Preprint

PROOF OF THREE CONJECTURES ON DETERMINANTS RELATED TO QUADRATIC RESIDUES

DARIJ GRINBERG, ZHI-WEI SUN AND LILU ZHAO

Abstract. In this paper we confirm three conjectures of Z.-W. Sun on determinants. We first show that any odd integer $n > 3$ divides the determiant

$$\left|(i^2+dj^2)\left(\frac{i^2+dj^2}{n}\right)\right|_{0\le i,j\le (n-1)/2},$$

where d is any integer and $(\frac{\cdot}{n})$ is the Jacobi symbol. Then we prove some divisibility results concerning $|(i+dj)^n|_{0\le i,j\le n-1}$ and $|(i^2+dj^2)^n|_{0\le i,j\le n-1}$, where $d \ne 0$ and $n > 2$ are integers. Finally, for any odd prime p and integers c and d with $p \nmid cd$, we determine completely the Legendre symbol $(\frac{S_c(d,p)}{p})$, where $S_c(d,p) := |(\frac{i^2+dj^2+c}{p})|_{1\le i,j\le (p-1)/2}$.

1. Introduction

For an $n\times n$ matrix $[a_{ij}]_{1\le i,j\le n}$ over a commutative ring with identity, we shall denote its determinant by $|a_{ij}|_{1\le i,j\le n}$. In this paper we study some determinants related to quadratic residues. For the standard theory of quadratic residues, one may consult [2, Chapter 5, pp. 50-65].

Our first theorem in the case $d = 1$ was originally conjectured by Sun [6, Conjecture 4.5(i)] amid a study of determinants involving Jacobi symbols.

Theorem 1.1. *Let $n > 3$ be an odd integer. For any integer d, we have*

$$\left|(i^2+dj^2)\left(\frac{i^2+dj^2}{n}\right)\right|_{0\le i,j\le (n-1)/2} \equiv 0 \pmod{n}, \qquad (1.1)$$

where $(\frac{\cdot}{n})$ denotes the Jacobi symbol.

Key words and phrases. Determinant, divisibility, Jacobi symbol, Vandermonde-type determinant.

2020 *Mathematics Subject Classification.* Primary 11C20; Secondary 11A07, 11A15, 15A15.

The second author is the corresponding author, and supported by the Natural Science Foundation of China (grant no. 11971222).

Let p be an odd prime. R. Chapman [1] evaluated the determinant

$$\left|\left(\frac{i+j-1}{p}\right)\right|_{1\le i,j\le (p+1)/2}=\left|\left(\frac{i+j}{p}\right)\right|_{0\le i,j\le (p-1)/2},$$

and M. Vsemirnov [7, 8] determined the exact value of

$$\left|\left(\frac{i-j}{p}\right)\right|_{0\le i,j\le (p-1)/2}$$

guessed by Chapman. Recall that $(\frac{a}{p})\equiv a^{(p-1)/2}\pmod p$ for any $a\in\mathbb{Z}$.

Our next theorem in the case $c=0$ and $d=1$ confirms a conjecture of Sun [5] posed in 2013.

Theorem 1.2. *Let c, d and n be integers with $d\ne 0$ and $n>2$. Set*

$$a_n=|(i+dj+c)^n|_{0\le i,j\le n-1} \quad \text{and} \quad b_n=\left|(i^2+dj^2)^n\right|_{0\le i,j\le n-1}. \tag{1.2}$$

Then

$$a_n'=\frac{a_n d^{-n(n-1)/2}}{(n-2)!n\prod_{k=1}^n k!} \text{ and } b_n'=\frac{b_n d^{-n(n-1)/2}}{2\prod_{k=1}^n(k!(2k-1)!)} \tag{1.3}$$

are integers; in particular,

$$d^{n(n-1)/2}n^2 \mid a_n \quad \text{and} \quad d^{n(n-1)/2}(2n)! \mid b_n. \tag{1.4}$$

Also, $(-1)^{n(n-1)/2}a_n>0$ and $(-1)^{n(n-1)/2}b_n>0$ if $d>0$ and $c\ge 0$.

