Bull. Aust. Math. Soc. **110** (2024), 199–210
doi:10.1017/S0004972724000303

ON GENERALISED LEGENDRE MATRICES INVOLVING ROOTS OF UNITY OVER FINITE FIELDS

NING-LIU WEI, YU-BO LI and HAI-LIANG WU

(Received 22 November 2023; accepted 14 March 2024; first published online 22 April 2024)

Abstract

Motivated by the work initiated by Chapman ['Determinants of Legendre symbol matrices', *Acta Arith.* **115** (2004), 231–244], we investigate some arithmetical properties of generalised Legendre matrices over finite fields. For example, letting $a_1, \ldots, a_{(q-1)/2}$ be all the nonzero squares in the finite field $\mathbb{F}_q$ containing q elements with $2 \nmid q$, we give the explicit value of the determinant $D_{(q-1)/2} = \det[(a_i + a_j)^{(q-3)/2}]_{1 \le i,j \le (q-1)/2}$. In particular, if $q = p$ is a prime greater than 3, then

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

where $(\frac{\cdot}{p})$ is the Legendre symbol and $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$.

2020 *Mathematics subject classification*: primary 11C20; secondary 05A19, 15A18, 15B57.

Keywords and phrases: Legendre symbols, finite fields, determinants.

1. Introduction

1.1. Related work and motivations. Let p be an odd prime and let $(\frac{\cdot}{p})$ be the Legendre symbol. Chapman [1, 2] investigated determinants involving Legendre matrices

$$C_1 = \left[\left(\frac{i+j-1}{p}\right)\right]_{1 \le i,j \le (p-1)/2}$$

and

$$C_2 = \left[\left(\frac{i+j-1}{p}\right)\right]_{1 \le i,j \le (p+1)/2}.$$

Surprisingly, these determinants are closely related to quadratic fields. In fact, letting $\varepsilon_p > 1$ and $h(p)$ be the fundamental unit and the class number of $\mathbb{Q}(\sqrt{p})$, and writing

This work was supported by the Natural Science Foundation of China (Grant No. 12101321).

$\varepsilon_p = a_p + b_p\sqrt{p}$ with $a_b, b_p \in \mathbb{Q}$, Chapman [1] proved that

$$\det C_1 = \begin{cases} (-1)^{(p-1)/4}2^{(p-1)/2}b_p & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\det C_2 = \begin{cases} (-1)^{(p+3)/4}2^{(p-1)/2}a_p & \text{if } p \equiv 1 \pmod 4, \\ -2^{(p-1)/2} & \text{otherwise.} \end{cases}$$

Later, Chapman [2] posed the following conjecture.

CONJECTURE 1.1 (Chapman). Let p be an odd prime and write $\varepsilon_p^{(2-(2/p))h(p)} = a'_p + b'_p\sqrt{p}$ with $a'_p, b'_p \in \mathbb{Q}$. Then

$$\det\left[\left(\frac{j-i}{p}\right)\right]_{1\le i,j\le (p+1)/2} = \begin{cases} -a'_p & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Due to the difficulty of the conjecture, Chapman called this determinant 'the evil determinant'. In 2012 and 2013, Vsemirnov [9, 10] confirmed the conjecture (the case $p \equiv 3 \pmod 4$ in [9] and the case $p \equiv 1 \pmod 4$ in [10]).

In 2019, Sun [8] studied some variants of Chapman's determinants. For example, let

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

Sun [8, Theorem 1.2] showed that $S(d,p) = 0$ whenever $(d/p) = -1$ and that $(-S(d,p)/p) = 1$ whenever $(d/p) = 1$. (See [3, 5, 11, 13] for recent progress on this topic.) Also, Sun [8, Theorem 1.4] proved that

$$\det\left[\frac{((i+j)/p)}{i+j}\right]_{1\le i,j\le (p-1)/2} \equiv \begin{cases} (2/p) \pmod p & \text{if } p \equiv 1 \pmod 4, \\ ((p-1)/2)! \pmod p & \text{otherwise,} \end{cases} \tag{1.1}$$

and that

$$\det\left[\frac{1}{i^2+j^2}\right]_{1\le i,j\le (p-1)/2} \equiv (-1)^{(p+1)/4} \pmod p$$

