Bull. Malays. Math. Sci. Soc. 48 (2025), no. 4, Article 132, 17 pages.

SOME DETERMINANTS INVOLVING BINARY FORMS

YUE-FENG SHE AND ZHI-WEI SUN

Abstract. In this paper, we study arithmetic properties of certain determinants involving powers of $i^2+cij+dj^2$, where c and d are integers. For example, for any odd integer $n>1$ with $(\frac{d}{n})=-1$ we prove that $\det[(\frac{i^2+cij+dj^2}{n})]_{0\leqslant i,j\leqslant n-1}$ is divisible by $\varphi(n)^2$, where $(\frac{\cdot}{n})$ is the Jacobi symbol and φ is Euler's totient function. This confirms a previous conjecture of Sun.

1. Introduction

For each $n\times n$ matrix $M=[a_{ij}]_{1\leqslant i,j\leqslant n}$ over a commutative ring, we denote its determinant by $\det(M)$ or $\det[a_{ij}]_{1\leqslant i,j\leqslant n}$. If $a_{ij}=0$ for all $1\leqslant i,j\leqslant n$ with $i\neq j$, then we simply write $M=[a_{ij}]_{1\leqslant i,j\leqslant n}$ as $\mathrm{diag}(a_{11},\ldots,a_{nn})$. For various results on evaluations of determinants, one may consult the excellent survey papers [3, 4]. In this paper we study some determinants involving certain binary forms and related Jacobi symbols.

Let a be any integer. For any odd prime p, the Legendre symbol $(\frac{a}{p})$ is given by

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{if } p\nmid a \text{ and } x^2\equiv a \pmod p \text{ for some } x\in\mathbb{Z},\\ -1 & \text{if } p\nmid a \text{ and } x^2\equiv a \pmod p \text{ for no } x\in\mathbb{Z},\\ 0 & \text{if } p\mid a.\end{cases}$$

For any positive odd integer n, the Jacobi symbol $(\frac{a}{n})$ is defined as follows:

$$\left(\frac{a}{n}\right)=\begin{cases}1 & \text{if } n=1,\\ \prod_{i=1}^k(\frac{a}{p_i}) & \text{if } n=p_1\cdots p_k \text{ for some primes } p_1,\ldots,p_k.\end{cases}$$

Let $c,d\in\mathbb{Z}$. For any odd number $n>1$, Sun [8] introduced

$$(c,d)_n:=\det\left[\left(\frac{i^2+cij+dj^2}{n}\right)\right]_{1\leqslant i,j\leqslant n-1}$$

and

$$[c,d]_n:=\det\left[\left(\frac{i^2+cij+dj^2}{n}\right)\right]_{0\leqslant i,j\leqslant n-1}.$$

By [8, Theorem 1.3], $(c,d)_n=0$ if $(\frac{d}{n})=-1$, and $[c,d]_p$ is divisible by $p-1$ if p is an odd prime with $(\frac{d}{p})=1$. For some results on $(c,d)_n$ and $[c,d]_n$ with c and d special, one may consult

Key words and phrases. Determinants, Legendre symbols, Jacobi symbols, Euler's totient function, polynomials over finite fields.

2020 *Mathematics Subject Classification.* Primary 11C20, 11T06; Secondary 15A15.

The second author is supported by the Natural Science Foundation of China (grant no. 12371004).

Krachun et al. [2]. For an odd prime p, the values of $(c,d)_p$ and $[c,d]_p$ are sometimes related to elliptic curves over the finite field $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ (cf. [2, 14]).

In Section 2, we will prove the following result, which was first conjectured by Sun [9, Conjecture 11.35].

Theorem 1.1. *Let $c,d\in\mathbb{Z}$. For any odd number $n>1$ with $(\frac{d}{n})=-1$, we have $\varphi(n)^2\mid[c,d]_n$, where φ is Euler's totient function.*

Let c and d be integers. By [10, Theorem 1.2], for any prime $p>3$ and $n\in\{(p+1)/2,\ldots,p-2\}$, we have

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

By [13, Theorem 1.1], for any odd prime p with $(\frac{d}{p})=-1$ we have

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

for all $n=1,\ldots,p-1$.

Suppose that $P(x,y)\in\mathbb{Z}[x,y]$ and its degree with respect to x is smaller than $n\in\mathbb{N}$. For each $j=1,\ldots,n$, write

$$P(x,j)=\sum_{k=1}^n a_{jk}x^{k-1}$$

with $a_{j1},\ldots,a_{jn}\in\mathbb{Z}$. By [4, Lemma 15], we have

$$\begin{aligned}\det[P(i,j)]_{1\leqslant i,j\leqslant n}&=\lim_{t\to 0}\det[ta_{j1}(-i)^n+P(i,j)]_{1\leqslant i,j\leqslant n}\\&=\lim_{t\to 0}(1-n!t)\prod_{1\leqslant i<j\leqslant n}(j-i)\times\det[a_{jk}]_{1\leqslant j,k\leqslant n}\\&=1!2!\cdots(n-1)!\times\det[a_{jk}]_{1\leqslant j,k\leqslant n}.\end{aligned}$$

In particular, if the degree of $P(x,y)$ with respect to x is smaller than $n-1$, then $a_{1n}=\ldots=a_{nn}=0$ and hence

$$\det[P(i,j)]_{1\leqslant i,j\leqslant n}=1!2!\cdots(n-1)!\times\det[a_{jk}]_{1\leqslant j,k\leqslant n}=0.$$

We will establish the following result in Section 3.

