A Conjecture of Zhi-Wei Sun on Determinants Over Finite Fields

Hai-Liang Wu\(^{1}\) · Yue-Feng She\(^{2}\) · He-Xia Ni\(^{3}\)

Received: 3 March 2022 / Revised: 28 June 2022 / Accepted: 30 June 2022 / Published online: 15 July 2022
© The Author(s), under exclusive licence to Malaysian Mathematical Sciences Society and Penerbit Universiti Sains Malaysia 2022

Abstract

In this paper, we study certain determinants over finite fields. Let \(\mathbb{F}_q\) be the finite field of \(q\) elements with \(q\) an odd prime power and \(q \equiv 2 \pmod{3}\). Let \(a_1, a_2, \ldots, a_{q-1}\) be all nonzero elements of \(\mathbb{F}_q\) and let \(T_q = \begin{bmatrix} 1 & a_2 & a_3 & \cdots & a_{q-1} \\ a_1 & a_1^2 & a_1^3 & \cdots & a_1^{q-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ a_{q-1} & a_{q-1}^2 & a_{q-1}^3 & \cdots & a_{q-1}^{q-1} \end{bmatrix}_{1 \leq i, j \leq q-1}\) be a matrix over \(\mathbb{F}_q\). We obtain the explicit value of \(\det(T_q)\). Also, as a consequence of our result, we confirm a conjecture posed by Zhi-Wei Sun.

Keywords Determinants · The Legendre symbol · Finite fields

Mathematics Subject Classification Primary 11C20; Secondary 11L05 · 11R29.

Communicated by Emrah Kilic.

\(^{1}\) School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, People’s Republic of China

\(^{2}\) Department of Mathematics, Nanjing University, Nanjing 210093, People’s Republic of China

\(^{3}\) Department of Applied Mathematics, Nanjing Audit University, Nanjing 211815, People’s Republic of China

Contact He-Xia Ni
nihexia@yeah.net

Contact Hai-Liang Wu
whel.math@smail.nju.edu.cn

Contact Yue-Feng She
she.math@smail.nju.edu.cn
1 Introduction

Let \( R \) be a commutative ring. Then for any \( n \times n \) matrix \( M = [a_{ij}]_{1 \leq i,j \leq n} \) with \( a_{ij} \in R \), we use \( \det(M) \) to denote the determinant of \( M \).

Let \( p \) be an odd prime and let \( (\cdot)^p \) be the Legendre symbol. Carlitz [1] studied the following matrix

\[
C_p(\lambda) = \left[ \lambda + \left( \frac{i-j}{p} \right) \right]_{1 \leq i,j \leq p-1}, \quad (\lambda \in \mathbb{C}).
\]

Carlitz [1, Theorem 4] proved that the characteristic polynomial of \( C_p(\lambda) \) is

\[
P_\chi(t) = (t^2 - (-1)^{(p-1)/2} p^{(p-3)/2})(t^2 - (p-1)\lambda - (-1)^{(p-1)/2}).
\]

Later Chapman [2, 3] investigated many interesting variants of \( C_p \). Moreover, Chapman [3] posed a challenging conjecture on the determinant of the \( \frac{p+1}{2} \times \frac{p+1}{2} \) matrix

\[
E_p = \left[ \left( \frac{j-i}{p} \right) \right]_{1 \leq i,j \leq \frac{p+1}{2}}.
\]

Due to the difficulty of the evaluation on \( \det(E_p) \), Chapman called this determinant “evil” determinant. Finally, by using sophisticated matrix decompositions, Vsemirnov [7, 8] solved this problem completely.

Along this line, in 2019 Sun [6] studied the following matrix

\[
S_p = \left[ \left( \frac{i^2 + j^2}{p} \right) \right]_{1 \leq i,j \leq \frac{p-1}{2}},
\]

and Sun [6, Theorem 1.2(iii)] showed that \(- \det(S_p)\) is always a quadratic residue modulo \( p \). In the same paper, Sun also investigated the matrix

\[
A_p = \left[ \frac{1}{i^2 + j^2} \right]_{1 \leq i,j \leq \frac{p-1}{2}}.
\]

Sun [6, Theorem 1.4(ii)] proved that when \( p \equiv 3 \pmod{4} \) the \( p \)-adic integer \( 2 \det(A_p) \) is always a quadratic residue modulo \( p \). In addition, let

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

Sun [6, Remark 1.3] posed the following conjecture.

