



INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Hai-Liang Wu

Determinants concerning Legendre symbols

Volume 359, issue 6 (2021), p. 651-655

Published online: 25 August 2021

<https://doi.org/10.5802/crmath.205>



This article is licensed under the
CREATIVE COMMONS ATTRIBUTION 4.0 INTERNATIONAL LICENSE.
<http://creativecommons.org/licenses/by/4.0/>



Les Comptes Rendus. Mathématique sont membres du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569



Combinatorics, Number theory / *Combinatoire, Théorie des nombres*

Determinants concerning Legendre symbols

Hai-Liang Wu^a

^a School of Science, Nanjing University of Posts and Telecommunications, Nanjing
210023, People's Republic of China
E-mail: whl.math@smail.nju.edu.cn

Abstract. The evaluations of determinants with Legendre symbol entries have close relation with combinatorics and character sums over finite fields. Recently, Sun [9] posed some conjectures on this topic. In this paper, we prove some conjectures of Sun and also study some variants. For example, we show the following result:

Let $p = a^2 + 4b^2$ be a prime with a, b integers and $a \equiv 1 \pmod{4}$. Then for the determinant

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

the number $S(1, p)/a$ is an integral square, which confirms a conjecture posed by Cohen, Sun and Vsemirnov.

2020 Mathematics Subject Classification. 11C20, 11L10, 11R18.

Funding. This research is supported by the National Natural Science Foundation of China (Grant No. 11971222) and by NUPTSF (Grant No. NY220159).

Manuscript received 8th January 2021, revised 27th March 2021, accepted 2nd April 2021.

1. Introduction

Given an $n \times n$ complex matrix $M = [a_{ij}]_{1 \leq i, j \leq n}$, we often use $\det M$ or $|M|$ to denote the determinant of M . The evaluation of determinants with Legendre symbol entries is a classical topic in number theory, combinatorics and finite fields. Krattenthaler's survey papers [7, 8] introduce many concrete examples and advanced techniques on determinant calculation.

Let p be an odd prime and let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol. Carlitz [2] studied the following $(p-1) \times (p-1)$ matrix

$$D_p := \left[\left(\frac{i-j}{p} \right) \right]_{1 \leq i, j \leq p-1}.$$

He obtained that the characteristic polynomial of D_p is precisely

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

where I_{p-1} is the $(p-1) \times (p-1)$ identity matrix.

Along this line, Chapman [3] further investigated the following matrices:

$$C_p(x) := \left[x + \left(\frac{i+j-1}{p} \right) \right]_{1 \leq i, j \leq \frac{p-1}{2}}$$

and

$$C_p^*(x) := \left[x + \left(\frac{i+j-1}{p} \right) \right]_{1 \leq i, j \leq \frac{p+1}{2}},$$

where x is a variable. In the case $p \equiv 1 \pmod{4}$, let $\varepsilon_p > 1$ and $h(p)$ be the fundamental unit and class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively and let $\varepsilon_p^{h(p)} = a_p + b_p\sqrt{p}$ with $2a_p, 2b_p \in \mathbb{Z}$. Chapman proved that

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

and that

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

Moreover, Chapman [4] posed a conjecture concerning the determinant of the $\frac{p+1}{2} \times \frac{p+1}{2}$ matrix

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

Due to the difficulty of the evaluation on this determinant, he called it “evil” determinant. Finally this conjecture was confirmed completely by Vsemirnov [11, 12].

Recently Sun [9] studied various determinants of matrices involving Legendre symbol entries. Let p be a prime and d be an integer with $p \nmid d$. Sun defined

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

In the same paper, Sun also studied some properties of the above determinant. For example, he showed that $-S(d, p)$ is always a quadratic residue modulo p if $\left(\frac{d}{p}\right) = 1$ and that $S(d, p) = 0$ if $\left(\frac{d}{p}\right) = -1$. Moreover, Sun posed the following conjecture:

Conjecture 1 (Sun). *Let $p \equiv 3 \pmod{4}$ be a prime. Then $-S(1, p)$ is an integral square.*

This conjecture was later confirmed by Alekseyev and Krachun by using some algebraic number theory. In the case $p \equiv 1 \pmod{4}$, Cohen, Sun and Vsemirnov also posed the following conjecture.