Theorem 1.2. *Let p be an odd prime, and let*

$$H(X,Y)=\sum_{k=0}^n a_kX^kY^{n-k}$$

with $a_0,\ldots,a_n\in\mathbb{Z}$.

(i) *If $n=p-1$, then*

$$\det[x+H(i,j)]_{1\leqslant i,j\leqslant p-1}\equiv(x+a_0+a_{p-1})\prod_{k=1}^{p-2}a_k \pmod p.$$

(ii) *If $n = p-2$ or $p-1 < n < 2p-2$, then*

$$\det[x + H(i,j)]_{1\leqslant i,j\leqslant p-1} \equiv (-1)^n \prod_{k=0}^{p-2} \sum_{\substack{0\leqslant j\leqslant n\\ p-1\mid j-k}} a_j \pmod p.$$

By taking $H(X,Y) = (X^2 + cXY + dY^2)^n$ with $c,d \in \mathbb{Z}$, we obtain the following result.

Corollary 1.1. *Let $p > 3$ be a prime, and let $c,d \in \mathbb{Z}$ and $n \in \{(p+1)/2, \ldots, p-2\}$. Then $\det[x + (i^2 + cij + dj^2)^n]_{1\leqslant i,j\leqslant p-1}$ modulo p is independent of x.*

Let p be an odd prime, and let $c,d \in \mathbb{Z}$. Sun [10] first introduced

$$D_p(c,d) = \det[(i^2 + cij + dj^2)^{p-2}]_{1\leqslant i,j\leqslant p-1}$$

motivated by his conjecture on $\det[1/(i^2 - ij + j^2)]_{1\leqslant i,j\leqslant p-1}$ for $p \equiv 2 \pmod 3$ (cf. [8, Remark 1.3]). For $(\frac{D_p(1,1)}{p})$ and $(\frac{D_p(2,2)}{p})$, one may consult [5, 16]. See also [7] and [6] for further results in this direction.

Let $c,d \in \mathbb{Z}$. Sun [11, Section 5] investigated

$$\{c,d\}_n = \det\left[\left(\frac{i^2 + cij + dj^2}{n}\right)\right]_{1<i,j<n-1}$$

with n an odd number greater than 3. Motivated by this, we study

$$D_p^-(c,d) := \det[(i^2 + cij + dj^2)^{p-2}]_{1<i,j<p-1}$$

for any prime $p > 3$. The difficulty of evaluating $D_p^-(c,d)$ lies in the fact that the indices do not run through a whole reduced system of residues modulo p.

For a prime p, let $\mathbb{Z}_p$ denote the ring of p-adic integers. It is well known that each p-adic integer α can be written uniquely as a p-adic series $\sum_{k=0}^{\infty} a_k p^k$ with $a_k \in \{0, \ldots, p-1\}$, which converges with respect to the p-adic norm $|\ |_p$. Hence we have the congruence $\alpha \equiv \sum_{k=0}^{n-1} a_k p^k \pmod{p^n}$ (in the ring $\mathbb{Z}_p$) for any positive integer n. For example,

$$\frac{1}{1-p} = \sum_{k=0}^{\infty} p^k \equiv \sum_{k=0}^{n-1} p^k = \frac{1-p^n}{1-p} \pmod{p^n}$$

for any positive integer n. A rational number is a p-adic integer if and only if its denominator is not divisible by p. For $a,b,c \in \mathbb{Z}$ with $p \nmid b$, the congruence $a/b \equiv c \pmod p$ in the ring $\mathbb{Z}_p$ is actually equivalent to the congruence $a \equiv bc \pmod p$ in the ring $\mathbb{Z}$. For instance, $2/3 \equiv 3 \pmod 7$.

We will prove the following result in Section 4.

Theorem 1.3. *Let $p > 3$ be a prime, and let*

$$P(T) = a_0 + a_1 T + a_2 T^2 + \cdots + a_{p-2} T^{p-2},$$

where $a_0,\ldots,a_{p-2}\in\mathbb{Z}_p$. *Then we have*

$$\det\left[P(ij^{-1})\right]_{1<i,j<p-1}\equiv 4\sum_{i=0}^{(p-3)/2}\hat{a}_{2i}\times\sum_{j=0}^{(p-3)/2}\hat{a}_{2j+1}\pmod p,$$

where

$$\hat{a}_k=\prod_{\substack{0\leqslant j\leqslant p-2\\ 2\mid j-k,\, j\neq k}}a_j\qquad \textit{for all}\ \ k=0,\ldots,p-2.$$

For an odd prime p and a p-adic integer α, we define $(\frac{\alpha}{p})$ as the Legendre symbol $(\frac{r}{p})$, where r is the unique integer in $\{0,\ldots,p-1\}$ with $\alpha\equiv r\pmod p$. If $\alpha=a/b$ with $a,b\in\mathbb{Z}$ and $p\nmid b$, then $(\frac{\alpha}{p})$ coincides with the Legendre symbol $(\frac{ab}{p})$.

As an application of Theorem 1.3, we will prove the following result.

Corollary 1.2. *Let* $p>3$ *be a prime.*

(i) *When* $p\equiv 2\pmod 3$, *we have*

$$D_p^-(1,1)\equiv 2^{(p-8)/3}3^4\pmod p\quad\textit{and}\quad\left(\frac{D_p^-(1,1)}{p}\right)=\left(\frac{2}{p}\right).$$

(ii) *When* $p\equiv 7\pmod 9$, *we have* $D_p^-(1,1)\equiv 0\pmod p$.

