Bull. Aust. Math. Soc. **106** (2022), 243–253
doi:10.1017/S0004972722000053

APPLICATIONS OF CIRCULANT MATRICES TO DETERMINANTS INVOLVING *k*TH POWER RESIDUES

HAI-LIANG WU and LI-YUAN WANG✉

(Received 3 November 2021; accepted 13 December 2021; first published online 9 Febuary 2022)

Abstract

We use circulant matrices and hyperelliptic curves over finite fields to study some arithmetic properties of certain determinants involving Legendre symbols and kth power residues.

2020 *Mathematics subject classification*: primary 11C20; secondary 11L05, 11R29.

Keywords and phrases: determinant, Legendre symbol, circulant matrix.

1. Introduction

Let n be an arbitrary positive integer and let R be a commutative ring. For every $n\times n$ matrix $M=[a_{ij}]_{1\le i,j\le n}$ with $a_{ij}\in R$, we use the symbol $\det M$ or $|M|$ to denote the determinant of M. Given any elements $b_0,b_1,\ldots,b_{n-1}\in R$, the *circulant matrix* of the n-tuple $(b_0,\ldots,b_{n-1})$ is the $n\times n$ matrix over R whose (i,j)-entry is b_{i-j}, where the indices are cyclic modulo n. We also denote this matrix by $C(b_0,b_1,\ldots,b_{n-1})$. Circulant matrices have many applications in both number theory and combinatorics. We refer to the survey paper [5] for results on circulant matrices.

1.1. Circulant matrices involving Legendre symbols. Let p be an odd prime and let $\chi(\cdot)$ be a multiplicative character modulo p. Carlitz [2] investigated the circulant matrix

$$C(c_0,c_1,\ldots,c_{p-1}):=[\mu+\chi(i-j)]_{1\le i,j\le p-1}\quad(\mu\in\mathbb{C}),$$

where $c_i=\mu+\chi(i)$ for $0\le i\le p-1$. Carlitz [2, Theorem 4] determined the characteristic polynomial of this circulant matrix. In particular, when $\chi(\cdot)=(\frac{\cdot}{p})$ is the Legendre

The first author was supported by the National Natural Science Foundation of China (Grant No. 12101321) and the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 21KJB110002). The second author was supported by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 21KJB110001).

symbol, the characteristic polynomial of the matrix $[\mu + ((i-j)/p)]_{1\le i,j\le p-1}$ is

$$F_\mu(t) = (t^2 - (-1)^{(p-1)/2}p)^{(p-3)/2}(t^2 - (p-1)\mu - (-1)^{(p-1)/2}).$$

Later, Chapman [3, 4] and Vsemirnov [10, 11] studied variants of Carlitz's results.

Let $p = 2n+1$ be an odd prime. Recently, Sun [9] studied the determinant

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

where $(\frac{\cdot}{p})$ is the Legendre symbol and $d \in \mathbb{Z}$ with $p \nmid d$. Sun [9, Theorems 1.2(iii) and 1.3(i)] proved that $-S(d,p)$ is a quadratic residue modulo p whenever $(\frac{d}{p}) = 1$. (See [6, 13] for recent progress on this topic.) Sun also investigated some global properties of this determinant and conjectured that $-S(1,p)$ is an integral square if $p \equiv 3 \pmod 4$. Later, by using a sophisticated matrix decomposition, Alekseyev and Krachun proved this conjecture. In the case $p \equiv 1 \pmod 4$, writing $p = a^2 + 4b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 4$, Cohen, Sun and Vsemirnov conjectured that $S(1,p)/a$ is an integral square (see [9, Remark 4.2]). This conjecture was later proved by the first author [12, Theorem 3].