whenever $p \equiv 3 \pmod 4$. In 2022, the third author and Wang [14, Theorem 1.7] considered the determinant $\det[1/(\alpha_i+\alpha_j)]_{1\le i,j\le (p-1)/k}$, where $0 < \alpha_1, \dots, \alpha_{(p-1)/k} < p$ are all the kth power residues modulo p and showed that for any positive even integer k such that $k \mid p-1$, if -1 is not a kth power modulo p, then

$$\det\left[\frac{1}{\alpha_i+\alpha_j}\right]_{1\le i,j\le m} \equiv \frac{(-1)^{(m+1)/2}}{(2k)^m} \pmod p,$$

where $m = (p-1)/k$.

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

Now let $\mathbb{F}_q$ be the finite field of q elements with $\mathrm{char}(\mathbb{F}_q) = p > 2$. It is known that $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is a cyclic group of order $q-1$ and that the subgroups

$$U_k = \{x \in \mathbb{F}_q : x^k = 1\} = \{a_1, \ldots, a_k\} \quad (k \geq 1, k \mid q-1)$$

are exactly all subgroups of $\mathbb{F}_q^\times$. Let ϕ be the unique quadratic character of $\mathbb{F}_q$, that is,

$$\phi(x) = \begin{cases} 1 & \text{if } x \text{ is a nonzero square,} \\ 0 & \text{if } x = 0, \\ -1 & \text{otherwise.} \end{cases}$$

As $\mathrm{char}(\mathbb{F}_q) > 2$, the subset $\{\pm 1\} \subseteq \mathbb{Z}$ can be viewed as a subset of $\mathbb{F}_q$. From now on, we always assume $\pm 1 \in \mathbb{F}_q$. Inspired by Sun's determinant (1.1), it is natural to consider the matrix

$$\left[\frac{\phi(a_i + a_j)}{a_i + a_j}\right]_{1 \leq i,j \leq k}.$$

However, if $k \mid q-1$ is even, then the denominator $a_i + a_j = 0$ for some i, j since $-1 \in U_k$ in this case. To overcome this obstacle, note that for any $x \in \mathbb{F}_q$, we have $\phi(x) = x^{(q-1)/2}$. Hence, we first focus on the matrix

$$D_k := [(a_i + a_j)^{(q-3)/2}]_{1 \leq i,j \leq k}.$$

The main results involving D_k will be given in Section 1.2.

We now consider another type of determinant. Sun [8, Remark 1.3] posed the following conjecture.

CONJECTURE 1.2 (Sun). Let $p \equiv 2 \pmod 3$ be an odd prime. Then

$$2 \det \left[\frac{1}{i^2 - ij + j^2}\right]_{1 \leq i,j \leq p-1} \tag{1.2}$$

is a quadratic residue modulo p.

The third author, She and Ni [12] obtained the following generalised result.

THEOREM 1.3 (Wu, She and Ni). *Let $q \equiv 2 \pmod 3$ be an odd prime power. Let $\beta_1, \ldots, \beta_{q-1}$ be all the nonzero elements of $\mathbb{F}_q$. Then*

$$\det \left[\frac{1}{\beta_i^2 - \beta_i\beta_j + \beta_j^2}\right]_{1 \leq i,j \leq q-1} = (-1)^{(q+1)/2} 2^{(q-2)/3} \in \mathbb{F}_p,$$

where $p = \mathrm{char}(\mathbb{F}_q)$.

Recently, Luo and Sun [6] investigated the determinant

$$\det S_p(c,d) = \det[(i^2 + cij + dj^2)^{p-2}]_{1 \leq i,j \leq p-1}. \tag{1.3}$$

For $(c,d) = (1,1)$ or $(2,2)$, they determined the explicit values of $(\det S_p(c,d)/p)$.

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

Motivated by Sun's determinants (1.1)–(1.3) and the above discussions, we also consider the matrix

$$T_k := [(a_i^2 + a_i a_j + a_j^2)^{(q-3)/2}]_{1\le i,j\le k}.$$

We will state our results concerning T_k in Section 1.3.