**Conjecture 1.1 (Zhi-Wei Sun)** Let \( p \equiv 2 \pmod{3} \) be an odd prime. Then \( 2 \det(T_p) \) is a quadratic residue modulo \( p \).
Let $\mathbb{F}_q$ be the finite field of $q$ elements and let

$$\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\} = \{a_1, a_2, \ldots, a_{q-1}\}.$$  

Motivated by this conjecture, we define a matrix $T_q$ over $\mathbb{F}_q$ by

$$T_q = \left[\frac{1}{a_i^2 - a_i a_j + a_j^2}\right]_{1 \leq i, j \leq q-1}.$$  

We obtain the following generalized result.

**Theorem 1.1** Let $q \equiv 2 \pmod{3}$ be an odd prime power and let

$$T_q = \left[\frac{1}{a_i^2 - a_i a_j + a_j^2}\right]_{1 \leq i, j \leq q-1}.$$  

Then

$$\det(T_q) = (-1)^{\frac{q-1}{2}} 2^{\frac{q-2}{3}} \in \mathbb{F}_p,$$

where $p$ is the characteristic of $\mathbb{F}_q$.

**Remark 1.1** We give two examples here. Note that we also view $T_p$ as a matrix over $\mathbb{F}_p$ if $p$ is an odd prime.

(i) If $p = 5$, then

$$\det(T_p) = \frac{11}{596232} = \frac{1}{2} = -2.$$  

(ii) If $p = 11$, then

$$\det(T_p) = \frac{393106620416000000}{23008992710579652367225919172202284572822491031943} = \frac{4}{6} = 2^3.$$  

As a direct consequence of our theorem, we confirm Sun’s conjecture.

**Corollary 1.1** Conjecture 1.1 holds.

The outline of this paper is as follows. In Sect. 2, we will prove some lemmas which are the key elements in the proof of our theorem. The proofs of Theorem 1.1 and Corollary 1.1 will be given in Sect. 3.

## 2 Some Preparations

Given any polynomials $A(T), B(T) \in \mathbb{F}_q[T]$, we say that $A(T)$ and $B(T)$ are equivalent (denoted by $A(T) \sim B(T)$) if $A(x) = B(x)$ for each $x \in \mathbb{F}_q$.

Let $\chi_3(\cdot) = \left(\frac{\cdot}{3}\right)$ be the quadratic character modulo 3. We first have the following lemma.
Lemma 2.1 Let \( q \equiv 2 \pmod{3} \) be an odd prime power and let

\[
G(T) = 1 + \frac{1}{3} \sum_{k=2}^{q-2} (\chi_3(k) + \chi_3(1-k)) T^{k-1} + \frac{1}{3} T^{q-2} - \frac{2}{3} T^{q-1}. \tag{2.1}
\]

Then

\[
(T^2 + T + 1)^{q-2} \sim G(T).
\]

**Proof** We first show that \( T^2 + T + 1 \) is irreducible over \( \mathbb{F}_q[T] \). Set \( q = p^r \) with \( p \) prime and \( r \in \mathbb{Z}^+ \). As \( q \equiv 2 \pmod{3} \), clearly \( p \equiv 2 \pmod{3} \) and \( 2 \nmid r \). Hence

\[
(-3)^{\frac{q-1}{2}} = (-3)^{\frac{p-1}{2}(1+p+p^2+\cdots+p^{r-1})} = \left( \frac{-3}{p} \right)^{1+p+p^2+\cdots+p^{r-1}} = (-1)^r = -1.
\]

This implies that \(-3\) is not a square over \( \mathbb{F}_q \). Suppose now \( T^2 + T + 1 \) is reducible over \( \mathbb{F}_q[T] \). Then there exists an element \( \alpha \in \mathbb{F}_q \) such that \( \alpha^2 + \alpha + 1 = 0 \). This implies \((2\alpha + 1)^2 = -3\), which is a contradiction. Hence \( T^2 + T + 1 \) is irreducible over \( \mathbb{F}_q[T] \). Moreover, since

\[
T^q - T = \prod_{x \in \mathbb{F}_q} (T - x),
\]

we have \( T^2 + T + 1 \nmid T^q - T \) and hence \( T^2 + T + 1 \) is coprime with \( T^q - T \).

