ACTA ARITHMETICA
Online First version

# The Pell sequence and cyclotomic matrices involving squares over finite fields

by

Hai-Liang Wu, Li-Yuan Wang and He-Xia Ni

**Abstract.** By using some arithmetic properties of the Pell sequence and some $p$-adic tools, we study certain cyclotomic matrices involving squares over finite fields. For example, let $1 = s_1, s_2, \ldots, s_{(q-1)/2}$ be all the nonzero squares over $\mathbb{F}_q$, where $q = p^f$ is an odd prime power with $q \geq 7$. We prove that the matrix

$$B_q((q-3)/2) = [(s_i + s_j)^{(q-3)/2}]_{2 \leq i,j \leq (q-1)/2}$$

is singular whenever $f \geq 2$. Also, for $q = p$, we show that

$$\det B_p((p-3)/2) = 0 \iff Q_p \equiv 2 \pmod{p^2\mathbb{Z}},$$

where $Q_p$ is the $p$th term of the companion Pell sequence $\{Q_i\}_{i=0}^{\infty}$ defined by $Q_0 = Q_1 = 2$ and $Q_{i+1} = 2Q_i + Q_{i-1}$.

## 1. Introduction

**1.1. Notation.** In this paper, the symbol $p$ always denotes an odd prime. We let $\mathbb{Q}_p$ be the $p$-adic number field and let $\mathbb{Z}_p$ be the ring of all $p$-adic integers. As usual, we use $\mathbb{C}_p$ to denote the completion of the algebraic closure of $\mathbb{Q}_p$. In addition, we let

$$\mathrm{ord}_p : \mathbb{C}_p \to \mathbb{R}$$

be the $p$-adic order function over $\mathbb{C}_p$.

Let $q = p^f$ be an odd prime power with $f \in \mathbb{Z}^+$. The symbol $\mathbb{F}_q$ denotes the finite field with $q$ elements and $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is the multiplicative cyclic group of all nonzero elements of $\mathbb{F}_q$. The group of all multiplicative characters of $\mathbb{F}_q$ is denoted by $\widehat{\mathbb{F}_q^\times}$, and the trivial character is indicated by $\varepsilon$. Throughout this paper, for any multiplicative character $\psi : \mathbb{F}_q^\times \to \mathbb{C}$ (or $\mathbb{C}_p$), we extend $\psi$ to $\mathbb{F}_q$ by letting $\psi(0) = 0$.

2020 *Mathematics Subject Classification*: Primary 11L05; Secondary 15A15, 11R18, 12E20.
*Key words and phrases*: Pell sequence, cyclotomic matrices, character sums over finite fields.
Received 11 March 2025; revised 5 October 2025.
Published online 27 May 2026.

 

Let $\zeta_p$ be a primitive $p$th root of unity over $\mathbb{C}$ (or $\mathbb{C}_p$). Then for any $\psi \in \widehat{\mathbb{F}_q^\times}$, the Gauss sum of $\psi$ is defined by

$$G_q(\psi) = \sum_{x\in\mathbb{F}_q} \psi(x)\zeta_p^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)},$$

where $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. Also, for any $\psi, \chi \in \widehat{\mathbb{F}_q^\times}$, the Jacobi sum of $\psi$ and $\chi$ is defined by

$$J_q(\psi,\chi) = \sum_{x\in\mathbb{F}_q} \psi(x)\chi(1-x).$$

**1.2. Background and motivation.** The investigations of cyclotomic matrices involving elements over finite fields were initiated by Lehmer [8] and Carlitz [1]. For instance, for any nontrivial multiplicative character $\psi$ modulo $p$, Carlitz [1] first studied the cyclotomic matrices

$$C_p^-(\psi) := [\psi(j-i)]_{1\le i,j\le p-1}, \tag{1.1}$$

$$C_p^+(\psi) := [\psi(j+i)]_{1\le i,j\le p-1}. \tag{1.2}$$

In [1, Theorems 4 and 5] he proved that

$$\det C_p^-(\psi) = (-1)^{(p-1)/m}\cdot\frac{G_p(\psi)^{p-1}}{p},$$

$$\det C_p^+(\psi) = \begin{cases} \frac{1}{p}(-1)^{\frac{p-1}{2m}}G_p(\psi)^{p-1} & \text{if } m\equiv 1 \pmod 2,\\ \frac{1}{p}(-1)^{\frac{p-1}{m}}\delta(\psi)^{p-1}G_p(\psi)^{p-1} & \text{if } m\equiv 0 \pmod 2,\end{cases}$$

where $m = \min\{k\in\mathbb{Z}^+ : \psi^k = \varepsilon\}$ is the order of $\psi$ and

$$\delta(\psi) = \begin{cases} 1 & \text{if } \psi(-1)=1,\\ -\mathbf{i} & \text{if } \psi(-1)=-1.\end{cases}$$

Following Carlitz's work, Chapman [2] further studied some variants of the matrix $C_p^+(\psi)$. Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol, i.e., the unique quadratic multiplicative character of $\mathbb{F}_p$. Chapman considered the matrices

$$C_p^{(0)} := \left[\left(\frac{i+j}{p}\right)\right]_{0\le i,j\le (p-1)/2}, \quad C_p^{(1)} := \left[\left(\frac{i+j}{p}\right)\right]_{1\le i,j\le (p-1)/2}.$$

Although Chapman only changed the sizes of the matrices, the calculations of $\det C_p^{(0)}$ and $\det C_p^{(1)}$ became extremely complicated. In fact, for $p\equiv 1 \pmod 4$, let $\epsilon_p > 1$ and $h_p$ denote the fundamental unit and class number of $\mathbb{Q}(\sqrt{p})$ respectively, and write

$$\epsilon_p^{h_p} = a_p + b_p\sqrt{p}$$

with $a_p, b_p \in \mathbb{Q}$. Chapman [2] showed that

$$\det C_p^{(0)} = \begin{cases} (-1)^{(p+3)/4} 2^{(p-1)/2} a_p & \text{if } p \equiv 1 \pmod 4, \\ -2^{(p-1)/2} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

$$\det C_p^{(1)} = \begin{cases} (-1)^{(p-1)/4} 2^{(p-1)/2} b_p & \text{if } p \equiv 1 \pmod 4, \\ 0 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Chapman also investigated some variants of $C_p^-(\psi)$; the most well-known among them is Chapman's "evil determinant"

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

Let

$$\epsilon_p^{(2+(-1)^{(p+3)/4})h_p} = a_p' + b_p'\sqrt{p}$$

with $a_p', b_p' \in \mathbb{Q}$. Chapman conjectured that

$$\det C_p^- = \begin{cases} -a_p' & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Vsemirnov [16, 17] later confirmed this conjecture by using ingenious and sophisticated matrix decompositions.

Sun [13] studied variants of the above matrices from another perspective. For example, he considered the matrix

$$S_p := \left[\left(\frac{i^2+j^2}{p}\right)\right]_{1\le i,j\le (p-1)/2} \tag{1.3}$$

which involves the nonzero squares over $\mathbb{F}_p$. In [13, Theorem 1.2] he proved that $-\det S_p \bmod p\mathbb{Z}$ is a nonzero square over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. Moreover, Sun conjectured that $-\det S_p$ is indeed the square of some integer whenever $p \equiv 3 \pmod 4$. This conjecture was later confirmed by Alekseyev and Krachun. For $p \equiv 1 \pmod 4$, if we write $p = a^2 + 4b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 4$, then Cohen, Sun and Vsemirnov conjectured that $S_p/a$ is also the square of an integer. This conjecture was later confirmed by the first author [18].

Recently, for any positive integer $m$, Sun [14] considered the matrix

$$S_p(m) := [(i^2+j^2)^m]_{1\le i,j\le (p-1)/2}, \tag{1.4}$$

and obtained several interesting results concerning $\det S_p(m)$. For example, when $p \equiv 3 \pmod 4$, in [14, Theorem 1.2(ii)] he proved that

$$\det S_p(p-3) \equiv \det\left[\frac{1}{(i^2+j^2)^2}\right]_{1\le i,j\le (p-1)/2} \equiv \frac{1}{4}\prod_{r=1}^{(p-3)/4}\left(r+\frac{1}{4}\right)^2 \pmod{p\mathbb{Z}_p}.$$

Having recalled the above results, we now state our research motivations. Inspired by Sun's matrix $S_p(m)$ defined by (1.4), in this paper, we mainly

consider a variant of $S_p(m)$. Let $q = 2n+1$ and let

$$\{s_1 = 1, s_2, \ldots, s_n\} = \{x^2 : x \in \mathbb{F}_q^\times\}$$

be the set of all nonzero squares in $\mathbb{F}_q$. Then we define the matrix

$$B_q(m) := [(s_i + s_j)^m]_{2 \le i,j \le n}. \tag{1.5}$$

Before studying the properties of $B_q(m)$, let us first have a brief discussion. Let

$$h(t) = a_{m-1}t^{m-1} + \cdots + a_1 t + a_0$$

be a polynomial over a commutative ring with $\deg(h(t)) \le m-1$. Then it is known (see [7, Lemma 9]) that

$$\det[h(x_i+y_j)]_{1\le i,j\le m} = a_{m-1}^m \cdot \prod_{r=0}^{m-1} \binom{m-1}{r} \cdot \prod_{1\le i<j\le m} (x_i - x_j)(y_j - y_i). \tag{1.6}$$

From this we immediately see that $B_q(m)$ is singular whenever $m \le n-3$. Hence it is meaningful to consider the cases of $n-2 \le m \le q-1$. In this paper, we focus on the cases of $m = n-2, n-1, n$; we will see that the methods used in each case are very different.