1.2. The main results involving $\det D_k$.

THEOREM 1.4. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$. *Then for any integer $k \mid q-1$ with $1 < k \le q-1$,*

$$\det D_k = (-1)^{(k+1)(q-3)/2} \cdot w_k \cdot k^k \in \mathbb{F}_p,$$

where

$$w_k = \prod_{s=0}^{k-1} \sum_{r=0}^{\lfloor (q-3-2s)/2k \rfloor} \binom{(q-3)/2}{s+rk} \in \mathbb{F}_p.$$

Suppose now that $k = (q-1)/2$, that is, $U_{(q-1)/2}$ is the set of all the nonzero squares over $\mathbb{F}_q$. Then we can obtain the following simplified result which will be proved in Section 2.

COROLLARY 1.5. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$. *Then*

$$\det D_{(q-1)/2} = \begin{cases} (-1)^{(q+3)/4} u^2 & \text{if } q \equiv 1 \pmod 4, \\ (-1)^{(q+5)/4} \binom{(q-3)/2}{(q-3)/4} v^2 & \text{if } q \equiv 3 \pmod 4 \text{ and } q > 3, \end{cases}$$

where $u, v \in \mathbb{F}_p$ are defined by

$$u = \prod_{s=0}^{(q-5)/4} \binom{(q-3)/2}{s} \quad \text{and} \quad v = \prod_{s=0}^{(q-7)/4} \binom{(q-3)/2}{s}.$$

In particular, if $q = p > 3$ is an odd prime, then $D_{(p-1)/2}$ is nonsingular and

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

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

From Theorem 1.4, we see that $\det D_k \in \mathbb{F}_p$. The next result gives the explicit value of $(\det D_k/p)$ when k is odd.

THEOREM 1.6. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$. *Let $1 < k \le q-1$ be an odd integer with $k \mid q-1$. Suppose that D_k is nonsingular. Then*

$$\left(\frac{\det D_k}{p}\right) = \left(\frac{s_k}{p}\right),$$

where

$$s_k := k \sum_{r=1}^{(q-1)/2k} \binom{(q-3)/2}{((2r-1)k-1)/2} \in \mathbb{F}_p.$$

1.3. The main results involving det T_k. To state the next results, we need to introduce some basic properties of trinomial coefficients. Let n be a positive integer. For any integer r, the trinomial coefficient $\binom{n}{r}_2$ is defined by

$$\left(x + \frac{1}{x} + 1\right)^n = \sum_{r=-\infty}^{+\infty} \binom{n}{r}_2 x^r.$$

This implies that $\binom{n}{r}_2 = 0$ whenever $|r| > n$ and that $\binom{n}{r}_2 = \binom{n}{-r}_2$ for any integer r. In particular, $\binom{n}{0}_2$ is usually called the central trinomial coefficient because $\binom{n}{0}_2$ is exactly the coefficient of x^n in the polynomial $(x^2 + x + 1)^n$. For simplicity, $\binom{n}{0}_2$ is also denoted by t_n.

THEOREM 1.7. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$. *Then for any integer $k \mid q-1$ with $1 < k \leq q-1$,*

$$\det T_k = l_k \cdot k^k \in \mathbb{F}_p,$$

where

$$l_k = \prod_{s=0}^{k-1} \sum_{r=0}^{\lfloor (q-3-s)/k \rfloor} \binom{(q-3)/2}{(q-3)/2 - s - kr}_2 \in \mathbb{F}_p.$$

As a direct consequence of Theorem 1.7, we have the following result.

COROLLARY 1.8. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$. *For any integer $k \mid q-1$ with $1 < k \leq q-1$, the matrix T_k is singular over $\mathbb{F}_q$ if and only if*

$$\sum_{r=0}^{\lfloor (q-3-s)/k \rfloor} \binom{(q-3)/2}{(q-3)/2 - s - kr}_2 \equiv 0 \pmod p$$

for some s with $0 \leq s \leq k-1$. In particular, T_{q-1} is a singular matrix over $\mathbb{F}_q$.

In the case $k = (q-1)/2$, similar to Corollary 1.5, by Theorem 1.7, we deduce the following simplified result.

COROLLARY 1.9. *Let $\mathbb{F}_q$ be the finite field of q elements with* $\mathrm{char}(\mathbb{F}_q) = p > 2$.

