ON SOME DETERMINANTS WITH LEGENDRE SYMBOL ENTRIES

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/∼zwsun

ABSTRACT. In this paper we mainly focus on some determinants with Legendre symbol entries. Let p be an odd prime and let $(\frac{\cdot}{p})$ be the Legendre symbol. We show that $(\frac{-S(d,p)}{p}) = 1$ for any $d \in \mathbb{Z}$ with $(\frac{d}{p}) = 1$, and that

$$
\left(\frac{W_p}{p}\right) = \begin{cases} (-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{\lfloor (p+1)/8 \rfloor} & \text{if } p \equiv 3 \pmod 4, \end{cases}
$$

where

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

and

$$
W_p = \det\left[\left(\frac{i^2 - ((p-1)/2)!j}{p}\right)\right]_{0 \leqslant i,j \leqslant (p-1)/2}.
$$

We also pose some conjectures on determinants, one of which states that $(-1)^{\lfloor (p+1)/8 \rfloor} W_p$ is a square when $p \equiv 3 \pmod 4$.

1. INTRODUCTION

For an $n \times n$ matrix $A = (a_{ij})_{0 \leqslant i,j \leqslant n-1}$ over the field of complex numbers, we often write the determinant $\det A$ (or $|A|$) in the form $|a_{ij}|_{0 \leqslant i,j \leqslant n-1}$. In this paper we study determinants with Legendre symbol entries.

1

Let p be an odd prime and let $(\frac{\cdot}{p})$ be the Legendre symbol. The circulant determinant

$$\left| \left(\frac{j-i}{p} \right) \right|_{0 \leqslant i,j \leqslant p-1} = \begin{vmatrix} (\frac{0}{p}) & (\frac{1}{p}) & (\frac{2}{p}) & \cdots & (\frac{p-1}{p}) \\ (\frac{p-1}{p}) & (\frac{0}{p}) & (\frac{1}{p}) & \cdots & (\frac{p-2}{p}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (\frac{1}{p}) & (\frac{2}{p}) & (\frac{3}{p}) & \cdots & (\frac{0}{p}) \end{vmatrix}$$

takes the value

$$\prod_{r=0}^{p-1} \sum_{k=0}^{p-1} \left(\frac{k}{p} \right) (e^{2\pi i r/p})^k = 0$$

since $\sum_{k=0}^{p-1}(\frac{k}{p}) = 0$. (See [K99, (2.41)] for the evaluation of a general circulant determinant.) For the matrix $A = (a_{ij})_{1 \leqslant i,j \leqslant p-1}$ with $a_{ij} = (\frac{i-j}{p})$, L. Carlitz [C59, Theorem 4] proved that its characteristic polynomial is

$$|xI_{p-1} - A| = \left(x^2 - \left(\frac{-1}{p} \right) p \right)^{(p-3)/2} \left(x^2 - \left(\frac{-1}{p} \right) \right),$$

where I_{p-1} is the $(p-1) \times (p-1)$ identity matrix. Putting $x = 0$ in Carlitz's formula, we obtain that

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

For $m \in \mathbb{Z}$ let $\{m\}_p$ denote the least nonnegative residue of an integer m modulo p. For any integer $a \not\equiv 0 \pmod{p}$, $\{aj\}_p$ ($j = 1, \ldots, p-1$) is a permutation of $1, \ldots, p-1$, and its sign is the Legendre symbol $(\frac{a}{p})$ by Zolotarev's lemma (cf. [DH] and [Z]). Therefore, for any integer $d \not\equiv 0 \pmod{p}$ we have

$$\left| \left(\frac{i+dj}{p} \right) \right|_{0 \leqslant i,j \leqslant p-1} = \left| \left(\frac{i - \{-dj\}_p}{p} \right) \right|_{0 \leqslant i,j \leqslant p-1}$$
$$= \left(\frac{-d}{p} \right) \left| \left(\frac{i-j}{p} \right) \right|_{0 \leqslant i,j \leqslant p-1} = 0 \quad (1.1)$$

and

$$\left| \left(\frac{i+dj}{p} \right) \right|_{1 \leqslant i,j \leqslant p-1} = \left(\frac{-d}{p} \right) \left| \left(\frac{i-j}{p} \right) \right|_{1 \leqslant i,j \leqslant p-1} = \left(\frac{-d}{p} \right) p^{(p-3)/2}. \quad (1.2)$$

Let p be an odd prime. In 2004, R. Chapman [Ch04] used quadratic Gauss sums to determine the values of

$$\left| \left(\frac{i+j-1}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2} \quad \text{and} \quad \left| \left(\frac{i+j-1}{p} \right) \right|_{1 \leqslant i,j \leqslant (p+1)/2}.$$

Since $(p+1)/2 - i + (p+1)/2 - j - 1 \equiv -(i+j) \pmod{p}$, we see that

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

and

$$\left| \left(\frac{i+j-1}{p} \right) \right|_{1 \leqslant i,j \leqslant (p+1)/2} = \left| \left(\frac{i+j}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2}. \tag{1.3}$$

Let ε_p and $h(p)$ stand for the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively, and write

$$\varepsilon_p^{(2-(\frac{2}{p}))h(p)} = r_p + s_p\sqrt{p} \text{ with } r_p, s_p \in \mathbb{Q}.$$

Chapman [Ch12] conjectured that

$$\left| \left(\frac{j-i}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2} = \begin{cases} -r_p & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.4}$$

As Chapman could not solve this problem for several years, he called the determinant *evil* (cf. [Ch12]). Chapman's conjecture on his "evil" determinant was finally confirmed by M. Vsemirnov [V12, V13] via matrix decomposition. We guess that if $p \equiv 3 \pmod 4$ then $|x + (\frac{j-i}{p})|_{1 \leqslant i,j \leqslant (p-1)/2} = x$.

Let $p \equiv 1 \pmod 4$ be a prime. In an unpublished manuscript [Ch03] written in 2003, Chapman conjectured that

$$s_p = \left(\frac{2}{p} \right) \left| \left(\frac{j-i}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2}. \tag{1.5}$$

Note that (1.4) and (1.5) together yield an interesting identity

$$\varepsilon_p^{(2-(\frac{2}{p}))h(p)} = \left(\frac{2}{p} \right) \left| \left(\frac{j-i}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2} \sqrt{p} - \left| \left(\frac{j-i}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2}.$$

Taking the norm with respect to the field extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$, we are led to the identity

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

since $N(\varepsilon_p) = -1$ and $2 \nmid h(p)$ (cf. Theorem 3 of [Co62, p. 185] and Theorem 6 of [Co62, p. 187]). This provides an *explicit* solution to the Diophantine equation $x^2 - py^2 = -1$ with $x, y \in \mathbb{Z}$.

Now we state our first theorem on evaluations of certain determinants over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with p prime.