In the particular case $c=0$ and $d=1$, our numerical computations yield the following data:

$$a_3'=-4,\ a_4'=229,\ a_5'=89200,\ a_6'=-336775500;$$

$$b_1=0,\ b_2=-1,\ b_3=-17280,\ b_4=1168415539200$$

and

$$b_3'=-1,\ b_4'=559,\ b_5'=10767500,\ b_6'=-9372614611500.$$

Let $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$. For any polynomial $P(z)=\sum_{k=0}^{n-1}a_kz^k$ of degree smaller than n with complex coefficients, it is known (cf. [3, Lemma 9]) that

$$|P(x_i+y_j)|_{1\le i,j\le n}=a_{n-1}^n\prod_{k=0}^{n-1}\binom{n-1}{k}\times\prod_{1\le i<j\le n}(x_i-x_j)(y_j-y_i). \tag{1.5}$$

In particular,

$$\left|(i+j)^k\right|_{0\le i,j\le n-1}=0 \quad \text{for all } k=0,\ldots,n-2,$$

and

$$\begin{aligned}\left|(i+j)^{n-1}\right|_{0\le i,j\le n-1} =&(-1)^{n(n-1)/2}\prod_{0\le i<j\le n-1}(j-i)^2\times\prod_{k=0}^{n-1}\binom{n-1}{k}\\ =&(-1)^{n(n-1)/2}((n-1)!)^n.\end{aligned}$$

But this is of no help in simplifying the determinants a_n and b_n given in (1.2) even if $c=0$ and $d=1$.

Our third theorem confirms Conjecture 4.3 of Sun [6].

Theorem 1.3. *Let p be an odd prime, and let $c,d\in\mathbb{Z}$ with $p\nmid cd$. Define*

$$S_c(d,p):=\left|\left(\frac{i^2+dj^2+c}{p}\right)\right|_{1\le i,j\le(p-1)/2}.$$

Then

$$\left(\frac{S_c(d,p)}{p}\right)=\begin{cases}1 & \text{if } (\frac{c}{p})=1 \text{ and } (\frac{d}{p})=-1,\\ (\frac{-1}{p}) & \text{if } (\frac{c}{p})=(\frac{d}{p})=-1,\\ (\frac{-2}{p}) & \text{if } (\frac{-c}{p})=(\frac{d}{p})=1,\\ (\frac{-6}{p}) & \text{if } (\frac{-c}{p})=-1 \text{ and } (\frac{d}{p})=1.\end{cases} \tag{1.6}$$

In contrast, for any odd prime p and $d\in\mathbb{Z}$ with $p\nmid d$, Sun [6, (1.15) and (1.20)] showed that

$$\left(\frac{S_0(d,p)}{p}\right)=\begin{cases}(\frac{-1}{p}) & \text{if } (\frac{d}{p})=1,\\ 0 & \text{if } (\frac{d}{p})=-1.\end{cases}$$

But the method used to prove this does not work for Theorem 1.3.

We will prove Theorem 1.1 in the next section. Using an auxiliary formula in Section 3, we are going to prove Theorems 1.2 and 1.3 in Sections 4 and 5 respectively.

2. Proof of Theorem 1.1

Lemma 2.1. *Let p be a prime and let $k\in\mathbb{N}=\{0,1,2,\ldots\}$. Then*

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

This is a well known fact, see, e.g., [2, Section 15.2, Lemma 2].

In our proof of Theorem 1.1 and further on, we shall freely use the ring isomorphism $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}\cong\mathbb{Z}/p\mathbb{Z}$, where p is a prime number and where $\mathbb{Z}_{(p)}$ is the ring of all rational numbers with nonnegative p-valuation. This allows us to work with fractions inside congruences modulo p as long as the denominators are not divisible by p.