Note that $S(d,p)$ is indeed a determinant of a certain circulant matrix. In fact, fix a primitive root g modulo p. Then it is clear that $S(d,p)$ is equal to

$$\det\left[\left(\frac{g^{2i}+dg^{2j}}{p}\right)\right]_{0\le i,j\le n-1} = \det\left[\left(\frac{g^{2(i-j)}+d}{p}\right)\right]_{0\le i,j\le n-1} = \det C(s_0, s_1, \dots, s_{n-1}),$$

where $s_i = ((g^{2i}+d)/p)$ for $0 \le i \le n-1$.

Motivated by Sun's determinant $S(d,p)$, we study some determinants containing kth power residues. Let p be an odd prime and let $k \ge 2$ be an integer dividing $p-1$. Write $p = km+1$ and let

$$0 < \alpha_1 < \alpha_2 < \cdots < \alpha_m < p$$

be all the kth power residues modulo p in the interval $(0,p)$. We consider the matrix

$$W_p(k) := \left[\left(\frac{\alpha_i+\alpha_j}{p}\right)\right]_{1\le i,j\le m}.$$

To state our results, we first introduce some notation. Let $\mathbb{F}_p$ denote the finite field of p elements. Let $C_{p,k,\psi}$ and $C_{p,k,\phi}$ be the curves over $\mathbb{F}_p$ defined by the equations $y^2 = x^k + 1$ and $y^2 = x(x^k+1)$, respectively. Define $a_p(k)$ and $b_p(k)$ by

$$p + 1 - a_p(k) = \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : \ y^2 = x^k + 1\} \cup \{\infty\}, \tag{1.1}$$

and

$$p + 1 - b_p(k) = \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : \ y^2 = x(x^k + 1)\} \cup \{\infty\}, \tag{1.2}$$

where ∞ denotes the point at infinity and $\#S$ denotes the cardinality of a set S.

When k is even, the following result generalises Sun's determinant $S(1,p)$.

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

THEOREM 1.1. *Let p be an odd prime and let $k \geq 2$ be an even integer dividing $p-1$. Let $m = (p-1)/k$.*

(i) *If m is odd, then* $\det W_p(k) = -(a_p(k)+1)u_p(k)^2/k$ *for some* $u_p(k) \in \mathbb{Z}$.
(ii) *If m is even, then* $\det W_p(k) = (a_p(k)+1)b_p(k)v_p(k)^2/k^2$ *for some* $v_p(k) \in \mathbb{Z}$.

REMARK 1.2. (1) When $k = 2$ and $p \equiv 3 \pmod 4$, it is easy to see that $a_p(2) = 1$. This implies that $-\det W_p(2) = -S(1,p)$ is an integral square, which also confirms the conjecture of Sun.

(2) When $k = 2$ and $p \equiv 1 \pmod 4$ with $p = a^2 + 4b^2$, where $a \equiv 1 \pmod 4$, it is known that $a_p(2) = 1$ and $b_p(2) = 2a$ [1, Theorem 6.2.9]. Thus, $\det W_p(2)/a = S(1,p)/a$ is an integral square, which coincides with the result in [12, Theorem 3].

Now we consider the case when k is odd. Fix a primitive root g modulo p. Let $E_{p,k,1}$ and $E_{p,k,g}$ be the hyperelliptic curves over $\mathbb{F}_p$ defined by the equations $y^2 = x(x^{2k}+1)$ and $y^2 = x(x^{2k}+g^k)$, respectively. Define $c_p(k)$ and $d_p(k)$ by

$$p + 1 - c_p(k) := \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : \ y^2 = x(x^{2k}+1)\} \cup \{\infty\}, \tag{1.3}$$

and

$$p + 1 - d_p(k) := \#\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : \ y^2 = x(x^{2k}+g^k)\} \cup \{\infty\}. \tag{1.4}$$

THEOREM 1.3.

