Bull. Iranian Math. Soc. 51 (2025), no. 4, Article No. 59, 13 pp.

ON SOME DETERMINANTS ARISING FROM QUADRATIC RESIDUES

CHEN-KAI REN AND ZHI-WEI SUN

Abstract. Let $p>3$ be a prime, and let $d\in\mathbb{Z}$ with $p\nmid d$. For $m\in\mathbb{Z}$ with $(p-1)/2\leqslant m\leqslant p-1$, Sun considered the determinant

$$S_m(d,p)=\det\left[(i^2+dj^2)^m\right]_{1\leqslant i,j\leqslant(p-1)/2},$$

and determined $S_m(d,p)$ modulo p when $m\in\{p-2,p-3\}$ and $(\frac{-d}{p})=-1$. In this paper, we obtain $S_{p-2}(d,p)$ modulo p in the remaining case $(\frac{-d}{p})=1$, and determine the Legendre symbols $(\frac{S_{p-3}(d,p)}{p})$ and $(\frac{S_{p-4}(d,p)}{p})$ in some special cases.

1. Introduction

Let p be an odd prime, and let $(\frac{\cdot}{p})$ be the Legendre symbol. In 1959, Carlitz [3, (4.9)] proved that the characteristic polynomial of the matrix

$$\left[\left(\frac{i-j}{p}\right)\right]_{1\leqslant i,j\leqslant p-1}$$

is

$$\left(x^2-\left(\frac{-1}{p}\right)\right)\left(x^2-\left(\frac{-1}{p}\right)p\right)^{(p-3)/2}.$$

In 2004, via quadratic Gauss sums Chapman [4] showed that for $p>3$ we have

$$\det\left[\left(\frac{i+j-1}{p}\right)\right]_{1\leqslant i,j\leqslant(p-1)/2}=\begin{cases}(-1)^{(p-1)/4}2^{(p-1)/2}b_p & \text{if } p\equiv 1\pmod 4,\\ 0 & \text{if } p\equiv 3\pmod 4,\end{cases}$$

and

$$\det\left[\left(\frac{i+j-1}{p}\right)\right]_{1\leqslant i,j\leqslant(p+1)/2}=\begin{cases}(-1)^{(p+3)/4}2^{(p-1)/2}a_p & \text{if } p\equiv 1\pmod 4,\\ 2^{(p-1)/2} & \text{if } p\equiv 3\pmod 4,\end{cases}$$

Key words and phrases. Determinants, Legendre symbols, quadratic residues modulo primes.

2020 *Mathematics Subject Classification.* Primary 11A15, 11C20; Secondary 15A15.

Supported by the Natural Science Foundation of China (grant 12371004).

where a_p and b_p are rational numbers given by $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$, and ε_p and $h(p)$ denote the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively. During 2012–2013, Vsemirnov [12, 13] confirmed a challenging conjecture of Chapman which states that

$$\det\left[\left(\frac{i-j}{p}\right)\right]_{0\leqslant i,j\leqslant (p-1)/2} = \begin{cases} -a_p' & \text{if } p\equiv 1 \pmod 4,\\ 1 & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

where we write $\varepsilon_p^{(2-(\frac{2}{p}))h(p)}$ as $a_p' + b_p'\sqrt{p}$ with $a_P', b_p' \in \mathbb{Q}$.

Let d be any integer not divisible by an odd prime p. Sun [9] studied the determinant

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

and proved that $(\frac{-S(d.p)}{p}) = 1$ if $(\frac{d}{p}) = 1$, and $S(d,p) = 0$ if $(\frac{d}{p}) = -1$. Grinberg, Sun and Zhao [6] showed that if $p > 3$ then

$$\det\left[(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\right]_{0\leqslant i,j\leqslant (p-1)/2} \equiv 0 \pmod p. \tag{1.1}$$

For any integer m in the interval $((p-1)/2, p-1)$, we have from [11] that

$$\det[(i^2+dj^2)^m]_{0\leqslant i,j\leqslant (p-1)/2} \equiv 0 \pmod p,$$

which extends (1.1). For each $m = (p-1)/2, \ldots, p-1$, Sun [11] introduced the determinant

$$S_m(d,p) = \det\left[(i^2+dj^2)^m\right]_{1\leqslant i,j\leqslant (p-1)/2}.$$

Let d be any integer not divisible by an odd prime p. In 2022, Wu, She and Wang [15] confirmed [9, Conjecture 4.5(ii)] which states that when $p > 3$ we have