**1.3. The Pell sequence.** Before stating our main results, we introduce the Pell sequence. The Pell sequence is an infinite sequence of integers that comprises the denominators of the closest rational approximations to the square root of 2. Specifically, the Pell sequence $\{P_i\}_{i=0}^\infty$ is defined by

$$P_0 = 0, \quad P_1 = 1, \quad P_{i+1} = 2P_i + P_{i-1},$$

and its companion sequence $\{Q_i\}_{i=0}^\infty$ is defined by

$$Q_0 = Q_1 = 2, \quad Q_{i+1} = 2Q_i + Q_{i-1}.$$

For any integer $i \ge 0$, it is known that

$$P_i = \frac{1}{2\sqrt{2}}\big((1+\sqrt{2})^i - (1-\sqrt{2})^i\big) = \sum_{k=0}^{\lfloor (i-1)/2 \rfloor} \binom{i}{2k+1} 2^k,$$

$$Q_i = (1+\sqrt{2})^i + (1-\sqrt{2})^i.$$

From this, it is easy to see that

$$P_p \equiv 2^{(p-1)/2} \equiv \left(\frac{2}{p}\right) \pmod{p\mathbb{Z}}, \quad Q_p \equiv 2 \pmod{p\mathbb{Z}}.$$

**1.4. Main results.** Now we state our first result, which concerns the cases $m = n-1, n-2$.

THEOREM 1.1. *Let $q = p^f = 2n+1 \ge 7$ be an odd prime power with $p$ prime and $f \in \mathbb{Z}^+$. Then the following results hold:*

(i) $B_q(n-1)$ *is a singular matrix whenever* $f \geq 2$. *Moreover, if* $f = 1$, *then*

$$\det B_p(n-1) = \frac{2 \cdot ((n-1)!)^n}{(0!1! \cdots (n-1)!)^2} \cdot a_p \in \mathbb{F}_p,$$

*where*

$$a_p = \frac{2 - Q_p}{p} \bmod p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

(ii) $B_q(n-2)$ *is singular if and only if* $f \geq 2$ *and* $q \neq 9$. *When* $f = 1$, *we have*

$$\det B_p(n-2) = \left(-\frac{1}{2}\right)^{n-2} \cdot \frac{((n-2)!)^{n-1}}{(0!1! \cdots (n-2)!)^2} \in \mathbb{F}_p^{\times}.$$

By Theorem 1.1, we obtain the following result.

COROLLARY 1.2. *Let* $p = 2n+1 \geq 7$ *be an odd prime. Then the following results hold:*

(i) $B_p(n-1)$ *is singular if and only if*

$$Q_p \equiv 2 \pmod{p^2\mathbb{Z}}.$$

*Moreover, if* $p \equiv 1 \pmod 4$, *then*

$$\left(\frac{\det B_p(n-1)}{p}\right) = \left(\frac{2a_p}{p}\right).$$

*If* $p \equiv 3 \pmod 4$, *then*

$$\left(\frac{\det B_p(n-1)}{p}\right) = (-1)^{\frac{h(-p)-1}{2}} \left(\frac{a_p}{p}\right),$$

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

(ii) *Suppose* $p \equiv 1 \pmod 4$. *Then*

$$\left(\frac{\det B_p(n-2)}{p}\right) = \left(\frac{6}{p}\right).$$

*Suppose* $p \equiv 3 \pmod 4$. *Then*

$$\left(\frac{\det B_p(n-2)}{p}\right) = \left(\frac{-2}{p}\right).$$

REMARK 1.3. With the help of a computer, one can verify that

$$\{p \text{ a prime} : 7 \leq p \leq 10^6 \text{ and } Q_p \equiv 2 \pmod{p^2\mathbb{Z}}\} = \{13, 31\}. \tag{1.7}$$

Motivated by this, we make the following conjecture.

CONJECTURE 1.4. *Let* $p \geq 7$ *be an odd prime. Then* $B_p(n-1)$ *is singular if and only if* $p \in \{13, 31\}$.

We next turn to the case $m = n$.

THEOREM 1.5. *Let $q=p^f=2n+1\ge 7$ be an odd prime power with $p$ prime and $f\in\mathbb{Z}^+$. Then $B_q(n)$ is singular whenever $f\ge 2$. Moreover, if $f=1$, then*

$$\det B_p(n)=(-1)^n\left(\frac{1}{2}\right)^{n-2}\cdot\frac{(n!)^{n+1}}{(0!1!\cdots n!)^2}\cdot b_p\in\mathbb{F}_p,$$

*where*

$$b_p=\frac{2\left(\frac{2}{p}\right)-2P_p-p}{p}\bmod p\mathbb{Z}\in\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p.$$

Similar to Corollary 1.2, we have the following result.

COROLLARY 1.6. *Let $p=2n+1\ge 7$ be a prime. Then*

$$\left(\frac{\det B_p(n)}{p}\right)=\left(\frac{-2b_p}{p}\right),$$

*and hence $B_p(n)$ is singular if and only if*

$$2P_p\equiv 2\left(\frac{2}{p}\right)-p\ (\mathrm{mod}\ p^2\mathbb{Z}).$$

REMARK 1.7. As in (1.7), it is natural to consider the odd primes $p$ which satisfy the congruence

$$2P_p\equiv 2\left(\frac{2}{p}\right)-p\ (\mathrm{mod}\ p^2\mathbb{Z}).$$

With the help of a computer, one can verify that

(1.8)

$$\left\{p\text{ a prime}: 7\le p\le 10^6\text{ and }2P_p\equiv 2\left(\frac{2}{p}\right)-p\ (\mathrm{mod}\ p^2\mathbb{Z})\right\}=\{29\}.$$

Using essentially the same method as in the proof of Theorem 1.5, we can obtain some results on certain variants of Carlitz's matrices $C_p^-(\psi)$ and $C_p^+(\psi)$ defined by (1.1) and (1.2) respectively.

In fact, let $\mathbb{F}_q^\times=\{x_1=1,x_2,\ldots,x_{q-1}\}$. For any nontrivial character $\psi\in\widehat{\mathbb{F}_q^\times}$, we define

$$D_q^-(\psi):=[\psi(x_j-x_i)]_{2\le i,j\le q-1},\qquad D_q^+(\psi):=[\psi(x_j+x_i)]_{2\le i,j\le q-1}.$$

We have the following result.

THEOREM 1.8. *Let $q=p^f\ge 3$ be an odd prime power. Then for any nontrivial character $\psi\in\widehat{\mathbb{F}_q^\times}$, we have*

$$\text{(i)}\ \det D_q^-(\psi) = -\frac{1+\psi(-1)}{q^2} G_q(\psi)^{q-1},$$

$$\text{(ii)}\ \det D_q^+(\psi) = \frac{(-1)^{(q+1)/2}\cdot\psi(-1)}{q^2}\big(2-\overline{\psi(2)}\big)G_q(\psi)^{q-1}.$$

Let $\psi=\phi$ be the unique quadratic character of $\mathbb{F}_q$, i.e.,

$$\phi(x)=\begin{cases}1 & \text{if } x\in\{s_1,\ldots,s_{(q-1)/2}\},\\ 0 & \text{if } x=0,\\ -1 & \text{otherwise.}\end{cases}$$

Then $D_p^-(\phi)$ is an integer matrix. Note that (see [3, Corollary 3.7.6])

$$G_q(\phi)=\begin{cases}(-1)^{f-1}\sqrt{q} & \text{if } p\equiv 1 \pmod 4,\\ (-1)^{f-1}\mathbf{i}^f\sqrt{q} & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

From this and Theorem 1.8, we can directly obtain the following corollary.