(i) *Let $p \equiv 1 \pmod 4$ be a prime and let $k \geq 3$ be an odd integer dividing $p-1$. Then,*

$$\det W_p(k) = \frac{z_p(k)^2}{4k^2}(c_p(k)^2 + d_p(k)^2)$$

for some $z_p(k) \in \mathbb{Z}$.
(ii) *Let $p \equiv 3 \pmod 4$ be a prime and let $k \geq 2$ be an odd integer dividing $p-1$. Then, $-\det W_p(k)$ is an integral square.*

When $k = 3$, we deduce the following consequence.

COROLLARY 1.4. *Suppose that $p \equiv 1 \pmod{12}$ is a prime and write $p = c^2 + 9d^2$ with $c, d \in \mathbb{Z}$. Then*

(i) $\det W_p(3)/(c^2+d^2)$ *is an integral square.*
(ii) *Moreover, if $p \nmid \det W_p(3)$, then*

$$\left(\frac{\det W_p(3)}{p}\right) = \left(\frac{2}{p}\right).$$

REMARK 1.5. There are primes $p \equiv 1 \pmod{12}$ such that $p \mid \det W_p(3)$. In fact, 1117, 1129, 1381, 1597, 1861, 2557, 2749 are all the primes $p \equiv 1 \pmod{12}$ less than 3000 such that $p \mid W_p(3)$.

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

COROLLARY 1.6.

(i) *Let* $p \equiv 1 \pmod 4$ *be a prime and let* $k \geq 2$ *be an odd integer dividing* $p-1$. *Then,* $\det W_p(k) \geq 0$.
(ii) *Let* $p \equiv 3 \pmod 4$ *be a prime and let* $k \geq 2$ *be an odd integer dividing* $p-1$. *Then,* $\det W_p(k) \leq 0$.

1.2. Determinants of the form $\det[1/(\alpha_i+\alpha_j)]_{1\leq i,j\leq m}$. Let p be an odd prime. For any integer t with $p \nmid t$, the element $1/t \bmod p$ denotes the multiplicative inverse of $t \bmod p$. In 2019, Sun [9] also studied the determinant

$$A_p := \det\left[\frac{1}{i^2+j^2}\right]_{1\leq i,j\leq (p-1)/2}.$$

When $p \equiv 3 \pmod 4$, Sun [9, Theorem 1.4(ii)] showed that

$$A_p \equiv \left(\frac{2}{p}\right) \pmod p.$$

In [9, Remark 1.3], Sun also conjectured that if $p \equiv 2 \pmod 3$ is odd, then $2B_p$ is a quadratic residue modulo p, where

$$B_p := \det\left[\frac{1}{i^2-ij+j^2}\right]_{1\leq i,j\leq p-1}.$$

This conjecture was later confirmed in [14]. With the notation established in the previous subsection, we consider the matrix

$$I_p(k) := \left[\frac{1}{\alpha_i+\alpha_j}\right]_{1\leq i,j\leq m}.$$

As a generalisation of Sun's determinant $\det A_p$, we obtain the following result.

THEOREM 1.7. *Let* p *be an odd prime and let* $k \geq 2$ *be an even integer dividing* $p-1$. *Write* $p = km+1$. *Suppose that* -1 *is not a* k*th power residue modulo* p. *Then*

$$\det I_p(k) \equiv \frac{(-1)^{m+1/2}}{(2k)^m} \pmod p.$$

REMARK 1.8. When $p \equiv 3 \pmod 4$ and $k = 2$, the theorem gives

$$\det I_p(2) \equiv (-1)^{p+1/4} = \left(\frac{2}{p}\right) \pmod p.$$

This coincides with Sun's result [9, Theorem 1.4(ii)].

The outline of the paper is as follows. We will prove Theorems 1.1–1.3 and their corollaries in Section 2. The proof of Theorem 1.7 will be given in Section 3.

2. Proofs of Theorems 1.1–1.3

Recall that $C(a_0, \ldots, a_{n-1})$ denotes the circulant matrix of the n-tuple $(a_0, \ldots, a_{n-1})$. The following lemma is Lemma 3.4 of [13] and is the key element of our proofs.