Theorem 1.1. *Let p be an odd prime. For $d \in \mathbb{Z}$ define*

$$R(d,p) := \left| \left(\frac{i+dj}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2}. \qquad (1.6)$$

If $p \equiv 1 \pmod 4$, then

$$R(d,p) \equiv \left(\left(\frac{d}{p} \right) d \right)^{(p-1)/4} \frac{p-1}{2}! \pmod p. \qquad (1.7)$$

When $p \equiv 3 \pmod 4$, we have

$$R(d,p) \equiv \begin{cases} \left(\frac{2}{p} \right) \pmod p & \text{if } \left(\frac{d}{p} \right) = 1, \\ 1 \pmod p & \text{if } \left(\frac{d}{p} \right) = -1. \end{cases} \qquad (1.8)$$

For the general odd prime p, we have

$$R(-d,p) \equiv \left(\frac{2}{p} \right) R(d,p) \pmod p, \qquad (1.9)$$

and

$$\left| \left(\frac{i+dj+c}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2} \equiv R(d,p) \pmod p \quad \text{for all } c \in \mathbb{Z}. \qquad (1.10)$$

Remark 1.1. (a) By Wilson's theorem, for any odd prime p we have

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

(b) For a general integer d, we have not found any interesting pattern for the exact values of $R(d,p)$ with $p > 2$ prime. For example, below are the values of $R(4,p)$ with p prime and $2 < p \leqslant 41$.

$$R(4,3) = -1, \ R(4,5) = -2, \ R(4,7) = 1, \ R(4,11) = 32, \ R(4,13) = 8,$$
$$R(4,17) = -72, \ R(4,19) = -2^7 \cdot 3 \cdot 5, \ R(4,23) = -2^5 \cdot 2719,$$
$$R(4,29) = -2^7 \cdot 7 \cdot 1301, \ R(4,31) = -2^7 \cdot 83 \cdot 1433,$$
$$R(4,37) = 2^9 \cdot 3 \cdot 14479, \ R(4,41) = 2^9 \cdot 38913779.$$

Corollary 1.1. *Let $p \equiv 1 \pmod 4$ be a prime, and write $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$ with $2a_p, 2b_p \in \mathbb{Z}$. Then*

$$a_p \equiv -\frac{p-1}{2}! \pmod p. \tag{1.11}$$

Proof. By (1.7) we have

$$R(1,p) \equiv \frac{p-1}{2}! \pmod p.$$

On the other hand, in view of (1.3) and Chapman [Ch04, Corollary 3],

$$R(1,p) = \left| \left(\frac{i+j-1}{p} \right) \right|_{1 \leqslant i,j \leqslant (p+1)/2} = -\left(\frac{2}{p} \right) 2^{(p-1)/2} a_p.$$

So (1.11) is valid. □

It is well known that for any odd prime p the $(p-1)/2$ squares

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2} \right)^2$$

give all the $(p-1)/2$ quadratic residues modulo p. So we think that it's natural to consider some determinants with Legendre symbol (or Jacobi symbol) entries related to binary quadratic forms.

For any integer d and odd integer $n > 1$, we define

$$S(d,n) := \left| \left(\frac{i^2 + dj^2}{n} \right) \right|_{1 \leqslant i,j \leqslant (n-1)/2} \tag{1.12}$$

and

$$T(d,n) := \left| \left(\frac{i^2 + dj^2}{n} \right) \right|_{0 \leqslant i,j \leqslant (n-1)/2}, \tag{1.13}$$

where $\left(\frac{\cdot}{n} \right)$ is the Jacobi symbol.

Theorem 1.2. (i) *Let $n > 1$ be an odd composite number. Then, for any $d \in \mathbb{Z}$ we have $S(d,n) = T(d,n) = 0$.*

(ii) *Let p be an odd prime and let $c,d \in \mathbb{Z}$ with $p \nmid c$. Then*

$$S(c^2 d, p) = \left(\frac{c}{p} \right)^{(p+1)/2} S(d,p) \quad and \quad T(c^2 d, p) = \left(\frac{c}{p} \right)^{(p+1)/2} T(d,p). \tag{1.14}$$

Also,

$$\left(\frac{d}{p} \right) = -1 \quad implies \quad S(d,p) = 0. \tag{1.15}$$

When $p \equiv 1 \pmod 4$, we have

$$S(-d, p) = \left(\frac{2}{p}\right) S(d, p) \quad and \quad T(-d, p) = \left(\frac{2}{p}\right) T(d, p). \tag{1.16}$$

(iii) *Let p be an odd prime and let $d \in \mathbb{Z}$. Then*

$$\left(\frac{T(d, p)}{p}\right) = \begin{cases} \left(\frac{2}{p}\right) & if \left(\frac{d}{p}\right) = 1, \\ 1 & if \left(\frac{d}{p}\right) = -1. \end{cases} \tag{1.17}$$

Also,

$$T(-d, p) \equiv \left(\frac{2}{p}\right) T(d, p) \pmod p \tag{1.18}$$

and

$$\left| \left(\frac{i^2 + dj^2 + c}{p}\right) \right|_{0 \leqslant i, j \leqslant (p-1)/2} \equiv T(d, p) \pmod p \quad for \ all \ c \in \mathbb{Z}. \tag{1.19}$$

Moreover, when $\left(\frac{d}{p}\right) = 1$, we have

$$S(d, p) = \frac{2}{p-1} T(d, p) \quad and \quad \left(\frac{-S(d, p)}{p}\right) = 1. \tag{1.20}$$

Remark 1.2. By Theorem 1.2(iii), for any odd prime p the number $-S(1, p) = 2T(1, p)/(1 - p)$ is a quadratic residue mod p. We note that $-S(1, p)$ is not always a square, and will pose a related conjecture in Section 4.

Example 1.1. Note that

$$S(1, 11) = \begin{vmatrix} -1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 \end{vmatrix} = -4^2 \ \ with \ \left(\frac{-S(1, 11)}{11}\right) = 1,$$

and

$$S(2, 13) = \begin{vmatrix} 1 & 1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 \end{vmatrix} = 0 \ \ with \ \left(\frac{2}{13}\right) = -1.$$

For any positive odd integer n and integers c and d, we define

$$(c,d)_n := \left| \left(\frac{i^2 + cij + dj^2}{n} \right) \right|_{1 \leqslant i,j \leqslant n-1} \tag{1.21}$$

and

$$[c,d]_n := \left| \left(\frac{i^2 + cij + dj^2}{n} \right) \right|_{0 \leqslant i,j \leqslant n-1}. \tag{1.22}$$

It is easy to see that $(-c,d)_n = (\frac{-1}{n})(c,d)_n$.

Now we present our third theorem.

Theorem 1.3. *Let $c,d \in \mathbb{Z}$.*
(i) *We have $(c,d)_n = 0$ for any positive odd integer n with $(\frac{d}{n}) = -1$.*
(ii) *If p is an odd prime with $(\frac{d}{p}) = 1$, then*

$$[c,d]_p = \begin{cases} \frac{p-1}{2}(c,d)_p & \text{if } p \nmid c^2 - 4d, \\ \frac{1-p}{p-2}(c,d)_p & \text{if } p \mid c^2 - 4d. \end{cases} \tag{1.23}$$

Now we state two more theorems.