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

$$\det T_{(q-1)/2} = \prod_{s=0}^{(q-5)/4} \left(\binom{(q-3)/2}{(q-3)/2 - s}_2 + \binom{(q-3)/2}{1+s}_2 \right)^2.$$

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

(ii) *If $q \equiv 3 \pmod 4$ and $q > 3$, then*

$$\det T_{(q-1)/2} = \binom{(q-3)/2}{0}_2 \prod_{s=0}^{(q-7)/4} \left(\binom{(q-3)/2}{(q-3)/2 - s}_2 + \binom{(q-3)/2}{1+s}_2 \right)^2.$$

In particular, if $T_{(q-1)/2}$ is nonsingular, then

$$\left(\frac{\det T_{(q-1)/2}}{p} \right) = \begin{cases} (-1)^{(q-1)/4} & \text{if } q \equiv 1 \pmod 4, \\ \left(\frac{t_{(q-3)/2}}{p} \right)(-1)^{(q+5)/4} & \text{if } q \equiv 3 \pmod 4 \text{ and } q > 3. \end{cases}$$

2. Proofs of Theorem 1.4 and Corollary 1.5

We begin with the following result (see [4, Lemma 10]).

LEMMA 2.1. *Let R be a commutative ring. Let $P(t) = p_0 + p_1 t + \cdots + p_{n-1} t^{n-1} \in R[t]$. Then*

$$\det[P(X_i Y_j)]_{1 \le i,j \le n} = \prod_{i=0}^{n-1} p_i \cdot \prod_{1 \le i < j \le n} (X_j - X_i)(Y_j - Y_i).$$

We also need the following result.

LEMMA 2.2. *Let $\mathbb{F}_q$ be the finite field of q elements with $\mathrm{char}(\mathbb{F}_q) = p$. For any positive integer $k \mid q-1$, if we set $U_k = \{a_1, \ldots, a_k\}$, then*

$$\prod_{1 \le i < j \le k} (a_j - a_i)\left(\frac{1}{a_j} - \frac{1}{a_i} \right) = k^k \in \mathbb{F}_p.$$

PROOF. It is clear that

$$\prod_{1 \le i < j \le k} (a_j - a_i)\left(\frac{1}{a_j} - \frac{1}{a_i} \right) = \prod_{1 \le i < j \le k} \frac{(a_j - a_i)(a_i - a_j)}{a_i a_j} = \prod_{1 \le i \ne j \le k} (a_j - a_i) \prod_{1 \le i < j \le k} \frac{1}{a_i a_j}. \quad (2.1)$$

Let $S_1 = \prod_{1 \le i \ne j \le k} (a_j - a_i)$ and let $S_2 = \prod_{1 \le i < j \le k} 1/(a_i a_j)$. We first consider S_1. Let

$$G_k(t) = \prod_{i=1}^{k} (t - a_i) \in \mathbb{F}_q[t]$$

and let $G_k'(t)$ be the formal derivative of $G_k(t)$. Then by the definition of U_k, we see that $G_k(t) = t^k - 1$. Thus, $G_k'(t) = kt^{k-1}$ and $\prod_{1 \le j \le k} a_j = (-1)^{k+1}$. Now we can verify that

$$S_1 = \prod_{1 \le i \ne j \le k} (a_j - a_i) = \prod_{1 \le j \le k} G_k'(a_j) = \prod_{1 \le j \le k} k a_j^{k-1} = k^k (-1)^{k+1}. \quad (2.2)$$

We turn to S_2. It is clear that

$$S_2 = \prod_{1 \le i < j \le k} \frac{1}{a_i a_j} = \prod_{1 \le j \le k} \frac{1}{a_j^{k-1}} = (-1)^{k+1}. \quad (2.3)$$

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

Combining (2.1) with (2.2) and (2.3),

$$\prod_{1\le i<j\le k}(a_j-a_i)\Big(\frac{1}{a_j}-\frac{1}{a_i}\Big)=S_1S_2=k^k\in\mathbb{F}_p.$$