Proof of Theorem 1.1. If n is composite, then n can be written as $n=pm$ for some odd integers $m\geq p>2$, and thus $i:=(m-p)/2$ and $i':=(m+p)/2$ are integers satisfying $0\leq i<i'\leq(n-1)/2$ and $i^2\equiv i'^2 \pmod n$. So, when n is composite, there are $0\leq i<i'\leq(n-1)/2$ such that

$$(i^2+dj^2)\left(\frac{i^2+dj^2}{n}\right)\equiv((i')^2+dj^2)\left(\frac{(i')^2+dj^2}{n}\right)\pmod n$$

for all $j=0,\ldots,(n-1)/2$, and hence (1.1) holds (since an integer matrix that has two rows congruent to each other modulo n must have a determinant congruent to 0 modulo n).

It thus remains to prove Theorem 1.1 in the case when n is a prime. So let us assume that n is a prime $p>3$.

Fix $j\in\{0,\ldots,(p-1)/2\}$. As $(\frac{a}{p})\equiv a^{(p-1)/2}\pmod p$ for all $a\in\mathbb{Z}$ (due to Euler), we have

$$\begin{aligned}&\sum_{i=1}^{(p-1)/2}(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\\ \equiv&\sum_{i=1}^{(p-1)/2}(i^2+dj^2)^{(p+1)/2}=\sum_{i=1}^{(p-1)/2}\ \sum_{k=0}^{(p+1)/2}\binom{(p+1)/2}{k}i^{2k}(dj^2)^{(p+1)/2-k}\\ =&\sum_{k=0}^{(p+1)/2}\binom{(p+1)/2}{k}(dj^2)^{(p+1)/2-k}\sum_{i=1}^{(p-1)/2}i^{2k}\pmod p.\end{aligned}$$

Multiplying this by 2, we obtain

$$\begin{aligned}&2\sum_{i=1}^{(p-1)/2}(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\\ \equiv&\sum_{k=0}^{(p+1)/2}\binom{(p+1)/2}{k}(dj^2)^{(p+1)/2-k}\cdot\sum_{i=1}^{(p-1)/2}(i^{2k}+(p-i)^{2k})\\ \equiv&\sum_{k=0}^{(p+1)/2}\binom{(p+1)/2}{k}(dj^2)^{(p+1)/2-k}\sum_{i=1}^{p-1}i^{2k}\pmod p.\end{aligned}\tag{2.1}$$

For each $k\in\{0,\ldots,(p+1)/2\}$, clearly

$$p-1\mid 2k\iff k=0\text{ or }k=(p-1)/2,$$

and hence by Lemma 2.1 we get

$$\sum_{i=1}^{p-1}i^{2k}\equiv\begin{cases}-1\pmod p & \text{if }k=0\text{ or }k=(p-1)/2,\\ 0\pmod p & \text{otherwise.}\end{cases}$$

Hence, (2.1) simplifies to

$$
\begin{aligned}
&2\sum_{i=1}^{(p-1)/2}(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\\
\equiv&\binom{(p+1)/2}{0}(dj^2)^{(p+1)/2}(-1)+\binom{(p+1)/2}{(p-1)/2}(dj^2)(-1)\\
\equiv&-dj^2\left(\left(\frac{dj^2}{p}\right)+\frac{p+1}{2}\right)\equiv-\frac{dj^2}{2}\left(\frac{dj^2}{p}\right)\left(2+\left(\frac{d}{p}\right)\right)\pmod p
\end{aligned}
$$

(where the last two congruence signs relied on $(\frac{a}{p})\equiv a^{(p-1)/2}\pmod p$ and on the easily verified congruence $dj^2\equiv dj^2(\frac{dj^2}{p})(\frac{d}{p})\pmod p$, respectively). In other words,

$$\sum_{i=1}^{(p-1)/2}\frac{4}{2+(\frac{d}{p})}(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)+(0^2+dj^2)\left(\frac{0^2+dj^2}{p}\right)\equiv 0\ (\mathrm{mod}\ p).$$

This congruence holds for all $j=0,\ldots,(p-1)/2$. Thus, if we add the last $(p-1)/2$ rows multiplied by $4/(2+(\frac{d}{p}))$ to the first row of the determinant

$$D:=\left|(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\right|_{0\le i,j\le(p-1)/2},$$

then all the entries in the first row of the resulting determinant are multiples of p. So we have $D\equiv 0\pmod p$ as desired.