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

where $h(-p)$ denotes the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Sun [11] proved that if $(\frac{-d}{p}) = -1$ then

$$\begin{aligned} S_{p-2}(d,p) &\equiv \det\left[\frac{1}{i^2+dj^2}\right]_{1\leqslant i,j\leqslant (p-1)/2}\\ &\equiv \begin{cases} d^{(p-1)/4} \pmod p & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{(p+1)/4} \pmod p & \text{if } p\equiv 3 \pmod 4,\end{cases}\end{aligned}$$

and

$$S_{p-3}(d,p)\equiv\det\left[\frac{1}{(i^2+dj^2)^2}\right]_{1\leqslant i,j\leqslant(p-1)/2}\equiv\frac{1}{4}\prod_{r=1}^{\lfloor p/4\rfloor}\left(r+\frac{1}{4}\right)^2\pmod p.$$

In this paper, we obtain some further results along this line. Our method is different from that of Sun [11].

We first present a general result.

Theorem 1.1. *Let p be a prime with $p\equiv 1\pmod 4$. For any integer d with $(\frac{d}{p})=1$ and any odd integer $m\in((p-1)/2,p-1)$, we have*

$$\left(\frac{S_m(d,p)}{p}\right)\neq -1.$$

Our following three theorems deal with $S_m(d,p)$ for $m=p-2,p-3,p-4$. For convenience, we define $n!!=\prod_{0\leqslant j<n/2}(n-2j)$ for any positive integer n.

Theorem 1.2. *Let p be an odd prime, and let $d\in\mathbb{Z}$ with $(\frac{-d}{p})=1$. Then*

$$S_{p-2}(d,p)\equiv\begin{cases}(-1)^{(p+3)/4}d^{(p-1)/4}(\frac{p-3}{2}!!)^2\pmod p & \text{if } p\equiv 1\pmod 4,\\ 0\pmod p & \text{if } p\equiv 3\pmod 4.\end{cases}\tag{1.2}$$

Remark 1.1. Let p be a prime with $p\equiv 1\pmod 4$, and write $p=x^2+y^2$ $(x,y\in\mathbb{Z})$ with $x\equiv 1\pmod 4$ and $y\equiv\frac{p-1}{2}!\,x\pmod p$. (Note that $(\frac{p-1}{2}!\,x)^2\equiv -x^2\pmod p$ by Wilson's theorem.) As $2x\equiv\binom{(p-1)/2}{(p-1)/4}\pmod p$ by Gauss' congruence (cf. [1, (9.0.1)] or [5]), we have

$$2y\equiv\frac{p-1}{2}!(2x)\equiv\frac{(\frac{p-1}{2}!)^2}{(\frac{p-1}{4}!)^2}=\left(2^{\frac{p-1}{4}}\frac{p-3}{2}!!\right)^2\equiv\left(\frac{2}{p}\right)\left(\frac{p-3}{2}!!\right)^2\pmod p.$$

Thus, for any $d\in\mathbb{Z}$ with $(\frac{d}{p})=1$, by (1.2) we have

$$S_{p-2}(d,p)\equiv -2yd^{(p-1)/4}\pmod p.$$

With the aid of [1, Theorem 6.2.9, p. 190], this implies Sun's conjecture (cf. [11, Conjecture 6.2]) that

$$S_{p-2}(1,p)\equiv -2y=2\delta(s,p)\sum_{k=1}^{(p-1)/2}\left(\frac{k(k^2+s)}{p}\right)\pmod p,$$

where s is any quadratic nonresidue modulo p, and

$$\delta(s,p)=\begin{cases}1 & \text{if } s^{(p-1)/4}\equiv\frac{p-1}{2}!\pmod p,\\ -1 & \text{otherwise.}\end{cases}$$

Theorem 1.3. *Let $p>3$ be a prime with $p\equiv 1 \pmod 4$, and let d be any integer with $p\nmid d$. Then*

$$\left(\frac{6S_{p-3}(d,p)}{p}\right)\neq -1.$$

Moreover, if $(\frac{d}{p})=1$ and $p\equiv 5 \pmod{12}$, then

$$\left(\frac{S_{p-3}(d,p)}{p}\right)=(-1)^{(p+3)/4}.$$

Theorem 1.4. *Let $p>3$ be a prime, and let d be any integer with $(\frac{d}{p})=1$. Then*

$$\left(\frac{S_{p-4}(d,p)}{p}\right)=-1 \quad \text{if and only if} \quad p\equiv 3,7 \pmod{20}. \tag{1.3}$$

We are going to provide some auxiliary results in the next section, and prove Theorems 1.1-1.4 in Section 3.