This completes the proof. □

PROOF OF THEOREM 1.4. As $\mathrm{char}(\mathbb{F}_q)=p>2$, the subset $\{1,-1\}\subseteq\mathbb{Z}$ can be naturally viewed as a subset of $\mathbb{F}_q$. One can verify that

$$\det D_k=\det[(a_i+a_j)^{(q-3)/2}]_{1\le i,j\le k}=\prod_{i=1}^{k}a_i^{(q-3)/2}\det\Big[\Big(1+\frac{a_j}{a_i}\Big)^{(q-3)/2}\Big]_{1\le i,j\le k}$$
$$=(-1)^{(k+1)(q-3)/2}\det\Big[\Big(1+\frac{a_j}{a_i}\Big)^{(q-3)/2}\Big]_{1\le i,j\le k}. \tag{2.4}$$

The last equality follows from $\prod_{1\le j\le k}a_j=(-1)^{k+1}$. Let

$$f_k(t)=\sum_{s=0}^{k-1}\Bigg(\sum_{r=0}^{\lfloor (q-3-2s)/2k\rfloor}\binom{(q-3)/2}{s+rk}\Bigg)t^s\in\mathbb{F}_p[t]$$

with $\deg(f_k)\le k-1$. Noting that $(a_j/a_i)^{k+s}=(a_j/a_i)^s$ for any integer s, by (2.4),

$$\det D_k=(-1)^{(k+1)(q-3)/2}\cdot\det\Big[f_k\Big(\frac{a_j}{a_i}\Big)\Big]_{1\le i,j\le k}.$$

Let

$$w_k:=\prod_{s=0}^{k-1}\sum_{r=0}^{\lfloor (q-3-2s)/2k\rfloor}\binom{(q-3)/2}{s+rk}\in\mathbb{F}_p.$$

Then by Lemmas 2.1 and 2.2,

$$\det D_k=(-1)^{(k+1)(q-3)/2}\cdot w_k\cdot\prod_{1\le i<j\le k}(a_j-a_i)\Big(\frac{1}{a_j}-\frac{1}{a_i}\Big)=(-1)^{(k+1)(q-3)/2}\cdot w_k\cdot k^k\in\mathbb{F}_p.$$

This completes the proof. □

PROOF OF COROLLARY 1.5. By Theorem 1.4, if $k=(q-1)/2$, then

$$\det D_{(q-1)/2}=(-1)^{(q-3)/2}\cdot\prod_{s=0}^{(q-3)/2}\binom{(q-3)/2}{s}\cdot(-1)^{(q-1)/2}\Big(\frac{1}{2}\Big)^{(q-1)/2}$$
$$=-1\cdot\prod_{s=0}^{(q-3)/2}\binom{(q-3)/2}{s}\cdot\phi(2). \tag{2.5}$$

The last equality follows from

$$(\tfrac{1}{2})^{(q-1)/2}=\phi(\tfrac{1}{2})=\phi(2).$$

We now divide the remaining part of the proof into two cases.

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

Case 1: $q \equiv 1 \pmod 4$.

In this case, we have $\sqrt{-1} \in \mathbb{F}_q$, where $\sqrt{-1}$ is an element in the algebraic closure of $\mathbb{F}_q$ such that $(\sqrt{-1})^2 = -1$. Since $2 = -\sqrt{-1}(1+\sqrt{-1})^2$, we have $\phi(2) = \phi(-\sqrt{-1})$ and hence

$$\phi(2) = \phi(-\sqrt{-1}) = (-\sqrt{-1})^{(q-1)/2} = (-1)^{(q-1)/4}. \tag{2.6}$$

Combining (2.5) with (2.6) and noting that

$$\binom{(q-3)/2}{s} = \binom{(q-3)/2}{(q-3)/2-s},$$

we obtain

$$\det D_{(q-1)/2} = (-1)^{(q+3)/4} \prod_{s=0}^{(q-5)/4} \binom{(q-3)/2}{s}^2. \tag{2.7}$$

This proves the case $q \equiv 1 \pmod 4$.

Case 2: $q \equiv 3 \pmod 4$ and $q > 3$.