COROLLARY 1.9. *Let $q=p^f\ge 3$ be an odd prime power. Then $D_q^-(\phi)$ is singular if and only if $q\equiv 3 \pmod 4$. For $q\equiv 1 \pmod 4$, we have*

$$\det D_q^-(\phi) = -2q^{(q-5)/2}.$$

**1.5. Outline of the paper.** We will prove Theorem 1.1 and its corollary in Section 2. In Section 3, we shall introduce some necessary results on almost circulant matrices and some $p$-adic tools. The proofs of Theorems 1.5 and 1.8 will be given in Sections 4 and 5 respectively.

**2. Proofs of Theorem 1.1 and its corollary.** Recall that $n=(q-1)/2$ and $s_1=1,s_2,\ldots,s_n$ are all the nonzero squares over $\mathbb{F}_q$. Also, for any integers $a,b$ with $a\le b$, we use the symbol $[a,b]$ to denote the set $\{a,a+1,\ldots,b\}$.

We begin with the following result.

LEMMA 2.1. *Let $q=p^f=2n+1\ge 5$ with $f\in\mathbb{Z}^+$. Then*

$$(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2=\left(-\frac{1}{2}\right)^{n-2}\in\mathbb{F}_p.$$

*Proof.* Let

$$F(t)=\frac{t^n-1}{t-1}=t^{n-1}+t^{n-2}+\cdots+t+1$$

be a polynomial over $\mathbb{F}_q$. Note that $x$ is a nonzero square over $\mathbb{F}_q$ if and only if $x^n=1$. Hence it is easy to verify that

$$F(t)=\prod_{2\le j\le n}(t-s_j). \tag{2.1}$$

By (2.1) we see that $(-1)^{n-1}\prod_{2\le j\le n} s_j$ is the constant term of $F(t)$, i.e.,

$$\prod_{2\le j\le n} s_j = (-1)^{n-1}. \tag{2.2}$$

Also, clearly $(-1)^{n-1}\prod_{2\le j\le n}(s_j-1)$ is the constant term of $F(t+1)$, that is,

$$\prod_{2\le j\le n} (s_j-1) = (-1)^{n-1}\cdot n. \tag{2.3}$$

Next we consider the product

$$(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2.$$

Let $F'(t)$ be the formal derivative of $F(t)$. Then one can verify that

$$\begin{aligned}(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2 &= \prod_{2\le i\ne j\le n}(s_j-s_i)\\ &= \prod_{2\le j\le n}\prod_{i\in[2,n]\setminus\{j\}}(s_j-s_i) = \prod_{2\le j\le n} F'(s_j).\end{aligned} \tag{2.4}$$

As $(t-1)F(t)=t^n-1$, we have $F(t)+(t-1)F'(t)=nt^{n-1}$, and hence

$$F'(s_j)=\frac{ns_j^{n-1}}{s_j-1}=\frac{n}{s_j(s_j-1)}$$

for any $j\in[2,n]$. By the above results,

$$(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2 = \prod_{2\le j\le n}\frac{n}{s_j(s_j-1)}. \tag{2.5}$$

Combining (2.5) with (2.2) and (2.3), we obtain

$$(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2 = n^{n-2} = \left(-\frac{1}{2}\right)^{n-2}\in\mathbb{F}_p. \ \blacksquare$$

Before the statement of the next lemma, we introduce the following notations. Let $l$ be a positive integer and let $t_1,\ldots,t_l$ be variables. Then for any $k\in[1,l]$, the $k$th elementary symmetric polynomial of $t_1,\ldots,t_l$ is defined by

$$\sigma_k(t_1,\ldots,t_l)=\sum_{1\le i_1<\cdots<i_k\le l}\prod_{1\le j\le k} t_{i_j}.$$

In addition, we let

$$\sigma_0(t_1,\ldots,t_l)=1.$$

In 2022, Grinberg, Sun and Zhao [5, Theorem 3.1] obtained the following result.

LEMMA 2.2. *Let $l$ be a positive integer. Then*

$$\det\left[(x_i+y_j)^l\right]_{1\le i,j\le l}=(-1)^{l(l-1)/2}\cdot\prod_{1\le i<j\le l}(x_j-x_i)(y_j-y_i)\cdot\sum_{k=0}^{l}U_k, \tag{2.6}$$

*where*

$$U_k=\sigma_k(x_1,\ldots,x_l)\sigma_{l-k}(y_1,\ldots,y_l)\cdot\prod_{r\in[0,l]\setminus\{k\}}\binom{l}{r}.$$

We need the following results related to some congruences involving the Pell sequence, which were obtained by Z.-H. Sun [10, Theorem 4.1], Z.-W. Sun [11, Final Remark] and Z.-W. Sun [12, Remark 3.1] respectively.

LEMMA 2.3. *Let $p\ge 7$ be a prime and let $B_{p-3}$ be the $(p-3)$th Bernoulli number. Then*

$$\sum_{k=1}^{p-1}\frac{2^k}{k}\equiv\frac{2-2^p}{p}-\frac{7}{12}p^2B_{p-3}\ (\mathrm{mod}\ p^3\mathbb{Z}_p), \tag{2.7}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k\cdot 2^k}\equiv-2^{\frac{p+1}{2}}\cdot\frac{P_p-2^{\frac{p-1}{2}}}{p}\ (\mathrm{mod}\ p\mathbb{Z}_p), \tag{2.8}$$

$$4\left(\frac{2}{p}\right)P_p\equiv 2+Q_p\ (\mathrm{mod}\ p^2\mathbb{Z}). \tag{2.9}$$

*Proof of Theorem 1.1.* (i) By Lemmas 2.2 and 2.1,

$$\begin{aligned}\det B_q(n-1)&=(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2\cdot\sum_{k=0}^{n-1}W_k\\&=\left(-\frac{1}{2}\right)^{n-2}\cdot\sum_{k=0}^{n-1}W_k,\end{aligned} \tag{2.10}$$

where

$$W_k=\sigma_k(s_2,\ldots,s_n)\sigma_{n-1-k}(s_2,\ldots,s_n)\cdot\prod_{r\in[0,n-1]\setminus\{k\}}\binom{n-1}{r} \tag{2.11}$$

for any $k\in[0,n-1]$.

We next consider $W_k$. By (2.1) we see that

$$\begin{aligned}F(t)=t^{n-1}+t^{n-2}+\cdots+t+1&=\prod_{2\le j\le n}(t-s_j)\\&=\sum_{k=0}^{n-1}(-1)^k\sigma_k(s_2,\ldots,s_n)t^{n-1-k},\end{aligned}$$

and hence for any $k \in [0, n-1]$ we have

$$\sigma_k(s_2, \ldots, s_n) = (-1)^k. \tag{2.12}$$

By (2.11) and (2.12) we obtain

$$W_k = (-1)^{n-1} \prod_{r \in [0,n-1]\setminus\{k\}} \binom{n-1}{r}. \tag{2.13}$$

Suppose that $f \geq 2$. As $q = p^f \geq 9$, we have

$$n-1 = \frac{q-3}{2} = \frac{p-3}{2} \cdot 1 + \frac{p-1}{2} \cdot p + \cdots + \frac{p-1}{2} \cdot p^{f-1} > \frac{p+1}{2}.$$

By the Lucas congruence, for $j \in \{(p-1)/2, (p+1)/2\}$ we have

$$\binom{n-1}{j} \equiv \binom{(p-3)/2}{j} \binom{(p-1)/2}{0} \cdots \binom{(p-1)/2}{0} \equiv 0 \pmod{p\mathbb{Z}}.$$

Thus,

$$\left| \left\{ r \in [0, n-1] : \binom{n-1}{r} \equiv 0 \pmod{p\mathbb{Z}} \right\} \right| \geq 2.$$

This, together with (2.13), implies that $W_k = 0$ (as an element of $\mathbb{F}_q$) if $f \geq 2$. Hence by (2.10) we see that $B_q(n-1)$ is singular whenever $f \geq 2$.