Theorem 1.4. (i) *For any odd prime p, we have*

$$\left| \frac{\left(\frac{i+j}{p} \right)}{i+j} \right|_{1 \leqslant i,j \leqslant (p-1)/2} \equiv \begin{cases} \left(\frac{2}{p} \right) \pmod{p} & \text{if } p \equiv 1 \pmod{4}, \\ ((p-1)/2)! \pmod{p} & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{1.24}$$

(ii) *Let $p \equiv 3 \pmod 4$ be a prime. Then*

$$\left| \frac{1}{i^2 + j^2} \right|_{1 \leqslant i,j \leqslant (p-1)/2} \equiv \left(\frac{2}{p} \right) \pmod{p}. \tag{1.25}$$

Remark 1.3. Similar to Theorem 1.4(ii), for any prime $p \equiv 5 \pmod 6$ we conjecture that $2 | \frac{1}{i^2 - ij + j^2}|_{1 \leqslant i,j \leqslant p-1}$ is a quadratic residue modulo p and the p-adic order of $|\frac{1}{i^2 - ij + j^2}|_{1 \leqslant i,j \leqslant (p-1)/2}$ is $(p+1)/6$. This has been verified for $p < 500$.

Theorem 1.5. *For any odd prime p, we have*

$$\left(\frac{W_p}{p} \right) = \begin{cases} (-1)^{|\{0 < k < \frac{p}{4}: (\frac{k}{p})=-1\}|} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{\lfloor (p+1)/8 \rfloor} & \text{if } p \equiv 3 \pmod{4}, \end{cases} \tag{1.26}$$

where

$$W_p := \left| \left(\frac{i^2 - \frac{p-1}{2}!j}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2}. \tag{1.27}$$

Remark 1.4. Below are the values of W_p for the first 6 odd primes p:

$$W_3 = 1, \ W_5 = -1, \ W_7 = -4, \ W_{11} = -16, \ W_{13} = -288, \ W_{17} = -840.$$

See also Conjecture 4.1 inspired by Theorem 1.5.

We are going to show Theorems 1.1-1.3 and Theorems 1.4-1.5 in Sections 2 and 3 respectively, and pose some new conjectures on determinants in Section 4.

2. PROOF OF THEOREMS 1.1-1.3

Lemma 2.1 ([K05, Lemma 9]). *Let* $P(z) = \sum_{k=0}^{n-1} a_k z^k$ *be a polynomial with complex coefficients. Then we have*

$$|P(x_i + y_j)|_{1 \leqslant i,j \leqslant n} = a_{n-1}^n \prod_{k=0}^{n-1} \binom{n-1}{k} \times \prod_{1 \leqslant i < j \leqslant n} (x_i - x_j)(y_j - y_i). \quad (2.1)$$

Remark 2.1. This lemma remains valid over any commutative ring as pointed out by one of the referees.

Proof of Theorem 1.1. Set $n = (p-1)/2$. For any $c \in \mathbb{Z}$, we have

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

and

$$|(i + dj + c)^n|_{0 \leqslant i,j \leqslant n} = |(i + dj + c - d - 1)^n|_{1 \leqslant i,j \leqslant n+1}$$

$$= \prod_{k=0}^{n} \binom{n}{k} \times \prod_{1 \leqslant i < j \leqslant n+1} (i - j)(dj + c - d - 1 - (di + c - d - 1))$$

$$= \frac{(n!)^{n+1}}{\prod_{k=0}^{n} k!(n-k)!} (-d)^{n(n+1)/2} \prod_{1 \leqslant i < j \leqslant n+1} (j - i)^2 = (-d)^{n(n+1)/2} (n!)^{n+1}$$

with the help of Lemma 2.1. Therefore (1.10) holds, and also

$$R(d, p) \equiv (-d)^{(p^2-1)/8} \left(\frac{p-1}{2}! \right)^{(p+1)/2} \pmod{p}. \quad (2.2)$$

In the case $p \equiv 1 \pmod 4$, by (2.2) and Remark 1.1(a) we have (1.7) since

$$R(d, p) \equiv (-d)^{(p-1)/4 \times (p+1)/2} \frac{p-1}{2}! \left(\frac{p-1}{2}! \right)^{2(p-1)/4}$$

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

In the case $p \equiv 3 \pmod 4$, by (2.2) and Remark 1.1(a) we obtain

$$R(d,p) \equiv (-d)^{(p-1)/2 \times (p+1)/4} \left(\frac{p-1}{2}! \right)^{2(p+1)/4} \equiv \left(\frac{-d}{p} \right)^{(p+1)/4} \pmod p$$

and hence (1.8) follows.

Now it remains to show (1.9) which holds trivially when $p \mid d$. If $p \equiv 1 \pmod 4$, then by (1.7) we get

$$R(-d,p) \equiv \left(\left(\frac{-d}{p} \right) (-d) \right)^{(p-1)/4} \frac{p-1}{2}! \equiv \left(\frac{2}{p} \right) R(d,p) \pmod p.$$

If $p \equiv 3 \pmod 4$, then $(\frac{-d}{p}) = -(\frac{d}{p})$ and hence we get (1.9) from (1.8).

The proof of Theorem 1.1 is now complete. $\square$

Motivated by Zolotarev's lemma, in 2006 H. Pan obtained the following lemma.

Lemma 2.2 (H. Pan [P06]). *Let $n > 1$ be an odd integer and let c be any integer relatively prime to n. For each $j = 1, \ldots, (n-1)/2$ let $\pi_c(j)$ be the unique $r \in \{1, \ldots, (n-1)/2\}$ with cj congruent to r or $-r$ modulo n. For the permutation π_c on $\{1, \ldots, (n-1)/2\}$, its sign is given by*

$$\operatorname{sign}(\pi_c) = \left(\frac{c}{n} \right)^{(n+1)/2}. \tag{2.3}$$

Lemma 2.3. *Let $p \equiv 1 \pmod 4$ be a prime. Then*

$$\left(\frac{((p-1)/2)!}{p} \right) = \left(\frac{2}{p} \right). \tag{2.4}$$

Proof. Since

$$(-4)^{(p-1)/4} = (-1)^{(p-1)/4} \times 2^{(p-1)/2} = \left(\frac{2}{p} \right) 2^{(p-1)/2} \equiv 1 \pmod p,$$

by Remark 1.1(a) there is an integer x such that

$$x^4 \equiv -4 \equiv 4 \left(\frac{p-1}{2}! \right)^2 \pmod p, \quad \text{i.e.,} \quad x^2 \equiv \pm 2 \times \frac{p-1}{2}! \pmod p.$$

Therefore (2.4) holds. $\square$

Proof of Theorem 1.2. (i) If $n = p^2$ for some odd prime p, then $1 < p+1 \leqslant (p+1)(p-1)/2 = (n-1)/2$ and

$$\left(\frac{1^2 + dj^2}{p^2} \right) = \left(\frac{(p+1)^2 + dj^2}{p^2} \right) \quad \text{for all } j \in \mathbb{Z}.$$

If $n = pm$ with p an odd prime and m an odd integer greater than p, then for $i_1 = (m-p)/2$ and $i_2 = (m+p)/2$ we have

$$1 \leqslant i_1 < i_2 < m = \frac{n}{p} < \frac{n}{2}, \quad i_2^2 - i_1^2 = pm = n,$$

and

$$\left(\frac{i_1^2 + dj^2}{n}\right) = \left(\frac{i_2^2 + dj^2}{n}\right) \quad \text{for all } j \in \mathbb{Z}.$$

Therefore $S(d,n) = T(d,n) = 0$.

(ii) Define the permutation π_c as in Lemma 2.2 with $n = p$. In view of (2.3), we have

$$S(c^2 d, p) = \left| \left(\frac{i^2 + d\pi_c(j)^2}{p}\right) \right|_{1 \leqslant i,j \leqslant p-1/2} = \left(\frac{c}{p}\right)^{(p+1)/2} S(d,p)$$

as well as the second equality in (1.14). Similarly, if $p \nmid d$ then

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

and hence (1.15) holds.