Noting that \( T^{qs} \sim T^{s+1} \) for any nonnegative integer \( s \) and that \( (T^2 + T + 1)^2 = T^4 + 2T^3 + 3T^2 + 2T + 1 \), via a computation one can verify that

\[
(T^2 + T + 1)^2 G(T) \equiv T^2 + T + 1 \equiv (T^2 + T + 1)^q \pmod{(T^q - T)\mathbb{F}_q[T]}.
\]

As \( T^2 + T + 1 \) is coprime with \( T^q - T \), we obtain

\[
(T^2 + T + 1)^{q-2} \equiv G(T) \pmod{(T^q - T)\mathbb{F}_q[T]}.
\]

This implies

\[
(T^2 + T + 1)^{q-2} \sim G(T).
\]

In view of the above, we have completed the proof. \( \Box \)

We need the following lemma (cf. [4, Lemma 10]).

**Lemma 2.2** Let \( R \) be a commutative ring and let \( n \) be a positive integer. Set \( P(T) = p_{n-1}T^{n-1} + \cdots + p_1T + p_0 \in R[T] \). Then

\[
\det[P(X_iY_j)]_{1 \leq i,j \leq n} = \prod_{i=0}^{n-1} p_i \prod_{1 \leq i < j \leq n} (X_j - X_i)(Y_j - Y_i).
\]
Now let \( m \) be a positive integer. We introduce some basic facts on the permutations of \( \mathbb{Z}/m\mathbb{Z} \). Fix an integer \( a \) with \((a, m) = 1\). Then the map \( x \mod m \mapsto ax \mod m \) induces a permutation \( \pi_a(m) \) of \( \mathbb{Z}/m\mathbb{Z} \). Lerch [5] determined the sign of this permutation.

**Lemma 2.3** Let \( \text{sgn}(\pi_a(m)) \) denote the sign of the permutation \( \pi_a(m) \). Then

\[
\text{sgn}(\pi_a(m)) = \begin{cases} 
\left( \frac{a}{m} \right) & \text{if } m \text{ is odd}, \\
1 & \text{if } m \equiv 2 \pmod{4}, \\
(-1)^{\frac{a-1}{2}} & \text{if } m \equiv 0 \pmod{4}, 
\end{cases}
\]

where \( \left( \frac{\cdot}{m} \right) \) denotes the Jacobi symbol if \( m \) is a positive odd integer.

Recall that

\[ \mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\} = \{a_1, a_2, \ldots, a_{q-1}\}. \]

The map \( a_j \mapsto a_j^{-1} \) \((j = 1, 2, \ldots, q - 1)\) induces a permutation \( \sigma_{-1} \) of \( \mathbb{F}_q^\times \). We also need the following lemma.

**Lemma 2.4** Let notations be as above. Then

\[
\text{sgn}(\sigma_{-1}) = \text{sgn}(\pi_{-1}(q - 1)) = (-1)^{\frac{q+1}{2}}.
\]

**Proof** Fix a generator \( g \) of \( \mathbb{F}_q^\times \). Let \( f \) be the bijection on \( \mathbb{F}_q^\times \) which sends \( a_j \) to \( g^j \) \((j = 1, 2, \ldots, q - 1)\). Then it is easy to see that

\[
\text{sgn}(\sigma_{-1}) = \text{sgn}(f \circ \sigma_{-1} \circ f^{-1}).
\]

Note that \( f \circ \sigma_{-1} \circ f^{-1} \) is the permutation of \( \mathbb{F}_q^\times \) which sends \( g^j \) to \( g^{-j} \) \((j = 1, 2, \ldots, q - 1)\). This permutation indeed corresponds to the permutation \( \pi_{-1}(q - 1) \) of \( \mathbb{Z}/(q - 1)\mathbb{Z} \) which sends \( j \mod (q - 1) \) to \(-j \mod (q - 1)\). Now our desired result follows from Lemma 2.3.