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

LEMMA 2.1. *Let R be a commutative ring, n a positive integer and $a_0, a_1, \dots, a_{n-1} \in R$ such that*

$$a_i = a_{n-i} \quad \text{for } 1 \le i \le n-1. \tag{2.1}$$

If n is even, then there exists an element $u \in R$ such that

$$\det C(a_0, a_1, \dots, a_{n-1}) = \Big(\sum_{i=0}^{n-1} a_i\Big)\Big(\sum_{i=0}^{n-1} (-1)^i a_i\Big)u^2.$$

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

$$\det C(a_0, a_1, \dots, a_{n-1}) = \Big(\sum_{i=0}^{n-1} a_i\Big)v^2.$$

PROOF OF THEOREM 1.1. Fix a primitive root g modulo p. As k is even,

$$\begin{aligned}\det W_p(k) &= \det\left[\left(\frac{1+\alpha_i/\alpha_j}{p}\right)\right]_{1\le i,j\le m} = \det\left[\left(\frac{1+g^{k(i-j)}}{p}\right)\right]_{0\le i,j\le m-1}\\ &= \det C(e_0, e_1, \dots, e_{m-1}), \quad \text{where } e_i = \left(\frac{1+g^{ki}}{p}\right) \text{ for } 0 \le i \le m-1.\end{aligned}$$

Clearly $e_0, \dots, e_{m-1}$ satisfy the condition (2.1). Moreover,

$$\sum_{i=0}^{m-1} e_i = \frac{1}{k}\sum_{x=1}^{p-1}\left(\frac{1+x^k}{p}\right) = \frac{1}{k}\left(-1 + \sum_{x=0}^{p-1}\left(\frac{1+x^k}{p}\right)\right) = -\frac{1+a_p(k)}{k}, \tag{2.2}$$

where $a_p(k)$ is defined by (1.1). Also,

$$\sum_{i=0}^{m-2}(-1)^i e_i = \frac{1}{k}\sum_{x=1}^{p-1}\left(\frac{x^k+1}{p}\right)\left(\frac{x}{p}\right) = -\frac{b_p(k)}{k}, \tag{2.3}$$

where $b_p(k)$ is defined by (1.2). Combining Lemma 2.1 with (2.2) and (2.3) yields the desired result. □

Now we turn to the proof of Theorem 1.3. We first need the following well-known result in linear algebra.

LEMMA 2.2. *Let M be an $n \times n$ complex matrix. Let $\lambda_1, \dots, \lambda_n$ be complex numbers and let $\mathbf{u}_1, \dots, \mathbf{u}_n$ be m-dimensional column vectors. Suppose that $M\mathbf{u}_i = \lambda_i \mathbf{u}_i$ for $1 \le i \le n$ and that $\mathbf{u}_1, \dots, \mathbf{u}_n$ are linearly independent. Then $\lambda_1, \dots, \lambda_n$ are exactly all the eigenvalues of M (counting multiplicities).*

Let $\widehat{\mathbb{F}_p^\times}$ denote the cyclic group of all multiplicative characters of $\mathbb{F}_p$ and let $\chi_p(\cdot)$ be a generator of $\widehat{\mathbb{F}_p^\times}$. For any matrix M, we use the symbol M^T to denote the transpose of M.

PROOF OF THEOREM 1.3. Recall that $k \ge 2$ is an odd integer dividing $p-1$ and $p = km+1$.