Conjecture 2 (Cohen, Sun and Vsemirnov). *Let $p = a^2 + 4b^2$ be a prime with a, b integers and $a \equiv 1 \pmod{4}$. Then $S(1, p)/a$ is an integral square.*

For example, if $p = 5 = 1^2 + 4 \times 1^2$, then $S(1, 5) = 1 = 1 \times 1^2$. If $p = 13 = (-3)^2 + 4 \times 1^2$, then $S(1, 13) = -27 = -3 \times 3^2$.

As the first result of this paper, by considering some character sums over finite fields, we confirm this conjecture and obtain the following result. For convenience, for each $d \in \mathbb{Z}$ we set

$$\varepsilon(d) = \begin{cases} -1 & \text{if } \left(\frac{d}{p}\right) = 1 \text{ and } d \text{ is not a biquadratic residue modulo } p, \\ 1 & \text{otherwise.} \end{cases}$$

Theorem 3. *Let $p = a^2 + 4b^2$ be a prime with a, b integers and $a \equiv 1 \pmod{4}$ and let d be an integer. Then $\varepsilon(d)S(d, p)/a$ is an integral square. In particular, when $d = 1$ the number $S(1, p)/a$ is an integral square.*

Sun [9] also made the following conjecture.

Conjecture 4 (Sun). *Let $S^*(1, p)$ denote the determinant obtained from $S(1, p)$ via replacing the entries $\left(\frac{1^2 + j^2}{p}\right)$ ($j = 1, \dots, \frac{p-1}{2}$) in the first row by $\left(\frac{j}{p}\right)$ ($j = 1, \dots, \frac{p-1}{2}$) respectively. Then $-S^*(1, p)$ is an integral square if $p \equiv 1 \pmod{4}$.*

As an application of Theorem 3, we confirm this conjecture.

Corollary 5. *Let $p \equiv 1 \pmod{4}$ be a prime. Then $-S^*(1, p)$ is an integral square.*

For example, $S^*(1, 5) = -1^2$, $S^*(1, 13) = -3^2$ and $S^*(1, 17) = -21^2$.

The proofs of our main results will be given in Section 2.

2. Proofs of the main results

We begin with the following permutation involving quadratic residues (readers may refer to [5, 10] for details on the recent progress on permutations over finite fields). Let $p \equiv 1 \pmod{4}$ be a prime and let $d \in \mathbb{Z}$ with $\left(\frac{d}{p}\right) = 1$. If we write $p = 2n + 1$, then clearly the sequence

$$d \cdot 1^2 \pmod{p}, \dots, d \cdot n^2 \pmod{p}$$

is a permutation $\pi_p(d)$ of the sequence

$$1^2 \pmod{p}, \dots, n^2 \pmod{p}.$$

Let $\text{sgn}(\pi_p(d))$ be the sign of $\pi_p(d)$. We first have the following result:

Lemma 6. *Let $p \equiv 1 \pmod{4}$ be a prime, and let $d \in \mathbb{Z}$ be a quadratic residue modulo p . Then*

$$\text{sgn}(\pi_p(d)) = \begin{cases} 1 & \text{if } d \text{ is a biquadratic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

Proof. It is clear that

$$\text{sgn}(\pi_p(d)) \equiv \prod_{1 \leq i < j \leq n} \frac{dj^2 - di^2}{j^2 - i^2} \pmod{p}.$$

By this we obtain

$$\text{sgn}(\pi_p(d)) \equiv \left(d^{\frac{p-1}{4}}\right)^{n-1} \equiv d^{\frac{p-1}{4}} \pmod{p}.$$

This implies the desired result. □

We also need the following known result concerning eigenvalues of a matrix.

Lemma 7. *Let M be an $m \times m$ complex matrix. Let μ_1, \dots, μ_m be complex numbers, and let $\mathbf{u}_1, \dots, \mathbf{u}_m$ be m -dimensional column vectors. Suppose that $M\mathbf{u}_k = \mu_k\mathbf{u}_k$ for each $1 \leq k \leq m$ and that $\mathbf{u}_1, \dots, \mathbf{u}_m$ are linear independent. Then μ_1, \dots, μ_m are exactly all the eigenvalues of M (counting multiplicities).*

Before the proof of Theorem 3, we first introduce some notation. In the remaining part of this section, we let $p = a^2 + 4b^2$ be a prime with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod{4}$, and let $n = \frac{p-1}{2}$. In addition, we let $\chi(\mathbb{Z}/p\mathbb{Z})$ denote the group of all multiplicative characters on the finite field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, and let χ_p be a generator of $\chi(\mathbb{Z}/p\mathbb{Z})$, i.e.,

$$\chi(\mathbb{Z}/p\mathbb{Z}) = \{\chi_p^k : k = 1, 2, \dots, p-1\}.$$

Readers may refer to [6, Chapter 8] for a detailed introduction to characters on finite fields. Also, given any matrix M , the symbol M^T denotes the transpose of M .

Now we are in a position to prove our first theorem.

Proof of Theorem 3. Throughout this proof, we define

$$M_p := \left[\left(\frac{i^2 + j^2}{p} \right) \right]_{1 \leq i, j \leq n}.$$

We first determine all the eigenvalues of M_p . For $k = 1, 2, \dots, n$, we let

$$\lambda_k := \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \chi_p^k(j^2). \tag{1}$$

We claim that $\lambda_1, \dots, \lambda_n$ are exactly all the eigenvalues of M_p (counting multiplicities). In fact, for any $1 \leq i, k \leq n$ we have

$$\begin{aligned} \sum_{1 \leq j \leq n} \left(\frac{i^2+j^2}{p} \right) \chi_p^k(j^2) &= \sum_{1 \leq j \leq n} \left(\frac{1+j^2+i^2}{p} \right) \chi_p^k(j^2/i^2) \chi_p^k(i^2) \\ &= \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \chi_p^k(j^2) \chi_p^k(i^2) = \lambda_k \chi_p^k(i^2). \end{aligned}$$

This implies that for each $k = 1, \dots, n$, we have

$$M_p \mathbf{v}_k = \lambda_k \mathbf{v}_k,$$

where

$$\mathbf{v}_k := (\chi_p^k(1^2), \chi_p^k(2^2), \dots, \chi_p^k(n^2))^T.$$

Since

$$\begin{vmatrix} \chi_p^1(1^2) & \chi_p^2(1^2) & \dots & \chi_p^n(1^2) \\ \chi_p^1(2^2) & \chi_p^2(2^2) & \dots & \chi_p^n(2^2) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_p^1(n^2) & \chi_p^2(n^2) & \dots & \chi_p^n(n^2) \end{vmatrix} = \pm \prod_{1 \leq i < j \leq n} (\chi_p(j^2) - \chi_p(i^2)) \neq 0,$$

the vectors $\mathbf{v}_1, \dots, \mathbf{v}_n$ are linear independent. By Lemma 7 our claim holds. Hence we have

$$S(1, p) = \det M_p = \prod_{1 \leq k \leq n} \lambda_k = \prod_{1 \leq k \leq n} \left(\sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \chi_p^k(j^2) \right). \tag{2}$$

Now we turn to the last product. When $k = n$, by [6, Chapter 5, Exercise 8] we have

$$\lambda_n = \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \chi_p^n(j^2) = \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) = -1. \tag{3}$$

When $k = n/2$, by [1, Theorem 6.2.9] we have

$$\lambda_{n/2} = \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \chi_p^{n/2}(j^2) = \sum_{1 \leq j \leq n} \left(\frac{1+j^2}{p} \right) \left(\frac{j}{p} \right) = -a. \tag{4}$$

As M_p is a real symmetric matrix, every eigenvalue λ_k of M_p is real. Hence for any $1 \leq k \leq \frac{p-5}{4}$ we have $\lambda_k = \lambda_{n-k}$. Let

$$f(x) := \det(xI_n - M_p)$$

be the characteristic polynomial of M_p . By the above we observe that all roots of $f(x)$ apart from $\lambda_n = -1$ and $\lambda_{n/2} = -a$ are of even multiplicity. Using unique factorisation in $\mathbb{Z}[x]$, one can obtain that

$$f(x) = (x+1)(x+a)g(x)^2,$$

where $g(x)$ is a polynomial with integer coefficients. Therefore we obtain that $S(1, p)/a = g(0)^2$ is an integral square.

Now we consider $S(d, p)$. If $p \mid d$, then clearly $S(d, p) = 0$. If $\left(\frac{d}{p}\right) = -1$, then by [9, Theorem 1.2] we know that $S(d, p) = 0$. Suppose now that d is a quadratic residue modulo p . Then clearly we have

$$S(d, p) = \text{sgn}(\pi_p(d)) S(1, p).$$

Now our desired result follows from Lemma 6. □

We now prove our next result.

Proof of Corollary 5. By [1, Theorem 6.2.9] for any $1 \leq i, j \leq n$ we have

$$\sum_{1 \leq i \leq n} \left(\frac{i^2 + j^2}{p} \right) \left(\frac{i}{p} \right) = -a \left(\frac{j}{p} \right)$$

and hence

$$- \sum_{2 \leq i \leq n} \left(\frac{i^2 + j^2}{p} \right) \left(\frac{i}{p} \right) - a \left(\frac{j}{p} \right) = \left(\frac{1 + j^2}{p} \right). \tag{5}$$

By this we have

$$S^*(1, p) = \frac{-1}{a} \begin{vmatrix} -a\left(\frac{1}{p}\right) & -a\left(\frac{2}{p}\right) & \dots & -a\left(\frac{n}{p}\right) \\ \left(\frac{2^2+1^2}{p}\right) & \left(\frac{2^2+2^2}{p}\right) & \dots & \left(\frac{2^2+n^2}{p}\right) \\ \vdots & \vdots & \ddots & \vdots \\ \left(\frac{n^2+1^2}{p}\right) & \left(\frac{n^2+2^2}{p}\right) & \dots & \left(\frac{n^2+n^2}{p}\right) \end{vmatrix} = -S(1, p)/a.$$

The last equality follows from (5). Now our desired result follows from Theorem 3. □

Acknowledgments

We thank the referee for helpful comments.

References

- [1] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, 1998.
- [2] L. Carlitz, "Some cyclotomic matrices", *Acta Arith.* **5** (1959), p. 293-308.
- [3] R. Chapman, "Determinants of Legendre symbol matrices", *Acta Arith.* **115** (2004), no. 3, p. 231-244.
- [4] ———, "My evil determinant problem", preprint, available at <http://empslocal.ex.ac.uk/people/staff/rjchapma/etc/evildet.pdf>, 2012.
- [5] X.-d. Hou, "Permutation polynomials over finite fields – a survey of recent advances", *Finite Fields Appl.* **32** (2015), p. 82-119.
- [6] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, vol. 84, Springer, 1990.
- [7] C. Krattenthaler, "Advanced determinant calculus", *Sémin. Lothar. Comb.* (1999), article no. B42q (67 pages).
- [8] ———, "Advanced determinant calculus: a complement", *Linear Algebra Appl.* **411** (2005), p. 68-166.
- [9] Z.-W. Sun, "On some determinants with Legendre symbol entries", *Finite Fields Appl.* **56** (2019), p. 285-307.
- [10] ———, "Quadratic residues and related permutations and identities", *Finite Fields Appl.* **59** (2019), p. 246-283.
- [11] M. Vsemirnov, "On the evaluation of R. Chapman's "evil determinant"", *Linear Algebra Appl.* **436** (2012), no. 11, p. 4101-4106.
- [12] ———, "On R. Chapman's "evil determinant": case $p \equiv 1 \pmod{4}$ ", *Acta Arith.* **159** (2013), no. 4, p. 331-344.