This completes the proof. \( \square \)

### 3 Proof of The Main Result

**Proof of Theorem 1.1.** Recall that

\[
T_q = \left[ \frac{1}{a_i^2 - a_i a_j + a_j^2} \right]_{1 \leq i, j \leq q-1}.
\]

By Lemma 2.3

\[
\det(T_q) = (-1)^{\frac{q-1}{2}} \det \left[ \frac{1}{a_i^2 + a_i a_j + a_j^2} \right]_{1 \leq i, j \leq q-1}.
\]
Also,

\[
\det \left[ \frac{1}{a_i^2 + a_i a_j + a_j^2} \right]_{1 \leq i, j \leq q-1} = \prod_{j=1}^{q-1} \frac{1}{a_j^2} \cdot \det \left[ \frac{1}{(a_i/a_j)^2 + a_i/a_j + 1} \right]_{1 \leq i, j \leq q-1}.
\]

Since \( q \equiv 2 \pmod{3} \), we have \( a_i^2 + a_i a_j + a_j^2 \neq 0 \) for any \( 1 \leq i, j \leq q - 1 \). Hence for any \( 1 \leq i, j \leq q - 1 \) we have

\[
\frac{1}{(a_i/a_j)^2 + a_i/a_j + 1} = \left( (a_i/a_j)^2 + a_i/a_j + 1 \right)^{q-2}.
\]

By Lemma 2.1 we have \((T^2 + T + 1)^q = G(T)\), where \( G(T) \) is defined by (2.1). Hence

\[
\left( (a_i/a_j)^2 + a_i/a_j + 1 \right)^{q-2} = G(a_i/a_j),
\]

for any \( 1 \leq i, j \leq q - 1 \). As \((a_i/a_j)^{q-1} = 1\) for any \( 1 \leq i, j \leq q - 1 \), we have

\[
G(a_i/a_j) = H(a_i/a_j),
\]

where

\[
H(T) = G(T) - \frac{2}{3} + \frac{2}{3} T^{q-1} = \frac{1}{3} + \frac{1}{3} \sum_{k=2}^{q-2} (\chi_3(k) + \chi_3(1-k)) T^{k-1} + \frac{1}{3} T^{q-2}.
\]

Let

\[
S(T) = \prod_{1 \leq j \leq q-1} (T - a_j)
\]

and let \( S'(T) \) be the formal derivative of \( S(T) \). It is easy to verify that

\[
S(T) = \prod_{1 \leq j \leq q-1} (T - a_j) = T^{q-1} - 1.
\]

By this it is clear that \( S'(T) = (q - 1)T^{q-2} = -T^{q-2} \) and

\[
\prod_{1 \leq j \leq q-1} a_j = -1. \quad (3.1)
\]

By the above we obtain

\[
\det(T_q) = (-1)^{\frac{q-1}{2}} \det \left[ H(a_i/a_j) \right]_{1 \leq i, j \leq q-1}. \quad (3.2)
\]
By Lemma 2.2 we know that det\(H(a_i/a_j)\)_{1 \leq i, j \leq q-1} is equal to
\[
\frac{1}{3^{q-1}} \prod_{k=2}^{q-2} (\chi_3(k) + \chi_3(1 - k)) \prod_{1 \leq i < j \leq q-1} (a_j - a_i) \left(\frac{1}{a_j} - \frac{1}{a_i}\right).
\]

We first consider the product
\[
\prod_{1 \leq i < j \leq q-1} (a_j - a_i) \left(\frac{1}{a_j} - \frac{1}{a_i}\right).
\]