Suppose now $f = 1$. Then for any $r \in [0, n-1]$ we have

$$\binom{n-1}{r} \not\equiv 0 \pmod{p\mathbb{Z}}.$$

Hence by (2.13) we obtain

$$\begin{aligned} \sum_{k=0}^{n-1} W_k &= (-1)^{n-1} \left( \sum_{k=0}^{n-1} \binom{n-1}{k}^{-1} \right) \cdot \prod_{r \in [0,n-1]} \binom{n-1}{r} \\ &= (-1)^{n-1} \cdot \frac{n}{2^n} \left( \sum_{k=1}^{n} \frac{2^k}{k} \right) \cdot \frac{((n-1)!)^n}{(0!1! \cdots (n-1)!)^2}, \end{aligned} \tag{2.14}$$

where the last equality follows from Sury's identity [15]

$$\sum_{k=0}^{n-1} \binom{n-1}{k}^{-1} = \frac{n}{2^n} \sum_{k=1}^{n} \frac{2^k}{k} \tag{2.15}$$

and

$$\prod_{r \in [0,n-1]} \binom{n-1}{r} = \frac{((n-1)!)^n}{(0!1! \cdots (n-1)!)^2}.$$

We next consider

$$\sum_{k=1}^{n} \frac{2^k}{k} \bmod p\mathbb{Z}_p.$$

One can verify that

$$\sum_{k=1}^{p-1}\frac{2^k}{k}=\sum_{k=1}^{n}\frac{2^k}{k}+\sum_{k=1}^{n}\frac{2^{p-k}}{p-k}$$
$$\equiv\sum_{k=1}^{n}\frac{2^k}{k}-2\sum_{k=1}^{n}\frac{1}{k\cdot 2^k}\ (\mathrm{mod}\ p\mathbb{Z}_p).$$

Combining this with (2.7) and (2.8), we obtain

$$\sum_{k=1}^{n}\frac{2^k}{k}\equiv\frac{2-2^p}{p}-2^{\frac{p+3}{2}}\frac{P_p-2^{\frac{p-1}{2}}}{p}$$
$$\equiv\frac{2-2^p}{p}-4\left(\frac{2}{p}\right)\frac{P_p-2^{\frac{p-1}{2}}}{p}\ (\mathrm{mod}\ p\mathbb{Z}_p).$$

From this and (2.9), we obtain

$$\sum_{k=1}^{n}\frac{2^k}{k}\equiv\frac{-Q_p-2^p+\left(\frac{2}{p}\right)2^{\frac{p+3}{2}}}{p}\equiv\frac{2-Q_p}{p}\ (\mathrm{mod}\ p\mathbb{Z}_p),\tag{2.16}$$

where the last congruence follows from

$$2-\left(-2^p+\left(\frac{2}{p}\right)2^{\frac{p+3}{2}}\right)=2\left(2^{\frac{p-1}{2}}-\left(\frac{2}{p}\right)\right)^2\equiv 0\ (\mathrm{mod}\ p^2\mathbb{Z}).$$

Now combining (2.16) with (2.14) and (2.10), one can verify that

$$\det B_p(n-1)=\frac{2\cdot((n-1)!)^n}{(0!1!\cdots(n-1)!)^2}\cdot a_p\in\mathbb{F}_p,$$

where

$$a_p=\frac{2-Q_p}{p}\ \mathrm{mod}\ p\mathbb{Z}\in\mathbb{Z}/p\mathbb{Z}=\mathbb{F}_p.$$

(ii) Let $h(t)=t^{n-2}$. Then by (1.6) and Lemma 2.1 we obtain

$$\det B_q(n-2)=\prod_{r=0}^{n-2}\binom{n-2}{r}\cdot\prod_{2\le i<j\le n}(-(s_j-s_i)^2)\tag{2.17}$$
$$=\prod_{r=0}^{n-2}\binom{n-2}{r}\cdot(-1)^{(n-1)(n-2)/2}\prod_{2\le i<j\le n}(s_j-s_i)^2$$
$$=\left(-\frac{1}{2}\right)^{n-2}\cdot\prod_{r=0}^{n-2}\binom{n-2}{r}.$$

Suppose first that $f\ge 2$. Noting that $q\ge 9$, we obtain

$$n-2=\frac{q-5}{2}=\frac{p-5}{2}\cdot 1+\frac{p-1}{2}\cdot p+\cdots+\frac{p-1}{2}\cdot p^{f-1}>\frac{p-1}{2}.$$

By the Lucas congruence again, we clearly have

$$\binom{n-2}{(p-1)/2} \equiv \binom{(p-5)/2}{(p-1)/2}\binom{(p-1)/2}{0}\cdots\binom{(p-1)/2}{0} \equiv 0 \pmod{p\mathbb{Z}}.$$

From this and (2.17), we see that $\det B_q(n-2)=0$ whenever $f\ge 2$.

Suppose now $f=1$. Then $\binom{n-2}{r}\not\equiv 0 \pmod{p\mathbb{Z}}$ for any $r\in[0,n-2]$. Hence by (2.17) again we obtain

$$\det B_p(n-2) = \left(-\frac{1}{2}\right)^{n-2}\cdot\frac{((n-2)!)^{n-1}}{(0!1!\cdots(n-2)!)^2}\in\mathbb{F}_p^\times. \ \blacksquare$$

*Proof of Corollary 1.2.* (i) If $p\equiv 1 \pmod 4$, then $n$ is even. Thus,

$$\left(\frac{\det B_p(n-1)}{p}\right) = \left(\frac{2a_p}{p}\right)\left(\frac{(n-1)!}{p}\right)^n = \left(\frac{2a_p}{p}\right).$$

Suppose now $p\equiv 3 \pmod 4$ and $p>3$. Then $n$ is odd and hence

$$\begin{aligned}\left(\frac{\det B_p(n-1)}{p}\right) &= \left(\frac{2a_p}{p}\right)\left(\frac{(n-1)!}{p}\right) = \left(\frac{-a_p}{p}\right)\left(\frac{n!}{p}\right)\\ &= (-1)^{\frac{h(-p)-1}{2}}\left(\frac{a_p}{p}\right).\end{aligned}$$

The last equality follows from the Mordell congruence [9]

$$n! = \frac{p-1}{2}! \equiv (-1)^{\frac{h(-p)+1}{2}} \pmod{p\mathbb{Z}},$$

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

(ii) Suppose $p\equiv 1 \pmod 4$. Then by the Wilson congruence, one can verify that

$$-1 \equiv (p-1)! \equiv (-1)^n\cdot(n!)^2 \equiv (n!)^2 \pmod{p\mathbb{Z}}.$$

This implies $n! = \sqrt{-1}$ over $\mathbb{F}_p$. Thus,

$$\left(\frac{n!}{p}\right) \equiv (n!)^n \equiv (-1)^{n/2} \equiv \left(\frac{2}{p}\right) \pmod{p\mathbb{Z}},$$

that is,

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

Now from this and Theorem 1.1(ii), and noting that $n$ is even in this case, we obtain

$$\left(\frac{\det B_p(n-2)}{p}\right) = \left(\frac{(n-2)!}{p}\right) = \left(\frac{n!}{p}\right)\left(\frac{(n-1)n}{p}\right) = \left(\frac{6}{p}\right),$$

where the last equality follows from $n(n-1)=3/4$ over $\mathbb{F}_p$.

Suppose now $p \equiv 3 \pmod 4$. Then $n$ is odd. By Theorem 1.1(ii) we clearly have

$$\left(\frac{\det B_p(n-2)}{p}\right) = \left(\frac{-2}{p}\right). \blacksquare$$

## 3. Preparations for the proof of Theorem 1.5

**3.1. A lemma on almost circulant matrices.** Let $n \geq 2$ be an integer and let $\boldsymbol{v} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{C}^n$. The *circulant matrix* of $\boldsymbol{v}$ is the $n \times n$ matrix defined by

$$C_n(\boldsymbol{v}) = [a_{j-i}]_{0 \leq i,j \leq n-1},$$

where $a_s = a_t$ whenever $s \equiv t \pmod n$, that is,

$$C_n(\boldsymbol{v}) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-3} & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_2 & a_3 & \cdots & a_0 & a_1 \\ a_1 & a_2 & \cdots & a_{n-1} & a_0 \end{bmatrix}.$$

Recently, the first two of the present authors [19, Theorem 4.1] defined the *almost circulant matrix* $W_n(\boldsymbol{v})$ of $\boldsymbol{v}$ by

$$W_n(\boldsymbol{v}) = [a_{j-i}]_{1 \leq i,j \leq n-1},$$

and obtained the following result.

LEMMA 3.1. *Let $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ be all the eigenvalues of $C_n(\boldsymbol{v})$. Then*

$$\det W_n(\boldsymbol{v}) = \frac{1}{n} \sum_{l=0}^{n-1} \prod_{k \in [0,n-1] \setminus \{l\}} \lambda_k.$$

**3.2. Some $p$-adic preparations.** Let $\pi \in \mathbb{C}_p$ with $\pi^{p-1} + p = 0$ and let $\zeta_\pi \in \mathbb{C}_p$ be a primitive $p$th root of unity with $\zeta_\pi \equiv 1 + \pi \pmod{\pi^2}$.