Now we assume that $p \equiv 1 \pmod 4$. As $((p-1)/2)!^2 \equiv -1 \pmod p$ by Remark 1.1(a), applying (1.14) with $c = ((p-1)/2)!$ and using (2.4) we immediately get (1.16).

(iii) For convenience we set $m = (p-1)/2$. In light of Lemma 2.1 with $n = m+1$ and $P(z) = z^m$, for any $c \in \mathbb{Z}$ we have

$$|(i^2 + dj^2 + c)^m|_{0 \leqslant i,j \leqslant m} = |((i-1)^2 + d(j-1)^2 + c)^m|_{1 \leqslant i,j \leqslant m+1}$$

$$= \prod_{k=0}^{m} \binom{m}{k} \times \prod_{1 \leqslant i < j \leqslant m+1} ((i-1)^2 - (j-1)^2)(d(j-1)^2 + c - d(i-1)^2 - c)$$

$$= \frac{(m!)^{m+1}}{\prod_{k=0}^{m} k!(m-k)!} (-d)^{m(m+1)/2} \prod_{0 \leqslant i < j \leqslant m} (j-i)^2 (j+i)^2$$

$$= (-d)^{m(m+1)/2} (m!)^{m+1} \prod_{0 \leqslant i < j \leqslant m} (i+j)^2.$$

Therefore (1.19) holds, and also

$$T(d,p) \equiv (-d)^{(p^2-1)/8} \left(\frac{p-1}{2}!\right)^{(p+1)/2} \prod_{0 \leqslant i < j \leqslant (p-1)/2} (i+j)^2$$

$$\equiv R(d,p) \prod_{0 \leqslant i < j \leqslant (p-1)/2} (i+j)^2 \pmod p$$

with the help of (2.2). Combining this with (1.9) we obtain (1.18). Note that

$$\left(\frac{T(d,p)}{p}\right) = \left(\frac{R(d,p)}{p}\right).$$

(2.5)

If $\left(\frac{d}{p}\right) = 1$, then by Theorem 1.1 we have

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

and hence $\left(\frac{R(d,p)}{p}\right) = \left(\frac{2}{p}\right)$ in view of Lemma 2.3. In the case $\left(\frac{d}{p}\right) = -1$, by Theorem 1.1 we have

$$R(d,p) \equiv \begin{cases} (-d)^{(p-1)/4}((p-1)/2)! \pmod{p} & \text{if } p \equiv 1 \pmod{4}, \\ 1 \pmod{p} & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and hence $\left(\frac{R(d,p)}{p}\right) = 1$ with the help of Lemma 2.3. Therefore (1.17) also holds in light of (2.5).

Assume that $p \nmid d$. Then the sum of entries in each column of the determinant $S(d,p)$ actually equals $-(1 + \left(\frac{d}{p}\right))/2$. In fact, for any $j = 1, \ldots, m$, clearly

$$\left| \sum_{i=1}^{m} \left(\frac{i^2 + dj^2}{p} \right) \right| \leqslant m < \frac{p}{2}$$

and also

$$\sum_{i=1}^{m} \left(\frac{i^2 + dj^2}{p} \right) \equiv \sum_{i=1}^{m} (i^2 + dj^2)^m$$

$$= \sum_{i=1}^{m} \left(i^{2m} + d^m j^{2m} + \sum_{0<k<m} \binom{m}{k} i^{2k}(dj^2)^{m-k} \right)$$

$$\equiv m \left(1 + \left(\frac{d}{p}\right) \right) + \frac{1}{2} \sum_{0<k<m} \binom{m}{k} \sum_{i=1}^{m} (i^{2k} + (p-i)^{2k})(dj^2)^{m-k}$$

$$\equiv -\frac{1 + \left(\frac{d}{p}\right)}{2} + \frac{1}{2} \sum_{0<k<m} \binom{m}{k} (dj^2)^{m-k} \sum_{i=1}^{p-1} i^{2k}$$

$$\equiv -\frac{1 + \left(\frac{d}{p}\right)}{2} \pmod{p}.$$

(It is well known that $\sum_{i=1}^{p-1} i^h \equiv 0 \pmod{p}$ for any $h \in \mathbb{Z}$ with $h \not\equiv 0 \pmod{p-1}$), see, e.g. [IR, p. 235].)

Now suppose that $(\frac{d}{p}) = 1$. By the last paragraph, adding the last m rows of $T(d,p)$ to the first row we see that the initial term in the first row becomes m while all the other terms in the first row turn out to be zero. It follows that

$$T(d,p) = mS(d,p) \equiv -\frac{1}{2}S(d,p) \quad (\text{mod } p).$$

Combining this with (1.17), we obtain that

$$\left(\frac{-S(d,p)}{p}\right) = \left(\frac{2T(d,p)}{p}\right) = 1.$$

This proves (1.20). □

Proof of Theorem 1.3. (i) Let n be any positive odd integer relatively prime to d. For $j = 0, \dots, n-1$ let $\sigma_d(j)$ be the least nonnegative residue of dj modulo n. Then σ_d is a permutation on $\{0, \dots, n-1\}$ with $\sigma_d(0) = 0$. By Frobenius' extension of the Zolotarev lemma (cf. [BC15]), we have $\text{sign}(\sigma_d) = (\frac{d}{n})$.

Now suppose that $(\frac{d}{n}) = -1$. Then $n > 1$ and $\text{sign}(\sigma_d) = -1$. Thus

$$(c,d)_n = \left(\frac{d}{n}\right)^{n-1} (c,d)_n = \left|\left(\frac{di^2 + ci(dj) + (dj)^2}{n}\right)\right|_{1 \leqslant i,j \leqslant n-1}$$

$$= \left|\left(\frac{di^2 + ci\sigma_d(j) + \sigma_d(j)^2}{n}\right)\right|_{1 \leqslant i,j \leqslant n-1}$$

$$= \sum_{\pi \in S_{n-1}} \text{sign}(\pi) \prod_{i=1}^{n-1} \left(\frac{di^2 + ci\sigma_d(\pi(i)) + \sigma_d(\pi(i))^2}{n}\right)$$

$$= \text{sign}(\sigma_d) \sum_{\tau \in S_{n-1}} \text{sign}(\tau) \prod_{i=1}^{n-1} \left(\frac{di^2 + ci\tau(i) + \tau(i)^2}{n}\right) = -(c,d)_n$$

and hence $(c,d)_n = 0$.