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

(i) We first consider the case $p \equiv 1 \pmod 4$. Clearly, the elements $\alpha_1 \bmod p, \ldots, \alpha_m \bmod p$ are exactly m distinct roots of the polynomial $X^m - 1$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Therefore,

$$X^m - 1 \equiv \prod_{i=1}^{m} (X - \alpha_i) \pmod p. \tag{2.4}$$

By (2.4),

$$\prod_{j=1}^{m} \alpha_j \equiv -1^{m+1} = -1 \pmod p. \tag{2.5}$$

By (2.5), it is easy to see that $\det W_p(k)$ is equal to

$$\left(\frac{-1}{p}\right) \det\left[\left(\frac{\alpha_i + \alpha_j}{p}\right)\right]_{1\le i,j\le m} = \det\left[\left(\frac{\alpha_i + \alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right)\right]_{1\le i,j\le m}.$$

Next, we determine all the eigenvalues of the matrix

$$W_p^*(k) := \left[\left(\frac{\alpha_i + \alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right)\right]_{1\le i,j\le m}.$$

For each r with $1 \le r \le m$,

$$\begin{aligned}\sum_{j=1}^{m} \left(\frac{\alpha_i + \alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right) \chi_p^r(\alpha_j) &= \sum_{j=1}^{m} \left(\frac{1 + \alpha_j/\alpha_i}{p}\right)\left(\frac{\alpha_j/\alpha_i}{p}\right) \chi_p(\alpha_j/\alpha_i)\, \chi_p^r(\alpha_i) \\ &= \sum_{j=1}^{m} \left(\frac{1 + \alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right) \chi_p^r(\alpha_j)\, \chi_p^r(\alpha_i).\end{aligned}$$

This implies that for $1 \le r \le m$,

$$W_p^*(k)\mathbf{v}_r = \lambda_r \mathbf{v}_r,$$

where

$$\lambda_r = \sum_{j=1}^{m} \left(\frac{1 + \alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right)\chi_p^r(\alpha_j) \quad \text{and} \quad \mathbf{v}_r = (\chi_p^r(\alpha_1), \ldots, \chi_p^r(\alpha_m))^T.$$

Note that

$$\begin{vmatrix} \chi_p^1(\alpha_1) & \chi_p^2(\alpha_1) & \ldots & \chi_p^m(\alpha_1) \\ \chi_p^1(\alpha_2) & \chi_p^2(\alpha_2) & \ldots & \chi_p^n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_p^1(\alpha_n) & \chi_p^2(\alpha_n) & \ldots & \chi_p^m(\alpha_m) \end{vmatrix} = \pm \prod_{1\le i<j\le m} (\chi_p(\alpha_j) - \chi_p(\alpha_i)) \ne 0.$$

Hence, the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_m$ are linearly independent. Now by Lemma 2.2, the numbers $\lambda_1, \ldots, \lambda_m$ are exactly all the eigenvalues of $W_p^*(k)$ (counting multiplicities).

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

When $r = m$,

$$\lambda_m = \sum_{j=1}^{m} \left(\frac{1+\alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right) = \frac{1}{k}\sum_{x=1}^{p-1}\left(\frac{1+x^k}{p}\right)\left(\frac{x}{p}\right).$$

When $r = m/2$,

$$\lambda_{m/2} = \sum_{j=1}^{m} \left(\frac{1+\alpha_j}{p}\right) = \frac{1}{k}\sum_{x=1}^{p-1}\left(\frac{1+x^k}{p}\right).$$

By [1, Proposition 6.1.7],

$$\lambda_m = \lambda_{m/2}. \tag{2.6}$$

In addition, when $1 \le r \le m/2-1$, it is clear that $\overline{\lambda_r} = \lambda_{m-r}$, where $\bar{z}$ denotes the complex conjugate of a complex number z. Combining this with (2.6),

$$\det W_p(k) = \det W_p^*(k) = \prod_{r=1}^{m} \lambda_r = \lambda_m^2 \prod_{1\le r\le m/2-1} \lambda_r\overline{\lambda_r} \ge 0. \tag{2.7}$$

