorem on triangular numbers modulo p

The following theorem confirms a conjecture of the speaker [Finite Fields Appl. 59(2019), 246-283].

Theorem 2. (F. Petrov and Z.-W. Sun [Electron. Res. Arch 28(2020)]) Let p be a prime with $p\equiv 3 \pmod 4$.

(i) We have

$$(-1)^{\left|\left\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2 \text{ and } \{j(j+1)\}_p>\{k(k+1)\}_p\right\}\right|}=(-1)^{\lfloor (p+1)/8\rfloor}.$$

(ii) Suppose $p>3$ and write $T_m=m(m+1)/2$ for $m\in\mathbb{N}$. Then

$$\begin{aligned}&(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant (p-1)/2\ \&\ \{T_j\}_p>\{T_k\}_p\}|}\\ =&(-1)^{\frac{h(-p)+1}{2}+|\{1\leqslant k\leqslant \lfloor \frac{p+1}{8}\rfloor:\ (\frac{k}{p})=1\}|}.\end{aligned}$$

A result of Sun needed

Let $p = 2n+1$ be a prime with n odd, and let $a \in \mathbb{Z}$ with $p \nmid a$. By Sun [Finite Fields Appl. 59(2019), 246-283],

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

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

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

$$\cot \pi\frac{aj^2}{p} < \cot \pi\frac{ak^2}{p} \iff \{aj^2\}_p > \{ak^2\}_p.$$

So

$$(-1)^{|\{(j,k):\ 1\leqslant j<k\leqslant n\ \&\ \{aj^2\}_p>\{ak^2\}_p\}|}$$

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

An auxiliary theorem

Auxiliary Theorem. Let $p = 2n+1$ be a prime with n odd, and let $a, b \in \{1, \ldots, p-1\}$. Then

$$(-1)^{|\{(s,t):\ 0\leqslant t<s\leqslant n\ \&\ \{as^2-b\}_p>\{at^2-b\}_p\}|-|\{0<r<b:\ (\frac{r}{p})=(\frac{a}{p})\}|}$$

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

Proof. Let $0 \leqslant t < s \leqslant n$. By comparing $\{as^2\}_p$ and $\{at^2\}_p$ with b, we verify case by case that

$$[\{as^2 - b\}_p > \{at^2 - b\}_p] + [\{as^2\}_p > \{at^2\}_p]$$

is odd if and only if

$$\{as^2\}_p \geqslant b > \{at^2\}_p \quad \text{or} \quad \{at^2\}_p \geqslant b > \{as^2\}_p,$$

where for an assertion A we define

$$[A] = \begin{cases} 1 & \text{if } A \text{ holds}, \\ 0 & \text{otherwise}. \end{cases}$$

Proof of the theorem (continued)

Note that

$$\begin{aligned}
&|\{(s,t): 0\leqslant t<s\leqslant n, \{as^2\}_p\geqslant b>\{at^2\}_p \text{ or } \{as^2\}_p<b\leqslant\{at^2\}_p\}|\\
=&\left|\left\{(r_1,r_2):\ 0\leqslant r_1<b\leqslant r_2\leqslant p-1\ \&\ \left(\frac{ar_1}{p}\right),\left(\frac{ar_2}{p}\right)\neq -1\right\}\right|\\
=&\left|\left\{r\in[0,b):\left(\frac{ar}{p}\right)\neq -1\right\}\right|\left(\frac{p+1}{2}-\left|\left\{r\in[0,b):\left(\frac{ar}{p}\right)\neq -1\right\}\right|\right)\\
\equiv&1+\left|\left\{r\in(0,b):\ \left(\frac{r}{p}\right)=\left(\frac{a}{p}\right)\right\}\right| \pmod 2
\end{aligned}$$

and

$$\begin{aligned}
&|\{(s,t):\ 0\leqslant t<s\leqslant n\ \&\ \{as^2\}_p>\{at^2\}_p\}|\\
=&\binom{n+1}{2}-|\{(s,t):\ 0\leqslant t<s\leqslant n\ \&\ \{as^2\}_p<\{at^2\}_p\}|
\end{aligned}$$

with $\binom{n+1}{2}\equiv\frac{p+1}{4} \pmod 2$. Now it suffices to use the known result of Sun on the parity of

$$|\{(s,t):\ 0\leqslant t<s\leqslant n\ \&\ \{as^2\}_p<\{at^2\}_p\}|.$$

A Lemma

Lemma. Let p be a prime with $p \equiv 3 \pmod 4$.