To end this section, we mention that there are some other works inspired by Sun [11]. For example, Conjectures 6.3–6.5 in [11] have been confirmed by Chaliha and Kalita [2], and also Ren and Luo [8] independently.

2. Some auxiliary results

For any odd prime p, by Wilson's theorem we have

$$(-1)^{(p+1)/2}\left(\frac{p-1}{2}!\right)^2\equiv -\prod_{k=1}^{(p-1)/2}k(p-k)=-(p-1)!\equiv 1 \pmod p. \tag{2.1}$$

We need the following auxiliary result (cf. [14, Lemma 2.2]).

Proposition 2.1. *Let p be an odd prime. Then*

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}(i^2-j^2)\left(\frac{1}{i^2}-\frac{1}{j^2}\right)\equiv (-1)^{\lfloor p/4\rfloor} \pmod p. \tag{2.2}$$

Remark 2.1. Actually,

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}(i^2-j^2)^2\equiv (-1)^{(p+1)/2} \pmod p$$

by [10, (1.5)] and the congruence (2.1). Thus it remains to prove

$$\prod_{1\leqslant i<j\leqslant (p-1)/2}(ij)^2\equiv (-1)^{(p+1)/2} \pmod p.$$

For any positive integers m and n, we clearly have

$$\prod_{1\leqslant i_1<\ldots<i_m\leqslant n} i_1\cdots i_m=\prod_{\substack{A\subseteq\{1,\ldots,n\}\\ |A|=m}}\prod_{k\in A}k$$
$$=\prod_{k=1}^n k^{|\{A\subseteq\{1,\ldots,n\}:\ k\in A\ \&\ |A\setminus\{k\}|=m-1\}|}=(n!)^{\binom{n-1}{m-1}}.$$

Thus we have an alternate proof of (2.2).

We also need the following known lemma [7, Lemma 10] on determinants.

Lemma 2.1. *Let R be a commutative ring with identity, and let $P(x)=\sum_{i=0}^{n-1}a_ix^i\in R[x]$. Then we have*

$$\det\left[P(X_iY_j)\right]_{1\leqslant i,j\leqslant n}=a_0a_1\cdots a_{n-1}\prod_{1\leqslant i<j\leqslant n}(X_i-X_j)(Y_i-Y_j).$$

Now we state our second auxiliary proposition.

Proposition 2.2. *Let $p=2n+1>3$ be a prime. For $d,m\in\mathbb{Z}$ with $p\nmid d$ and $(p-1)/2<m<p-1$, we have*

$$S_m(d,p)\equiv a_m(d,p)^2b_m(d,p)\pmod p,\tag{2.3}$$

where

$$a_m(d,p)=\prod_{k=0}^{\lfloor(m-n-1)/2\rfloor}\left(\binom{m}{k}+\left(\frac{d}{p}\right)\binom{m}{m-n-k}\right)$$
$$\times\prod_{0\leqslant k<n-1-\lfloor m/2\rfloor}\binom{m}{m-n+1+k}$$

and

$$b_m(d,p)=\begin{cases}(-d)^{n/2}\left(1+\left(\frac{d}{p}\right)\right)\binom{m}{(m-n)/2}\binom{m}{m/2} & \text{if } 2\mid m \text{ and } 2\mid n,\\ (-1)^{(n-1)/2}\left(\frac{d}{p}\right)^{m/2}\binom{m}{m/2} & \text{if } 2\mid m \text{ and } 2\nmid n,\\ (-1)^{n/2+1}d^{n/2}\left(\frac{d}{p}\right)^{(m-1)/2} & \text{if } 2\nmid m \text{ and } 2\mid n,\\ (-1)^{(n-1)/2}\left(1+\left(\frac{d}{p}\right)\right)\binom{m}{(m-n)/2} & \text{if } 2\nmid m \text{ and } 2\nmid n.\end{cases}$$

Remark 2.2. Proposition 2.2 clearly implies the following result: Let $p>5$ be a prime, and let d be an integer with $(\frac{d}{p})=-1$. If m be an integer in the interval $((p-1)/2,p-1)$ with $m\equiv(p-1)/2\pmod 2$, then $S_m(d,p)\equiv 0\pmod p$.