(iii) *When* $p\equiv 1,4\pmod 9$, *we have*

$$\left(\frac{D_p^-(1,1)}{p}\right)=\left(\frac{\Sigma_1\Sigma_2}{p}\right),$$

where

$$\Sigma_1=\sum_{k=1}^{(p-1)/6}\left(\frac{1}{18k-13}-\frac{1}{18k-2}\right)+\frac{1}{6},$$

and

$$\Sigma_2=\sum_{k=1}^{(p-1)/6}\left(\frac{1}{18k-4}-\frac{1}{18k-11}\right)+\frac{1}{6}.$$

Example 1.1. Let us illustrate Corollary 1.2(iii) with $p=19$. It is easy to verify that

$$D_p^-(1,1)\equiv -5\pmod p,\ \ \Sigma_1\equiv 3\pmod p\ \text{and}\ \Sigma_2\equiv -8\pmod p.$$

Thus

$$\left(\frac{D_p^-(1,1)}{p}\right)=\left(\frac{-5}{19}\right)=\left(\frac{3\times(-8)}{19}\right)=\left(\frac{\Sigma_1\Sigma_2}{p}\right).$$

The following conjecture of the second author might stimulate further research.

Conjecture 1.1. *Let $p>3$ be a prime.*

(i) *We have $p \mid D_p^-(2,2)$ if $p \equiv 7 \pmod 8$.*

(ii) *We have $p \mid D_p^-(3,3)$ if $p>5$ and $p \equiv 2 \pmod 3$.*

(iii) *We have $p \mid D_p^-(3,1)$ if $p \equiv 3,7 \pmod{20}$.*

We are going to prove Theorem 1.1, Theorem 1.2, Theorem 1.3 and Corollary 1.2 in Sections 2, 3, 4 and 5, respectively.

For convenience, for a matrix $M=[m_{ij}]_{0\leqslant i,j\leqslant n}$, we call the row $(m_{i0},\ldots,m_{in})$ with $0\leqslant i\leqslant n$ the *i-row* of M which is actually the $(i+1)$-th row of M, and define the *j-column* with $0\leqslant j\leqslant n$ similarly. Such terms will be used in Sections 3 and 4.

2. Proof of Theorem 1.1

Lemma 2.1. *Suppose that $n>1$ is odd and not squarefree. Then, for any $c,d\in\mathbb{Z}$ we have $[c,d]_n=0$.*

Proof. Write $n=p^\alpha m$, where p is an odd prime and $\alpha,m\in\mathbb{Z}^+=\{1,2,3,\ldots\}$ such that $\alpha>1$ and $p\nmid m$. By the Chinese Remainder Theorem, there exists a number $k\in\{1,\ldots,n-1\}$ such that $m\mid k$ and $k\equiv p \pmod{p^\alpha}$. For any $0\leqslant i\leqslant n-1$, we have

$$\left(\frac{i^2+cik+dk^2}{n}\right)=\left(\frac{i^2+cik+dk^2}{m}\right)\left(\frac{i^2+cik+dk^2}{p}\right)^\alpha=\left(\frac{i^2}{m}\right)\left(\frac{i^2}{p}\right)^\alpha=\left(\frac{i^2+ci0+d0^2}{n}\right).$$

Therefore $[c,d]_n=0$. □

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. In light of Lemma 2.1, it suffices to assume that n is squarefree. Let

$$P^+(n):=\left\{p:\ p \text{ is a prime divisor of } n \text{ with } \left(\frac{d}{p}\right)=1\right\}$$

and

$$P^-(n)=\left\{p:\ p \text{ is a prime divisor of } n \text{ with } \left(\frac{d}{p}\right)=-1\right\}.$$

By the Chinese Remainder Theorem and [1, p. 63, Exercise 8], for $0\leqslant j\leqslant n-1$ we have

$$\begin{aligned}&\sum_{\substack{0\leqslant i\leqslant n-1\\(i,n)=1}}\left(\frac{i^2+cij+dj^2}{n}\right)\\&=\sum_{\substack{0\leqslant i\leqslant n-1\\(i,n)=1}}\prod_{p\in P^+(n)\cup P^-(n)}\left(\frac{i^2+cij+dj^2}{p}\right)\\&=\prod_{p\in P^+(n)\cup P^-(n)}\sum_{1\leqslant x\leqslant p-1}\left(\frac{x^2+cxj+dj^2}{p}\right)\end{aligned}$$

$$=\prod_{\substack{p\in P^+(n)\\ p\mid(c^2-4d)j}}\left(p-1-\left(\frac{j}{p}\right)^2\right)\times\prod_{\substack{p\in P^+(n)\\ p\nmid(c^2-4d)j}}(-2)\times\prod_{\substack{p\in P^-(n)\\ p\mid j}}(p-1)\times\prod_{\substack{p\in P^-(n)\\ p\nmid j}}0$$

with the aid of the fact that $(\frac{d}{p})=-1$ implies $p\nmid(c^2-4d)$.