Let $\mathbf{i} \in \mathbb{C}$ be a primitive fourth root of unity. Fix a primitive root g modulo p. Then

$$\begin{aligned}
\det W_p^*(k) &= \det\left[\left(\frac{\alpha_i+\alpha_j}{p}\right)\left(\frac{\alpha_j}{p}\right)\mathbf{i}^{i-j}\right]_{1\le i,j\le m} \\
&= \det\left[\left(\frac{1+g^{k(i-j)}}{p}\right)\mathbf{i}^{i-j}\right]_{0\le i,j\le m-1} \\
&= \det C(\omega_0,\dots,\omega_{m-1}) \quad \text{where } \omega_r = \left(\frac{1+g^{kr}}{p}\right)\mathbf{i}^r \text{ for } 0 \le r \le m-1.
\end{aligned}$$

One can verify that $\omega_0,\dots,\omega_{m-1}$ satisfy the condition (2.1). Fix a multiplicative character $\psi \in \widehat{\mathbb{F}_p^\times}$ of order 4 with $\psi(g) = \mathbf{i}$. Then

$$\sum_{r=0}^{m-1}\omega_r = \sum_{r=0}^{m-1}\left(\frac{1+g^{kr}}{p}\right)\psi(g^r) = \frac{1}{k}\sum_{r=0}^{p-2}\left(\frac{1+g^{kr}}{p}\right)\psi(g^r).$$

One can also verify the following equalities:

$$\begin{aligned}
\sum_{r=0}^{p-2}\left(\frac{1+g^{kr}}{p}\right)\psi(g^r) &= \sum_{r=0}^{(p-3)/2}\left(\frac{1+g^{2kr}}{p}\right)\left(\frac{g^r}{p}\right) + \mathbf{i}\sum_{r=0}^{(p-3)/2}\left(\frac{1+g^{2kr}g^k}{p}\right)\left(\frac{g^r}{p}\right) \\
&= \frac{1}{2}\sum_{x=1}^{p-1}\left(\frac{1+x^{2k}}{p}\right)\left(\frac{x}{p}\right) + \frac{1}{2}\mathbf{i}\sum_{x=1}^{p-1}\left(\frac{1+x^{2k}g^k}{p}\right)\left(\frac{x}{p}\right) \\
&= \frac{1}{2}\sum_{x=1}^{p-1}\left(\frac{1+x^{2k}}{p}\right)\left(\frac{x}{p}\right) + \frac{1}{2}\mathbf{i}\sum_{x=1}^{p-1}\left(\frac{g^k+x^{2k}}{p}\right)\left(\frac{x}{p}\right) \\
&= -\frac{c_p(k)+\mathbf{i}d_p(k)}{2},
\end{aligned}$$

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

where $c_p(k)$ and $d_p(k)$ are defined by (1.3) and (1.4), respectively. Hence,

$$\sum_{r=0}^{m-1} \omega_r = -\frac{c_p(k) + \mathbf{i}d_p(k)}{2k}. \tag{2.8}$$

With essentially the same method, one can also verify that

$$\sum_{r=0}^{m-1} (-1)^r \omega_r = -\frac{c_p(k) - \mathbf{i}d_p(k)}{2k}. \tag{2.9}$$

If $\det W_p(k) = 0$, then one can get the desired result directly. Suppose now that $\det W_p(k) \neq 0$. By (2.7), we have $\det W_p(k) > 0$ under this assumption. Combining Lemma 2.1 with (2.8) and (2.9), there exists an element $z_p(k) \in \mathbb{Z}[\mathbf{i}]$ such that

$$\det W_p(k) = \det W_p^*(k) = \frac{z_p(k)^2}{4k^2}(c_p(k)^2 + d_p(k)^2).$$

As $\det W_p(k) \in \mathbb{Z}$ and $\det W_p(k) > 0$, the number $z_p(k)$ must be an integer. This completes the proof of (i).