In view of the above, this completes the proof of Theorem 1.1. □

3. A general formula for $|(x_i+y_j)^n|_{1\le i,j\le n}$

For each $k=1,\ldots,n$, the kth elementary symmetric polynomial σ_k in $x_1,\ldots,x_n$ is defined by

$$\sigma_k(x_1,\ldots,x_n)=\sum_{1\le i_1<\ldots<i_k\le n}\prod_{j=1}^{k}x_{i_j}.$$

In addition, we set $\sigma_0(x_1,\ldots,x_n)=1$ as usual.

To prove Theorem 1.2, we need the following auxiliary theorem which improves a result of [4, Section 354(a)].

Theorem 3.1. *Let n be a positive integer, and let $x_1, \ldots, x_n, y_1, \ldots, y_n$ be elements of any commutative ring with identity. Then*

$$\begin{aligned}|(x_i+y_j)^n|_{1\le i,j\le n} &= (-1)^{n(n-1)/2}\prod_{1\le i<j\le n}(x_j-x_i)(y_j-y_i)\\ &\times\sum_{k=0}^{n}\Bigg(\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}\Bigg)\sigma_k(x_1,\ldots,x_n)\sigma_{n-k}(y_1,\ldots,y_n),\end{aligned}\tag{3.1}$$

where $[0,n]$ denotes the set $\{0,\ldots,n\}$.

Proof. Define an $n\times(n+1)$-matrix A and an $(n+1)\times n$-matrix B by

$$A=\left[\binom{n}{k}x_i^k\right]_{\substack{1\le i\le n\\ 0\le k\le n}}\quad\text{and}\quad B=\left[y_j^{n-k}\right]_{\substack{0\le k\le n\\ 1\le j\le n}}.$$

As the binomial formula yields

$$(x_i+y_j)^n=\sum_{k=0}^{n}\binom{n}{k}x_i^k y_j^{n-k},$$

we have

$$AB=\left[(x_i+y_j)^n\right]_{1\le i,j\le n}.$$

Applying the Cauchy-Binet formula, we therefore get

$$\begin{aligned}&|(x_i+y_j)^n|_{1\le i,j\le n} &(3.2)\\ =&\sum_{k=0}^{n}\left|\binom{n}{j}x_i^j\right|_{\substack{1\le i\le n\\ j\in[0,n]\setminus\{k\}}}\left|y_j^{n-i}\right|_{\substack{1\le j\le n\\ i\in[0,n]\setminus\{k\}}}\\ =&\sum_{k=0}^{n}\Bigg(\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}\Bigg)\left|x_j^i\right|_{\substack{i\in[0,n]\setminus\{k\}\\ 1\le j\le n}}\times(-1)^{n(n-1)/2}\left|y_j^i\right|_{\substack{i\in[0,n]\setminus\{n-k\}\\ 1\le j\le n}}\end{aligned}\tag{3.3}$$

(by standard properties of determinants). For each $k\in\{0,\ldots,n\}$, comparing the coefficient of x^k on both sides of the polynomial equality

$$\begin{vmatrix}1 & 1 & \cdots & 1 & 1\\ x_1 & x_2 & \cdots & x_n & x\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ x_1^{n-1} & x_2^{n-1} & \cdots & x_n^{n-1} & x^{n-1}\\ x_1^n & x_2^n & \cdots & x_n^n & x^n\end{vmatrix}=\prod_{1\le i<j\le n}(x_j-x_i)\times\prod_{i=1}^{n}(x-x_i)$$