Let $Q=\prod_{p\in P^-(n)}p$, and define the function $f:P^+(n)\to\mathbb{Z}$ by

$$f(p)=\begin{cases}p-2 & \text{if } p\mid(c^2-4d),\\ -2 & \text{if } p\nmid(c^2-4d).\end{cases}$$

Then

$$\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=1}}\left(\frac{i^2+cij+dj^2}{n}\right)=\begin{cases}0 & \text{if } Q\nmid j,\\ \varphi(Q)\times\prod_{\substack{p\in P^+(n)\\ p\mid j}}(p-1)\times\prod_{\substack{p\in P^+(n)\\ p\nmid j}}f(p) & \text{if } Q\mid j.\end{cases}$$

For any subset A of $P^+(n)$, define $p(A)=\prod_{p\in A}p$. Via similar arguments, we get

$$\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=p(A)}}\left(\frac{i^2+cij+dj^2}{n}\right)$$
$$=\begin{cases}0 & \text{if } Q\nmid j \text{ or } (p(A),j)>1,\\ \varphi(Q)\times\prod_{\substack{p\in P^+(n)\setminus A\\ p\mid j}}(p-1)\times\prod_{\substack{p\in P^+(n)\setminus A\\ p\nmid j}}f(p) & \text{if } Q\mid j \text{ and } (p(A),j)=1.\end{cases}$$

Thus, when $Q\nmid j$ we have

$$\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=1}}\left(\frac{i^2+cij+dj^2}{n}\right)=\prod_{p\in A}f(p)\times\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=p(A)}}\left(\frac{i^2+cij+dj^2}{n}\right)=0.$$

When $Q\mid j$, we have

$$\left(\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=1}}\left(\frac{i^2+cij+dj^2}{n}\right)\right)^{-1}\prod_{p\in A}f(p)\times\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=p(A)}}\left(\frac{i^2+cij+dj^2}{n}\right)$$
$$=\begin{cases}0 & \text{if } (p(A),j)>1,\\ 1 & \text{if } (p(A),j)=1.\end{cases}$$

Let μ be the Möbius function. Then

$$\sum_{A\subseteq P^+(n)}\mu(p(A))\prod_{p\in A}f(p)\times\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=p(A)}}\left(\frac{i^2+cij+dj^2}{n}\right)$$
$$=\sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=1}}\left(\frac{i^2+cij+dj^2}{n}\right)\times\sum_{\substack{A\subseteq P^+(n)\\ (p(A),j)=1}}\mu(p(A))$$

$$= \sum_{\substack{0\leqslant i\leqslant n-1\\ (i,n)=1}} \left(\frac{i^2+cij+dj^2}{n}\right) \times \sum_{d \mid \frac{p(P^+(n))}{(p(P^+(n)),j)}} \mu(d)$$

$$= \begin{cases} \varphi(n) & \text{if } j=0,\\ 0 & \text{otherwise.} \end{cases}$$

The last equality follows from the well-known identity (cf. [1, p. 19])

$$\sum_{d\mid k} \mu(d) = \begin{cases} 1 & \text{if } k=1,\\ 0 & \text{if } k\in\{2,3,\ldots\}. \end{cases}$$

Thus, via certain elementary row transformations we get the equality $[c,d]_n = \det[a_{ij}]_{0\leqslant i,j\leqslant n-1}$, where

$$a_{ij} = \begin{cases} \varphi(n) & \text{if } i=1 \text{ and } j=0,\\ 0 & \text{if } i=1 \text{ and } j\neq 0,\\ \left(\frac{i^2+cij+dj^2}{n}\right) & \text{otherwise.} \end{cases}$$

Similarly, for $0\leqslant i\leqslant n-1$ we have

$$\sum_{A\subseteq P^+(n)} \mu(p(A)) \prod_{p\in A} f(p) \times \sum_{\substack{0\leqslant j\leqslant n-1\\ (j,n)=p(A)}} \left(\frac{i^2+cij+dj^2}{n}\right) = \begin{cases} -\varphi(n) & \text{if } i=0,\\ 0 & \text{otherwise,} \end{cases}$$

and hence $\det[a_{ij}]_{0\leqslant i,j\leqslant n-1} = \det[b_{ij}]_{0\leqslant i,j\leqslant n-1}$, where

$$b_{ij} = \begin{cases} \varphi(n) & \text{if } i=1 \text{ and } j=0,\\ -\varphi(n) & \text{if } i=0 \text{ and } j=1,\\ 0 & \text{if } i=1 \text{ and } j\neq 0, \text{ or } i\neq 0 \text{ and } j=1,\\ \left(\frac{i^2+cij+dj^2}{n}\right) & \text{otherwise.} \end{cases}$$

Therefore,

$$[c,d]_n = \det[a_{ij}]_{0\leqslant i,j\leqslant n-1} = \det[b_{ij}]_{0\leqslant i,j\leqslant n-1} \equiv 0 \pmod{\varphi(n)^2}.$$

This concludes our proof. □

3. Proof of Theorem 1.2

We need the following well-known Weinstein-Aronszajn identity (cf. [15]).

Lemma 3.1. *Suppose that A and B are matrices over the complex field of sizes $l\times m$ and $m\times l$, respectively. Then*

$$\lambda^m \det(\lambda I_l - AB) = \lambda^l \det(\lambda I_m - BA),$$

where I_n denotes the identity matrix of order n.