(ii) We now consider the case $p \equiv 3 \pmod 4$. As k is odd, it is clear that

$$-\alpha_1 \bmod p, \ldots, -\alpha_m \bmod p$$

is a permutation π of the sequence

$$\alpha_1 \bmod p, \ldots, \alpha_m \bmod p,$$

and clearly

$$\operatorname{sgn}(\pi) \equiv \prod_{1 \le i < j \le m} \frac{-\alpha_j - (-\alpha_i)}{\alpha_j - \alpha_i} = (-1)^{m(m-1)/2} \pmod p,$$

where $\operatorname{sgn}(\pi)$ is the sign of π. When $p \equiv 3 \pmod 4$ and k is odd, since $m \equiv 2 \pmod 4$, the number $\det W_p(k)$ is equal to

$$\operatorname{sgn}(\pi) \det\left[\left(\frac{\alpha_i - \alpha_j}{p}\right)\right]_{1 \le i,j \le m} = -\det\left[\left(\frac{\alpha_i - \alpha_j}{p}\right)\right]_{1 \le i,j \le m}.$$

Clearly, the matrix $M_p := [((\alpha_i - \alpha_j)/p)]_{1 \le i,j \le m}$ is skew-symmetric, that is, $M_p^T = -M_p$. The determinant of a skew-symmetric matrix of even order with integer entries is always an integral square (see [8, Proposition 2.2]). This implies that $-\det W_p(k)$ is an integral square.

This completes the proof. □

Proof of Corollary 1.4. (i) Let $k = 3$ and $p \equiv 1 \pmod{12}$. Write $p = \alpha^2 + \beta^2$ with $\alpha, \beta \in \mathbb{Z}$ and $\alpha \equiv -(2/p) \pmod 4$. From [1, Theorem 6.2.5],

$$c_p(3)^2 = \begin{cases} 36\alpha^2 & \text{if } 3 \nmid \alpha, \\ 4\alpha^2 & \text{if } 3 \mid \alpha, \end{cases}, \quad d_p(3)^2 = \begin{cases} 4\beta^2 & \text{if } 3 \nmid \alpha, \\ 36\beta^2 & \text{if } 3 \mid \alpha. \end{cases}$$

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

Hence, if we write $p = c^2 + 9d^2$ with $c, d \in \mathbb{Z}$, then one can easily verify that

$$\frac{c_p(3)^2 + d_p(3)^2}{36} = c^2 + d^2.$$

By Theorem 1.3, $\det W_p(3)/(c^2 + d^2)$ is an integral square if $p \equiv 1 \pmod{12}$.

(ii) If $p \nmid \det W_p(3)$, then

$$\left(\frac{\det W_p(3)}{p}\right) = \left(\frac{c^2 + d^2}{p}\right) = \left(\frac{8c^2 + p}{p}\right) = \left(\frac{2}{p}\right).$$

This completes the proof. □

3. Proof of Theorem 1.7

Recall that

$$I_p(k) = \left[\frac{1}{\alpha_i + \alpha_j}\right]_{1\le i,j\le m}.$$

As -1 is not a kth power residue modulo p, clearly we have $2 \nmid m$.

PROOF OF THEOREM 1.7. By [7, Theorem 12(5.5)],

$$\det I_p(k) = \frac{\prod_{1\le i<j\le m}(\alpha_i - \alpha_j)^2}{\prod_{1\le i\le m}\prod_{1\le j\le m}(\alpha_i + \alpha_j)}.$$

We first consider the numerator. One can verify the equalities

$$\begin{aligned} N_p := \prod_{1\le i<j\le m}(\alpha_i - \alpha_j)^2 &= (-1)^{m(m-1)/2}\prod_{1\le i\ne j\le m}(\alpha_i - \alpha_j) \\ &= (-1)^{(m-1)/2}\prod_{1\le j\le m}\prod_{i\ne j}(\alpha_j - \alpha_i) \\ &= (-1)^{(m-1)/2}\prod_{1\le j\le m} G'(\alpha_j), \end{aligned}$$

where $G'(X)$ is the derivative of $G(X) = \prod_{1\le i\le m}(X - \alpha_i)$. Observe that