Recall that $q = p^f$. Let $\zeta_{q-1} \in \mathbb{C}_p$ be a primitive $(q-1)$th root of unity. Then it is known that $\mathbb{Q}_p(\zeta_{q-1})/\mathbb{Q}_p$ is an unramified extension and $[\mathbb{Q}_p(\zeta_{q-1}) : \mathbb{Q}_p] = f$. Hence

$$\mathbb{Z}_p[\zeta_{q-1}]/\mathfrak{p} \cong \mathbb{F}_q,$$

where $\mathfrak{p} = p\mathbb{Z}_p[\zeta_{q-1}]$ is a prime ideal of $\mathbb{Z}[\zeta_{q-1}]$. From now on, we identify $\mathbb{F}_q$ with $\mathbb{Z}_p[\zeta_{q-1}]/\mathfrak{p}$. The *Teichmüller character* $\omega_q : \mathbb{F}_q \to \mathbb{C}_p$ is the multiplicative character of $\mathbb{F}_q$ defined by

$$\omega_q(x \bmod \mathfrak{p}) \equiv x \pmod{\mathfrak{p}} \tag{3.1}$$

for any $x \in \mathbb{Z}_p[\zeta_{q-1}]$. Also, it is easy to verify that $\omega_q$ is a generator of $\widehat{\mathbb{F}_q^\times}$. For any integer $r \in [0, q-2]$, letting

$$r = r_0 \cdot 1 + r_1 \cdot p + \cdots + r_{f-1} \cdot p^{f-1}$$

be the decomposition of $r$ in base $p$, we define

$$s(r) = \sum_{i=0}^{f-1} r_i. \tag{3.2}$$

For $s(r)$, we have the following result (see [3, Lemma 3.6.7]).

LEMMA 3.2. *For any $r \in [0, q-2]$, we have*

$$s(r) = (p-1) \sum_{i=0}^{f-1} \left\{ \frac{rp^i}{q-1} \right\},$$

*where $\{x\}$ denotes the fractional part of a real number $x$.*

Recall that $n = (q-1)/2 = (p^f - 1)/2$. Using Lemma 3.2, we obtain the following result.

LEMMA 3.3. *Suppose $r \in [0, n-1]$. Then*

$$s(n) + s(n+r) > s(r).$$

*Proof.* For any $i \in [0, f-1]$, we set

$$x_i(r) := \left\{ \frac{rp^i}{q-1} \right\}.$$

Then it is easy to verify that

$$\frac{1}{2} + \left\{ \frac{1}{2} + x_i(r) \right\} = \begin{cases} x_i(r) + 1 & \text{if } 0 \le x_i(r) < 1/2, \\ x_i(r) & \text{if } 1/2 \le x_i(r) < 1. \end{cases} \tag{3.3}$$

As $0 \le r \le n-1$, we have $x_0(r) < 1/2$. Hence by (3.3) we obtain

$$\frac{1}{2} + \left\{ \frac{1}{2} + x_0(r) \right\} > x_0(r).$$

From this, Lemma 3.2 and (3.3), one can verify that

$$\begin{aligned} s(n) + s(n+r) &= (p-1) \sum_{i=0}^{f-1} \left( \frac{1}{2} + \left\{ \frac{(n+r)p^i}{q-1} \right\} \right) \\ &= (p-1) \sum_{i=0}^{f-1} \left( \frac{1}{2} + \left\{ \frac{p^i}{2} + \frac{rp^i}{q-1} \right\} \right) \end{aligned}$$

$$= (p-1)\sum_{i=0}^{f-1}\left(\frac{1}{2}+\left\{\frac{p^i-1}{2}+\frac{1}{2}+\frac{rp^i}{q-1}\right\}\right)$$
$$= (p-1)\sum_{i=0}^{f-1}\left(\frac{1}{2}+\left\{\frac{1}{2}+x_i(r)\right\}\right)$$
$$> (p-1)\sum_{i=0}^{f-1} x_i(r) = s(r). \ \blacksquare$$

Recall that $p$ is an odd prime. We next introduce the $p$-adic Gamma function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$, where $\mathbb{Z}_p^\times$ denotes the group of all $p$-adic units. For any $n \in \mathbb{Z}^+$, we define

$$\Gamma_p(n) = (-1)^n \prod_{k\in[1,n-1]\cap\mathbb{Z}_p^\times} k.$$

Since $\mathbb{Z}^+$ is dense in $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ is a closed multiplicative group, the *p-adic Gamma function* $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$ is defined by

$$\Gamma_p(x) = \lim_{i\to\infty} \Gamma_p(x_i),$$

where $\{x_i\}_{i=1}^\infty$ is a sequence of positive integers $x_i$ with $\lim_{i\to\infty} x_i = x$.

In this paper, we need the following result on $\Gamma_p$.

LEMMA 3.4. *Suppose that $p \geq 5$ is a prime. Let $n \in \mathbb{Z}^+$. Then for any $x, y \in \mathbb{Z}_p$ we have*

$$x \equiv y \pmod{p^n\mathbb{Z}_p} \implies \Gamma_p(x) \equiv \Gamma_p(y) \pmod{p^n\mathbb{Z}_p}.$$

We conclude this section with the following result, which is known as the *Gross–Koblitz formula* [6, Theorem 1.7].

LEMMA 3.5. *Let notations be as above. For any $r \in [0, q-2]$, consider the Gauss sum*

$$G_q(\omega_q^{-r}) = \sum_{x\in\mathbb{F}_q} \omega_q^{-r}(x)\zeta_\pi^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}.$$

*Then*

$$G_q(\omega_q^{-r}) = -\pi^{s(r)} \cdot \prod_{i=0}^{f-1} \Gamma_p\left(\left\{\frac{rp^i}{q-1}\right\}\right),$$

*where $\Gamma_p$ is the p-adic Gamma function and $\{x\}$ is the fractional part of $x$.*

**4. Proof of Theorem 1.5.** Let notations be as in Section 3. In this section, we fix a generator $g$ of the cyclic group $\mathbb{F}_q^\times$. Recall that $n = (q-1)/2$. For any $i \in [0, n-1]$, we let

$$a_i = \omega_q^{-n}(1+g^{2i}),$$

and let

$$\boldsymbol{v} = (a_0, a_1, \ldots, a_{n-1}).$$

We begin with the following result.

LEMMA 4.1. *For any $r \in [0, n-1]$, let*

$$\lambda_r := \frac{(-1)^r}{2} J_q(\omega_q^{-n}, \omega_q^{-r}) + \frac{(-1)^{n+r}}{2} J_q(\omega_q^{-n}, \omega_q^{-(n+r)}). \tag{4.1}$$

*Then $\lambda_0 = -1, \lambda_1, \ldots, \lambda_{n-1}$ are all the eigenvalues of the circulant matrix $C_n(\boldsymbol{v})$.*

*Proof.* For any $r \in [0, n-1]$, one can verify that

$$\begin{aligned}\sum_{0\le j\le n-1} &\omega_q^{-n}(1+g^{2j-2i})\omega_q^{-r}(g^{2j}) \\ &= \sum_{0\le j\le n-1} \omega_q^{-n}(1+g^{2j-2i})\omega_q^{-r}(g^{2j-2i})\omega_q^{-r}(g^{2i}) \\ &= \sum_{0\le j\le n-1} \omega_q^{-n}(1+g^{2j})\omega_q^{-r}(g^{2j})\omega_q^{-r}(g^{2i}).\end{aligned}$$

This implies that for any $r \in [0, n-1]$,

$$C_n(\boldsymbol{v})\boldsymbol{u}_r = y_r \boldsymbol{u}_r$$

with the column vector

$$\boldsymbol{u}_r = (\omega_q^{-r}(g^0), \omega_q^{-r}(g^2), \ldots, \omega_q^{-r}(g^{2(n-1)}))^T,$$

and

$$y_r = \sum_{0\le j\le n-1} \omega_q^{-n}(1+g^{2j})\omega_q^{-r}(g^{2j}).$$

As $\boldsymbol{u}_0, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{n-1}$ are clearly linearly independent over $\mathbb{C}$, the numbers $y_0, y_1, \ldots, y_{n-1}$ are all the eigenvalues of $C_n(\boldsymbol{v})$. Note that

$$\frac{1}{2}(\varepsilon(x) + \omega_q^{-n}(x)) = \begin{cases} 1 & \text{if } x \in \{s_1, s_2, \ldots, s_n\}, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, for each $r \in [0, n-1]$, we have

$$\begin{aligned} y_r &= \sum_{0\le j\le n-1} \omega_q^{-n}(1+g^{2j})\omega_q^{-r}(g^{2j}) = \sum_{1\le j\le n} \omega_q^{-n}(1+s_j)\omega_q^{-r}(s_j) \\ &= \frac{1}{2}\sum_{x\in\mathbb{F}_q} (\varepsilon(x) + \omega_q^{-n}(x))\omega_q^{-n}(1+x)\omega_q^{-r}(x) \\ &= \frac{(-1)^r}{2}\sum_{x\in\mathbb{F}_q} \omega_q^{-n}(1+x)\omega_q^{-r}(-x) + \frac{(-1)^{n+r}}{2}\sum_{x\in\mathbb{F}_q} \omega_q^{-n}(1+x)\omega_q^{-(n+r)}(-x) \\ &= \lambda_r. \end{aligned}$$