Proof of Theorem 1.2. We set $A = [i^j]_{\substack{1\leqslant i\leqslant p-1\\ 0\leqslant j\leqslant n}}$ and $C = [c_{i,j}]_{0\leqslant i,j\leqslant n}$ with

$$c_{i,j} = \begin{cases} x & \text{if } i = 0 \text{ and } j = 0,\\ a_i & \text{if } i + j = n,\\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 3.1,

$$\begin{aligned} &\det(\lambda I_{p-1} - [x + H(i,j)]_{1\leqslant i,j\leqslant p-1})\\ =&\det(\lambda I_{p-1} - ACA^T)\\ =&\lambda^{p-n-2}\det(\lambda I_{n+1} - CA^TA)\\ =&\lambda^{p-n-2}\det(\lambda I_{n+1} - C[s_{i+j}]_{0\leqslant i,j\leqslant n}), \end{aligned} \tag{3.1}$$

where $s_k = \sum_{i=1}^{p-1} i^k$. According to [1, p. 235],

$$\sum_{i=1}^{p-1} i^k \equiv \begin{cases} -1 \pmod p & \text{if } p-1 \mid k,\\ 0 \pmod p & \text{if } p-1 \nmid k. \end{cases} \tag{3.2}$$

So, when $n = p - 2$ we have

$$\begin{aligned} \det[x + H(i,j)]_{1\leqslant i,j\leqslant p-1} &\equiv \det C \times \det[s_{i+j}]_{0\leqslant i,j\leqslant n}\\ &\equiv (-1)^{(p-1)/2}\prod_{k=0}^{n} a_k \times (-1)^{(p-3)/2} = -\prod_{k=0}^{n} a_k \pmod p. \end{aligned}$$

Let $D = [d_{ij}]_{0\leqslant i,j\leqslant n}$ be the matrix $C[s_{i+j}]_{0\leqslant i,j\leqslant n}$.

Case 1. $3(p-1)/2 \leqslant n < 2p-2$.
In this case, we have

$$d_{ij} \equiv \begin{cases} -x \pmod p & \text{if } i = 0 \text{ and } j \in \{0, p-1\},\\ -a_0 \pmod p & \text{if } i = 0 \text{ and } j + n \in \{2p-2, 3p-3\},\\ -a_i \pmod p & \text{if } i \geqslant 1 \text{ and } i - j \equiv n \pmod{p-1},\\ 0 \pmod p & \text{otherwise.} \end{cases}$$

Hence $\lambda I_{n+1} - D$ is congruent to the matrix

$$\begin{bmatrix}
\lambda+x & & a_0 & & & & x & & a_0 & & \\
 & \lambda & & \ddots & & & & & & \ddots & \\
 & & \ddots & & \ddots & & & & & & a_{2n-3p+3} \\
 & & & \ddots & & \ddots & & & & & \\
a_{n-p+1} & & & & \ddots & & \ddots & & & & \\
 & \ddots & & & & \ddots & & \ddots & & & \\
 & & \ddots & & & & \ddots & & \ddots & & \\
 & & & \ddots & & & & \ddots & & \ddots & \\
 & & & & \ddots & & & & \ddots & & a_{2n-2p+2} \\
 & & & & & \ddots & & & & \ddots & \\
a_n & & & & & & a_n & & & & \lambda
\end{bmatrix}.$$

(whose entries 0 are not indicated) modulo p. Subtracting the k-column from the $(k+p-1)$-column for $0 \leqslant k \leqslant n-p+1$, we find that the last matrix is transformed to the matrix

$$\begin{bmatrix}
\lambda+x & & a_0 & & & & -\lambda & & & & \\
 & \lambda & & \ddots & & & & \ddots & & & \\
 & & \ddots & & \ddots & & & & \ddots & & \\
 & & & \ddots & & a_{n-p} & & & & \ddots & \\
a_{n-p+1} & & & & \ddots & & 0 & & & & -\lambda \\
 & \ddots & & & & \ddots & & & & & \\
 & & \ddots & & & & \ddots & & & & \\
 & & & \ddots & & & & \ddots & & & \\
 & & & & \ddots & & & & \ddots & & \\
 & & & & & a_{n-1} & & & & \ddots & \\
a_n & & & & & & 0 & & & & \lambda
\end{bmatrix}.$$

Adding the k-row to the $(k-p+1)$-row for $p-1 \leqslant k \leqslant n$, we see that the last matrix is transformed to

$$\begin{bmatrix} \lambda+x & & a_0+a_{p-1} & & & & & & \\ & \lambda & & \ddots & & & & & \\ & & \ddots & & a_{n-p}+a_{n-1} & & & & \\ a_{n-p+1}+a_n & & & \ddots & & 0 & & & \\ & \ddots & & & \ddots & & & & \\ & & \ddots & & & \ddots & & & \\ & & & \ddots & & & \ddots & & \\ & & & & a_{n-1} & & & \ddots & \\ a_n & & & & & 0 & & & \lambda \end{bmatrix}.$$

Thus, by (3.1), $\det(\lambda I_{p-1} - [x+H(i,j)]_{1\leqslant i,j\leqslant p-1})$ is congruent to

$$\det \begin{bmatrix} \lambda+x & & & a_0+a_{p-1} & & \\ & \lambda & & & \ddots & \\ & & \ddots & & & a_{n-p}+a_{n-1} \\ a_{n-p+1}+a_n & & & \ddots & & \\ & \ddots & & & \ddots & \\ & & a_{p-2} & & & \lambda \end{bmatrix}$$

modulo p. Taking $\lambda = 0$ we obtain that

$$\det[x+H(i,j)]_{1\leqslant i,j\leqslant p-1} \equiv (-1)^n \prod_{k=0}^{n-p+1} (a_k + a_{k+p-1}) \times \prod_{n-p+1<k<p-1} a_k \pmod{p}.$$