(ii) Let p be an odd prime. For any $a, b \in \mathbb{Z}$, it is known (cf. [BEW, p. 58]) that

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + ax + b}{p}\right) = \begin{cases} -1 & \text{if } p \nmid a^2 - 4b, \\ p-1 & \text{if } p \mid a^2 - 4b. \end{cases}$$

So, for each $j = 1, \dots, p-1$, we have

$$\sum_{i=1}^{p-1} \left(\frac{i^2 + cij + dj^2}{p}\right) = \begin{cases} -1 - (\frac{d}{p}) & \text{if } p \nmid c^2 - 4d, \\ p - 1 - (\frac{d}{p}) & \text{if } p \mid c^2 - 4d. \end{cases}$$

Now assume that $(\frac{d}{p}) = 1$. Set

$$\lambda = \begin{cases} 1/2 & \text{if } p \nmid c^2 - 4d, \\ 1/(2-p) & \text{if } p \mid c^2 - 4d. \end{cases}$$

Then

$$\lambda \sum_{i=1}^{p-1} \left(\frac{i^2 + cij + dj^2}{p} \right) = -1.$$

By adding the last $p-1$ rows multiplied by λ to the first row of $[c, d]_p$, the initial term of the resulting determinant becomes $(p-1)\lambda$ while all other terms in the first row vanish. It follows that

$$[c, d]_p = (p-1)\lambda(c, d)_p$$

which is equivalent to (1.23). This ends the proof. $\square$

3. Proofs of Theorems 1.4-1.5

Lemma 3.1. *Let p be an odd prime. For any $d \in \mathbb{Z}$ with $(\frac{d}{p}) = -1$, we have the new congruence*

$$\prod_{x=1}^{(p-1)/2} (x^2 - d) \equiv (-1)^{(p+1)/2} \, 2 \pmod{p}. \tag{3.1}$$

Proof. As $1^2, \ldots, (\frac{p-1}{2})^2$ give all the $\frac{p-1}{2}$ quadratic residues modulo p, we have

$$\prod_{x=1}^{(p-1)/2} (z - x^2) \equiv z^{(p-1)/2} - 1 \pmod{p}. \tag{3.2}$$

Thus

$$\prod_{x=1}^{(p-1)/2} (d - x^2) \equiv d^{(p-1)/2} - 1 \equiv -2 \pmod{p}$$

and hence (3.1) follows. $\square$

Proof of Theorem 1.4. (i) Set $m = (p-1)/2$. Clearly

$$\left| \frac{\left(\frac{i+j}{p} \right)}{i+j} \right|_{1 \leqslant i, j \leqslant (p-1)/2} \equiv |(i+j)^{m-1}|_{1 \leqslant i, j \leqslant m} \pmod{p}.$$

By Lemma 2.1,

$$|(i+j)^{m-1}|_{1 \leqslant i, j \leqslant m} = \prod_{k=0}^{m-1} \binom{m-1}{k} \times \prod_{1 \leqslant i < j \leqslant m} (i-j)(j-i)$$

$$= \frac{(m-1)!^m}{\prod_{k=0}^{m-1} k!(m-1-k)!} (-1)^{m(m-1)/2} \prod_{1 \leqslant i < j \leqslant m} (j-i)^2$$

$$= (-1)^{m(m-1)/2} (m-1)!^m$$

$$= (-1)^{(p-1)(p-3)/8} \frac{2^{(p-1)/2}}{(p-1)^{(p-1)/2}} \left(\frac{p-1}{2}! \right)^{(p-1)/2}.$$

Since $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, by the above we have

$$\left|\frac{\left(\frac{i+j}{p}\right)}{i+j}\right|_{1\leqslant i,j\leqslant(p-1)/2} \equiv \left(\frac{p-1}{2}!\right)^{(p-1)/2} \quad (\text{mod } p). \qquad (3.3)$$

Recall that

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{(p+1)/2} \quad (\text{mod } p)$$

by Remark 1.1(a). In the case $p \equiv 1 \pmod 4$, from (3.3) we get

$$\left|\frac{\left(\frac{i+j}{p}\right)}{i+j}\right|_{1\leqslant i,j\leqslant(p-1)/2} \equiv (-1)^{(p-1)/4} = \left(\frac{2}{p}\right) \quad (\text{mod } p).$$

If $p \equiv 3 \pmod 4$, then by (3.3) we have

$$\left|\frac{\left(\frac{i+j}{p}\right)}{i+j}\right|_{1\leqslant i,j\leqslant(p-1)/2} \equiv \frac{p-1}{2}! \left(\frac{p-1}{2}!\right)^{2(p-3)/4} \equiv \frac{p-1}{2}! \quad (\text{mod } p).$$

So (1.24) always holds.

(ii) It is known (cf. [K05, (5.5)]) that

$$\left|\frac{1}{x_i + y_j}\right|_{1\leqslant i,j\leqslant m} = \frac{\prod_{1\leqslant i<j\leqslant m}(x_j - x_i)(y_j - y_i)}{\prod_{i=1}^m \prod_{j=1}^m (x_i + y_j)}.$$

Taking $m = (p-1)/2$ and $x_i = y_i = i^2$ for $i = 1, \ldots, m$, we get

$$\left|\frac{1}{i^2 + j^2}\right|_{1\leqslant i,j\leqslant(p-1)/2} = \frac{\prod_{1\leqslant i<j\leqslant(p-1)/2}(j^2 - i^2)^2}{\prod_{i=1}^{(p-1)/2} \prod_{j=1}^{(p-1)/2}(i^2 + j^2)}. \qquad (3.4)$$

Observe that

$$\prod_{1\leqslant i<j\leqslant(p-1)/2}(j^2 - i^2)^2 = \prod_{j=1}^{(p-1)/2}((j-1)!(j+1)\cdots(2j-1))^2$$

$$= \prod_{j=1}^{(p-1)/2} \frac{(2j-1)!^2}{j^2} = \frac{\prod_{j=1}^{(p-1)/2}(2j-1)!(p-2j)!}{((p-1)/2)!^2}$$

$$= \frac{\binom{p-1}{(p-1)/2}}{(p-1)!} \prod_{j=1}^{(p-1)/2} \frac{(p-1)!}{\binom{p-1}{2j-1}}$$

$$\equiv \frac{(-1)^{(p-1)/2}}{-1} \prod_{j=1}^{(p-1)/2} \frac{-1}{(-1)^{2j-1}} = 1 \ (\text{mod } p)$$

in view of Wilson's theorem and the congruence $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for $k = 0, \ldots, p-1$. Also,

$$\prod_{i=1}^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (i^2 + j^2) = \prod_{i=1}^{(p-1)/2} \left(\prod_{j=1}^{(p-1)/2} i^2 \left(1 + \frac{j^2}{i^2} \right) \right)$$

$$\equiv \prod_{i=1}^{(p-1)/2} \left(i^{p-1} \prod_{x=1}^{(p-1)/2} (1 + x^2) \right) \pmod{p}.$$

As -1 is a quadratic non-residue modulo p, applying (3.1) with $d = -1$ we get

$$\prod_{x=1}^{(p-1)/2} (x^2 + 1) \equiv (-1)^{(p+1)/2} 2 = 2 \pmod{p}.$$

Therefore

$$\prod_{i=1}^{(p-1)/2} \prod_{j=1}^{(p-1)/2} (i^2 + j^2) \equiv \prod_{i=1}^{(p-1)/2} 2 = 2^{(p-1)/2} \equiv \left(\frac{2}{p} \right) \pmod{p}.$$

So the desired congruence (1.25) follows from (3.4). We are done. $\square$

Lemma 3.2. *Let p be an odd prime. If $p \equiv 1 \pmod{4}$, then*

$$\left(\frac{((p-3)/2)!!}{p} \right) = (-1)^{|\{0 < k < \frac{p}{4}: \, (\frac{k}{p}) = -1\}|}. \tag{3.5}$$

If $p \equiv 3 \pmod{4}$, then

$$\left(\frac{((p-2+(\frac{2}{p}))/2)!!}{p} \right) = (-1)^{\lfloor (p+1)/8 \rfloor}. \tag{3.6}$$