For $\lambda_0$, one can verify that

$$\begin{aligned}\lambda_0 &= \frac{1}{2}J_q(\omega_q^{-n},\varepsilon)+\frac{(-1)^n}{2}J_q(\omega_q^{-n},\omega_q^{-n})\\ &= \frac{1}{2}J_q(\omega_q^{-n},\varepsilon)+\frac{(-1)^n}{2}J_q(\omega_q^{-n},\omega_q^{n})\\ &= -\frac{1}{2}\omega_q(1)+\frac{(-1)^n}{2}(-\omega_q^{-n}(-1))=-1.\end{aligned}$$

In view of the above, we have completed the proof. ∎

*Proof of Theorem 1.5.* Recall that $g$ is a generator of $\mathbb{F}_q^\times$. Then it is clear that

$$\det B_q(n)=\det\left[(1+s_j/s_i)^n\right]_{2\le i,j\le n}=\det\left[(1+g^{2j-2i})^n\right]_{1\le i,j\le n-1}.$$

By the definition (3.1) of the Teichmüller character $\omega_q$ of $\mathbb{F}_q$, we see that

$$\begin{aligned}\det B_q(n) &= \det\left[\omega_q^{-n}(1+g^{2j-2i})\right]_{1\le i,j\le n-1} \bmod \mathfrak{p}\\ &= \det W_n(\boldsymbol{v}) \bmod \mathfrak{p},\end{aligned}\tag{4.2}$$

where

$$\boldsymbol{v}=(\omega_q^{-n}(1+g^0),\omega_q^{-n}(1+g^2),\dots,\omega_q^{-n}(1+g^{2(n-1)})),$$

and $\mathfrak{p}=p\mathbb{Z}_p[\zeta_{q-1}]$ is a prime ideal. Hence we focus on the determinant of the almost circulant matrix $W_n(\boldsymbol{v})$. By Lemmas 4.1 and 3.1 we have

$$\det B_q(n)=\det W_n(\boldsymbol{v}) \bmod \mathfrak{p}=\frac{1}{n}\sum_{l=0}^{n-1}\prod_{r\in[0,n-1]\setminus\{l\}}\lambda_r \bmod \mathfrak{p},\tag{4.3}$$

where $\lambda_r$ is defined by (4.1). We next consider $\lambda_r \bmod \mathfrak{p}$. Suppose $r\in[1,n-1]$. Then

$$J_q(\omega_q^{-n},\omega_q^{-(n+r)})=\frac{G_q(\omega_q^{-n})G_q(\omega_q^{-(n+r)})}{G_q(\omega_q^{-r})}.$$

By Lemmas 3.5 and 3.3, we obtain

$$\operatorname{ord}_p(J_q(\omega_q^{-n},\omega_q^{-(n+r)}))=\frac{1}{p-1}(s(n)+s(n+r)-s(r))>0.$$

This implies that

$$J_q(\omega_q^{-n},\omega_q^{-(n+r)})\equiv 0 \pmod{\mathfrak{p}}$$

for any $r\in[1,n-1]$. Hence by (4.1) we have

$$\lambda_r\equiv\frac{(-1)^r}{2}J_q(\omega_q^{-n},\omega_q^{-r}) \pmod{\mathfrak{p}}\tag{4.4}$$

whenever $r\in[1,n-1]$.

Case I: $f \geq 2$. Suppose $r \in [1, n-1]$. Then

$$J_q(\omega_q^{-n}, \omega_q^{-r}) = \frac{G_q(\omega_q^{-n}) G_q(\omega_q^{-r})}{G_q(\omega_q^{-(n+r)})}.$$

By Lemma 3.5 we obtain

$$\operatorname{ord}_p(J_q(\omega_q^{-n}, \omega_q^{-r})) = \frac{1}{p-1}(s(n) + s(r) - s(n+r)). \tag{4.5}$$

As $q = p^f \geq 9$, we have $n - 1 \geq (p+3)/2$. From this, for $r \in \{(p+1)/2, (p+3)/2\} \subseteq [1, n-1]$, we have

$$s(n) + s(r) > s(n+r).$$

This, together with (4.5), implies that

$$\begin{aligned} &|\{1 \leq r \leq n-1 : J_q(\omega_q^{-n}, \omega_q^{-r}) \equiv 0 \pmod{\mathfrak{p}}\}| \\ &\qquad = |\{1 \leq r \leq n-1 : \lambda_r \equiv 0 \pmod{\mathfrak{p}}\}| \geq 2. \end{aligned}$$

From this, (4.4) and (4.3), we see that $B_q(n)$ is singular if $f \geq 2$.

Case II: $f = 1$. Note first that, in this case, $\mathbb{Q}_p(\zeta_{q-1}) = \mathbb{Q}_p$ and $\mathfrak{p} = p\mathbb{Z}_p$. By (4.5), for any $r \in [1, n-1]$, we see that

$$\begin{aligned} \operatorname{ord}_p(J_p(\omega_p^{-n}, \omega_p^{-r})) &= \frac{1}{p-1}(s(n) + s(r) - s(n+r)) \\ &= \frac{1}{p-1}(n + r - (n+r)) = 0. \end{aligned}$$

Thus, for any $r \in [1, n-1]$,

$$\lambda_r \equiv \frac{(-1)^r}{2} J_q(\omega_p^{-n}, \omega_p^{-r}) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

that is, $\lambda_r$ is a $p$-adic unit. From this and (4.3), we obtain

$$\det B_q(n) = -2\lambda_0\lambda_1 \cdots \lambda_{n-1}\left(\frac{1}{\lambda_0} + \frac{1}{\lambda_1} + \cdots + \frac{1}{\lambda_{n-1}}\right) \bmod p\mathbb{Z}_p. \tag{4.6}$$

We next consider $\lambda_r \bmod p\mathbb{Z}_p$. Suppose $r \in [1, n-1]$. Then by Lemmas 3.4 and 3.5, one can verify that

$$\begin{aligned} \lambda_r &\equiv \frac{(-1)^r}{2} J_p(\omega_p^{-n}, \omega_p^{-r}) \equiv \frac{(-1)^r}{2} \cdot \frac{G_p(\omega_p^{-n}) G_p(\omega_p^{-r})}{G_p(\omega_p^{-(n+r)})} \\ &\equiv \frac{(-1)^{r+1}}{2} \cdot \frac{\Gamma_p\left(\frac{n}{p-1}\right)\Gamma_p\left(\frac{r}{p-1}\right)}{\Gamma_p\left(\frac{n+r}{p-1}\right)} \equiv \frac{(-1)^{r+1}}{2} \cdot \frac{\Gamma_p(p-n)\Gamma_p(p-r)}{\Gamma_p(p-n-r)} \end{aligned}$$

$$\equiv \frac{(-1)^r}{2}\cdot\frac{(p-n-1)!\cdot(p-r-1)!}{(p-1-n-r)!}\equiv\frac{(-1)^{r+1}}{2}\cdot\frac{(n+r)!}{n!\cdot r!}$$
$$\equiv\frac{(-1)^{r+1}}{2}\binom{n+r}{r}\equiv-\frac{1}{2}\binom{n}{r}\pmod{p\mathbb{Z}_p}.$$

The last congruence follows from

$$(-1)^r\cdot\binom{n+r}{r}\equiv\binom{n}{r}\pmod{p\mathbb{Z}}$$

for any $r\in[1,n-1]$.

By the above results and Sury's identity (2.15), we obtain

$$\begin{aligned}
&-2\lambda_0\lambda_1\cdots\lambda_{n-1}\left(\frac{1}{\lambda_0}+\frac{1}{\lambda_1}+\cdots+\frac{1}{\lambda_{n-1}}\right)\\
&\quad\equiv(-1)^{n-1}\left(\frac{1}{2}\right)^{n-2}\cdot\prod_{r=0}^{n}\binom{n}{r}\cdot\left(3-2\sum_{r=0}^{n}\binom{n}{r}^{-1}\right)\\
&\quad\equiv(-1)^{n-1}\left(\frac{1}{2}\right)^{n-2}\cdot\frac{(n!)^{n+1}}{(0!1!\cdots n!)^2}\cdot\left(3-\frac{n+1}{2^n}\sum_{k=1}^{n+1}\frac{2^k}{k}\right)\\
&\quad\equiv(-1)^{n-1}\left(\frac{1}{2}\right)^{n-2}\cdot\frac{(n!)^{n+1}}{(0!1!\cdots n!)^2}\cdot\left(3-\frac{1}{2^{n+1}}\sum_{k=1}^{n+1}\frac{2^k}{k}\right)\\
&\quad\equiv(-1)^{n-1}\left(\frac{1}{2}\right)^{n-2}\cdot\frac{(n!)^{n+1}}{(0!1!\cdots n!)^2}\cdot\left(1-\frac{1}{2^{n+1}}\sum_{k=1}^{n}\frac{2^k}{k}\right)\pmod{p\mathbb{Z}_p}.
\end{aligned}$$