Case 2. $p-1 < n < 3(p-1)/2$.
In this case, we have

$$d_{ij} \equiv \begin{cases} -x \pmod{p} & \text{if } i=0 \text{ and } j \in \{0, p-1\}, \\ -a_0 \pmod{p} & \text{if } i=0 \text{ and } j = 2p-2-n, \\ -a_i \pmod{p} & \text{if } i \geqslant 1 \text{ and } i-j \equiv n \pmod{p-1}, \\ 0 \pmod{p} & \text{otherwise.} \end{cases}$$

Hence $\lambda I_{n+1} - D$ is congruent to the matrix

$$\begin{bmatrix}
\lambda + x & & a_0 & & & x & & & \\
& \lambda & & \ddots & & & & & \\
& & \ddots & & \ddots & & & & \\
a_{n-p+1} & & & \ddots & & \ddots & & & \\
& \ddots & & & \ddots & & \ddots & & \\
& & \ddots & & & \ddots & & \ddots & \\
& & & \ddots & & & \ddots & & a_{2n-2p+2} \\
& & & & \ddots & & & \ddots & \\
a_n & & & & & a_n & & & \lambda
\end{bmatrix}.$$

modulo p. Via some arguments similar to the discussion in Case 1, we obtain that

$$\det[x + H(i,j)]_{1\leqslant i,j\leqslant p-1} \equiv (-1)^n \prod_{k=0}^{n-p+1} (a_k + a_{k+p-1}) \times \prod_{k=n-p+2}^{p-2} a_k \pmod p.$$

Case 3. $n = p-1$.

In this case, we have

$$d_{ij} \equiv \begin{cases} -x - a_0 \pmod p & \text{if } i = 0 \text{ and } j \in \{0, p-1\}, \\ -a_i \pmod p & \text{if } i \geqslant 1 \text{ and } i - j \equiv 0 \pmod{p-1}, \\ 0 \pmod p & \text{otherwise.} \end{cases}$$

In light of (3.1), we have

$$\det(\lambda I_{p-1} - [x + H(i,j)]_{1\leqslant i,j\leqslant p-1}) \equiv (\lambda + x + a_0 + a_{p-1}) \prod_{k=1}^{p-2} (\lambda + a_k) \pmod p.$$

Taking $\lambda = 0$, we immediately obtain the desired result.

In view of the above, we have completed our proof of Theorem 1.2. $\square$

4. Proof of Theorem 1.3

We shall use the following useful lemma (cf. [12]).

Lemma 4.1 (The Matrix-Determinant Lemma)**.** *Let H be an $n \times n$ matrix over the complex field, and let $\mathbf{u}$ and $\mathbf{v}$ be two n-dimensional column vectors whose components are complex numbers. Then*

$$\det(H + \mathbf{u}\mathbf{v}^T) = \det H + \mathbf{v}^T \mathrm{adj}(H)\mathbf{u},$$

where $\mathrm{adj}(H)$ *is the adjugate matrix of H.*

Proof of Theorem 1.3. We set $A=[i^j]_{\substack{2\leqslant i\leqslant p-2\\ 0\leqslant j\leqslant p-2}}$ and $C=[c_{ij}]_{0\leqslant i,j\leqslant p-2}$ with

$$c_{ij}=\begin{cases}a_i & \text{if } i+j=p-2,\\ 0 & \text{if } i+j\neq p-2.\end{cases}$$

We also define $s_k:=\sum_{i=2}^{p-2} i^k$ for $k=0,1,2,\ldots$. In view of (3.2),

$$s_k\equiv\begin{cases}-3 \pmod p & \text{if } p-1\mid k,\\ -2 \pmod p & \text{if } 2\mid k \text{ and } p-1\nmid k,\\ 0 \pmod p & \text{if } 2\nmid k.\end{cases}\tag{4.1}$$

By Wilson's theorem, we have

$$\det[P(ij^{-1})]_{1<i,j<p-1}\equiv\det[P(ij^{-1})j^{p-2}]_{1<i,j<p-1}\equiv\det(ACA^T)\pmod p.$$

Hence it suffices to focus on the matrix ACA^T from now on. Applying Lemma 3.1 and (4.1), we obtain

$$\begin{aligned}&\det(\lambda I_{p-3}-ACA^T)\\ =&\ \lambda^{-2}\det(\lambda I_{p-1}-CAA^T)\\ =&\ \lambda^{-2}\det(\lambda I_{p-1}-C[s_{i+j}]_{0\leqslant i,j\leqslant p-2})\\ \equiv&\ \lambda^{-2}\det(\lambda I_{p-1}-[d_{ij}]_{0\leqslant i,j\leqslant p-2})\pmod p,\end{aligned}\tag{4.2}$$

where

$$d_{ij}=\begin{cases}-3a_i & \text{if } p-1\mid j-i-1,\\ -2a_i & \text{if } 2\mid j-i-1 \text{ and } p-1\nmid j-i-1,\\ 0 & \text{if } 2\nmid j-i-1.\end{cases}$$