In this case, since $q \equiv 3 \pmod 4$, $(1+\sqrt{-1})^q = 1 + (\sqrt{-1})^q = 1 - \sqrt{-1}$. This, together with $2 = -\sqrt{-1}(1+\sqrt{-1})^2$, implies that

$$\begin{aligned}\phi(2) = 2^{(q-1)/2} &= (-\sqrt{-1})^{(q-3)/2}(-\sqrt{-1})(1+\sqrt{-1})^{q-1} \\ &= (-1)^{(q-3)/4}(-\sqrt{-1})\frac{1-\sqrt{-1}}{1+\sqrt{-1}} \\ &= (-1)^{(q+1)/4}.\end{aligned} \tag{2.8}$$

Combining (2.5) with (2.8),

$$\det D_{(q-1)/2} = (-1)^{(q+5)/4} \binom{(q-3)/2}{(q-3)/4} \prod_{s=0}^{(q-7)/4} \binom{(q-3)/2}{s}^2. \tag{2.9}$$

This proves the case $q \equiv 3 \pmod 4$ and $q > 3$.

Now we assume that $q = p$ is an odd prime. Suppose first $p \equiv 1 \pmod 4$. Then by (2.7), we see that $\det D_{(q-1)/2}$ is a nonzero square in $\mathbb{F}_p$, that is, $(\det D_{(p-1)/2}/p) = 1$. In the case $p \equiv 3 \pmod 4$ and $p > 3$, by (2.9) and $(-2/p) = (-\frac{1}{2}/p) = (-1)^{(p+5)/4}$,

$$\left(\frac{\det D_{(q-1)/2}}{p}\right) = (-1)^{(p+5)/4}\left(\frac{\frac{p-3}{2}!}{p}\right) = (-1)^{(p+5)/4}\left(\frac{\frac{p-1}{2}!}{p}\right)\left(\frac{\frac{-1}{2}}{p}\right) = \left(\frac{\frac{p-1}{2}!}{p}\right) = (-1)^{(h(-p)+1)/2}.$$

The last equality follows from Mordell's result [7] which states that

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

whenever $p \equiv 3 \pmod 4$ and $p > 3$. This completes the proof. □

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

3. Proof of Theorem 1.6

To prove Theorem 1.6, we first need the following well-known result.

LEMMA 3.1. *Let $\mathbb{F}_q$ be the finite field of q elements and let r be a positive integer. Then*

$$\sum_{x\in\mathbb{F}_q} x^r = \begin{cases} 0 & \text{if } q-1 \nmid r, \\ -1 & \text{if } q-1 \mid r. \end{cases}$$

We will see later in the proof that $\det D_k$ has close relations with the determinant of a circulant matrix. Hence, we now introduce the definition of circulant matrices. Let R be a commutative ring. Let $b_0, b_1, \ldots, b_{s-1} \in R$. We define the circulant matrix $C(b_0, \ldots, b_{s-1})$ to be an $s \times s$ matrix whose (i, j)-entry is b_{j-i} where the indices are cyclic module s, that is, $b_i = b_j$ whenever $i \equiv j \pmod{s}$. The third author [11, Lemma 3.4] obtained the following result.

LEMMA 3.2. *Let R be a commutative ring. Let s be a positive integer. Let $b_0, b_1, \ldots, b_{s-1} \in R$ such that $b_i = b_{s-i}$ for $1 \leqslant i \leqslant s-1$.*
If s is even, then there exists an element $u \in R$ such that

$$\det C(b_0, \ldots, b_{s-1}) = \Big(\sum_{i=0}^{s-1} b_i\Big)\Big(\sum_{i=0}^{s-1}(-1)^i b_i\Big) \cdot u^2.$$

If s is odd, then there exists an element $v \in R$ such that

$$\det C(b_0, \ldots, b_{s-1}) = \Big(\sum_{i=0}^{s-1} b_i\Big) \cdot v^2.$$

PROOF OF THEOREM 1.6. As k is odd, we have $2 \mid (q-1)/k$. For simplicity, we let $q-1 = nk = 2mk$. Since $k \mid (q-1)/2$ in this case, $\phi(a_i) = a_i^{(q-1)/2} = 1$ for each $a_i \in U_k$. Let g be a generator of the cyclic group $\mathbb{F}_q^\times$. By the above, one can verify that

$$\det D_k = \prod_{i=1}^{k} a_i^{(q-3)/2} \det\Big[\Big(1 + \frac{a_j}{a_i}\Big)^{(q-3)/2}\Big]_{1\le i,j\le k} = \det[(1 + g^{nj-ni})^{(q-3)/2}]_{0\le i,j\le k-1}.$$