From this and using (2.16) and (2.9), we finally obtain

$$\begin{aligned}
&-2\lambda_0\lambda_1\cdots\lambda_{n-1}\left(\frac{1}{\lambda_0}+\frac{1}{\lambda_1}+\cdots+\frac{1}{\lambda_{n-1}}\right)\\
&\quad\equiv(-1)^n\left(\frac{1}{2}\right)^{n-2}\cdot\frac{(n!)^{n+1}}{(0!1!\cdots n!)^2}\cdot\frac{2(\frac{2}{p})-2P_p-p}{p}\pmod{p\mathbb{Z}_p}.
\end{aligned}$$

In view of the above, we have completed the proof. ∎

**5. Proof of Theorem 1.8.** We begin with the following lemma.

LEMMA 5.1. *Let $\chi_q$ be a generator of $\widehat{\mathbb{F}_q^\times}$. Then for any nontrivial character $\psi\in\widehat{\mathbb{F}_q^\times}$, the following results hold:*

$$A_q=\prod_{r=0}^{q-2}J_q(\psi,\chi_q^r)=\frac{G_q(\psi)^{q-1}}{q},\tag{5.1}$$

$$S_q=\sum_{r=0}^{q-2}\frac{1}{J_q(\psi,\chi_q^r)}=\frac{1-q}{q}(1+\psi(-1)), \tag{5.2}$$

$$T_q=\sum_{r=0}^{q-2}\frac{(-1)^r}{J_q(\psi,\chi_q^r)}=\frac{1-q}{q}(2-\overline{\psi(2)}). \tag{5.3}$$

*Proof.* Since $\chi_q$ is a generator of $\widehat{\mathbb{F}_q^\times}$ and $\psi\neq\varepsilon$, there is a unique integer $j\in[1,q-2]$ such that $\chi_q^{-j}=\psi$. One can verify that

$$\begin{aligned}\prod_{r=0}^{q-2}J_q(\psi,\chi_q^r)&=\prod_{r=0}^{q-2}J_q(\chi_q^{-j},\chi_q^r)=J_q(\chi_q^{-j},\chi_q^j)\cdot\prod_{r\in[0,q-2]\setminus\{j\}}J_q(\chi_q^{-j},\chi_q^r)\\&=(-1)^{j+1}\cdot\prod_{r\in[0,q-2]\setminus\{j\}}\frac{G_q(\chi_q^{-j})G_q(\chi_q^r)}{G_q(\chi_q^{-j+r})}\\&=(-1)^{j+1}\cdot\frac{G_q(\varepsilon)}{G_q(\chi_q^{-j})G_q(\chi_q^j)}\cdot\prod_{r\in[0,q-2]}\frac{G_q(\chi_q^{-j})G_q(\chi_q^r)}{G_q(\chi_q^{-j+r})}\\&=\frac{G_q(\chi_q^{-j})^{q-1}}{q}\cdot\prod_{r\in[0,q-2]}\frac{G_q(\chi_q^r)}{G_q(\chi_q^{-j+r})}=\frac{G_q(\psi)^{q-1}}{q}.\end{aligned}$$

This completes the proof of (5.1).

Now we prove (5.2). As $|J_q(\chi_q^{-j},\chi_q^r)|=\sqrt{q}$ whenever $r\in[1,q-2]\setminus\{j\}$, one can verify that

$$\begin{aligned}\sum_{r=0}^{q-2}\frac{1}{J_q(\psi,\chi_q^r)}&=\sum_{r=0}^{q-2}\frac{1}{J_q(\chi_q^{-j},\chi_q^r)}\\&=\frac{1}{J_q(\chi_q^{-j},\varepsilon)}+\frac{1}{J_q(\chi_q^{-j},\chi_q^j)}+\frac{1}{q}\sum_{r\in[1,q-2]\setminus\{j\}}\frac{q}{J_q(\chi_q^{-j},\chi_q^r)}\\&=-(1+(-1)^j)+\frac{1}{q}\sum_{r\in[1,q-2]\setminus\{j\}}\overline{J_q(\chi_q^{-j},\chi_q^r)}\\&=-(1+\psi(-1))+\frac{1}{q}\sum_{r\in[0,q-2]}\overline{J_q(\chi_q^{-j},\chi_q^r)}-\frac{1}{q}\overline{J_q(\psi,\varepsilon)}-\frac{1}{q}\overline{J_q(\psi,\psi^{-1})}\\&=\frac{1-q}{q}(1+\psi(-1)),\end{aligned}$$

where the last equality follows from

$$\sum_{r\in[0,q-2]}J_q(\chi_q^{-j},\chi_q^r)=0.$$

This completes the proof of (5.2).

Finally, we prove (5.3). We first claim that

$$\sum_{r\in[0,(q-3)/2]} J_q(\psi,\chi_q^{2r}) = \frac{(q-1)\psi(2)}{2}. \tag{5.4}$$

In fact, it is easy to verify that

$$\begin{aligned}\sum_{r\in[0,(q-3)/2]} J_q(\psi,\chi_q^{2r}) &= \sum_{r\in[0,(q-3)/2]}\sum_{x\in\mathbb{F}_q}\psi(1-x)\chi_q^{2r}(x)\\ &= \sum_{x\in\mathbb{F}_q}\psi(1-x)\sum_{r\in[0,(q-3)/2]}\chi_q^{2r}(x) = \frac{q-1}{2}\psi(2),\end{aligned}$$

where the last equality follows from

$$\sum_{r\in[0,(q-3)/2]}\chi_q^{2r}(x) = \begin{cases}(q-1)/2 & \text{if } x=\pm1,\\ 0 & \text{otherwise.}\end{cases}$$

By (5.4) we obtain

$$\begin{aligned}S_q+T_q &= 2\sum_{r\in[0,(q-3)/2]}\frac{1}{J_q(\psi,\chi_q^{2r})}\\ &= \frac{2}{J_q(\psi,\varepsilon)}+\frac{1+\psi(-1)}{J_q(\psi,\psi^{-1})}+\frac{2}{q}\sum_{\substack{r\in[1,(q-3)/2]\\ \chi_q^{2r}\neq\psi^{-1}}}\frac{q}{J_q(\psi,\chi_q^{2r})}\\ &= -(3+\psi(-1))+\frac{2}{q}\sum_{\substack{r\in[1,(q-3)/2]\\ \chi_q^{2r}\neq\psi^{-1}}}\overline{J_q(\psi,\chi_q^{2r})}\\ &= -(3+\psi(-1))+\frac{2}{q}\sum_{r\in[0,(q-3)/2]}\overline{J_q(\psi,\chi_q^{2r})}\\ &\quad -\frac{2}{q}\overline{J_q(\psi,\varepsilon)}-\frac{1+\psi(-1)}{q}\overline{J_q(\psi,\psi^{-1})}\\ &= \frac{1-q}{q}(3+\psi(-1)-\overline{\psi(2)}).\end{aligned}$$

Combining this with (5.2), we have

$$T_q = (S_q+T_q)-S_q = \frac{1-q}{q}(2-\overline{\psi(2)}). \ \blacksquare$$

Remark 5.2. In 1987, Greene [4, Definition 2.4] used Jacobi sums to obtain a finite field analogue of binomial coefficients. In fact, for any $A,B\in\widehat{\mathbb{F}_q^\times}$, Green defined

$$\binom{A}{B} := \frac{B(-1)}{q}J_q(A,\overline{B}).$$

By (5.3) for any nontrivial character $\psi$, we obtain

$$\sum_{r=0}^{q-2}\binom{\psi}{\chi_q^r}^{-1}=q\sum_{r=0}^{q-2}\frac{(-1)^r}{J_q(\psi,\chi_q^{-r})}=qT_q=(1-q)(2-\overline{\psi(2)}). \tag{5.5}$$

The identity (5.5) can be viewed as a finite field analogue of Sury's identity

$$\sum_{r=0}^{n-1}\binom{n-1}{r}^{-1}=\frac{n}{2^n}\sum_{k=1}^{n}\frac{2^k}{k}.$$

From now on, we fix a generator $g$ of $\mathbb{F}_q^\times$. For any nontrivial character $\psi\in\widehat{\mathbb{F}_q^\times}$, define the circulant matrices

$$M_q(\psi):=[\psi(g^{j-i}-1)]_{0\le i,j\le q-2}, \tag{5.6}$$

$$N_q(\psi):=[\psi(g^{j-i}+1)]_{0\le i,j\le q-2}. \tag{5.7}$$

We need the following lemma.