Proof. We first handle the case $p \equiv 1 \pmod{4}$. By Lemma 2.3,

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

Thus

$$\left(\frac{((p-3)/2)!!}{p} \right) = \left(\frac{2}{p} \right) \left(\frac{\prod_{0 < k < p/4}(2k)}{p} \right)$$

$$= \left(\frac{2}{p} \right)^{(p+3)/4} (-1)^{|\{0 < k < \frac{p}{4}: \, (\frac{k}{p}) = -1\}|}.$$

This implies (3.5) since

$$\left(\frac{2}{p}\right)^{(p+3)/4} = (-1)^{\frac{p+1}{2} \cdot \frac{p-1}{4} \cdot \frac{p+3}{4}} = 1.$$

If $p \equiv 3 \pmod 8$, then $\sum_{0<k<p/4}(\frac{k}{p}) = 0$ by [BC], and hence

$$\left(\frac{((p-3)/2)!!}{p}\right) = \left(\frac{\prod_{0<k<p/4}(2k)}{p}\right) = (-1)^{|\{1\leqslant k\leqslant\frac{p-3}{4}:\ (\frac{k}{p})=1\}|} = (-1)^{(p-3)/8}$$

since $(\frac{2}{p}) = -1$. Similarly, if $p \equiv 7 \pmod 8$, then $\sum_{p/4<k<p/2}(\frac{k}{p}) = 0$ by [BC], and hence

$$\left(\frac{((p-1)/2)!!}{p}\right) = (-1)^{|\{1\leqslant k\leqslant\frac{p-1}{2}:\ 2\nmid k \text{ and } (\frac{k}{p})=-1\}|}$$

$$= (-1)^{|\{1\leqslant k\leqslant\frac{p-1}{2}:\ (\frac{k}{p})=-1\}|-|\{1\leqslant j\leqslant\frac{p-3}{4}:\ (\frac{2j}{p})=-1\}|}$$

$$= (-1)^{|\{\frac{p}{4}<k<\frac{p}{2}:\ (\frac{k}{p})=-1\}|} = (-1)^{\frac{1}{2}|\{k\in\mathbb{Z}:\ \frac{p-3}{4}<k\leqslant\frac{p-1}{2}\}|}$$

$$= (-1)^{(p+1)/8}.$$

So (3.6) holds when $p \equiv 3 \pmod 4$. $\square$

Proof of Theorem 1.5. Set $m := (p-1)/2$. Applying Lemma 2.1 with $n = m+1$ and $P(z) = z^m$, we obtain

$$W_p \equiv \left|(i^2 - m!j)^m\right|_{0\leqslant i,j\leqslant m} = \prod_{k=0}^{m}\binom{m}{k} \times \prod_{0\leqslant i<j\leqslant m}(i^2 - j^2)(-m!j - (-m!i))$$

$$= \prod_{k=0}^{m}\binom{m}{k} \times (m!)^{m(m+1)/2} \prod_{0\leqslant i<j\leqslant m}(j-i)^2(i+j) \pmod p.$$

Observe that

$$\prod_{0\leqslant i<j\leqslant m}(i+j) = \prod_{k=1}^{m} k^{|\{i\in\mathbb{Z}:\ 0\leqslant i\leqslant\lfloor\frac{k-1}{2}\rfloor\}|}(p-k)^{|\{i\in\mathbb{Z}:\ m+1-k\leqslant i\leqslant\lfloor m-\frac{k}{2}\rfloor\}|}$$

$$= \prod_{k=1}^{m} k^{\lfloor(k+1)/2\rfloor}(p-k)^{\lfloor k/2\rfloor}$$

$$\equiv (-1)^{\sum_{k=1}^{m}\lfloor k/2\rfloor} \prod_{k=1}^{m} k^k = (-1)^{m-m/(2-\{m\}_2)} \prod_{k=1}^{m} k^k \pmod p.$$

So we have

$$W_p \equiv (-1)^{m-m/(2-\{m\}_2)}(m!)^{m(m+1)/2} \prod_{k=0}^{m}\binom{m}{k} \times \prod_{j=1}^{m}(j!)^2 \times \prod_{k=1}^{m} k^k \pmod p.$$

$$(3.7)$$

Case 1. $p \equiv 1 \pmod 4$ (i.e., $2 \mid m$).
In this case,

$$\prod_{k=0}^{m} \binom{m}{k} = \prod_{k=0}^{m/2-1} \binom{m}{k}^2 \times \binom{m}{m/2}.$$

Write $p = x^2 + 4y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$. By a result of Gauss (cf. [BEW, (9.0.1)]),

$$\binom{(p-1)/2}{(p-1)/4} \equiv 2x \pmod p \tag{3.8}$$

and hence

$$\left(\frac{\binom{m}{m/2}}{p}\right) = \left(\frac{2x}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{|x|}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{|x|}\right) = \left(\frac{2}{p}\right)\left(\frac{x^2+4y^2}{|x|}\right) = \left(\frac{2}{p}\right).$$

Combining this with (3.7), (2.4) and (3.5), we obtain that

$$\left(\frac{W_p}{p}\right) = \left(\frac{-1}{p}\right)^{m/2}\left(\frac{2}{p}\right)\left(\frac{m!}{p}\right)^{m(m+1)/2}\left(\frac{\prod_{k=1}^{m} k^k}{p}\right)$$

$$= \left(\frac{2}{p}\right)^{1+(p^2-1)/8}\left(\frac{(m-1)!!}{p}\right) = \left(\frac{((p-3)/2)!!}{p}\right)$$

$$= (-1)^{|\{0<k<\frac{p}{4}: \, (\frac{k}{p})=-1\}|}.$$

Case 2. $p \equiv 3 \pmod 4$ (i.e., $2 \nmid m$).
In this case,

$$\prod_{k=0}^{m} \binom{m}{k} = \prod_{k=0}^{(m-1)/2} \binom{m}{k}^2.$$

Combining this with (3.7) and (3.6), we see that

$$\left(\frac{W_p}{p}\right) = \left(\frac{m!}{p}\right)^{m(m+1)/2}\left(\frac{\prod_{k=1}^{m} k^k}{p}\right) = \left(\frac{m!}{p}\right)^{(p^2-1)/8}\left(\frac{m!!}{p}\right)$$

$$= \begin{cases} (\frac{m!}{p})(\frac{m!!}{p}) = (\frac{(m-1)!!}{p}) = (-1)^{\lfloor(p+1)/8\rfloor} & \text{if } p \equiv 3 \pmod 8, \\ (\frac{m!!}{p}) = (-1)^{(p+1)/8} & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

In view of the above, we have completed the proof of (1.26). $\square$

4. SOME OPEN CONJECTURES ON DETERMINANTS

By Remark 1.1(a),

$$\frac{p-1}{2}! \equiv \pm 1 \pmod p \quad \text{for any prime } p \equiv 3 \pmod 4.$$

In 1961 L. J. Mordell [M61] proved that for any prime $p > 3$ with $p \equiv 3 \pmod 4$ we have

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

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

Motivated by Theorem 1.5, we pose the following conjecture which looks quite challenging.