(a consequence of Vandermonde's determinant), we find that

$$(-1)^{n-k}\left|x_j^i\right|_{\substack{i\in[0,n]\setminus\{k\}\\ 1\le j\le n}}=(-1)^{n-k}\sigma_{n-k}(x_1,\ldots,x_n)\prod_{1\le i<j\le n}(x_j-x_i)$$

(where the left-hand side was computed by expanding the determinant along its last column). Hence,

$$\left|x_j^i\right|_{\substack{i\in[0,n]\setminus\{k\}\\1\le j\le n}} = \sigma_{n-k}(x_1,\ldots,x_n)\prod_{1\le i<j\le n}(x_j-x_i).$$

Similarly,

$$\left|y_j^i\right|_{\substack{i\in[0,n]\setminus\{n-k\}\\1\le j\le n}} = \sigma_k(y_1,\ldots,y_n)\prod_{1\le i<j\le n}(y_j-y_i).$$

Therefore, we can rewrite (3.3) as

$$\begin{aligned}|(x_i+y_j)^n|_{1\le i,j\le n} =&(-1)^{n(n-1)/2}\prod_{1\le i<j\le n}(x_j-x_i)(y_j-y_i)\\ &\times\sum_{k=0}^{n}\Bigg(\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}\Bigg)\sigma_{n-k}(x_1,\ldots,x_n)\sigma_k(y_1,\ldots,y_n).\end{aligned}$$

Substituting $n-k$ for k on the right-hand side, and observing that $\prod_{r\in[0,n]\setminus\{n-k\}}\binom{n}{r}=\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}$, we obtain the desired (3.1). □

4. Proof of Theorem 1.2

Proof of Theorem 1.2. Clearly (1.4) holds if $a_n', b_n' \in \mathbb{Z}$.

(i) Let us first discuss a_n and $a_n' \in \mathbb{Z}$. We can easily verify the desired result for $n = 3, 4$; so let us assume that $n \ge 5$.

Define

$$S(n) := \sum_{k=0}^{n}\sigma_k(0,\ldots,n-1)\sigma_{n-k}(d0+c,\ldots,d(n-1)+c)\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r},$$

which is positive if $c \ge 0$ and $d > 0$. Applying Theorem 3.1, we find that

$$\begin{aligned}a_n =&(-1)^{n(n-1)/2}\prod_{0\le i<j\le n-1}(j-i)(dj-di)\times S(n)\\ =&(-d)^{n(n-1)/2}S(n)\prod_{j=1}^{n-1}(j!)^2.\end{aligned}$$

Hence, $(-1)^{n(n-1)/2}a_n > 0$ if $c \ge 0$ and $d > 0$. To prove $a_n' \in \mathbb{Z}$ it suffices to show that

$$1!2!\ldots(n-3)!S(n) \equiv 0 \pmod{n^2}. \tag{4.1}$$

Fix $k \in [0, n]$. The product $\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}$ contains at least two of the three factors $\binom{n}{1}$, $\binom{n}{2}$ and $\binom{n}{n-1}$ (since $n \ge 5$). But each of these three factors is divisible by n or (in the case of the second factor) by

$n/2$ (when n is even). Thus, the product $\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}$ is divisible by $n\cdot n$ or (when n is even) by $n\cdot(n/2)$. In either case, it follows that $2\cdot\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}$ is divisible by n^2. Since $n\ge 5$ yields $2\mid 1!2!\dots(n-3)!$, we thus conclude that $1!2!\dots(n-3)!\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}$ is divisible by n^2. Since we have shown this for all $k\in[0,n]$, it follows that $1!2!\dots(n-3)!S(n)$ is divisible by n^2. This proves (4.1).

(ii) For $n=3,\dots,8$ we can verify directly the desired result for b_n and b_n'.