LEMMA 5.3. *Let $\chi_q$ be a generator of $\widehat{\mathbb{F}_q^\times}$. Then the numbers*

$$\alpha_r=\psi(-1)J_q(\psi,\chi_q^r)\quad(r=0,1,\ldots,q-2)$$

*are all the eigenvalues of $M_q(\psi)$. Also, the numbers*

$$\beta_r=(-1)^rJ_q(\psi,\chi_q^r)\quad(r=0,1,\ldots,q-2)$$

*are all the eigenvalues of $N_q(\psi)$.*

*Proof.* For any $r\in[0,q-2]$, it is easy to see that

$$\begin{aligned}\sum_{j=0}^{q-2}\psi(g^{j-i}-1)\chi_q^r(g^j)&=\sum_{j=0}^{q-2}\psi(g^{j-i}-1)\chi_q^r(g^{j-i})\chi_q^r(g^i)\\&=\sum_{j=0}^{q-2}\psi(g^j-1)\chi_q^r(g^j)\chi_q^r(g^i)\\&=\sum_{x\in\mathbb{F}_q}\psi(x-1)\chi_q^r(x)\chi_q^r(g^i)\\&=\psi(-1)J_q(\psi,\chi_q^r)\chi_q^r(g^i).\end{aligned}$$

This implies that

$$M_q(\psi)\boldsymbol{\xi}_r=\alpha_r\boldsymbol{\xi}_r,$$

where

$$\boldsymbol{\xi}_r=(\chi_q^r(g^0),\chi_q^r(g^1),\ldots,\chi_q^r(g^{q-2}))^T.$$

As the $\boldsymbol{\xi}_r$ are linearly independent over $\mathbb{C}$, the numbers $\alpha_0,\alpha_1,\ldots,\alpha_{q-2}$ are all the eigenvalues of $M_q(\psi)$. Using essentially the same method, one can see that all the eigenvalues of $N_q(\psi)$ are $\beta_0,\beta_1,\ldots,\beta_{q-2}$. ∎

*Proof of Theorem 1.8.* (i) It is clear that

$$G(t)=\frac{t^{q-1}-1}{t-1}=1+t+\cdots+t^{q-2}=\prod_{i=2}^{q-1}(t-x_i)$$

over $\mathbb{F}_q$. This implies

$$\prod_{i=2}^{q-2}x_i=-1. \tag{5.8}$$

Recall that $g$ is a generator of $\mathbb{F}_q^\times$. By (5.8) we obtain

$$\begin{aligned}\det D_q^-(\psi)&=\prod_{i=2}^{q-1}\psi(x_i)\cdot\det\left[\psi\left(\frac{x_j}{x_i}-1\right)\right]_{2\le i,j\le q-1}\\&=\psi(-1)\cdot\det\left[\psi(g^{j-i}-1)\right]_{1\le i,j\le q-2}.\end{aligned} \tag{5.9}$$

Note that $[\psi(g^{j-i}-1)]_{1\le i,j\le q-2}$ is an almost circulant matrix. By Lemmas 3.1, 5.1 and 5.3, we obtain

$$\begin{aligned}\det\left[\psi(g^{j-i}-1)\right]_{1\le i,j\le q-2}&=\frac{1}{q-1}\cdot\alpha_0\alpha_1\cdots\alpha_{q-2}\cdot\left(\frac{1}{\alpha_0}+\frac{1}{\alpha_1}+\cdots+\frac{1}{\alpha_{q-2}}\right)\\&=\frac{\psi(-1)}{q-1}\cdot\prod_{r=0}^{q-2}J_q(\psi,\chi_q^r)\cdot\left(\sum_{r=0}^{q-2}\frac{1}{J_q(\psi,\chi_q^r)}\right)\\&=-\frac{1+\psi(-1)}{q^2}G_q(\psi)^{q-1}.\end{aligned}$$

Combining this with (5.9), we obtain

$$\det D_q^-(\psi)=-\frac{1+\psi(-1)}{q^2}G_q(\psi)^{q-1}.$$

(ii) Similar to (5.9), we have

$$\det D_q^+(\psi)=\psi(-1)\cdot\det\left[\psi(g^{j-i}+1)\right]_{1\le i,j\le q-2}. \tag{5.10}$$

Since $[\psi(g^{j-i}+1)]_{1\le i,j\le q-2}$ is an almost circulant matrix, by Lemmas 3.1, 5.1 and 5.3 one can verify that

$$\begin{aligned}\det\left[\psi(g^{j-i}+1)\right]_{1\le i,j\le q-2}&=\frac{1}{q-1}\cdot\beta_0\beta_1\cdots\beta_{q-2}\cdot\left(\frac{1}{\beta_0}+\frac{1}{\beta_1}+\cdots+\frac{1}{\beta_{q-2}}\right)\\&=\frac{(-1)^{(q-1)/2}}{q-1}\cdot\prod_{r=0}^{q-2}J_q(\psi,\chi_q^r)\cdot\left(\sum_{r=0}^{q-2}\frac{(-1)^r}{J_q(\psi,\chi_q^r)}\right)\\&=\frac{(-1)^{(q+1)/2}}{q^2}(2-\overline{\psi(2)})G_q(\psi)^{q-1}.\end{aligned}$$

From this and (5.10), we finally obtain

$$\det D_q^+(\psi) = \frac{(-1)^{(q+1)/2}\cdot\psi(-1)}{q^2}(2-\overline{\psi(2)})G_q(\psi)^{q-1}. \ \blacksquare$$

**Acknowledgements.** The authors would like to thank the referee for helpful comments. We also thank Prof. Hao Pan for his helpful comments and steadfast encouragement.

It is with great pleasure that we dedicate this paper to our advisor Professor Zhi-Wei Sun on the occasion of his 60th birthday.

**Funding.** This research was supported by the Natural Science Foundation of China (Grant Nos. 12101321, 12201291 and 12371004). The first author was supported by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 25KJB110010).

## References

[1] L. Carlitz, *Some cyclotomic matrices*, Acta Arith. 5 (1959), 293–308.
[2] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. 115 (2004), 231–244.
[3] H. Cohen, *Number Theory, Vol. I. Tools and Diophantine Equations*, Springer, 2007.
[4] J. Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. 301 (1987), 77–101.
[5] D. Grinberg, Z.-W. Sun and L. Zhao, *Proof of three conjectures on determinants related to quadratic residues*, Linear Multilinear Algebra 70 (2022), 3734–3746.
[6] B. Gross and N. Koblitz, *Gauss sums and the p-adic $\Gamma$-function*, Ann. of Math. 109 (1979), 569–581.
[7] C. Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. 411 (2005), 68–166.
[8] D. H. Lehmer, *On certain character matrices*, Pacific J. Math. 6 (1956), 491–499.
[9] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod p$, Amer. Math. Monthly 68 (1961), 145–146.
[10] Z.-H. Sun, *Congruences involving Bernoulli and Euler numbers*, J. Number Theory 128 (2008), 280–312.
[11] Z.-W. Sun, *A congruence for primes*, Proc. Amer. Math. Soc. 123 (1995), 1341–1346.
[12] Z.-W. Sun, *On the sum* $\sum_{k\equiv r\,(\mathrm{mod}\,m)}\binom{n}{k}$ *and related congruences*, Israel J. Math. 128 (2002), 135–156.
[13] Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. 56 (2019), 285–307.
[14] Z.-W. Sun, *Some determinants involving quadratic residues modulo primes*, Front. Math., in press.
[15] B. Sury, *Sum of reciprocals of the binomial coefficients*, Eur. J. Combin. 14 (1993), 351–353.
[16] M. Vsemirnov, *On the evaluation of R. Chapman's "evil determinant"*, Linear Algebra Appl. 436 (2012), 4101–4106.
[17] M. Vsemirnov, *On R. Chapman's "evil determinant": case* $p \equiv 1 \pmod 4$, Acta Arith. 159 (2013), 331–344.

[18] H.-L. Wu, *Determinants concerning Legendre symbols*, C. R. Math. Acad. Sci. Paris 359 (2021), 651–655.
[19] H.-L. Wu and L.-Y. Wang, *The Gross–Koblitz formula and almost circulant matrices related to Jacobi sums*, Finite Fields Appl. 103 (2025), art. 102581, 21 pp.

Hai-Liang Wu
School of Science
Nanjing University of Posts
and Telecommunications
210023 Nanjing, P. R. China
E-mail: whl.math@smail.nju.edu.cn

Li-Yuan Wang
School of Physical
and Mathematical Sciences
Nanjing Tech University
211816 Nanjing, P. R. China
E-mail: wly@smail.nju.edu.cn

He-Xia Ni (corresponding author)
Department of Applied Mathematics
Nanjing Audit University
211815 Nanjing, P. R. China
E-mail: nihexia@yeah.net