Conjecture 4.1. *Let p be an odd prime. Then*

$$\left| \left(\frac{i^2 - ((p-1)/2)!j}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2} = 0 \quad \text{if and only if } p \equiv 3 \pmod 4. \quad (4.1)$$

When $p \equiv 3 \pmod 4$, both

$$(-1)^{\lfloor (p+1)/8 \rfloor} \left| x + \left(\frac{i^2 - ((p-1)/2)!j}{p} \right) \right|_{0 \leqslant i,j \leqslant (p-1)/2}$$

and

$$\frac{(-1)^{\lfloor (p+1)/8 \rfloor}}{x} \left| x + \left(\frac{i^2 - ((p-1)/2)!j}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2}$$

are positive squares not depending on x.

Remark 4.1. We have verified that (4.1) holds for all odd primes $p < 2500$, and that $(-1)^{\lfloor (p+1)/8 \rfloor} W_p$ is a positive square for every prime $p < 3000$ with $p \equiv 3 \pmod 4$. See [Su13, A226163] for the sequence

$$\left| \left(\frac{i^2 - ((p_n-1)/2)!j}{p_n} \right) \right|_{1 \leqslant i,j \leqslant (p_n-1)/2} \quad (n = 2, 3, \ldots),$$

where p_n denotes the nth prime.

Inspired by Theorem 1.2(iii), we formulate the following conjecture.

Conjecture 4.2. *Let p be an odd prime.*

(i) Let $S^*(1,p)$ denote the determinant obtained from $S(1,p) = |(\frac{i^2+j^2}{p})|_{1 \leqslant i,j \leqslant (p-1)/2}$ via replacing the entries $(\frac{1^2+j^2}{p})$ $(j = 1, \ldots, (p-1)/2)$ in the first row by $(\frac{j}{p})$ $(j = 1, \ldots, (p-1)/2)$ respectively. Then $-S_p$ is always a positive square, where

$$S_p := \begin{cases} S^*(1,p) & \text{if } p \equiv 1 \pmod 4, \\ S(1,p)/2^{(p-3)/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \quad (4.2)$$

(ii) If $p = x^2 + 4y^2$ with x and y positive integers, then for any $d \in \mathbb{Z}$ with $(\frac{d}{p}) = -1$, the number $|T(d,p)|/(2^{(p-1)/2}y)$ is a positive square not depending on d.

Remark 4.2. We have verified this for all odd primes $p < 2000$; for example,

$$S_3 = S_5 = S_7 = S_{11} = -1^2, \ S_{13} = -3^2, \ S_{17} = -21^2, \ S_{19} = -2^2, \ S_{23} = -1^2.$$

After learning part (i) of this conjecture in the case $p \equiv 3 \pmod 4$ from the author, H. Cohen and M. Vsemirnov informed the author their supplemental conjecture which states that for any prime $p = x^2 + 4y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$, the number $S(1, p)/x$ is an integer square.

The following conjecture can be viewed as a supplement to Theorem 1.2(iii).

Conjecture 4.3. *Let p be an odd prime, and let $c, d \in \mathbb{Z}$ with $p \nmid cd$. Define*

$$S_c(d, p) := \left| \left(\frac{i^2 + dj^2 + c}{p} \right) \right|_{1 \leqslant i, j \leqslant (p-1)/2}. \tag{4.3}$$

Then

$$\left(\frac{S_c(d, p)}{p} \right) = \begin{cases} 1 & \text{if } (\frac{c}{p}) = 1 \text{ and } (\frac{d}{p}) = -1, \\ (\frac{-1}{p}) & \text{if } (\frac{c}{p}) = (\frac{d}{p}) = -1, \\ (\frac{-2}{p}) & \text{if } (\frac{-c}{p}) = (\frac{d}{p}) = 1, \\ (\frac{-6}{p}) & \text{if } (\frac{-c}{p}) = -1 \text{ and } (\frac{d}{p}) = 1. \end{cases} \tag{4.4}$$

Remark 4.3. We have verified Conjecture 4.3 for all odd primes $p < 225$. See [Su13, A228005] for the sequence $S_1(1, p_n)$ ($n = 2, 3, \dots$). Let p be an odd prime and let $b, c, d \in \mathbb{Z}$ with $p \nmid bcd$. It is easy to see that

$$\left| \left(\frac{i^2 + dj^2 + b^2 c}{p} \right) \right|_{1 \leqslant i, j \leqslant (p-1)/2} = \left| \left(\frac{(bi)^2 + d(bj)^2 + b^2 c}{p} \right) \right|_{1 \leqslant i, j \leqslant (p-1)/2}$$

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

Conjecture 4.4. *For any prime $p \equiv \pm 3 \pmod 8$, the number*

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

is a quadratic nonresidue modulo p.

Remark 4.4. We have verified this conjecture for $p < 1000$. Let p be an odd prime. By using Lemma 2.1, and Gauss' congruence (3.8) for $p \equiv 1 \pmod 4$, we are able to show that $2|(\frac{i(i+1)+j(j+1)}{p})|_{0 \leqslant i, j \leqslant (p-1)/2}$ is always a quadratic residue modulo p.

Conjecture 4.5. (i) *For any positive odd integer $n > 3$, we have*

$$\left| (i^2 + j^2) \left(\frac{i^2 + j^2}{n} \right) \right|_{0 \leqslant i,j \leqslant (n-1)/2} \equiv 0 \pmod{n}. \qquad (4.5)$$

(ii) *Let $p > 5$ be a prime with $p \equiv 1 \pmod 4$. Then*

$$\left(\frac{D_p^+}{p} \right) = \left(\frac{D_p^-}{p} \right) = 1, \qquad (4.6)$$

where

$$D_p^+ := \left| (i+j) \left(\frac{i+j}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2} \quad and \quad D_p^- := \left| (j-i) \left(\frac{j-i}{p} \right) \right|_{1 \leqslant i,j \leqslant (p-1)/2}.$$

(iii) *For any prime $p > 3$ and integer $d \not\equiv 0 \pmod p$, we have*

$$\left(\frac{|(i^2 + dj^2)^{(p+1)/2}|_{1 \leqslant i,j \leqslant (p-1)/2}}{p} \right) = \begin{cases} \left(\frac{d}{p} \right)^{(p-1)/4} & \text{if } 4 \mid p-1, \\ \left(\frac{d}{p} \right)^{(p+1)/4} (-1)^{(h(-p)-1)/2} & \text{if } 4 \mid p-3. \end{cases}$$

Remark 4.5. We have verified part (i) and parts (ii)-(iii) of Conjecture 4.5 for $n < 1200$ and $p < 1200$ respectively. It is known that a skew-symmetric determinant of even order with integer entries is always a square (cf. [St90] and [K99]).