Proof of Proposition 2.2. Observe that

$$\begin{aligned} S_m(d,p) &= \prod_{j=1}^{n}(j^2)^m \times \det\left[\left(i^2j^{-2}+d\right)^m\right]_{1\leqslant i,j\leqslant n} \\ &= (n!)^{2m}\det\left[\left(i^2j^{-2}+d\right)^m\right]_{1\leqslant i,j\leqslant n}. \end{aligned}$$

By (2.1),

$$(n!)^{2m}\equiv(-1)^{m(n+1)}\pmod p.$$

For $i,j\in\{1,\ldots,n\}$, clearly

$$\begin{aligned} \left(i^2j^{-2}+d\right)^m &= \sum_{k=0}^{m}\binom{m}{k}d^{m-k}\left(i^2j^{-2}\right)^k \\ &\equiv \sum_{k=0}^{m-n}\left(\binom{m}{k}d^{m-k}+\binom{m}{n+k}d^{m-k-n}\right)\left(i^2j^{-2}\right)^k \\ &\quad+\sum_{m-n+1\leqslant k<n}\binom{m}{k}d^{m-k}\left(i^2j^{-2}\right)^k \\ &\equiv f(i^2j^{-2})\pmod p, \end{aligned}$$

where

$$\begin{aligned} f(x) = &\sum_{k=0}^{m-n}\left(\binom{m}{k}+d^{-n}\binom{m}{m-n-k}\right)d^{m-k}x^k \\ &+\sum_{0\leqslant k<p-2-m}\binom{m}{m-n+1+k}d^{n-1-k}x^{m-n+1+k}. \end{aligned}$$

Combining the above, we obtain

$$S_m(d,p)\equiv(-1)^{m(n+1)}\det[f(i^2j^{-2})]_{1\leqslant i,j\leqslant n}\pmod p. \tag{2.4}$$

By Lemma 2.1 and the congruence (2.2), we have

$$\begin{aligned} &\det[f(i^2j^{-2})]_{1\leqslant i,j\leqslant n} \\ &\equiv(-1)^{\lfloor p/4\rfloor}\prod_{0\leqslant k<p-2-m}\binom{m}{m-n+1+k}d^{n-1-k} \\ &\quad\times\prod_{k=0}^{m-n}\left(\binom{m}{k}+d^{-n}\binom{m}{m-n-k}\right)d^{m-k}\pmod p. \end{aligned}$$

It is easy to see that

$$\prod_{0\leqslant k<p-2-m}d^{n-1-k}\times\prod_{k=0}^{m-n}d^{m-k}=d^{n(2m-n+1)/2}.$$

Note also that

$$\prod_{0\leqslant k<p-2-m}\binom{m}{m-n+1+k}=\binom{m}{\delta_m m/2}\prod_{0\leqslant k<n-1-\lfloor m/2\rfloor}\binom{m}{m-n+1+k}^2,$$

where $\delta_m=(1+(-1)^m)/2$. As $d^{-n}\equiv(\frac{d}{p})=\pm1\pmod p$, for each $k=0,\ldots,m-n$ we have

$$\begin{aligned}&\left(\binom{m}{k}+d^{-n}\binom{m}{m-n-k}\right)\left(\binom{m}{m-n-k}+d^{-n}\binom{m}{k}\right)\\&\quad\equiv\left(\frac{d}{p}\right)\left(\binom{m}{k}+\left(\frac{d}{p}\right)\binom{m}{m-n-k}\right)^2\pmod p.\end{aligned}$$