Subtracting the 0-column from the $2k$-column, and subtracting the 1-column from the $(2k+1)$-column for $1\leqslant k\leqslant(p-3)/2$, we find that the matrix $\lambda I_{p-1}-[d_{ij}]_{0\leqslant i,j\leqslant p-2}$ is converted to

$$\begin{bmatrix}\lambda & 3a_0 & -\lambda & -a_0 & \cdots & -\lambda & -a_0\\ 2a_1 & \lambda & a_1 & -\lambda & \cdots & 0 & -\lambda\\ 0 & 2a_2 & \lambda & a_2 & & & \\ \vdots & \vdots & & \ddots & \ddots & & \\ \vdots & \vdots & & & \ddots & \ddots & \\ 0 & 2a_{p-3} & & & & \lambda & a_{p-3}\\ 3a_{p-2} & 0 & -a_{p-2} & 0 & \cdots & -a_{p-2} & \lambda\end{bmatrix}.$$

Subtracting the $2k$-column times 2 from the 0-column, and subtracting the $(2k+1)$-column times 2 from the 1-column for $1 \leqslant k \leqslant (p-3)/2$, we see that the last matrix is transformed to

$$\begin{bmatrix} (p-2)\lambda & pa_0 & -\lambda & -a_0 & \cdots & -\lambda & -a_0 \\ 0 & (p-2)\lambda & a_1 & -\lambda & \cdots & 0 & -\lambda \\ (p-2)\lambda & 0 & \lambda & a_2 & & & \\ \vdots & \vdots & & \ddots & \ddots & & \\ \vdots & \vdots & & & \ddots & \ddots & \\ (p-2)\lambda & 0 & & & & \lambda & a_{p-3} \\ pa_{p-2} & (p-2)\lambda & -a_{p-2} & 0 & \cdots & -a_{p-2} & \lambda \end{bmatrix}.$$

It follows from (4.2) that

$$\det(ACA^T) \equiv 4\det \begin{bmatrix} 1 & & & -a_0 & \cdots & & -a_0 \\ & 1 & a_1 & & & & \\ 1 & & & a_2 & & & \\ \vdots & \vdots & & & \ddots & & \\ \vdots & \vdots & & & & \ddots & \\ 1 & & & & & & a_{p-3} \\ & 1 & -a_{p-2} & & \cdots & -a_{p-2} & \end{bmatrix}$$

$$= 4\det \begin{bmatrix} 1 & -a_0 & \cdots & -a_0 & & & & \\ 1 & a_2 & & & & & & \\ \vdots & & \ddots & & & & & \\ 1 & & & a_{p-3} & & & & \\ & & & & a_1 & & & 1 \\ & & & & & \ddots & & \vdots \\ & & & & & & a_{p-3} & 1 \\ & & & & -a_{p-2} & \cdots & -a_{p-2} & 1 \end{bmatrix} \pmod p.$$

Let $\mathbf{1}$ denote the $(p-3)/2$-dimensional column vector whose entries are all 1. By Lemma 4.1,

$$\begin{aligned} &\det(ACA^T) \\ &\equiv 4\det \begin{bmatrix} 1 & & & \\ \mathbf{1} & \mathrm{diag}(a_2,\cdots,a_{p-3}) + a_0\mathbf{1}\mathbf{1}^T & & \\ & & \mathrm{diag}(a_1,\cdots,a_{p-4}) + a_{p-2}\mathbf{1}\mathbf{1}^T & \mathbf{1} \\ & & & 1 \end{bmatrix} \\ &\equiv 4\det(\mathrm{diag}(a_2,\cdots,a_{p-3}) + a_0\mathbf{1}\mathbf{1}^T)\det(\mathrm{diag}(a_1,\cdots,a_{p-4}) + a_{p-2}\mathbf{1}\mathbf{1}^T) \\ &\equiv 4(\hat{a}_0 + \mathbf{1}^T\mathrm{diag}(\hat{a}_2,\cdots,\hat{a}_{p-3})\mathbf{1})(\hat{a}_{p-2} + \mathbf{1}^T\mathrm{diag}(\hat{a}_1,\cdots,\hat{a}_{p-4})\mathbf{1}) \\ &\equiv 4\sum_{i=0}^{(p-3)/2}\hat{a}_{2i} \times \sum_{j=0}^{(p-3)/2}\hat{a}_{2j+1} \pmod p. \end{aligned}$$

This concludes our proof of Theorem 1.3. □

5. Deduce Corollary 1.2 from Theorem 1.3

Proof of Theorem 1.3. By Fermat's little theorem, there exists a polynomial

$$P(T)=\sum_{k=0}^{p-2}a_kT^k\in\mathbb{Z}_p[T]$$

such that

$$(T^2+T+1)^{p-2}\equiv P(T)\pmod p$$

for any $T\in\{1,2,\ldots,p-1\}$. When $p\equiv 1\pmod 3$, by [5, Corollary 2.1] we may take

$$a_k=\begin{cases}k+5/3 & \text{if } k\equiv 0\pmod 3,\\ -k-4/3 & \text{if } k\equiv 1\pmod 3,\\ -1/3 & \text{if } k\equiv 2\pmod 3.\end{cases}\tag{5.1}$$

When $p\equiv 2\pmod 3$, by [16, Lemma 2.1] we may take

$$a_k=\begin{cases}1/3 & \text{if } k\equiv 0,2\pmod 3,\\ -2/3 & \text{if } k\equiv 1\pmod 3.\end{cases}\tag{5.2}$$

Case 1. $p\equiv 2\pmod 3$.