Now we assume $n\ge 9$ and define

$$\begin{aligned}T(n):=&\sum_{k=0}^{n}\sigma_k(0^2,\dots,(n-1)^2)\sigma_{n-k}(d0^2,\dots,d(n-1)^2)\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r}\\ =&\sum_{k=1}^{n-1}d^{n-k}\sigma_k(0^2,\dots,(n-1)^2)\sigma_{n-k}(0^2,\dots,(n-1)^2)\prod_{r\in[0,n]\setminus\{k\}}\binom{n}{r},\end{aligned}$$

which is positive if $d>0$ and always satisfies $d\mid S(n)$. In view of Theorem 3.1,

$$\begin{aligned}\left|(i^2+dj^2)^n\right|_{0\le i,j\le n-1}=&(-1)^{n(n-1)/2}\prod_{0\le i<j\le n-1}(j^2-i^2)(dj^2-di^2)\times T(n)\\ =&(-d)^{n(n-1)/2}T(n)\prod_{j=1}^{n-1}((2j-1)!j)^2\end{aligned}$$

and so

$$b_n=(-d)^{n(n-1)/2}T(n)((n-1)!)^2\prod_{j=1}^{n-1}((2j-1)!)^2. \tag{4.2}$$

Thus $(-1)^{n(n-1)/2}b_n>0$ if $d>0$. Also, (4.2) yields

$$\begin{aligned}(-1)^{n(n-1)/2}b_n'=&\frac{(n-1)!^2\prod_{j=1}^{n-1}(2j-1)!}{(2n-1)!\times 2\prod_{k=1}^{n}k!}T(n)\\ =&\frac{\prod_{k=1}^{n-2}\frac{(2k-1)!}{k!}}{2n(2n-1)(2n-2)}T(n).\end{aligned} \tag{4.3}$$

As $n+4\le 2n-5$ and one of $n+1,n+2,n+3,n+4$ is divisible by 4, we have

$$4(n-1)n\ \Bigg|\ \frac{(2(n-2)-1)!}{(n-2)!}.$$

Therefore, (4.3) leads to $(2n-1)b_n'\in\mathbb{Z}$. If we can furthermore show that $2n(2n-2)b_n'\in\mathbb{Z}$, then we will conclude that $b_n'\in\mathbb{Z}$ (since $2n-1$

is coprime to $2n(2n-2)$). So it remains to show that $2n(2n-2)b_n' \in \mathbb{Z}$, i.e., that $2n-1 \mid T(n)\prod_{k=1}^{n-2}\frac{(2k-1)!}{k!}$.

If $2n-1 = pq$ with $p, q \in \mathbb{Z}^+$ and $3 \le p < q$, then $p < q \le \frac{2n-1}{3} \le n-3$, and hence $2n-1 = pq$ divides

$$\frac{(2(p-1)-1)!}{(p-1)!} \times \frac{(2(q-1)-1)!}{(q-1)!}.$$

If $2n-1 = p^2$ with p an odd prime, then $5 \le p = \sqrt{2n-1} < n-2$ since $2n-1 > n \ge 9$, hence $2n-1 = p^2$ divides

$$\frac{(2(p-2)-1)!}{(p-2)!} \times \frac{(2(p-1)-1)!}{(p-1)!}.$$

If $2n-1$ is a prime p, then $p > 3$ and

$$\begin{aligned} b_n &= \left|(i^2+dj^2)^{(p+1)/2}\right|_{0\le i,j\le(p-1)/2} \\ &\equiv \left|(i^2+dj^2)\left(\frac{i^2+dj^2}{p}\right)\right|_{0\le i,j\le(p-1)/2} \\ &\equiv 0 \pmod{p} \end{aligned}$$

by Theorem 1.1, hence $2n-1 = p$ divides $T(n)$ by (4.2) and due to $d \mid T(n)$. In either case, we obtain $2n-1 \mid T(n)\prod_{k=1}^{n-2}\frac{(2k-1)!}{k!}$.