Therefore

$$\begin{aligned}&\det[f(i^2j^{-2})]_{1\leqslant i,j\leqslant n}\\&\equiv(-1)^{\lfloor p/4\rfloor}d^{n(2m-n+1)/2}\binom{m}{\delta_m m/2}\prod_{0\leqslant k<n-1-\lfloor m/2\rfloor}\binom{m}{m-n+1+k}^2\\&\quad\times c_m(d,p)\left(\frac{d}{p}\right)^{\lfloor(m-n+1)/2\rfloor}\prod_{k=0}^{\lfloor(m-n-1)/2\rfloor}\left(\binom{m}{k}+\left(\frac{d}{p}\right)\binom{m}{m-n-k}\right)^2\\&\equiv(-1)^{\lfloor p/4\rfloor}d^{n((2m-n+1)/2-\lfloor(m-n+1)/2\rfloor)}a_m(d,p)^2\binom{m}{\delta_m m/2}c_m(d,p)\pmod p,\end{aligned}$$

where

$$c_m(d,p):=\begin{cases}(1+(\frac{d}{p}))\binom{m}{(m-n)/2}&\text{if } m\equiv n\pmod 2,\\1&\text{otherwise.}\end{cases}$$

Combining this with (2.4), we obtain the desired (2.3) since

$$(-1)^{m(n+1)+\lfloor p/4\rfloor}d^{n((2m-n+1)/2-\lfloor(m-n+1)/2\rfloor)}\binom{m}{\delta_m m/2}c_m(d,p)$$

is congruent to $b_m(d,p)$ modulo p. This ends our proof. □

3. Proofs of Theorems 1.1-1.4

Proof of Theorem 1.1. Since $(\frac{-1}{p})=1$, by Proposition 2.2 we obtain

$$\left(\frac{b_m(d,p)}{p}\right)=\left(\frac{d}{p}\right)^{n/2}=1.$$

Thus

$$\left(\frac{S_m(d,p)}{p}\right)=\left(\frac{a_m(d,p)}{p}\right)^2\left(\frac{b_m(d,p)}{p}\right)=\left(\frac{a_m(d,p)}{p}\right)^2\neq-1.$$

□

Proof of Theorem 1.2. Set $n=(p-1)/2$. When $p\equiv 3\pmod 4$ and $(\frac{d}{p})=-1$, we have

$$S_{p-2}(d,p)\equiv 0\pmod p$$

by Remark 2.2.

Now we assume $p\equiv 1\pmod 4$. Then $(\frac{d}{p})=1$ and $2\mid n$. By Proposition 2.2, we have

$$S_{p-2}(d,p)\equiv a_{p-2}(d,p)^2b_{p-2}(d,p)\pmod p,$$

where

$$a_{p-2}(d,p)=\prod_{k=0}^{n/2-1}\left(\binom{p-2}{k}+\binom{p-2}{n-1-k}\right)$$

and

$$b_{p-2}(d,p)=(-1)^{n/2+1}d^{n/2}.$$

Since

$$\binom{p-r-1}{k}\equiv\binom{-r-1}{k}\equiv(-1)^k\binom{k+r}{r}\pmod p$$

for each $r=0,1,2,\ldots$, we can verify that

$$\begin{aligned}\binom{p-2}{k}+\binom{p-2}{n-1-k}&\equiv(-1)^k\binom{k+1}{1}+(-1)^{n-1-k}\binom{n-k}{1}\\&\equiv(-1)^k(2k-n+1)\pmod p.\end{aligned}$$

Combining the above, we obtain

$$\begin{aligned}S_{p-2}(d,p)&\equiv(-1)^{n/2+1}d^{n/2}\prod_{k=0}^{n/2-1}\left(\binom{p-2}{k}+d^{-n}\binom{p-2}{n-1-k}\right)^2\\&\equiv(-1)^{n/2+1}d^{n/2}\prod_{k=0}^{n/2-1}\left((-1)^k(2k-n+1)\right)^2\\&\equiv(-1)^{(p+3)/4}d^{(p-1)/4}\left(\frac{p-3}{2}!!\right)^2\pmod p.\end{aligned}$$