Conjecture 4.6. *Let p be an odd prime.*
(i) *Define M_p as the matrix obtaining from $[(\frac{i-j}{p})]_{0 \leqslant i,j \leqslant (p-1)/2}$ via replacing all the entries in the first row by 1. Then*

$$\det M_p = \begin{cases} (-1)^{(p-1)/4} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(h(-p)-1)/2} & \text{if } p > 3 \text{ and } p \equiv 3 \pmod 4. \end{cases} \qquad (4.7)$$

(ii) *Let M_p^+ be the matrix obtaining from $[(\frac{i+j}{p})]_{0 \leqslant i,j \leqslant (p-1)/2}$ via replacing all the entries in the first row by 1. Then*

$$\det M_p^+ = 2^{(p-1)/2} \det M_p. \qquad (4.8)$$

(iii) *Define N_p as the matrix obtaining from $[(\frac{i-j}{p})]_{1 \leqslant i,j \leqslant (p-1)/2}$ via replacing all the entries in the first row by 1, and also define N_p^+ as the matrix obtaining from $[(\frac{i+j}{p})]_{1 \leqslant i,j \leqslant (p-1)/2}$ via replacing all the entries in the first row by 1. Then*

$$\det N_p = (-1)^{\lfloor (p+3)/4 \rfloor} \det M_p \quad and \quad \det N_p^+ = -2^{(p-3)/2} \det M_p. \qquad (4.9)$$

Remark 4.6. We have verified Conjecture 4.6 for all odd primes $p < 2000$.

Recall that for any $c, d \in \mathbb{Z}$ and positive odd integer n, $(c,d)_n$ and $[c,d]_n$ are defined by (1.21) and (1.22).

Conjecture 4.7. *Let c and d be integers.*

(i) *If d is nonzero, then $[c, d]_p = 0$ for infinitely many primes p.*

(ii) *If $[c, d]_p$ is nonzero for some odd prime p, then its p-adic valuation (i.e., p-adic order) must be even.*

Remark 4.7. We have verified Conjecture 4.7(ii) for all odd primes $p < 200$. Let $c, d \in \mathbb{Z}$. If d is not a square, then by [IR, pp. 57-58] there are infinitely many odd primes p with $(\frac{d}{p}) = -1$ and hence $(c, d)_p = 0$ by Theorem 1.3(i). If p is an odd prime with $p \nmid d$ and $(c, d)_p \neq 0$, then $(\frac{d}{p}) = 1$, $[c, d]_p \neq 0$ and $\mathrm{ord}_p(c, d)_p = \mathrm{ord}_p[c, d]_p$ by Theorem 1.3, where $\mathrm{ord}_p x$ denotes the p-adic order of a nonzero p-adic number x.

Conjecture 4.8. (i) *For any odd integer $n > 3$ we have $(2, 3)_n \equiv 0 \pmod{n^2}$. Also, for any odd integer $n > 5$ we have $(6, 15)_n \equiv 0 \pmod{n^2}$.*

(ii) *For any positive integer $n \equiv 3 \pmod 4$, we have*

$$(6, 1)_n = [6, 1]_n = (3, 2)_n = [3, 2]_n = 0 \tag{4.10}$$

and

$$(4, 2)_n = (8, 8)_n = (3, 3)_n = (21, 112)_n = 0. \tag{4.11}$$

(iii) *For any prime $p \equiv 1 \pmod 4$ with $p = x^2 + 4y^2$ ($x, y \in \mathbb{Z}$ and $4 \mid x - 1$), we have*

$$(6, 1)_p = (-1)^{(p-1)/4} x u^2 \quad and \quad (3, 2)_p = (-1)^{(p-1)/4} x v^2$$

for some $u, v \in \mathbb{Z}$. For each prime $p \equiv 1 \pmod 8$ with $p = x^2 + 2y^2$ ($x, y \in \mathbb{Z}$ and $4 \mid x - 1$), we have $(4, 2)_p = (8, 8)_p = (-1)^{(p-1)/8} x w^2$ for some $w \in \mathbb{Z}$. For every prime $p \equiv 1 \pmod{12}$ with $p = x^2 + 3y^2$ ($x, y \in \mathbb{Z}$ and $3 \mid x - 1$), the number $(3, 3)_p/x$ is a square. Also, for any prime $p \equiv 1, 9, 25 \pmod{28}$ with $p = x^2 + 7y^2$ ($x, y \in \mathbb{Z}$ and $(\frac{x}{7}) = 1$) the number $(21, 112)_p/x$ is a square.

(iv) *$(10, 9)_p = 0$ for any prime $p \equiv 5 \pmod{12}$, $[5, 5]_p = 0$ for each prime $p \equiv 13, 17 \pmod{20}$, and $(8, 18)_p = [8, 18]_p = 0$ for every prime $p \equiv 13, 17 \pmod{24}$.*

Remark 4.8. We have verified parts (i) and (ii) of Conjecture 4.8 for $n < 1000$, and parts (iii) and (iv) of Conjecture 4.8 for primes $p < 1000$. See [Su13, A225611] for the sequence $(6, 1)_{p_n}$ ($n = 2, 3, \ldots$). For any positive integer $n \equiv \pm 5 \pmod{12}$, we have $(\frac{3}{n}) = -1$ and hence $(2, 3)_n = (3, 3)_n = 0$ by Theorem 1.3(i). Similarly, for any positive integer $n \equiv \pm 3 \pmod 8$, we have $(\frac{2}{n}) = -1$ and hence $(3, 2)_n = (4, 2)_n = (8, 8)_n = 0$ by Theorem 1.3(i). Also, for any positive integer $n \equiv 3, 7 \pmod{10}$, we have $(\frac{5}{n}) = -1$ and hence $(5, 5)_n = 0$ by Theorem 1.3(i). For any prime $p \equiv 5 \pmod{12}$, clearly $(10, 9)_p = 0$ if and only if $[10, 9]_p = 0$ (by Theorem 1.3(ii)).

References

[BC]   B. C. Berndt and S. Chowla, *Zero sums of the Legendre symbol*, Nordisk Mat. Tidskr. 22 (1974), 5–8.

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

[BC15] A. Brunyate and P. L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity*, Ramanujan J. 37 (2015), 25–50.

[C59]   L. Carlitz, *Some cyclotomic matrices*, Acta Arith. 5 (1959), 293–308.

[Ch03] R. Chapman, *Determinants of Legendre matrices*, preprint (August 5, 2003).

[Ch04] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. 115 (2004), 231–244.

[Ch12] R. Chapman, *My evil determinant problem*, preprint (Dec. 12, 2012), available from `http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf`.

[Co62] H. Cohn, *Advanced Number Theory*, Dover Publ., New York, 1962.

[DH]   W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly 112 (2005), 251–256.

[IR]   K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math., Vol. 84, 2nd ed., Springer, New York, 1990.

[K99]   C. Krattenthaler, *Advanced determinant calculus*, Séminaire Lotharingien Combin. **42** (1999), Article B42q, 67pp.

[K05]   C. Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. 411 (2005), 68–166.

[M61]   L. J. Mordell, *The congruence $((p-1)/2)! \equiv \pm 1 \pmod{p}$*, Amer. Math. Monthly 68 (1961), 145–146.

[P06]   H. Pan, *A remark on Zolotarev's theorem*, preprint (2006), `arXiv:0601026`.

[St90] J. R. Stembridge, *Nonintersecting paths, pfaffians and plane partitions*, Adv. in Math. 83 (1990), 96–131.

[Su13] Z.-W. Sun, Sequences A225611, A226163 and A228005 in OEIS, `http://oeis.org`, 2013.

[V12]   M. Vsemirnov, *On the evaluation of R. Chapman's "evil determinant"*, Linear Algebra Appl. 436 (2012), 4101–4106.

[V13]   M. Vsemirnov, *On R. Chapman's "evil determinant": case $p \equiv 1 \pmod 4$*, Acta Arith. 159 (2013), 331–344.

[Z]   G. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Ann. Math. 11 (1872), 354–362.