The proof of Theorem 1.2 is now complete. □

5. Proof of Theorem 1.3

We need the following known lemma (see [6, Lemma 2.3]):

Lemma 5.1. *Let p be a prime with $p \equiv 1 \pmod 4$, and write $n = (p-1)/2$. Then*

$$\left(\frac{n!}{p}\right) = \left(\frac{2}{p}\right).$$

Proof of Theorem 1.3. For convenience we set $n = (p-1)/2$. Applying Theorem 3.1, we see that

$$\begin{aligned}
&\left|(i^2+dj^2+c)^n\right|_{1\le i,j\le n}\\
=&(-1)^{n(n-1)/2}\prod_{1\le i<j\le n}(j^2-i^2)(dj^2+c-(di^2+c))\times\prod_{r=0}^{n}\binom{n}{r}\\
&\times\sum_{k=0}^{n}\frac{\sigma_k(1^2,\ldots,n^2)\sigma_{n-k}(d1^2+c,\ldots,dn^2+c)}{\binom{n}{k}}\\
=&(-d)^{n(n-1)/2}\prod_{1\le i<j\le n}(j^2-i^2)^2\times\prod_{r=0}^{n}\binom{n}{r}\times R_n, \qquad (5.1)
\end{aligned}$$

where

$$\begin{aligned}
R_n :=&\sigma_n(1^2,\ldots,n^2)+\sigma_n(d1^2+c,\ldots,dn^2+c)\\
&+\sum_{0<k<n}\frac{\sigma_k(1^2,\ldots,n^2)\sigma_{n-k}(d1^2+c,\ldots,dn^2+c)}{\binom{n}{k}}. \qquad (5.2)
\end{aligned}$$

As observed in [6, (3.2)], we have the polynomial congruence

$$\begin{aligned}
&\sum_{k=0}^{n}(-1)^k\sigma_k(1^2,\ldots,n^2)x^{n-k}\\
=&\prod_{r=1}^{n}(x-r^2)\equiv x^n-1 \pmod p. \qquad (5.3)
\end{aligned}$$

So $\sigma_n(1^2,\ldots,n^2)\equiv-(-1)^n \pmod p$ and $\sigma_k(1^2,\ldots,n^2)\equiv 0 \pmod p$ for all $k=1,\ldots,n-1$. Note also that $p\nmid\binom{n}{k}$ for all $k=0,\ldots,n$. Therefore, (5.2) yields

$$\begin{aligned}
&R_n+(-1)^n\\
\equiv&\sigma_n(d1^2+c,\ldots,dn^2+c)=\prod_{r=1}^{n}(c+dr^2)=(-d)^n\prod_{r=1}^{n}\left(-\frac{c}{d}-r^2\right)\\
\equiv&(-d)^n\left(\left(-\frac{c}{d}\right)^n-1\right)=c^n-(-d)^n\equiv\left(\frac{c}{p}\right)-\left(\frac{-d}{p}\right) \pmod p,
\end{aligned}$$

where we have used (5.3) in the third-to-last congruence. Solving this for R_n and substituting the result into (5.1), and noting that the left-hand side of (5.1) is congruent to $S_c(d,p)$ modulo p (since

$(\frac{a}{p}) \equiv a^n \pmod p$ for all $a \in \mathbb{Z}$), we find

$$\begin{aligned} &S_c(d,p)\\ \equiv&(-d)^{n(n-1)/2}\left(\prod_{1\le i<j\le n}(j^2-i^2)^2\right)\times\prod_{r=0}^{n}\binom{n}{r}\\ &\times\left(\left(\frac{c}{p}\right)-\left(\frac{-d}{p}\right)-(-1)^n\right) \pmod p. \end{aligned}\tag{5.4}$$

Clearly,

$$\prod_{r=0}^{n}\binom{n}{r}=\frac{n!^{n+1}}{(0!1!\cdots n!)^2},$$

whence

$$\left(\frac{\prod_{r=0}^{n}\binom{n}{r}}{p}\right)=\left(\frac{n!^{n+1}}{p}\right)=\left(\frac{n!}{p}\right)^{n+1}=\left(\frac{2}{p}\right)^{n+1}$$

by Lemma 5.1. In view of Gauss's known identity $(\frac{2}{p})=(-1)^{(p^2-1)/8}=(-1)^{n(n+1)/2}$, we can rewrite this as

$$\left(\frac{\prod_{r=0}^{n}\binom{n}{r}}{p}\right)=((-1)^{n(n+1)/2})^{n+1}=(-1)^{n(n+1)^2/2}.$$