This concludes the proof. □

Proof of Theorem 1.3. Set $n=(p-1)/2$. By [11, Theorem 1.2], if $(\frac{d}{p})=-1$, then

$$\left(\frac{S_{p-3}(d,p)}{p}\right)=0.$$

Below we assume that $(\frac{d}{p})=1$. By Proposition 2.2,

$$S_{p-3}(d,p)\equiv a_{p-3}(d,p)^2 b_{p-3}(d,p)\pmod p, \tag{3.1}$$

where

$$a_{p-3}(d,p)=\prod_{k=0}^{n/2-2}\left(\binom{p-3}{k}+\binom{p-3}{n-2-k}\right)$$

and

$$b_{p-3}(d,p)=2(-d)^{n/2}\binom{p-3}{(n-2)/2}\binom{p-3}{n-1}.$$

Case 1. $a_{p-3}(d,p)\equiv 0\pmod p$.
In this case we have $S_{p-3}(d,p)\equiv 0\pmod p$ by (3.1).

Case 2. $a_{p-3}(d,p)\not\equiv 0\pmod p$.
Observe that

$$\begin{aligned}2\binom{p-3}{(n-2)/2}\binom{p-3}{n-1}&\equiv 2\binom{-3}{n/2-1}\binom{-3}{n-1}\\&=2(-1)^{n/2-1}\binom{n/2+1}{2}(-1)^{n-1}\binom{n+1}{2}\\&=(-1)^{n/2}\frac{n^2(n+1)(n+2)}{8}\\&\equiv\frac{(-1)^{n/2}}{8}\times\frac14\times\frac12\times\frac32=\frac{6(-1)^{n/2}}{16^2}\pmod p,\end{aligned}$$

and thus

$$\left(\frac{b_{p-3}(d,p)}{p}\right)=\left(\frac{d}{p}\right)^{n/2}\left(\frac{6}{p}\right)=\left(\frac{6}{p}\right).$$

Thus, applying (3.1) we obtain

$$\left(\frac{6S_{p-3}(d,p)}{p}\right)=1.$$

In view of the above, we get

$$\left(\frac{6S_{p-3}(d,p)}{p}\right)\neq -1.$$

Suppose that $p\equiv 5\pmod{12}$ and $(\frac{d}{p})=1$. We claim that

$$p\nmid\left(\binom{p-3}{k}+\binom{p-3}{n-2-k}\right)$$

for any integer k with $0 \leqslant k \leqslant n/2-2$. Note that

$$\begin{aligned}\binom{p-3}{k}+\binom{p-3}{n-2-k} &\equiv (-1)^k\binom{k+2}{2}+(-1)^{n-2-k}\binom{n-k}{2}\\ &\equiv \frac{(-1)^k}{2}\left((k+1)(k+2)+(k-n)(k-n+1)\right)\\ &\equiv (-1)^k\left(\left(k+\frac{5}{4}\right)^2-\frac{3}{16}\right)\pmod p.\end{aligned}$$

Since $(\frac{3}{p})=-1$, the claim holds.

In view of the above discussion, we obtain

$$\left(\frac{S_{p-3}(d,p)}{p}\right)=\left(\frac{6}{p}\right)=(-1)^{\frac{p+3}{4}}.$$

This ends the proof. □

Proof of Theorem 1.4. Set $n=(p-1)/2$.

If

$$\left(\frac{S_{p-4}(d,p)}{p}\right)=-1,$$

then $p\equiv 3 \pmod 4$ by Theorem 1.1. Below we suppose $p\equiv 3 \pmod 4$. In light of Proposition 2.2, we have

$$S_{p-4}(d,p)\equiv a_{p-4}(d,p)^2 b_{p-4}(d,p)\pmod p, \tag{3.2}$$

where

$$a_{p-4}(d,p)=\binom{p-4}{n-2}\prod_{k=0}^{(n-5)/2}\left(\binom{p-4}{k}+\binom{p-4}{n-3-k}\right)$$

and

$$b_{p-4}(d,p)=2(-1)^{(n-1)/2}\binom{p-4}{(n-3)/2}.$$

If $p\mid a_{p-4}(d,p)$, then

$$\left(\frac{S_{p-4}(d,p)}{p}\right)=0\neq -1$$

by (3.2).