The last equality follows from

$$\prod_{i=1}^{k} a_i = (-1)^{k+1} = 1.$$

By the above and using the properties of determinants, one can verify that

$$\det D_k = \det[(1 + g^{nj-ni})^{(q-3)/2} g^{mj-mi}(-1)^{j-i}]_{0\le i,j\le k-1}. \tag{3.1}$$

For $0 \le i \le k-1$,

$$b_i = (1 + g^{ni})^{(q-3)/2} g^{mi}(-1)^i.$$

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

We claim that $b_i = b_{k-i}$ for $1 \le i \le k-1$. In fact, for $1 \le i \le k-1$, noting that

$$g^{km} = \phi(g) = -1, \quad g^{nk} = 1,\ 2 \nmid k \quad \text{and} \quad \Big(\frac{1}{g^{ni}}\Big)^{(q-3)/2} = g^{ni},$$

one can verify that

$$\begin{aligned} b_{k-i} &= (1+g^{nk-ni})^{(q-3)/2} g^{mk-mi}(-1)^{k-i} \\ &= \Big(\frac{1+g^{ni}}{g^{ni}}\Big)^{(q-3)/2} g^{-mi}(-1)^i \\ &= (1+g^{ni})^{(q-3)/2} g^{(n-m)i}(-1)^i \\ &= b_i. \end{aligned}$$

Hence, by (3.1), $\det D_k = \det C(b_0, b_1, \ldots, b_{k-1})$. Now by Lemma 3.2 and (3.1),

$$\det D_k = \Big(\sum_{i=0}^{k-1} b_i\Big) v^2 \tag{3.2}$$

for some $v \in \mathbb{F}_q$. Now we consider the sum $\sum_{i=0}^{k-1} b_i$. It is easy to verify that

$$\begin{aligned} \sum_{i=0}^{k-1} b_i &= \sum_{i=0}^{k-1} (1+g^{ni})^{(q-3)/2} g^{mi}(-1)^i = \sum_{i=0}^{k-1} (1+g^{ni})^{(q-3)/2} g^{mi} g^{mki} \\ &= \frac{1}{n} \sum_{x \in \mathbb{F}_q} (1+x^n)^{(q-3)/2} x^{m+mk} = \frac{1}{n} \sum_{r=0}^{mk-1} \binom{(q-3)/2}{r} \sum_{x \in \mathbb{F}_q} x^{m+mk+2mr}. \end{aligned} \tag{3.3}$$

Now by Lemma 3.1, since $2 \nmid k$,

$$\sum_{x \in \mathbb{F}_q} x^{m+mk+2mr} = \begin{cases} 0 & \text{if } k \nmid 1+2r, \\ -1 & \text{if } k \mid 1+2r. \end{cases}$$

Applying this and Lemma 3.1 to (3.3) and noting that $-1/n = k$ in $\mathbb{F}_p$,

$$s_k := \sum_{i=0}^{k-1} b_i = k \sum_{r=1}^{m} \binom{(q-3)/2}{((2r-1)k-1)/2}. \tag{3.4}$$

Suppose that D_k is nonsingular. Then by Theorem 1.4, we have $\det D_k \in \mathbb{F}_p^{\times}$. Hence, by (3.2) and (3.4),

$$\Big(\frac{\det D_k}{p}\Big) = \Big(\frac{s_k}{p}\Big).$$

This completes the proof. □

https://doi.org/10.1017/S0004972724000303 Published online by Cambridge University Press

4. Proof of Theorem 1.7

It is clear that

$$\det T_k = \prod_{i=1}^{k} (a_i^2)^{(q-3)/2} \cdot \det\left[\left(1 + \frac{a_j}{a_i} + \left(\frac{a_j}{a_i}\right)^2\right)^{(q-3)/2}\right]_{1\le i,j\le k}$$
$$= \det\left[\left(1 + \frac{a_j}{a_i} + \left(\frac{a_j}{a_i}\right)^2\right)^{(q-3)/2}\right]_{1\le i,j\le k}. \tag{4.1}$$