Hence, (5.4) yields

$$\left(\frac{S_c(d,p)}{p}\right)=\left(\frac{-d}{p}\right)^{n(n-1)/2}(-1)^{n(n+1)^2/2}\left(\frac{(\frac{c}{p})-(\frac{-d}{p})-(-1)^n}{p}\right).\tag{5.5}$$

Note that $(\frac{-1}{p})=(-1)^n$ and

$$(-1)^{n(n+1)^2/2-n^2(n-1)/2}=(-1)^{n(3n+1)/2}=(-1)^{n(n-1)/2}.$$

So (5.5) can be rewritten as

$$\left(\frac{S_c(d,p)}{p}\right)=(-1)^{n(n-1)/2}\left(\frac{d}{p}\right)^{n(n-1)/2}\left(\frac{(\frac{c}{p})-(-1)^n(1+(\frac{d}{p}))}{p}\right).\tag{5.6}$$

Now it remains to deduce (1.6) from (5.6).

Case 1. $(\frac{c}{p})=1$ and $(\frac{d}{p})=-1$.

In this case, (5.6) becomes

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

Case 2. $(\frac{c}{p})=(\frac{d}{p})=-1$.

In this case, (5.6) gives

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

Case 3. $(\frac{-c}{p}) = (\frac{d}{p}) = 1$.

In this case, $(\frac{c}{p}) = (\frac{-1}{p}) = (-1)^n$. Hence, (5.6) yields

$$\begin{aligned}\left(\frac{S_c(d,p)}{p}\right) &= (-1)^{n(n-1)/2}\left(\frac{(-1)^n-(-1)^n 2}{p}\right) = (-1)^{n(n+1)/2-n}\left(\frac{-1}{p}\right)^{n+1} \\ &= (-1)^{(p^2-1)/8}(-1)^n(-1)^{n(n+1)} = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right).\end{aligned}$$

Case 4. $(\frac{-c}{p}) = -1$ and $(\frac{d}{p}) = 1$.

In this case, $(\frac{c}{p}) = -(\frac{-1}{p}) = -(-1)^n$. Hence, by (5.6) we have

$$\begin{aligned}\left(\frac{S_c(d,p)}{p}\right) &= (-1)^{n(n-1)/2}\left(\frac{-(-1)^n-(-1)^n 2}{p}\right) \\ &= (-1)^{n(n+1)/2-n}\left(\frac{-1}{p}\right)^{n}\left(\frac{-3}{p}\right) \\ &= (-1)^{n(n+1)/2}(-1)^n\left((-1)^n\right)^n\left(\frac{-3}{p}\right) \\ &= (-1)^{n(n+1)/2}\left(\frac{-3}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-3}{p}\right) = \left(\frac{-6}{p}\right).\end{aligned}$$

In view of the above, (1.6) holds as desired. This concludes the proof. □

Acknowledgment. We thank Prof. Guo-Niu Han for helpful comments.

References

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

[2] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd edition, Grad. Texts Math., vol. 84, Springer, New York, 1990.

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

[4] T. Muir and W. H. Metzler, A Treatise on the Theory of Determinants, Dover Publ. Inc., New York, 1960.

[5] Z.-W. Sun, Sequence A228379 at OEIS (On-Line Encyclopedia of Integer Sequences), August 21, 2013. `http://oeis.org/A228379`.

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

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

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

(Darij Grinberg) Mathematics Department, Drexel University, Philadelphia, PA, USA
E-mail address: darijgrinberg@gmail.com

(Zhi-Wei Sun) Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: zwsun@nju.edu.cn

(Lilu Zhao) School of Mathematics, Shandong University, Jinan 250100, People's Republic of China
E-mail address: zhaolilu@sdu.edu.cn