$$G(X) \equiv X^m - 1 \pmod{p}. \tag{3.1}$$

Hence, $G'(X) \equiv mX^{m-1} \pmod{p}$ and $\prod_{1\le i\le m}\alpha_i \equiv (-1)^{m+1} = 1 \pmod{p}$. This gives

$$\begin{aligned} N_p = \prod_{1\le i<j\le m}(\alpha_i - \alpha_j)^2 &= (-1)^{(m-1)/2}\prod_{1\le j\le m} G'(\alpha_j) \\ &\equiv (-1)^{(m-1)/2} m^m \prod_{1\le j\le m}\alpha_j^{m-1} \equiv (-1)^{(m-1)/2} m^m \pmod{p}. \end{aligned} \tag{3.2}$$

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

Now we turn to the denominator. One can verify the equalities

$$D_p := \prod_{i=1}^{m}\prod_{j=1}^{m}(\alpha_i+\alpha_j) = \prod_{i=1}^{m}\alpha_i^m\prod_{j=1}^{m}(1+\alpha_j/\alpha_i)$$
$$\equiv \prod_{i=1}^{m}\prod_{j=1}^{m}(1+\alpha_j) = \prod_{j=1}^{m}(1+\alpha_j)^m \pmod p.$$

Hence, by (3.1),

$$D_p \equiv (-1)^m G(-1)^m \equiv 2^m \pmod p. \tag{3.3}$$

Combining (3.2) with (3.3), we finally obtain

$$\det I_p(k) \equiv \frac{(-1)^{(m-1)/2}m^m}{2^m} \equiv \frac{(-1)^{(m+1)/2}}{(2k)^m} \pmod p.$$

This completes the proof. □

Acknowledgement

We would like to thank the referee for helpful comments.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley, New York, 1998).
[2] L. Carlitz, 'Some cyclotomic matrices', *Acta Arith.* **5** (1959), 293–308.
[3] R. Chapman, 'Determinants of Legendre symbol matrices', *Acta Arith.* **115** (2004), 231–244.
[4] R. Chapman, 'My evil determinant problem', Preprint, 2012, available from http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf.
[5] I. Kra and S. R. Simanca, 'On circulant matrices', *Notices Amer. Math. Soc.* **59** (2012), 368–377.
[6] D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, 'On some determinants involving Jacobi symbols', *Finite Fields Appl.* **64** (2020), 101672.
[7] C. Krattenthaler, 'Advanced determinant calculus: a complement', *Linear Algebra Appl.* **411** (2005), 68–166.
[8] J. R. Stembridge, 'Nonintersecting paths, pfaffians and plane partitions', *Adv. Math.* **83** (1990), 96–131.
[9] Z.-W. Sun, 'On some determinants with Legendre symbol entries', *Finite Fields Appl.* **56** (2019), 285–307.
[10] M. Vsemirnov, 'On the evaluation of R. Chapman's "evil determinant"', *Linear Algebra Appl.* **436** (2012), 4101–4106.
[11] M. Vsemirnov, 'On R. Chapman's "evil determinant": case $p \equiv 1 \pmod 4$', *Acta Arith.* **159** (2013), 331–344.
[12] H.-L. Wu, 'Determinants concerning Legendre symbols', *C. R. Math. Acad. Sci. Paris* **359**(6) (2021), 651–655.
[13] H.-L. Wu, 'Elliptic curves over F_p and determinants of Legendre matrices', *Finite Fields Appl.* **76** (2021), 101929.
[14] H.-L. Wu, Y.-F. She and H.-X. Ni, 'Trinomial coefficients and a determinant of Sun', Preprint, 2021, arXiv:2108.10624.

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press

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

LI-YUAN WANG, School of Physical and Mathematical Sciences,
Nanjing Tech University, Nanjing 211816, PR China
e-mail: wly@smail.nju.edu.cn

https://doi.org/10.1017/S0004972722000053 Published online by Cambridge University Press