The last equality follows from

$$\prod_{i=1}^{k} a_i = (-1)^{k+1}.$$

Let

$$g_k(t) = \sum_{s=0}^{k-1} \left(\sum_{r=0}^{\lfloor (q-3-s)/k \rfloor} \binom{(q-3)/2}{s + rk - (q-3)/2}_2 \right) t^s \in \mathbb{F}_p[t]$$

with $\deg(g_k) \le k-1$. Then by (4.1), Lemma 2.1 and the definition of trinomial coefficients,

$$\det T_k = \det\left[g_k\left(\frac{a_j}{a_i}\right)\right]_{1\le i,j\le k}$$
$$= \prod_{1\le i<j\le k} (a_j - a_i)\left(\frac{1}{a_j} - \frac{1}{a_i}\right) \cdot \prod_{s=0}^{k-1} \sum_{r=0}^{\lfloor (q-3-s)/k \rfloor} \binom{(q-3)/2}{s + rk - (q-3)/2}_2$$
$$= l_k k^k \in \mathbb{F}_p.$$

The last equality follows from Lemma 2.2. This completes the proof. □

Acknowledgement

We would like to thank the referee for helpful comments.

References

[1] R. Chapman, 'Determinants of Legendre symbol matrices', *Acta Arith.* **115** (2004), 231–244.
[2] R. Chapman, 'My evil determinant problem', Online lecture notes, December 12, 2012. Available at http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf.
[3] D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, 'On some determinants involving Jacobi symbols', *Finite Fields Appl.* **64** (2020), Article no. 101672.
[4] C. Krattenthaler, 'Advanced determinant calculus: a complement', *Linear Algebra Appl.* **411** (2005), 68–166.
[5] Y.-B. Li and N.-L. Wei, 'A variant of some cyclotomic matrices involving trinomial coefficients', *Colloq. Math.* **174** (2023), 37–43.
[6] X.-Q. Luo and Z.-W. Sun, 'Legendre symbols related to certain determinants', *Bull. Malays. Math. Sci. Soc.* **46** (2023), Article no. 119.

[7] L. J. Mordell, 'The congruence $((p-1)/2)! \equiv \pm 1 \pmod{p}$', *Amer. Math. Monthly* **68** (1961), 145–146.
[8] Z.-W. Sun, 'On some determinants with Legendre symbols entries', *Finite Fields Appl.* **56** (2019), 285–307.
[9] M. Vsemirnov, 'On the evaluation of R. Chapman's "evil determinant"', *Linear Algebra Appl.* **436** (2012), 4101–4106.
[10] M. Vsemirnov, 'On R. Chapman's "evil determinant": case $p \equiv 1 \pmod{4}$', *Acta Arith.* **159** (2013), 331–344.
[11] H.-L. Wu, 'Elliptic curves over F_p and determinants of Legendre matrices', *Finite Fields Appl.* **76** (2021), Article no. 101929.
[12] H.-L. Wu, Y.-F. She and H.-X. Ni, 'A conjecture of Zhi-Wei Sun on determinants over finite fields', *Bull. Malays. Math. Sci. Soc.* **45** (2022), 2405–2412.
[13] H.-L. Wu, Y.-F. She and L.-Y. Wang, 'Cyclotomic matrices and hypergeometric functions over finite fields', *Finite Fields Appl.* **82** (2022), Article no. 102054.
[14] H.-L. Wu and L.-Y. Wang, 'Applications of circulant matrices to determinants involving kth power residues', *Bull. Aust. Math. Soc.* **106** (2022), 243–253.

NING-LIU WEI, School of Science,
Nanjing University of Posts and Telecommunications, Nanjing 210023,
Jiangsu Province, PR China
e-mail: weiningliu6@163.com

YU-BO LI, School of Science,
Nanjing University of Posts and Telecommunications, Nanjing 210023,
Jiangsu Province, PR China
e-mail: lybmath2022@163.com

HAI-LIANG WU, School of Science,
Nanjing University of Posts and Telecommunications, Nanjing 210023,
Jiangsu Province, PR China
e-mail: whl.math@smail.nju.edu.cn