(i) (Dirichlet) If $p > 3$ then

$$\left(2 - \left(\frac{2}{p}\right)\right) h(-p) = \sum_{k=1}^{(p-1)/2} \left(\frac{k}{p}\right).$$

(ii) (B. C. Berndt and S. Chowla, 1974) If $p \equiv 3 \pmod 8$, then

$$\sum_{0<k<p/4} \left(\frac{k}{p}\right) = 0.$$

If $p \equiv 7 \pmod 8$, then

$$\sum_{p/4<k<p/2} \left(\frac{k}{p}\right) = 0.$$

Proof of Theorem 2

We just prove part (ii) since part (i) can be proved similarly.

Write $n = (p-1)/2$, and set

$$a = \frac{p+1}{2} \quad \text{and} \quad b = \begin{cases} (5p+1)/8 & \text{if } p \equiv 3 \pmod 8, \\ (p+1)/8 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

For any $r \in \mathbb{Z}$, we have

$$T_{n-r} = \frac{n(n+1)}{2} - (2n+1)\frac{r}{2} + \frac{r^2}{2} \equiv ar^2 - b \pmod p.$$

Thus

$$\begin{aligned} &|\{(j,k) :\ 0 \leqslant j < k \leqslant n \ \&\ \{T_j\}_p > \{T_k\}_p\}| \\ =&|\{(t,s) :\ 0 \leqslant t < s \leqslant n \ \&\ \{T_{n-s}\}_p > \{T_{n-t}\}_p\}| \\ =&|\{(t,s) :\ 0 \leqslant t < s \leqslant n \ \&\ \{as^2 - b\}_p > \{at^2 - b\}_p\}|. \end{aligned}$$

Proof of Theorem 2 (continued)

Note that $(\frac{a}{p}) = (\frac{2}{p})$. Set

$$B := \left| \left\{ 0 < r < b : \ \left(\frac{r}{p}\right) = \left(\frac{2}{p}\right) \right\} \right|.$$

Applying the Auxiliary Theorem, from the above we obtain

$$\begin{aligned} &|\{(j,k) : \ 1 \leqslant j < k \leqslant n \ \& \ \{T_j\}_p > \{T_k\}_p\}| \\ \equiv & B + \begin{cases} 0 \pmod 2 & \text{if } p \equiv 3 \pmod 8, \\ (h(-p)-1)/2 \pmod 2 & \text{if } p \equiv 7 \pmod 8. \end{cases} \end{aligned}$$

So it suffices to determine the parity of B.

When $p \equiv 7 \pmod 8$, we have $b = (p+1)/8$ and hence

$$B + 1 = \left| \left\{ 1 \leqslant k \leqslant \frac{p+1}{8} : \ \left(\frac{k}{p}\right) = 1 \right\} \right|.$$

Proof of Theorem 2 (continued)

Now we handle the case $p \equiv 3 \pmod 8$. Observe that

$$B = \sum_{k=1}^{(p-1)/2} \frac{1-(\frac{k}{p})}{2} + \left|\left\{\frac{p}{2} < k < \frac{5p+1}{8} : \left(\frac{2k-p}{p}\right) = 1\right\}\right|$$

$$= \frac{p-1}{4} - \frac{1}{2}\sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right) + \left|\left\{0 < r < \frac{p+1}{4} : 2 \nmid r \ \&\ \left(\frac{r}{p}\right) = 1\right\}\right|.$$

Applying the Lemma, we obtain

$$B = \frac{p-1}{4} - \frac{3h(-p)}{2} + \sum_{0<k<p/4} \frac{1+(\frac{k}{p})}{2}$$

$$- \left|\left\{0 < r < \frac{p+1}{4} : 2 \mid r \ \&\ \left(\frac{r}{p}\right) = 1\right\}\right|$$

$$\equiv \frac{h(-p)+1}{2} + \frac{p-3}{8} - \left|\left\{0 < k < \frac{p+1}{8} : \left(\frac{2k}{p}\right) = 1\right\}\right|$$

$$= \frac{h(-p)+1}{2} + \left|\left\{0 < k < \frac{p+1}{8} : \left(\frac{2k}{p}\right) = -1\right\}\right| \pmod 2.$$

Main References:

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

2. F. Petrov and Z.-W. Sun, *Proof of some conjectures involving quadratic residues*, Electron. Res. Arch. **28** (2020), no. 2, to appear.

Thank you!