Combining Theorem 1.3 with (5.2), we obtain that

$$\begin{aligned}D_p^-(1,1)&\equiv\det[P(ij^{-1})]_{1<i,j<p-1}\\ &\equiv 4\prod_{k=0}^{p-2}a_k\times\bigg(\sum_{k=0}^{(p-3)/2}\frac{1}{a_{2k}}\bigg)\times\sum_{k=0}^{(p-3)/2}\frac{1}{a_{2k+1}}\\ &\equiv 2^{(p-8)/3}3^4\pmod p.\end{aligned}$$

Case 2. $p\equiv 7\pmod 9$.

Note that $(p-4)/3,(2p-5)/3\in\{0,1,\ldots,p-2\}$. Since $(p-4)/3\equiv 1\pmod 3$, by (5.1) we have $a_{(p-4)/3}=-p/3\equiv 0\pmod p$. Similarly, $a_{(2p-5)/3}=2p/3\equiv 0\pmod p$ since $(2p-5)/3\equiv 0\pmod 3$. Furthermore, both $(p-4)/3$ and $(2p-5)/3$ are odd and hence $\hat{a}_k\equiv 0\pmod p$ when $2\nmid k$. It follows from Theorem 1.3 that $D_p^-(1,1)\equiv 0\pmod p$.

Case 3. $p\equiv 1,4\pmod 9$.

Suppose that $a_k\equiv 0\pmod p$ for some $k\in\{0,\ldots,p-2\}$. Then $k\equiv 0,1\pmod 3$. If $k\equiv 0\pmod 3$, then $p\mid 3k+5$ and $0\leqslant k\leqslant p-4$, hence $3k+5=p$ or $3k+5=2p$, which implies that $p\equiv 5,7\not\equiv 1,4\pmod 9$. If $k\equiv 1\pmod 3$, then $p\mid 3k+4$ and $1\leqslant k\leqslant p-3$, hence $3k+4=p$ or $3k+4=2p$, which implies that $p\equiv 7,8\not\equiv 1,4\pmod 9$.

By the last paragraph, $a_k\not\equiv 0\pmod p$ for all $k\in\{0,\ldots,p-2\}$. It is easy to verify that $a_k\equiv a_{p-3-k}\pmod p$ for all $k=0,\ldots,p-3$. Hence we may derive from Theorem 1.3 and (5.1) that

$$\left(\frac{D_p^-(1,1)}{p}\right) = \left(\frac{a_{(p-3)/2}a_{p-2} \times \sum_{j=0}^{(p-3)/2} \frac{1}{a_{2j}} \times \sum_{k=0}^{(p-3)/2} \frac{1}{a_{2k+1}}}{p}\right) = \left(\frac{3\Sigma_1 3\Sigma_2}{p}\right) = \left(\frac{\Sigma_1\Sigma_2}{p}\right).$$

This completes the proof of Corollary 1.2. □

Acknowledgment. We are indebted to the anonymous referees for helpful comments.

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

References

[1] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Grad. Texts. Math., vol. 84, Springer, New York, 1990.
[2] D. Krachun, F. Petrov, Z.-W. Sun and M. Vsemirnov, *On some determinants involving Jacobi symbols*, Finite Fields Appl. **64** (2020), Article 101672.
[3] C. Krattenthaler, *Advanced determinant calculus*, Sém. Lothar. Combin. **42** (1999), Article B42q, 67pp.
[4] C. Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. **411** (2005), 68–166.
[5] X.-Q. Luo and Z.-W. Sun, *Legendre symbols related to certain determinants*, Bull. Malays. Math. Sci. Soc. **46** (2023), no. 4, Paper No. 199, 20pp.
[6] X.-Q. Luo and W. Xia, *Legendre symbols related to* $D_p(b,1)$, arXiv:2405.19728, preprint, 2024.
[7] Y.-F. She and H.-L. Wu, *Trinomial coefficients and matrices over finite fields*, arXiv:2210.16826, preprint, 2022.
[8] Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. **56** (2019), 285–307.
[9] Z.-W. Sun, *New Conjectures in Number Theory and Combinatorics* (in Chinese), Harbin Institute of Technology Press, Harbin, 2021.
[10] Z.-W. Sun, *On some determinants and permanents*, Acta Math. Sinica Chin. Ser. **67** (2024), 286–295.
[11] Z.-W. Sun, *Problems and results on determinants involving Legendre symbols*, Bull. Math. Soc. Sci. Math. Roumanie, in press. See also arXiv:2405.03626.
[12] R. Vrabel, *A note on the matrix determinant lemma*, Int. J. Pure Appl. Math. 111 (2016), 643–646.
[13] H. Wang and Z.-W. Sun, *On certain determinants and related Legendre symbols*, Bull. Malays. Math. Sci. Soc. **47** (2024), no. 2, Article No. 58.
[14] H.-L. Wu, *Elliptic curves over* $\mathbb{F}_p$ *and determinants of Legendre matrices*, Finite Fields Appl. **76** (2021), Article 101929.
[15] Wikipedia, Weinstein-Aronszajn identity, https://en.wikipedia.org/wiki/Weinstein-Aronszajn_identity.
[16] 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), no. 5, 2405-2412.

(Yue-Feng She) Department of Applied Mathematics, Nanjing Forestry University, Nanjing 210037, People's Republic of China
E-mail address: `she.math@njfu.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`