Now assume that $p\nmid a_{p-4}(d,p)$. Clearly,

$$\begin{aligned}2\binom{p-4}{(n-3)/2}&\equiv 2\binom{-4}{(n-3)/2}=2(-1)^{(n-3)/2}\binom{(n+3)/2}{3}\\&=\frac{(-1)^{(n+1)/2}}{3}\times\frac{n+3}{2}\times\frac{n+1}{2}\times\frac{n-1}{2}\\&\equiv\frac{5(-1)^{(n-1)/2}}{64}\pmod p\end{aligned}$$

and thus

$$\left(\frac{b_{p-4}(d,p)}{p}\right)=\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right).$$

Combining this with (3.2), we obtain

$$\left(\frac{S_{p-4}(d,p)}{p}\right)=\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right).$$

Suppose that $(\frac{S_{p-4}(d,p)}{p})=-1$. Then $p\equiv\pm2\pmod 5$. As $p\equiv3\pmod 4$ and $p\equiv\pm2\pmod 5$, we get $p\equiv3,7\pmod{20}$. This proves one direction of (1.3).

Now suppose that $p\equiv3,7\pmod{20}$. We claim that

$$p\nmid\left(\binom{p-4}{k}+\binom{p-4}{n-3-k}\right)\tag{3.3}$$

for any integer k with $0\leqslant k\leqslant(n-5)/2$. Note that

$$\begin{aligned}&\binom{p-4}{k}+\binom{p-4}{n-3-k}\\&\equiv(-1)^k\binom{k+3}{3}+(-1)^{n-3-k}\binom{n-k}{3}\\&\equiv\frac{(-1)^k}{6}\left((k+1)(k+2)(k+3)-\left(k+\frac12\right)\left(k+\frac32\right)\left(k+\frac52\right)\right)\\&\equiv\frac{(-1)^k}{4}\left(\left(k+\frac74\right)^2-\frac{5}{16}\right)\pmod p.\end{aligned}$$

Since $(\frac{5}{p})=-1$, we do have (3.3). In view of this, using previous arguments we obtain

$$\left(\frac{S_{p-4}(d,p)}{p}\right)=\left(\frac{5}{p}\right)=-1.$$

So the other direction of (1.3) also holds.

In view of the above, the proof of Theorem 1.4 is now complete. □

Acknowledgments. The authors are grateful to the three referees for their helpful comments.

Statements and Declarations. There are no competing interests. This paper is original, and it has not been submitted elsewhere.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, 1998.

[2] R. Chaliha and G. Kalita, *On some conjectural determinants of Sun involving residues*, preprint, arXiv:2407.07085, 2024.

[3] L. Carlitz, *Some cyclotomic matrices*, Acta Arith. **5** (1959), 293–308.

[4] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. **115** (2004), 231–244.

[5] S. Chowla, B. Dwork and R. J. Evans, *On the mod p^2 determination of* $\binom{(p-1)/2}{(p-1)/4}$, J. Number Theory **24** (1986), 188–196.

[6] D. Grinberg, Z.-W. Sun and L. Zhao, *Proof of three conjectures on determinants related to quadratic residues*, Linear Multilinear Algebra **70** (2022), 3734–3746.

[7] C. Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. **411** (2005), 68–166.

[8] C.-K. Ren and X.-Q. Luo, *On certain determiannts and the square roots of some determinants involving Legendre symbols*, preprint, arXiv:2407.04556.

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

[10] Z.-W. Sun, *Quadratic residues and related permutations and identities*, Finite FieldsAppl. **59** (2019), Article 246283.

[11] Z.-W. Sun, *Some determinants involving quadratic residues modulo primes* arXiv:2401.14301, 2024.

[12] M. Vsemirnov, *On the evaluation of R. Chapman's "evil determinant"*, Linear Algebra Appl. **436** (2012), 4101–4106.

[13] M. Vsemirnov, *On R. Chapman's "evil determinant": case $p \equiv 1 \pmod 4$*, Acta Arith. **159** (2013), 331–344.

[14] N.-L. Wei, Y.-B. Li and H.-L. Wu, *On generalised Legendre matrices involving roots of unity over finite fields*, Bull. Aust. Math. Soc. **110** (2024), 199–210.

[15] H.-L. Wu, Y.-F. She and L.-Y. Wang, *Cyclotomic matrices and hypergeometric functions over finite fields*, Finite Fields Appl. **82** (2022), Article ID 102054.

(Chen-kai Ren) School of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: ckren@smail.nju.edu.cn

(Zhi-Wei Sun, corresponding author) School of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn