Finite Fields Appl. 64 (2020), Article 101672.

ON SOME DETERMINANTS INVOLVING JACOBI SYMBOLS

DMITRY KRACHUN, FEDOR PETROV, ZHI-WEI SUN, MAXIM VSEMIRNOV

Abstract. In this paper we study some conjectures on determinants with Jacobi symbol entries posed by Z.-W. Sun. For any positive integer $n \equiv 3 \pmod 4$, we show that

$$(6,1)_n = [6,1]_n = (3,2)_n = [3,2]_n = 0$$

and

$$(4,2)_n = (8,8)_n = (3,3)_n = (21,112)_n = 0$$

as conjectured by Sun, where

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

and

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

with $(\frac{\cdot}{n})$ the Jacobi symbol. We also prove that $(10,9)_p = 0$ for any prime $p \equiv 5 \pmod{12}$, and $[5,5]_p = 0$ for any prime $p \equiv 13, 17 \pmod{20}$, which were also conjectured by Sun. Our proofs involve character sums over finite fields.

1. Introduction

For an $n \times n$ matrix $[a_{ij}]_{1 \leqslant i,j \leqslant n}$ over a field, we simply denote its determinant by $|a_{ij}|_{1 \leqslant i,j \leqslant n}$. In this paper we study some conjectures on determinants with Jacobi symbol entries posed by Z.-W. Sun [11].

Let p be an odd prime. In 2004, R. Chapman [2] determined the values of

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

and

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

Key words and phrases. Determinants, Jacobi symbols, character sums over finite fields.

2020 *Mathematics Subject Classification.* Primary 11C20, 11T24; Secondary 11E16, 15A15.

The work is supported by the NSFC (Natural Science Foundation of China)-RFBR (Russian Foundation for Basic Research) Cooperation and Exchange Program (grants NSFC 11811530072 and RFBR 18-51-53020-GFEN-a). The third author is also supported by the Natural Science Foundation of China (grant 11971222).

where $(\frac{\cdot}{p})$ denotes the Legendre symbol. Chapman's conjecture on the evaluation of

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

was confirmed by M. Vsemirnov [12, 13] via matrix decomposition. With this background, Z.-W. Sun [11] studied some new kinds of determinants with Legendre symbol or Jacobi symbol entries.

For any odd integer $n>1$ and integers c and d, Sun [11] introduced the notations

$$(c,d)_n := \left|\left(\frac{i^2+cij+dj^2}{n}\right)\right|_{1\leqslant i,j\leqslant n-1} \tag{1.1}$$

and

$$[c,d]_n := \left|\left(\frac{i^2+cij+dj^2}{n}\right)\right|_{0\leqslant i,j\leqslant n-1}, \tag{1.2}$$

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

$$\left(\frac{d}{n}\right) = -1 \Rightarrow (c,d)_n = 0, \tag{1.3}$$

and that for any odd prime p we have

$$\left(\frac{d}{p}\right) = 1 \Rightarrow [c,d]_p = \begin{cases} \frac{p-1}{2}(c,d)_p & \text{if } p\nmid c^2-4d,\\ \frac{1-p}{p-2}(c,d)_p & \text{if } p\mid c^2-4d. \end{cases} \tag{1.4}$$

For $a\in\mathbb{Z}$ and $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$, if a is relatively prime to n and $x^2\equiv a \pmod n$ for some $x\in\mathbb{Z}$, then a is called a *quadratic residue* modulo n. If n is odd and a is a quadratic residue modulo n, then $(\frac{a}{n})=1$ since a is a quadratic residue modulo any prime divisor of n.

Now we state our first theorem.

Theorem 1.1. *Let $n>1$ be an odd integer.*

(i) *If -1 is not a quadratic residue modulo n, then*

$$(6,1)_n = (3,2)_n = 0 \quad \textit{and} \quad [6,1]_n = [3,2]_n = 0.$$

(ii) *If -2 is not a quadratic residue modulo n, then*

$$(4,2)_n = (8,8)_n = 0 \quad \textit{and} \quad [4,2]_n = [8,8]_n = 0.$$

(iii) *If -3 is not a quadratic residue modulo n, then*

$$(3,3)_n = (6,-3)_n = 0 \quad \textit{and} \quad [3,3]_n = [6,-3]_n = 0.$$

(iv) *If -7 is not a quadratic residue modulo n, then*

$$(21,112)_n = (42,-7)_n = 0 \quad \textit{and} \quad [21,112]_n = [42,-7]_n = 0.$$

Combining Theorem 1.1 with (1.3), we immediately obtain the following consequence which was conjectured by Sun [11, Conjecture 4.8(ii)].

Corollary 1.1. *For any positive integer $n \equiv 3 \pmod 4$, we have*

$$(6,1)_n = [6,1]_n = (3,2)_n = [3,2]_n = 0$$

and

$$(4,2)_n = (8,8)_n = (3,3)_n = (21,112)_n = 0.$$

Actually we deduce Theorem 1.1 from the following theorems.

Theorem 1.2. *Let n be a positive odd integer which is squarefree. For any $c, d, i \in \mathbb{Z}$, we have*

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+cij+dj^2}{n}\right)=\sum_{j=0}^{n-1}\left(\frac{-j}{n}\right)\left(\frac{i^2+2cij+(c^2-4d)j^2}{n}\right). \tag{1.5}$$

Theorem 1.3. *Let n be a positive odd integer which is squarefree, and let $i \in \mathbb{Z}$. Then*

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+3ij+2j^2}{n}\right)=0 \quad \text{if } -1\ R\ n \text{ fails}, \tag{1.6}$$

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+4ij+2j^2}{n}\right)=0 \quad \text{if } -2\ R\ n \text{ fails}, \tag{1.7}$$

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+3ij+3j^2}{n}\right)=0 \quad \text{if } -3\ R\ n \text{ fails}, \tag{1.8}$$

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+21ij+112j^2}{n}\right)=0 \quad \text{if } -7\ R\ n \text{ fails}, \tag{1.9}$$

where the notation $m\ R\ n$ means that m is a quadratic residue modulo n.

Our following result was originally conjectured by Sun [11, Conjecture 4.8(iv)].

Theorem 1.4. (i) $(10,9)_p = 0$ *for any prime* $p \equiv 5 \pmod{12}$.

(ii) $[5,5]_p = 0$ *for any prime* $p \equiv 13, 17 \pmod{20}$.

In fact, our proof of Theorem 1.4 yields a stronger result: For each integer y, we have

$$\sum_{x=0}^{p-1}\left(\frac{x^5+10x^3y+9xy^2}{p}\right)=0$$

for any prime $p \equiv 5 \pmod{12}$, and

$$\sum_{x=0}^{p-1}\left(\frac{x^5+5x^3y+5xy^2}{p}\right)=0$$

for any prime $p \equiv 13, 17 \pmod{20}$.

We will prove Theorem 1.2, Theorems 1.3 and 1.1, and Theorem 1.4 in Sections 2-4 respectively.

Sun [11, Conjecture 4.8(iv)] also conjectured that $(8,18)_p = [8,18]_p = 0$ for any prime $p \equiv 13, 17 \pmod{24}$. Moreover, Sun [10] conjectured that

$$\sum_{x=0}^{p-1} \left(\frac{x^5 + 8x^3y + 18xy^2}{p}\right) = 0$$

for any prime $p \equiv 13, 17 \pmod{24}$ and integer y, and this was confirmed by M. Stoll via two elliptic curves with complex multiplication by $\mathbb{Z}[\sqrt{-6}]$ (see the answer in [10]).

For any prime $p \equiv 1 \pmod 4$ and $a, b, c \in \mathbb{Z}$, we provide in Section 5 a sufficient condition for

$$\sum_{x=0}^{p-1} \left(\frac{ax^5 + bx^3 + cx}{p}\right) = 2 \sum_{x=1}^{(p-1)/2} \left(\frac{x}{p}\right)\left(\frac{a(x^2)^2 + bx^2 + c}{p}\right) = 0.$$

2. Proof of Theorem 1.2

Lemma 2.1. *Let p be an odd prime and let $c, d, i \in \mathbb{Z}$ with $p \nmid c$. Then*

$$\sum_{j=0}^{p-1} \left(\frac{j}{p}\right)\left(\frac{i^2 + cij + dj^2}{p}\right) \equiv -\left(\frac{ci}{p}\right) \sum_{k=0}^{p-1} \binom{4k}{2k}\binom{2k}{k}\left(\frac{d}{16c^2}\right)^k \pmod p. \tag{2.1}$$

Proof. If $p \mid i$, then both sides of the congruence (2.1) are zero.

Below we assume $p \nmid i$ and let L denote the left-hand side of the congruence (2.1). As $\{ir : r = 0, \ldots, p-1\}$ is a complete system of residues modulo p, we have

$$\begin{aligned} L &= \sum_{r=0}^{p-1} \left(\frac{ir}{p}\right)\left(\frac{i^2 + ci(ir) + d(ir)^2}{p}\right) = \left(\frac{i^3}{p}\right) \sum_{r=0}^{p-1} \left(\frac{r}{p}\right)\left(\frac{1 + cr + dr^2}{p}\right) \\ &\equiv \left(\frac{i}{p}\right) \sum_{r=1}^{p-1} r^{(p-1)/2}(1 + cr + dr^2)^{(p-1)/2} \\ &\equiv \left(\frac{i}{p}\right) \sum_{r=1}^{p-1} \left(r^{-1} + c + dr\right)^{(p-1)/2} \pmod p. \end{aligned}$$

We may write $(x^{-1} + c + dx)^{(p-1)/2} = \sum_{s=-(p-1)/2}^{(p-1)/2} a_s x^s$ with $a_s \in \mathbb{Z}$. For any integer s, it is well known (cf. [4, p. 235]) that

$$\sum_{r=1}^{p-1} r^s \equiv \begin{cases} -1 \pmod p & \text{if } p - 1 \mid s, \\ 0 \pmod p & \text{otherwise.} \end{cases} \tag{2.2}$$

Therefore,

$$\sum_{r=1}^{p-1} \left(r^{-1} + c + dr\right)^{(p-1)/2} = \sum_{s=-(p-1)/2}^{(p-1)/2} a_s \sum_{r=1}^{p-1} r^s \equiv -a_0 \pmod p.$$

Clearly,

$$\begin{aligned}
a_0 &= \sum_{k=0}^{(p-1)/2} \binom{(p-1)/2}{2k}\binom{2k}{k} c^{(p-1)/2-2k} d^k \\
&\equiv \sum_{k=0}^{(p-1)/2} \binom{-1/2}{2k}\binom{2k}{k}\left(\frac{c}{p}\right)\left(\frac{d}{c^2}\right)^k = \left(\frac{c}{p}\right)\sum_{k=0}^{(p-1)/2}\frac{\binom{4k}{2k}\binom{2k}{k}}{(-4)^{2k}}\left(\frac{d}{c^2}\right)^k \\
&= \left(\frac{c}{p}\right)\sum_{k=0}^{p-1}\binom{4k}{2k}\binom{2k}{k}\left(\frac{d}{16c^2}\right)^k \pmod p.
\end{aligned}$$

So, by the above, we finally obtain (2.1). □

Lemma 2.2. *Let p be any odd prime. Then we have the congruence*

$$\sum_{k=0}^{p-1}\frac{\binom{4k}{2k}\binom{2k}{k}}{64^k}\left(x^k - \left(\frac{-2}{p}\right)(1-x)^k\right) \equiv 0 \pmod{p^{2-\delta_{p,3}}} \tag{2.3}$$

in the ring $\mathbb{Z}_p[x]$, where $\mathbb{Z}_p$ is the ring of all p-adic integers, and $\delta_{p,3}$ is 1 or 0 according as $p = 3$ or not.

Remark 2.1. For any prime $p > 3$, the congruence (2.3) is due to Sun [9, (1.15)]. We can easily verify that (2.3) also holds for $p = 3$.

Proof of Theorem 1.2. Clearly both sides of (1.5) vanish if $n = 1$. Below we assume $n > 1$ and distinguish three cases.

Case 1. n is an odd prime p.

Define

$$D := \sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+cij+dj^2}{p}\right) - \sum_{j=0}^{p-1}\left(\frac{-j}{p}\right)\left(\frac{i^2+2cij+(c^2-4d)j^2}{p}\right).$$

If $p \mid c$ and $p \equiv 3 \pmod 4$, then

$$\begin{aligned}
D =& \sum_{j=1}^{(p-1)/2}\left(\left(\frac{j}{p}\right)+\left(\frac{p-j}{p}\right)\right)\left(\frac{i^2+dj^2}{p}\right) \\
&- \sum_{j=1}^{(p-1)/2}\left(\left(\frac{-j}{p}\right)+\left(\frac{-(p-j)}{p}\right)\right)\left(\frac{i^2-4dj^2}{p}\right) \\
=& 0 - 0 = 0.
\end{aligned}$$

When $p \mid c$ and $p \equiv 1 \pmod 4$, for $q = ((p-1)/2)!$ we have $q^2 \equiv -1 \pmod p$ and $(\frac{2q}{p}) = 1$ (cf. [11, Remark 1.1 and Lemma 2.3]), thus

$$D = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+dj^2}{p}\right) - \sum_{j=1}^{p-1}\left(\frac{-j}{p}\right)\left(\frac{i^2-4dj^2}{p}\right)$$

$$=\sum_{j=1}^{p-1}\left(\frac{2qj}{p}\right)\left(\frac{i^2+d(2qj)^2}{p}\right)-\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2-4dj^2}{p}\right)=0.$$

Now suppose that $p\nmid c$. By Lemma 2.2,

$$\begin{aligned}&\sum_{k=0}^{p-1}\binom{4k}{2k}\binom{2k}{k}\left(\frac{d}{16c^2}\right)^k\\&=\sum_{k=0}^{p-1}\frac{\binom{4k}{2k}\binom{2k}{k}}{64^k}\left(\frac{4d}{c^2}\right)^k\\&\equiv\left(\frac{-2}{p}\right)\sum_{k=0}^{p-1}\frac{\binom{4k}{2k}\binom{2k}{k}}{64^k}\left(1-\frac{4d}{c^2}\right)^k\\&=\left(\frac{-2}{p}\right)\sum_{k=0}^{p-1}\binom{4k}{2k}\binom{2k}{k}\left(\frac{c^2-4d}{16(2c)^2}\right)^k\pmod{p^{2-\delta_{p,3}}}.\end{aligned}$$

Combining this with Lemma 2.1, we obtain that

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+cij+dj^2}{p}\right)\\&\equiv-\left(\frac{-2ci}{p}\right)\sum_{k=0}^{p-1}\binom{4k}{2k}\binom{2k}{k}\left(\frac{c^2-4d}{16(2c)^2}\right)^k\\&\equiv\left(\frac{-1}{p}\right)\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+2cij+(c^2-4d)j^2}{p}\right)\pmod p.\end{aligned}$$

Thus $D\equiv 0\pmod p$. Clearly $|D|<2p$.

If $p\mid i$, then

$$\begin{aligned}D&=\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{dj^2}{p}\right)-\sum_{j=0}^{p-1}\left(\frac{-j}{p}\right)\left(\frac{(c^2-4d)j^2}{p}\right)\\&=\left(\left(\frac{d}{p}\right)-\left(\frac{4d-c^2}{p}\right)\right)\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)=0.\end{aligned}$$

Now assume that $p\nmid i$. If neither c^2-4d nor $(2c)^2-4(c^2-4d)=16d$ is divisible by p, then

$$|\{1\leqslant j\leqslant p-1:\ i^2+cij+dj^2\equiv 0\pmod p\}|\in\{0,2\}$$

and

$$|\{1\leqslant j\leqslant p-1:\ i^2+2cij+(c^2-4d)j^2\equiv 0\pmod p\}|\in\{0,2\},$$

hence D is even. When $p\mid d$, we also have $2\mid D$ since

$$|\{1\leqslant j\leqslant p-1:\ p\mid i(i+cj)\}|=|\{1\leqslant j\leqslant p-1:\ p\mid i(i+cj)^2\}|=1.$$

If $p \mid c^2 - 4d$, then $2 \mid D$ since

$$|\{1 \leqslant j \leqslant p-1 :\ p \mid i(i+2cj)\}| = 1$$

and

$$\left|\left\{1 \leqslant j \leqslant p-1 :\ i^2 + cij + dj^2 \equiv \left(i + \frac{c}{2}j\right)^2 \equiv 0 \pmod p\right\}\right| = 1.$$

So D is always even, and hence $D = 0$ as $p \mid D$ and $|D| < 2p$.

Case 2. $n = p_1 \dots p_r$ with $r \geqslant 2$, where $p_1, \dots, p_r$ are distinct primes.

By the Chinese Remainder Theorem,

$$\begin{aligned}\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+cij+dj^2}{n}\right) &= \sum_{j=0}^{n-1}\prod_{s=1}^{r}\left(\frac{j}{p_s}\right)\left(\frac{i^2+cij+dj^2}{p_s}\right)\\ &= \sum_{j_1=0}^{p_1-1}\cdots\sum_{j_r=0}^{p_r-1}\prod_{s=1}^{r}\left(\frac{j_s}{p_s}\right)\left(\frac{i^2+cij_s+dj_s^2}{p_s}\right)\end{aligned}$$

and hence

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+cij+dj^2}{n}\right) = \prod_{s=1}^{r}\sum_{j_s=0}^{p_s-1}\left(\frac{j_s}{p_s}\right)\left(\frac{i^2+cij_s+dj_s^2}{p_s}\right). \tag{2.4}$$

Similarly,

$$\begin{aligned}&\sum_{j=0}^{n-1}\left(\frac{-j}{n}\right)\left(\frac{i^2+2cij+(c^2-4d)j^2}{n}\right)\\ &= \prod_{s=1}^{r}\sum_{j_s=0}^{p_s-1}\left(\frac{-j_s}{p_s}\right)\left(\frac{i^2+2cij_s+(c^2-4d)j_s^2}{p_s}\right).\end{aligned}$$

Thus, (1.5) holds in view of Case 1. This concludes the proof. $\square$

3. Proofs of Theorems 1.3 and 1.1

Lemma 3.1. *Let $p > 3$ be a prime. If $p \equiv 1, 3 \pmod 8$ and $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ and $x \equiv 1 \pmod 4$, then*

$$\sum_{k=0}^{p-1}\frac{\binom{4k}{2k}\binom{2k}{k}}{128^k} \equiv (-1)^{\lfloor (p+5)/8 \rfloor}\left(2x - \frac{p}{2x}\right) \pmod{p^2}.$$

If $(\frac{-2}{p}) = -1$, i.e., $p \equiv 5, 7 \pmod 8$, then

$$\sum_{k=0}^{p-1}\frac{\binom{4k}{2k}\binom{2k}{k}}{128^k} \equiv 0 \pmod{p^2}.$$

Remark 3.1. The first assertion in Lemma 3.1 was conjectured by Z.-W. Sun [8] and confirmed by his twin brother Z.-H. Sun [7, Theorem 4.3]. The second assertion was proved by Z.-W. Sun [9, Corollary 1.3] as a consequence of (2.3) with $x = 1/2$.

Lemma 3.2. *Let p be an odd prime and let $c, d, i \in \mathbb{Z}$ with $p \nmid d$. Then*

$$\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3cij+dj^2}{p}\right)=\left(\frac{i}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-(3c^2-d)x+c(2c^2-d)}{p}\right). \tag{3.1}$$

Proof. Both sides of (3.1) vanish if $p \mid i$. Below we assume $p \nmid i$.

Clearly,

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3cij+dj^2}{p}\right)\\ =&\sum_{j=0}^{p-1}\left(\frac{dj}{p}\right)\left(\frac{di^2+3ci(dj)+(dj)^2}{p}\right)\\ =&\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\left(\frac{k^2+3cik+di^2}{p}\right)=\sum_{r=0}^{p-1}\left(\frac{ir}{p}\right)\left(\frac{(ir)^2+3ci^2r+di^2}{p}\right)\\ =&\left(\frac{i}{p}\right)\sum_{r=0}^{p-1}\left(\frac{r}{p}\right)\left(\frac{r^2+3cr+d}{p}\right)\end{aligned}$$

and

$$\begin{aligned}\sum_{r=0}^{p-1}\left(\frac{r^3+3cr^2+dr}{p}\right)&=\sum_{x=0}^{p-1}\left(\frac{(x-c)^3+3c(x-c)^2+d(x-c)}{p}\right)\\ &=\sum_{x=0}^{p-1}\left(\frac{x^3+(d-3c^2)x+c(2c^2-d)}{p}\right).\end{aligned}$$

So (3.1) holds. □

Lemma 3.3. *Let p be any odd prime and let $i \in \mathbb{Z}$.*

(i) *We have*

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+4ij+2j^2}{p}\right)\\ =&\begin{cases}(-1)^{\lfloor (p-3)/8\rfloor}(\frac{i}{p})2x & \text{if } p=x^2+2y^2\ (x,y\in\mathbb{Z}\ \&\ 4\mid x-1),\\ 0 & \text{if } (\frac{-2}{p})=-1,\ \text{i.e.},\ p\equiv 5,7 \pmod 8).\end{cases}\end{aligned} \tag{3.2}$$

(ii) *We have*

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3ij+2j^2}{p}\right)\\&=\begin{cases}-(\frac{2i}{p})2x & \text{if } p=x^2+4y^2\ (x,y\in\mathbb{Z}\ \&\ 4\mid x-1),\\ 0 & \text{if } (\frac{-1}{p})=-1,\ \text{i.e., } p\equiv 3\pmod 4).\end{cases}\end{aligned}\tag{3.3}$$

Also,

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3ij+3j^2}{p}\right)\\&=\begin{cases}-(\frac{-i}{p})2x & \text{if } p=x^2+3y^2\ (x,y\in\mathbb{Z}\ \&\ 3\mid x-1),\\ 0 & \text{if } (\frac{-3}{p})\neq 1,\ \text{i.e., } p\equiv 0,2\pmod 3),\end{cases}\end{aligned}\tag{3.4}$$

and

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+21ij+112j^2}{p}\right)\\&=\begin{cases}-(\frac{i}{p})2x & \text{if } p=x^2+7y^2\ (x,y\in\mathbb{Z}\ \&\ (\frac{x}{7})=1),\\ 0 & \text{if } (\frac{-7}{p})\neq 1,\ \text{i.e., } p\equiv 0,3,5,6\pmod 7).\end{cases}\end{aligned}\tag{3.5}$$

Remark 3.2. It is well known that any prime $p\equiv 1\pmod 4$ can be written as x^2+4y^2 with $x,y\in\mathbb{Z}$. Also, for each $m\in\{2,3,7\}$ any odd prime p with $(\frac{-m}{p})=1$ can be written x^2+my^2 with $x,y\in\mathbb{Z}$ (cf. [3]).

Proof of Lemma 3.3. It is easy to verify that (3.2)-(3.5) hold for $p=3$. Below we assume $p>3$.

(i) As $16\times 4^2/2=128$, combining Lemma 2.1 and Lemma 3.1 we find that

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+4ij+2j^2}{p}\right)\\&\equiv\begin{cases}(-1)^{\lfloor (p-3)/8\rfloor}(\frac{i}{p})2x \pmod p & \text{if } p=x^2+2y^2\ (x,y\in\mathbb{Z}\ \&\ 4\mid x-1),\\ 0 \pmod p & \text{if } (\frac{-2}{p})=-1,\ \text{i.e., } p\equiv 5,7\pmod 8).\end{cases}\end{aligned}$$

Observe that

$$\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+4ij+2j^2}{p}\right)=\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+4ij+2j^2}{p}\right)$$

is even (since $|\{1\leqslant j\leqslant p-1:\ i^2+4ij+2j^2\equiv 0\pmod p)\}|\in\{0,2\}$), and its absolute value is smaller than p. If $p=x^2+2y^2$ with $x,y\in\mathbb{Z}$ and $x\equiv 1\pmod 4$, then $|2x|<2\sqrt{p}<p$. So (3.2) holds.

(ii) In light of Lemma 3.2,

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3ij+2j^2}{p}\right)\\ =&\left(\frac{i}{p}\right)\sum_{r=0}^{p-1}\left(\frac{r^3-r}{p}\right)=\left(\frac{2i}{p}\right)\sum_{r=0}^{p-1}\left(\frac{2r}{p}\right)\left(\frac{4r^2-4}{p}\right)\\ =&\left(\frac{2i}{p}\right)\sum_{s=0}^{p-1}\left(\frac{s^3-4s}{p}\right)\end{aligned}$$

and

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+3ij+3j^2}{p}\right)\\ =&\left(\frac{i}{p}\right)\sum_{r=0}^{p-1}\left(\frac{r^3-1}{p}\right)=\left(\frac{2i}{p}\right)\sum_{r=0}^{p-1}\left(\frac{(2r)^3-8}{p}\right)\\ =&\left(\frac{2i}{p}\right)\sum_{s=0}^{p-1}\left(\frac{s^3-8}{p}\right).\end{aligned}$$

On the other hand, by [1, Theorem 6.2.9] and [1, pp. 195-196],

$$\sum_{s=0}^{p-1}\left(\frac{s^3-4s}{p}\right)=\begin{cases}-2x & \text{if } p=x^2+4y^2\ (x,y\in\mathbb{Z}\ \&\ 4\mid x-1),\\ 0 & \text{if } p\equiv 3 \pmod 4,\end{cases}$$

and

$$\sum_{s=0}^{p-1}\left(\frac{s^3-8}{p}\right)=\begin{cases}-2x(\frac{-2}{p}) & \text{if } p=x^2+3y^2\ (x,y\in\mathbb{Z}\ \&\ 3\mid x-1),\\ 0 & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

So we have (3.3) and (3.4).

Now we prove (3.5). Clearly, (3.5) is valid if $p\mid i$ or $p=7$. Below we assume that $p\nmid i$ and $p\neq 7$. Observe that

$$\begin{aligned}&\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\left(\frac{i^2+21ij+112j^2}{p}\right)\\ =&\sum_{r=0}^{p-1}\left(\frac{112ir}{p}\right)\left(\frac{112i^2+21i^2(112r)+(112ir)^2}{p}\right)\\ =&\left(\frac{i}{p}\right)\sum_{s=0}^{p-1}\left(\frac{s^3+21s^2+112s}{p}\right).\end{aligned}$$

By a result of Rajwade [6],

$$\sum_{s=0}^{p-1}\left(\frac{s^3+21s^2+112s}{p}\right)=\begin{cases}-2x & \text{if } p=x^2+7y^2\ (x,y\in\mathbb{Z}\ \&\ (\frac{x}{7})=1),\\ 0 & \text{if } (\frac{-7}{p})=-1.\end{cases}$$

Therefore (3.5) holds.

The proof of Lemma 3.3 is now complete. □

Proof of Theorem 1.3. Write $n=p_1\dots p_r$ with $p_1,\dots,p_r$ distinct primes. In light of (2.4) and Lemma 3.3(i), if $-2\ R\ n$ fails (i.e., $(\frac{-2}{p_s})=-1$ for some $s=1,\dots,r$) then

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+4ij+2j^2}{n}\right)=\prod_{s=1}^{r}\sum_{j=0}^{p_s-1}\left(\frac{j_s}{p_s}\right)\left(\frac{i^2+4ij_s+2j_s^2}{p_s}\right)=0,$$

Thus (1.7) holds. Note that if $-2\ R\ n$ then for each $s=1,\dots,r$ we may write $p_s=x_s^2+2y_s^2$ with $x_s,y_s\in\mathbb{Z}$ and $x_s\equiv 1 \pmod 4$ and hence

$$\sum_{j=0}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+4ij+2j^2}{n}\right)=\prod_{s=1}^{r}\left((-1)^{\lfloor (p_s-3)/8\rfloor}\left(\frac{i}{p_s}\right)2x_s\right).$$

Similarly, (1.6), (1.8) and (1.9) also hold in view of (2.4) and Lemma 3.3(ii). This concludes our proof of Theorem 1.3. □

Proof of Theorem 1.1. Suppose that $n=\prod_{s=1}^{r}p_s^{a_s}$, where $p_1,\dots,p_r$ are distinct primes and $a_1,\dots,a_r$ are positive integers. If $a_t>1$ with $1\leqslant t\leqslant r$, then $n/p_t\equiv 0 \pmod{p_1\dots p_r}$ and hence for any $i\in\mathbb{Z}$ we have

$$\begin{aligned}\left(\frac{i^2+cij+dj^2}{n}\right)&=\prod_{s=1}^{r}\left(\frac{i^2+cij+dj^2}{p_s}\right)^{a_s}\\&=\prod_{s=1}^{r}\left(\frac{(i+n/p_t)^2+c(i+n/p_t)j+dj^2}{p_s}\right)^{a_s}\\&=\left(\frac{(i+n/p_t)^2+c(i+n/p_t)j+dj^2}{n}\right)\end{aligned}$$

for all $j=0,\dots,n-1$. Therefore

$$(c,d)_n=[c,d]_n=0.$$

Below we assume that n is squarefree. If $-1\ R\ n$ fails, then by Theorems 1.2 and 1.3 we have

$$\sum_{j=1}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+3ij+2j^2}{n}\right)=0=\sum_{j=1}^{n-1}\left(\frac{j}{n}\right)\left(\frac{i^2+6ij+j^2}{n}\right)$$

for all $i=0,\dots,n-1$, hence $(3,2)_n=(6,1)_n=0$ and $[3,2]_n=[6,1]_n=0$. This proves part (i) of Theorem 1.1. Similarly, parts (ii)-(iv) of Theorem 1.1 follow from Theorems 1.2 and 1.3. This ends the proof. □

4. Proof of Theorem 1.4

Let $q>1$ be a prime power and let $\mathbb{F}_q$ be the finite field of order q. A multiplicative character χ on $\mathbb{F}_q$ is called *trivial* (or *principal*) if $\chi(a)=1$ for all $a\in\mathbb{F}_q^*=\mathbb{F}_q\setminus\{0\}$. For a polynomial $P(x)=\sum_{s=0}^n c_s x^s\in\mathbb{F}_q[x]$, we define the homogenous polynomial

$$P^*(x,y)=\sum_{s=0}^n c_s x^{n-s}y^s=x^nP\left(\frac{y}{x}\right). \tag{4.1}$$

Fix a list of the elements of $\mathbb{F}_q$. For a multiplicative character χ on $\mathbb{F}_q$, we introduce the matrices

$$M(P,\chi)=[\chi(P^*(a,b))]_{a,b\in\mathbb{F}_q^*} \text{ and } M_0(P,\chi)=[\chi(P^*(a,b))]_{a,b\in\mathbb{F}_q}. \tag{4.2}$$

Lemma 4.1. *Let $q>1$ be a prime power and let χ be a nontrivial multiplicative character on $\mathbb{F}_q$. Suppose that $P(x)\in\mathbb{F}_q[x]$ and $\sum_{x\in\mathbb{F}_q}\chi(xP(x))=0$. Then $M(P,\chi)$ is singular (i.e., $\det M(P,\chi)=0$). If the character χ^{n+1} is nontrivial with $n=\deg P$, then the matrix $M_0(P,\chi)$ is singular too.*

Proof. We introduce the column vector v whose coordinates are $v_b=\chi(b)$ for $b\in\mathbb{F}_q^*$. Let $M=M(P,\chi)$. Then, for any $a\in\mathbb{F}_q^*$ we have

$$(Mv)_a=\sum_{b\in\mathbb{F}_q^*}\chi\left(a^nP\left(a^{-1}b\right)\right)\chi(b)=\chi(a^{n+1})\sum_{b\in\mathbb{F}_q^*}\chi\left(a^{-1}bP\left(a^{-1}b\right)\right)=0.$$

Since v is a nonzero vector, the matrix M is singular.

Now suppose that the degree of P is n and the character χ^{n+1} is nontrivial. Let $M_0=M_0(P,\chi)$ and introduce the vector v with coordinates $v_b=\chi(b)$ for $b\in\mathbb{F}_q$. Then $(M_0v)_a=0$ for all $a\in\mathbb{F}_q^*$ as before. Let c_n be the leading coefficient of the polynomial $P(x)$. Then

$$(M_0v)_0=\sum_{b\in\mathbb{F}_q}\chi(c_nb^n)\chi(b)=\chi(c_n)\sum_{b\in\mathbb{F}_q}\chi^{n+1}(b)=0.$$

Therefore M_0v is the zero vector and hence M_0 is singular. □

Motivated by Lemma 4.1, we give the following more sophisticated lemma.

Lemma 4.2. *Let $q>1$ be an odd prime power. Suppose that $g\in\mathbb{F}_q$ is not a square and χ is a nontrivial multiplicative character on $\mathbb{F}_q$ with $\chi(-1)=1$. Assume that $P(x)\in\mathbb{F}_q[x]$ and*

$$\sum_{x\in\mathbb{F}_q}\chi(xP(x^2))=\sum_{x\in\mathbb{F}_q}\chi(xP(gx^2))=0. \tag{4.3}$$

(i) *We have* $\dim(\mathrm{Ker}(M(P,\chi)))\geqslant 2$*, in particular $M(P,\chi)$ is singular.*

(ii) *Assume that the character χ^{2n+1} with $n=\deg P$ is nontrivial. Then* $\dim(\mathrm{Ker}(M_0(P,\chi)))\geqslant 2$.

Proof. For $a,b\in\mathbb{F}_q$, set

$$v_{a,b}:=\begin{cases}\chi(c)=\chi(\sqrt{ab}) & \text{if } ab=c^2 \text{ for some } c\in\mathbb{F}_q,\\ 0 & \text{otherwise.}\end{cases}$$

This is well defined since $\chi(\pm1)=1$, The matrix $V=[v_{a,b}]_{a,b\in\mathbb{F}_q^*}$ has rank 2; in fact, if $b'=bc^2$ for some $c\in\mathbb{F}_q$ then columns b and b' in V are proportional, but columns 1 and g are not proportional.

(i) Write M for $M(P,\chi)$. It suffices to show that MV is the zero matrix. For $a,b\in\mathbb{F}_q^*$, the (a,b)-entry of the matric MV is

$$\begin{aligned}\sum_{c\in\mathbb{F}_q}\chi(P^*(a,c))v_{c,b}=&\sum_{\substack{c\in\mathbb{F}_q\\ bc\ \text{ is a square}}}\chi\left(a^nP\left(a^{-1}c\right)\right)\chi(\sqrt{bc})\\ =&\frac{1}{2}\sum_{d\in\mathbb{F}_q}\chi\left(a^nP\left(a^{-1}bd^2\right)\right)\chi(bd)\\ =&\frac{1}{2}\chi(a^nb)\sum_{d\in\mathbb{F}_q}\chi\left(P_{a^{-1}b}(d)\right),\end{aligned}$$

where $P_c(x)=xP(cx^2)$ for any $c\in\mathbb{F}_q$.

Now it remains to show for any $c\in\mathbb{F}_q^*$ the identity

$$\sum_{x\in\mathbb{F}_q}\chi(P_c(x))=0.$$

Clearly, $c=c_0d^2$ for some $c_0\in\{1,g\}$ and $d\in\mathbb{F}_q^*$. Thus

$$\begin{aligned}\sum_{x\in\mathbb{F}_q}\chi(P_c(x))=\sum_{x\in\mathbb{F}_q}\chi(xP(c_0d^2x^2))=&\sum_{y\in\mathbb{F}_q}\chi(d^{-1}yP(c_0y^2))\\ =\chi(d)^{-1}\sum_{y\in\mathbb{F}_q}\chi(P_{c_0}(y))=0.&\end{aligned}$$

This proves part (i) of Lemma 4.2.

(ii) Write M_0 for $M_0(P,\chi)$, and define $V_0=[v_{a,b}]_{a,b\in\mathbb{F}_q}$. (Note the slight difference between V_0 and V.) The rank of V_0 is still equal to 2, so it suffices to show that M_0V_0 is the zero matrix. Note that the (a,b)-entry of M_0V_0 is trivially zero if $b=0$ since $v_{c,0}=0$ for all $c\in\mathbb{F}_q$. For $a,b\neq0$ we can repeat the computation for MV verbatim. Let c_n denote the leading coefficient of $P(x)$. If $a=0$ and $b\neq0$, then the (a,b)-entry of M_0V_0 is

$$\begin{aligned}\sum_{c\in\mathbb{F}_q}\chi(P^*(0,c))v_{c,b}=&\sum_{\substack{c\in\mathbb{F}_q\\ bc\text{ is a square}}}\chi(c_nc^n)\chi(\sqrt{bc})\\ =&\frac{1}{2}\sum_{d\in\mathbb{F}_q^*}\chi(c_n(b^{-1}d^2)^nd)=\frac{\chi(b^{-1}c_n)}{2}\sum_{d\in\mathbb{F}_q}\chi^{2n+1}(d).\end{aligned}$$

This is zero since χ^{2n+1} is nontrivial. We are done. $\square$

Theorem 4.1. *Let $q > 1$ be an odd prime power and let $m \in \mathbb{Z}^+$ with $\gcd(m, q-1) = 1$. Let χ be a nontrivial quadratic character on $\mathbb{F}_q$, and let*

$$P_m(x, a) = \sum_{k=0}^{m-1} \binom{2m}{2k+1} a^k x^{m-1-k} \tag{4.4}$$

with $a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Then

$$\sum_{x \in \mathbb{F}_q} \chi(xP_m(gx^2, a)) = 0 \quad \text{for all } g \in \mathbb{F}_q^*. \tag{4.5}$$

If $\chi(-1) = 1$, then both $M(P_m(x, a), \chi)$ and $M_0(P_m(x, a), \chi)$ are singular, and moreover either of them has a kernel of dimension at least two.

Proof. In view of Lemma 4.2, we only need to prove (4.5). As $P_m(gx^2, a) = g^{m-1}P_m(x^2, ag^{-1})$ for all $g \in \mathbb{F}_q^*$, it suffices to show that

$$\sum_{x \in \mathbb{F}_q} \chi(xP_m(x^2, a)) = 0 \tag{4.6}$$

for any $a \in \mathbb{F}_q^*$.

Clearly, m is odd since $\gcd(m, q-1) = 1$. Recall that χ^2 is the trivial character, and note that

$$\begin{aligned}
\sum_{x \in \mathbb{F}_q} \chi(xP_m(x^2, a)) &= \sum_{x \in \mathbb{F}_q^*} \chi(ax^{-1}P_m((ax^{-1})^2, a)) \\
&= \sum_{x \in \mathbb{F}_q^*} \chi\bigg(\sum_{k=0}^{m-1} \binom{2m}{2(m-1-k)+1} a^{2m-1-k} x^{2k+1-2m}\bigg) \\
&= \sum_{x \in \mathbb{F}_q^*} \chi\bigg(\sum_{j=0}^{m-1} \binom{2m}{2j+1} a^{m+j} x^{-1-2j}\bigg) \\
&= \sum_{x \in \mathbb{F}_q^*} \chi(a^m x^{-2m} xP_m(x^2, a)) = \chi(a)^m \sum_{x \in \mathbb{F}_q} \chi(xP_m(x^2, a)).
\end{aligned}$$

If a is not a square in $\mathbb{F}_q$, then $\chi(a)^m = (-1)^m = -1$ and hence (4.6) holds by the above.

Now assume that $a = b^2$ with $b \in \mathbb{F}_q^*$. Since

$$\sum_{x \in \mathbb{F}_q} \chi(xP_m(x^2, a)) = \sum_{x \in \mathbb{F}_q} \chi(b^{2m-2}xP_m((b^{-1}x)^2, 1)) = \chi(b)^{2m-1} \sum_{y \in \mathbb{F}_q} \chi(yP_m(y^2, 1)),$$

it remains to show that $\sum_{x \in \mathbb{F}_q} \chi(xP_m(x^2, 1)) = 0$. Since $\chi = \chi^{-1}$ and

$$2xP_m(x^2, 1) = (x+1)^{2m} - (x-1)^{2m} = ((x+1)^m + (x-1)^m)((x+1)^m - (x-1)^m),$$

we have

$$\sum_{x \in \mathbb{F}_q} \chi(2xP_m(x^2, 1))$$

$$
\begin{aligned}
=&\chi(2^{2m}) + \sum_{x\in\mathbb{F}_q\setminus\{1\}} \chi((x+1)^m + (x-1)^m)\chi^{-1}((x+1)^m - (x-1)^m) \\
=&1 + \sum_{x\in\mathbb{F}_q\setminus\{1\}} \chi\left(\frac{(x+1)^m + (x-1)^m}{(x+1)^m - (x-1)^m}\right) \\
=&1 + \sum_{x\in\mathbb{F}_q\setminus\{1\}} \chi\left(\frac{(1+2/(x-1))^m + 1}{(1+2/(x-1))^m - 1}\right) \\
=&1 + \sum_{y\in\mathbb{F}_q\setminus\{1\}} \chi\left(\frac{y^m+1}{y^m-1}\right) = 1 + \sum_{y\in\mathbb{F}_q\setminus\{1\}} \chi\left(\frac{y+1}{y-1}\right) \\
=&1 + \sum_{y\in\mathbb{F}_q\setminus\{1\}} \chi\left(1 + \frac{2}{y-1}\right) = 1 + \sum_{z\in\mathbb{F}_q\setminus\{1\}} \chi(z) = 0
\end{aligned}
$$

Thus $\sum_{x\in\mathbb{F}_q} \chi(xP_m(x^2,1)) = 0$ as desired.

The proof of Theorem 4.1 is now complete. □

Proof of Theorem 1.4(i). Let p be any prime with $p \equiv 5 \pmod{12}$, and let χ be the quadratic character of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with $\chi(x+p\mathbb{Z}) = (\frac{x}{p})$ for all $x \in \mathbb{Z}$. Note that $\chi(-1) = 1$ since $p \equiv 1 \pmod 4$. Clearly,

$$P_3(x,3) = \binom{6}{1}x^2 + \binom{6}{3}3x + \binom{6}{5}3^2 = 6(x^2+10x+9).$$

Applying Theorem 4.1, we obtain that

$$(10,9)_p = \det\left[\left(\frac{i^2+10ij+9j^2}{p}\right)\right]_{1\leqslant i,j\leqslant p-1} = 0$$

and

$$[10,9]_p = \det\left[\left(\frac{i^2+10ij+9j^2}{p}\right)\right]_{0\leqslant i,j\leqslant p-1} = 0.$$

Note that Sun stated in [S19, Remark 4.9] that $(10,9)_p = 0$ if and only if $[10,9]_p = 0$. □

Let $\mathbb{F}_q$ be a finite field of order q. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if P is bijective as a function on $\mathbb{F}_q$. If χ is a nontrivial multiplicative character on $\mathbb{F}_q$ and $P(x) \in \mathbb{F}_q[x]$ is a permutation polynomial, then

$$\sum_{x\in\mathbb{F}_q} \chi(P(x)) = \sum_{y\in\mathbb{F}_q} \chi(y) = 0,$$

and also

$$\sum_{x\in\mathbb{F}_q^*} \chi(P(x)) = 0$$

provided that $P(0) = 0$.

Theorem 4.2. *Let $q>1$ be an odd prime power and let $m\in\mathbb{Z}^+$ with $\gcd(m,q^2-1)=1$. Let χ be a nontrivial multiplicative character on $\mathbb{F}_q$ with $\chi(-1)=1$. For the polynomial*

$$Q_m(x,a):=\sum_{i=0}^{(m-1)/2}\frac{m}{m-i}\binom{m-i}{i}(-a)^i x^{(m-1)/2-i} \tag{4.7}$$

with $a\in\mathbb{F}_q^*$, we have

$$\dim(\mathrm{Ker}(M(Q_m(x,a),\chi)))\geqslant 2.$$

Moreover, if the character χ^m is nontrivial, then

$$\dim(\mathrm{Ker}(M_0(Q_m(x,a),\chi)))\geqslant 2.$$

Proof. Let $a\in\mathbb{F}_q$. It is a classical result (cf. [5, pp. 355-357]) that the Dickson polynomial $D_m(x,a):=xQ_m(x^2,a)$ is a permutation polynomial on $\mathbb{F}_q$. For any $g\in\mathbb{F}_q^*$, as $Q_m(gx^2,a)=g^{(m-1)/2}Q_m(x^2,ag^{-1})$, the polynomial $xQ_m(gx^2,a)$ is also a permutation polynomial on $\mathbb{F}_q$. Thus

$$\sum_{x\in\mathbb{F}_q}\chi(xQ_m(gx^2,a))=0\quad\text{for all } g\in\mathbb{F}_q^*. \tag{4.8}$$

Combining this with Lemma 4.2, we immediately obtain the desired results. □

Proof of Theorem 1.4(ii). Let p be any prime with $p\equiv 13,17 \pmod{20}$. Then $\gcd(5,p^2-1)=1$. Let χ be the quadratic character of $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ with $\chi(x+p\mathbb{Z})=(\frac{x}{p})$ for all $x\in\mathbb{Z}$. Then $\chi(-1)=1$ since $p\equiv 1 \pmod 4$. Clearly $\chi^5=\chi$ is nontrivial and $Q_5(x,-1)=x^2+5x+5$. Applying Theorem 4.2, we get that

$$[5,5]_p=\det\left[\left(\frac{i^2+5ij+5j^2}{p}\right)\right]_{0\leqslant i,j\leqslant p-1}=0.$$

This concludes the proof. □

Note that actually our method to prove Theorem 1.4 yields a stronger result stated after Theorem 1.4 in Section 1.

5. A sufficient condition for $\sum_{x=0}^{p-1}(\frac{ax^5+bx^3+cx}{p})=0$

For an odd prime power $q>1$, we let χ_q denote the quadratic multiplicative character on the finite field $\mathbb{F}_q$.

Let $p\equiv 1 \pmod 4$ be a prime and let a be a nonzero element of $\mathbb{F}_p$. If $\chi_p(a)=1$, then we define $\sqrt{a}$ as an element $\alpha\in\mathbb{F}_p$ with $\alpha^2=a$. When $\chi_p(a)=-1$, the finite field $\mathbb{F}_{p^2}\cong\mathbb{F}_p[x]/(x^2-a)$ contains an element α with $\alpha^2=a$, and we denote such an $\alpha\in\mathbb{F}_{p^2}$ by $\sqrt{a}$.

Theorem 5.1. *Let $p \equiv 1 \pmod 4$ be a prime and let a, b, c be nonzero elements of the field $\mathbb{F}_p$. Let q be p or p^2 according as $\chi_p(ac)$ is 1 or -1, and set*

$$\gamma = \frac{b + 2\sqrt{ac}}{16\sqrt{ac}} \in \mathbb{F}_q.$$

Let N be the number of $\mathbb{F}_q$-points on the affine curve $y^2 = x^4 + x^2 + \gamma$. If $N \equiv -1 \pmod p$, then

$$\sum_{x \in \mathbb{F}_p} \chi_p(ax^5 + bx^3 + cx) = 0.$$

For the sake of convenience, for an odd prime p we introduce the following two polynomials over $\mathbb{F}_p$:

$$f(z) = 1 + \sum_{k=1}^{\lfloor (p-1)/8 \rfloor} \prod_{j=0}^{k-1} \frac{(8j+1)(8j+5)}{4(j+1)(4j+3)} z^k, \tag{5.1}$$

and

$$g(z) = 1 + \sum_{k=1}^{\lfloor (p-1)/4 \rfloor} \frac{(4k-1)!!}{4^k (k!)^2} z^k. \tag{5.2}$$

Lemma 5.1. *Let p be a prime with $p \equiv 1 \pmod 4$, and let $a, b, c \in \mathbb{F}_p \setminus \{0\}$. Define*

$$A_p = \sum_{x \in \mathbb{F}_p} \chi_p(ax^5 + bx^3 + cx).$$

Viewing $A_p \pmod p$ as an element of $\mathbb{F}_p$, we have

$$A_p \pmod p = -\binom{(p-1)/2}{(p-1)/4} b^{(p-1)/4} (a^{(p-1)/4} + c^{(p-1)/4}) f\left(\frac{ac}{b^2}\right).$$

Consequently, $A_p = 0$ if $(a^{-1}c)^{(p-1)/4} = -1$ or $f(ac/b^2) = 0$.

Proof. As $A_p = \sum_{x \in \mathbb{F}_p \setminus \{0\}} \chi_p(ax^5 + bx^3 + cx)$, we have $|A_p| < p$. So, the second assertion in Lemma 5.1 follows from the first one.

Now we come to prove the first assertion. With the help of (2.2), in $\mathbb{F}_p$ we have

$$\begin{aligned} A_p \pmod p &= \sum_{x \in \mathbb{F}_p} (ax^5 + bx^3 + cx)^{(p-1)/2} \\ &= \sum_{k_5 + k_3 + k_1 = (p-1)/2} \frac{((p-1)/2)!}{k_5! k_3! k_1!} a^{k_5} b^{k_3} c^{k_1} \sum_{x=0}^{p-1} x^{5k_5 + 3k_3 + k_1} \\ &= -\sum_{\substack{k_5 + k_3 + k_1 = (p-1)/2 \\ 5k_5 + 3k_3 + k_1 = p-1}} \frac{((p-1)/2)!}{k_5! k_3! k_1!} a^{k_5} b^{k_3} c^{k_1} \\ &\quad - \sum_{\substack{k_5 + k_3 + k_1 = (p-1)/2 \\ 5k_5 + 3k_3 + k_1 = 2(p-1)}} \frac{((p-1)/2)!}{k_5! k_3! k_1!} a^{k_5} b^{k_3} c^{k_1}. \end{aligned}$$

(Note that if k_1, k_3, k_5 are nonnegative integers with $k_1+k_3+k_5 = (p-1)/2$ then $k_1 + 3k_3 + 5k_5 \leqslant 5(k_1 + k_3 + k_5) < 3(p-1)$.) Thus,

$$\begin{aligned}
&A_p \pmod p \\
&= -\sum_{\substack{k_5+k_3+k_1=(p-1)/2\\ k_3+2k_5=(p-1)/4}} \frac{((p-1)/2)!}{k_5!k_3!k_1!} a^{k_5} b^{k_3} c^{k_1} - \sum_{\substack{k_5+k_3+k_1=(p-1)/2\\ k_3+2k_1=(p-1)/4}} \frac{((p-1)/2)!}{k_5!k_3!k_1!} a^{k_5} b^{k_3} c^{k_1} \\
&= -\sum_{k=0}^{\lfloor (p-1)/8\rfloor} \frac{((p-1)/2)!}{k!((p-1)/4-2k)!((p-1)/4+k)!} a^k b^{(p-1)/4-2k} c^{(p-1)/4+k} \\
&\quad - \sum_{k=0}^{\lfloor (p-1)/8\rfloor} \frac{((p-1)/2)!}{((p-1)/4+k)!((p-1)/4-2k)!k!} a^{(p-1)/4+k} b^{(p-1)/4-2k} c^{k} \\
&= -\binom{(p-1)/2}{(p-1)/4} b^{(p-1)/4}(c^{(p-1)/4} + a^{(p-1)/4}) \\
&\quad \times \left(1 + \sum_{k=1}^{\lfloor (p-1)/8\rfloor} \prod_{i=0}^{2k-1}\left(\frac{p-1}{4} - i\right) \cdot \prod_{j=1}^{k} \frac{1}{((p-1)/4+j)} \cdot \frac{1}{k!}\left(\frac{ac}{b^2}\right)^k\right) \\
&= -\binom{(p-1)/2}{(p-1)/4} b^{(p-1)/4}(a^{(p-1)/4} + c^{(p-1)/4}) f\left(\frac{ac}{b^2}\right)
\end{aligned}$$

as desired.

□

Lemma 5.2. *Let p be an odd prime and let $q = p^n$ with $n \in \mathbb{Z}^+$. For any polynomial*

$$H(x) = \sum_{k=0}^{2(p-1)} c_k x^k \in \mathbb{F}_q[x],$$

we have

$$\sum_{x\in\mathbb{F}_q} H(x)^{1+p+\cdots+p^{n-1}} = -c_{p-1}^{1+p+\cdots+p^{n-1}} - c_{2(p-1)}^{1+p+\cdots+p^{n-1}}. \tag{5.3}$$

Proof. As the multiplicative group $\mathbb{F}_q \setminus \{0\}$ is cyclic, similar to (2.2), for each $s = 0, 1, 2, \ldots$ we have

$$\sum_{x\in\mathbb{F}_q} x^s = \begin{cases} -1 & \text{if } s \in (q-1)\mathbb{Z}^+, \\ 0 & \text{otherwise,} \end{cases}$$

where we treat 0^0 as 1 when $s = 0$. Note also that

$$H(x)^{p^i} = \sum_{k=0}^{2(p-1)} c_k^{p^i} x^{kp^i}$$

for all integers $i \geqslant 0$. Thus

$$\sum_{x\in\mathbb{F}_q} H(x)^{1+p+\cdots+p^{n-1}} = \sum_{x\in\mathbb{F}_q}\prod_{i=0}^{n-1}\left(\sum_{k_i=0}^{2(p-1)} c_{k_i}^{p^i} x^{k_i p^i}\right) = -{\sum}^*_{k_0,\ldots,k_{n-1}}\prod_{i=0}^{n-1} c_{k_i}^{p^i}$$

where $\sum^*$ means that the sum is taken over all $k_0,\ldots,k_{n-1}\in\{0,1,\ldots,2p-2\}$ subject to the condition

$$k_0 + k_1 p + \cdots + k_{n-1}p^{n-1} \in (q-1)\mathbb{Z}^+. \tag{5.4}$$

Write $k_i = p-1+t_i$, where $-(p-1)\leqslant t_i \leqslant p-1$. Then

$$\sum_{i=0}^{n-1} k_i p^i = q-1+\sum_{i=0}^{n-1} t_i p^i.$$

Note that

$$\left|\sum_{i=0}^{n-1} t_i p^i\right| \leqslant q-1,$$

and the equality is possible only if $t_0=\cdots=t_{n-1}=p-1$ (i.e., $k_0=\cdots=k_{n-1}=2(p-1)$) or $t_0=\cdots=t_{n-1}=-(p-1)$ (i.e., $k_0+k_1p+\cdots+k_{n-1}p^{n-1}=0$). Since $|t_i|<p$, if $\sum_{i=0}^{n-1} t_ip^i=0$ then we obtain step by step that $t_0=\cdots=t_{n-1}=0$ (i.e., $k_0=\cdots=k_{n-1}=p-1$).

Combining the above, we finally obtain (5.3). □

Lemma 5.3. *Let p be an odd prime and let $q=p^n$ with $n\in\mathbb{Z}^+$. Let $\alpha,\beta,\gamma\in\mathbb{F}_q\setminus\{0\}$ and set*

$$B_q = \sum_{x\in\mathbb{F}_q}\chi_q(\alpha x^4+\beta x^2+\gamma).$$

Viewing $B_q \pmod p$ as an element of $\mathbb{F}_q$, we have

$$B_q \pmod p = -\chi_q(\alpha) - \chi_q(\beta) g\left(\frac{\alpha\gamma}{\beta^2}\right)^{1+p+\cdots+p^{n-1}}. \tag{5.5}$$

Proof. Write

$$H(x) := (\alpha x^4+\beta x^2+\gamma)^{(p-1)/2} = \sum_{k=0}^{2(p-1)} c_k x^k.$$

In view of Lemma 5.2, we have

$$\begin{aligned} B_q \pmod p &= \sum_{x\in\mathbb{F}_q}(\alpha x^4+\beta x^2+\gamma)^{(q-1)/2} = \sum_{x\in\mathbb{F}_q} H(x)^{1+p+\cdots+p^{n-1}} \\ &= -c_{p-1}^{1+p+\cdots+p^{n-1}} - c_{2(p-1)}^{1+p+\cdots+p^{n-1}}. \end{aligned} \tag{5.6}$$

Clearly,

$$c_{2(p-1)}^{1+p+\cdots+p^{n-1}} = \alpha^{(q-1)/2} = \chi_q(\alpha). \tag{5.7}$$

Note also that

$$\begin{aligned}
c_{p-1} = & \sum_{\substack{k_4+k_2+k_0=(p-1)/2 \\ 4k_4+2k_2=p-1}} \frac{((p-1)/2)!}{k_4!k_2!k_0!}\alpha^{k_4}\beta^{k_2}\gamma^{k_0} \\
= & \sum_{0\leqslant k\leqslant (p-1)/4} \frac{((p-1)/2)!}{((p-1)/2-2k)!(k!)^2}\alpha^k\beta^{((p-1)/2-2k)}\gamma^k \\
= & \beta^{(p-1)/2} + \beta^{(p-1)/2}\sum_{k=1}^{\lfloor (p-1)/4\rfloor}\prod_{j=0}^{2k-1}\left(\frac{p-1}{2}-j\right)\cdot\frac{1}{(k!)^2}\left(\frac{\alpha\gamma}{\beta^2}\right)^k \\
= & \beta^{(p-1)/2} g\left(\frac{\alpha\gamma}{\beta^2}\right)
\end{aligned}$$

and hence

$$c_{p-1}^{1+p+\cdots+p^{n-1}} = \chi_q(\beta) g\left(\frac{\alpha\gamma}{\beta^2}\right)^{1+p+\cdots+p^{n-1}}. \tag{5.8}$$

Combining (5.6) with (5.7) and (5.8), we immediately obtain the desired (5.5). □

Now we study further properties of the polynomials f and g defined by (5.1) and (5.2). They may be viewed as truncated versions of certain hypergeometric series.

Lemma 5.4. *Let p be an odd prime and let $q = p^n$ with $n \in \mathbb{Z}^+$.*

(i) *A polynomial $u \in \mathbb{F}_q[z]$ with $\deg u \leqslant \lfloor (p-1)/4\rfloor$ satisfies the differential equation*

$$(4z-16z^2)u'' + (4-32z)u' - 3u = 0 \tag{5.9}$$

if and only if $u = cg$ for some $c \in \mathbb{F}_q$.

(ii) *Suppose that $p \equiv 1 \pmod 4$. Then a polynomial $v \in \mathbb{F}_q[z]$ with $\deg v \leqslant \lfloor (p-1)/8\rfloor$ satisfies the differential equation*

$$(16z-64z^2)v'' + (12-112z)v' - 5v = 0 \tag{5.10}$$

if and only if $v = cf$ for some $c \in \mathbb{F}_q$.

Proof. It is straightforward to verify that $u = g$ and $v = f$ satisfy (5.9) and (5.10) respectively. So, the "if" parts of (i) and (ii) are easy.

Now we prove the "only if" part of (i). If a polynomial $u \in \mathbb{F}_q[z]$ with $\deg u \le \lfloor (p-1)/4\rfloor$ satisfies (5.9), then there is a constant $c \in \mathbb{F}_q$ such that $\tilde{u} = u - cg$ is a solution of (5.9) with $\deg\tilde{u} < \lfloor (p-1)/4\rfloor$. Thus, it suffices to show that (5.9) has no nonzero solution $u = c_d z^d + \cdots + c_0$ with $\deg u = d < \lfloor (p-1)/4\rfloor$. In fact, the coefficient of z^d in $(4z-16z^2)u'' + (4-32z)u' - 3u$ is $-(4d+1)(4d+3)c_d \neq 0$ provided $d < \lfloor (p-1)/4\rfloor$.

Similarly, we can show the "only if" part of (ii). □

Lemma 5.5. *Let $p = 4n+1$ be a prime with $n \in \mathbb{Z}^+$. Then*

$$-(2n)!(n!)^2 g(z) = (16z-2)^n f\left(\frac{1}{(16z-2)^2}\right).$$

Proof. Clearly, $u = (16z-2)^n f((16z-2)^{-2})$ is a polynomial of degree $n=(p-1)/4$ with the leading coefficient 1. A direct computation based on (5.10) shows that u satisfies (5.9). Now we apply Lemma 5.4 and compare the leading terms of both sides. Since

$$\frac{(p-2)!!}{4^n(n!)^2} = \frac{(p-1)!}{2^{p-1}(2n)!(n!)^2} \equiv -\frac{1}{(2n)!(n!)^2} \pmod p,$$

we immediately get the desired result. □

Proof of Theorem 5.1. Since

$$N = \sum_{x\in\mathbb{F}_q}(1+\chi_q(x^4+x^2+\gamma)) = q + \sum_{x\in\mathbb{F}_q}\chi_q(x^4+x^2+\gamma),$$

the assumption $N \equiv -1 \pmod p$, together with Lemma 5.3 in the case $\alpha=\beta=1$, implies that $g(\gamma)=0$. As $(16\gamma-2)^{-2} = ac/b^2$, we have $f(ac/b^2)=0$ by Lemma 5.5. Applying Lemma 5.1 we obtain the desired result. □

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

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

[3] D. A. Cox, *Primes of the Form x^2+ny^2*, John Wiley & Sons, 1989.

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

[5] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd Edition, Encyclopedia of Math. and its Applications, 20, Cambridge Univ. Press, Cambridge, 1997.

[6] A. R. Rajwade, *The Diophantine equation $y^2 = x(x^2+21Dx+112D^2)$ and the conjectures of Birch and Swinnerton-Dyer*, J. Austral. Math. Soc. Ser. A **24** (1977), 286–295.

[7] Z.-H. Sun, *Congruences involving Legendre polynomials II*, J. Number Theory **133** (2013), 1950–1976.

[8] Z.-W. Sun, *Super congruences and Euler numbers*, Sci. China Math. **54** (2011), 2509–2535.

[9] Z.-W. Sun, *Supercongruences involving products of two binomial coefficients*, Finite Fields Appl. **22** (2013), 24–44.

[10] Z.-W. Sun, *A series of conjectures on $\sum_{x=0}^{(p-1)/2}(\frac{x^5+cx^3+dx}{p})$ (III)*, Question 319259 on MathOverflow, December 22, 2018. Available from `https://mathoverflow.net/questions/319259`,

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

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

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

(Dmitry Krachun) St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Fontanka 27, 191023, St. Petersburg, Russia

E-mail address: dmitrykrachun@gmail.com

(Fedor Petrov) St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Fontanka 27, 191023, St. Petersburg, Russia

E-mail address: fedyapetrov@gmail.com

(Zhi-Wei Sun) Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

E-mail address: zwsun@nju.edu.cn

(Maxim Vsemirnov) St. Petersburg Department of Steklov Mathematical Institute of Russian Academy of Sciences, Fontanka 27, 191023, St. Petersburg, Russia

E-mail address: vsemir@pdmi.ras.ru