By Lemma 2.4 it is easy to see that
\[
\prod_{1 \leq i < j \leq q-1} (a_j - a_i) \left(\frac{1}{a_j} - \frac{1}{a_i}\right) = (-1)^{\frac{q+1}{2}} \prod_{1 \leq i < j \leq q-1} (a_j - a_i)^2.
\]

It is easy to verify that
\[
\prod_{1 \leq i < j \leq q-1} (a_j - a_i)^2 = (-1)^{\frac{(q-1)}{2}} \prod_{1 \leq i < j \leq q-1} (a_j - a_i)
\]
\[
= (-1)^{\frac{(q-1)}{2}} \prod_{1 \leq i < j \leq q-1, i \neq j} (a_j - a_i)
\]
\[
= (-1)^{\frac{(q-1)}{2}} \prod_{1 \leq i \leq q-1} S'(a_i)
\]
\[
= (-1)^{\frac{(q-1)}{2}} \prod_{1 \leq i \leq q-1} \frac{-1}{a_i} = (-1)^{\frac{q+1}{2}}.
\]

The last equality follows from (3.1). Hence
\[
\prod_{1 \leq i < j \leq q-1} (a_j - a_i) \left(\frac{1}{a_j} - \frac{1}{a_i}\right) = 1. \tag{3.3}
\]

We now turn to the product
\[
\prod_{k=2}^{q-2} (\chi_3(k) + \chi_3(1 - k)) .
\]

By definition
\[
\chi_3(k) + \chi_3(1 - k) = \begin{cases} 
1 & \text{if } k \equiv 0, 1 \pmod{3}, \\
-2 & \text{if } k \equiv 2 \pmod{3}.
\end{cases}
\]
Hence
\[
q^{-2} \prod_{k=2}^{q-2} (\chi_3(k) + \chi_3(1-k)) = (-2)^{\frac{q-2}{3}}. \tag{3.4}
\]

In view of (3.2)–(3.4), we obtain
\[
\det(T_q) = (-1)^{\frac{q+1}{2}} 2^{\frac{q-2}{3}} \in \mathbb{F}_p,
\]
where \( p \) is the characteristic of \( \mathbb{F}_q \). This completes the proof. \( \Box \)

**Proof of Corollary 1.1.** Let \( p \equiv 2 \pmod{3} \) be an odd prime. Then by Theorem 1.1 we have

\[
\left( \frac{\det(T_p)}{p} \right) = \left( \frac{-1}{p} \right)^{\frac{p+1}{2}} \left( \frac{2}{p} \right)^{\frac{p-2}{3}} = \left( \frac{2}{p} \right).
\]

This completes the proof. \( \Box \)

**Acknowledgements** We thank the two referees for their helpful comments. The first author was supported by the National Natural Science Foundation of China (Grant No. 12101321 and Grant No. 11971222) and the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 21KJB110002). The third author was supported by the National Natural Science Foundation of China (Grant No. 12001279).

**References**

1. Carlitz, L.: Some cyclotomic matrices. Acta Arith. 5, 293–308 (1959)
2. Chapman, R.: Determinants of Legendre symbol matrices. Acta Arith. 115, 231–244 (2004)
3. Chapman, R.: My evil determinant problem, preprint, December 12, 2012. Available from http:// empslocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf
4. Krattenthaler, C.: Advanced determinant calculus: a complement. Linear Algebra Appl. 411, 68–166 (2005)
5. Lerch, M.: Sur un théorème arithmétique de Zolotarev. Bull. Intern. de l’Acad. François Joseph 3, 34–37 (1896)
6. Sun, Z.-W.: Sur un théorème arithmétique de Zolotarev. Bull. Intern. de l’Acad. François Joseph 3, 34–37 (1896)
7. Sun, Z.-W.: On some determinants with Legendre symbol entries. Finite Fields Appl. 56, 285–307 (2019)
8. Vsemirnov, M.: On the evaluation of R Chapman’s, evil determinant. Linear Algebra Appl. 436, 4101–4106 (2012)
9. Vsemirnov, M.: On R. Chapman’s, evil determinant: case \( p \equiv 1 \pmod{4} \). Acta Arith. 159, 331–344 (2013)

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.