# THE OPEN HALF OF SUN'S CONJECTURE 4.10(II): NONVANISHING OF $\det\big[\big(\frac{j+k}{p}\big)+\big(\frac{j^2+k^2}{p}\big)\big]$ FOR EVERY PRIME $p\equiv 3 \pmod 4$ BELOW 1500

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $p$ be an odd prime, $n=(p-1)/2$, and let $A(p)=\big[\big(\frac{j+k}{p}\big)+\big(\frac{j^2+k^2}{p}\big)\big]_{0\le j,k\le n}$ be the integer matrix of Legendre symbols studied by Jiang and Sun. Sun's Conjecture 4.10(ii) asserts that $2\det A(p)$ is a quadratic residue modulo $p$ whenever $p\equiv 3 \pmod 4$. Jiang and Sun proved $\big(\frac{2\det A(p)}{p}\big)\neq -1$ and remarked that they are unable to prove $p\nmid \det A(p)$; as a quadratic residue is by definition nonzero, that nonvanishing is the entire remaining content of the conjecture. We prove $p\nmid \det A(p)$ for every prime $p\equiv 3 \pmod 4$ with $p\le 1500$ — 122 primes, matrices of side up to 750 — by exhibiting for each such $p$ a right inverse of $A(p)$ over $\mathbb{F}_p$ and verifying the product; the verification is machine-checked, so the window is a theorem rather than the report of a computation. With Jiang and Sun's theorem this settles Conjecture 4.10(ii) for those 122 primes. We also show that the hypothesis $p\equiv 3 \pmod 4$ cannot be dropped and that Jiang and Sun's theorem does not by itself imply the conjecture: $5\mid \det A(5)$ and $13\mid \det A(13)$, each witnessed by an explicit kernel vector, while at $p=5$ the conclusion $\big(\frac{2\det A(5)}{5}\big)\neq -1$ still holds, the symbol being 0. Outside the formal development, an independent sweep confirms the full conjecture for all 399 primes $p\equiv 3 \pmod 4$ below 6000, and records the behaviour of the same matrix at $p\equiv 1 \pmod 4$. Finally we point out that a Vandermonde factor in Jiang and Sun's own displayed identity reduces $p\nmid \det A(p)$ to $p\nmid \det C_2$ on a matrix of side $(p+1)/4$.

## 1. Introduction

1.1. **The determinant.** Let $p$ be an odd prime, let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol with $\left(\frac{0}{p}\right)=0$, and set

$$n=\frac{p-1}{2},\qquad A=A(p)=\left[\left(\frac{j+k}{p}\right)+\left(\frac{j^2+k^2}{p}\right)\right]_{0\le j,k\le n}.$$

This is an *integer* matrix of side $n+1=(p+1)/2$, indexed from 0; its entries lie in $\{-2,-1,0,1,2\}$ and its $(0,0)$ entry is $\left(\frac{0}{p}\right)+\left(\frac{0}{p}\right)=0$. Determinants of matrices of Legendre symbols have a long history; the two evaluations that $A(p)$ superposes are recalled in §1 of [1]. Chapman [4] evaluated $\det\big[\big(\frac{j+k}{p}\big)\big]_{0\le j,k\le n}$ — it equals $2^{(p-1)/2}$ for $p>3$ with $p\equiv 3 \pmod 4$ — and Sun [5] introduced $S_p=\det\big[\big(\frac{j^2+k^2}{p}\big)\big]_{1\le j,k\le n}$ and $T_p=\det\big[\big(\frac{j^2+k^2}{p}\big)\big]_{0\le j,k\le n}$ and proved $S_p=\frac{2}{p-1}T_p$ and $\left(\frac{T_p}{p}\right)=\left(\frac{2}{p}\right)$. The matrix $A(p)$ is the entrywise sum of the two matrices occurring in those two evaluations, and its determinant is the subject of the last conjecture of [2, §4], which we quote in the notation of that paper, where $|a_{jk}|$ denotes a determinant:

**Conjecture 4.10.** Let $p$ be an odd prime.

(i) When $p\equiv 1 \pmod 4$, for any $\delta_1,\delta_2\in\{\pm 1\}$ the number

$$2\left|\left(\frac{j+k}{p}\right)+\left(\frac{j-k}{p}\right)+\delta_1\left(\frac{j^2+\delta_2k^2}{p}\right)\right|_{0\le j,k\le (p-1)/2}$$

is a quadratic residue modulo $p$.

(ii) If $p \equiv 3 \pmod 4$, then the number

$$2\left|\left(\frac{j+k}{p}\right)+\left(\frac{j^2+k^2}{p}\right)\right|_{0\le j,k\le (p-1)/2}$$

is a quadratic residue modulo $p$.

Part (ii) is the statement about $A(p)$: it says that $2\det A(p)$ is a quadratic residue modulo $p$, that is, that $\left(\frac{2\det A(p)}{p}\right)=1$. No verification range is attached to Conjecture 4.10 in [2]: the remarks in that paper that record one — for instance "We have verified this conjecture for odd primes $p<2000$" — are all attached to conjectures of its §5.

1.2. **What Jiang and Sun prove, and what is left.** Jiang and Sun [1] prove the following.

**Theorem 1.1** ([1]). Let $p$ be a prime with $p\equiv 3 \pmod 4$. For the matrix $A=\left[\left(\frac{j+k}{p}\right)+\left(\frac{j^2+k^2}{p}\right)\right]_{0\le j,k\le (p-1)/2}$ we have $\left(\frac{2\det(A)}{p}\right)\neq -1$.

Their proof, which we recall in §2, produces the sharper statement that $\left(\frac{2\det A}{p}\right)$ is a square in $\{0,1\}$, and the paper is explicit about what that leaves open. Immediately after Theorem 1.1 they write, verbatim:

> **Remark.** Actually, Sun [2] conjectured $2\det(A)$ is a quadratic residue modulo $p$ but we are unable to prove that $p\nmid \det(A)$.

The distinction is not a technicality. A quadratic residue modulo $p$ is a nonzero square, so Conjecture 4.10(ii) is the conjunction of two assertions: that the class of $2\det A$ is a square, and that it is not the zero class. Theorem 1.1 gives the first and says nothing about the second, and the Remark records exactly this.[1] So the whole open content of Conjecture 4.10(ii) is the single sentence

$$p\nmid \det A(p) \qquad \text{for } p\equiv 3 \pmod 4.$$

That sentence is the subject of this paper. It is not vacuous: for the same matrix at primes $p\equiv 1 \pmod 4$ the determinant *is* divisible by $p$ at $p=5$ and $p=13$ (Theorem 5.1), and at those primes Theorem 1.1's conclusion nevertheless holds, because the symbol of 0 is 0 and not $-1$.

1.3. **Part (i) is already a theorem.** Part (i) of Conjecture 4.10 — the case $p\equiv 1 \pmod 4$, with its two sign parameters — has been proved. Yang and Zhang [3] give a uniform exact congruence modulo $p$ for the determinant underlying Conjecture 4.10(i) and deduce from it, for every $\delta_1,\delta_2\in\{\pm 1\}$, that the residue class of $2\det\left[\left(\frac{j+k}{p}\right)+\left(\frac{j-k}{p}\right)+\delta_1\left(\frac{j^2+\delta_2 k^2}{p}\right)\right]_{0\le j,k\le (p-1)/2}$ is a nonzero quadratic residue modulo $p$; that is Corollary 1.3 of their v3, and their abstract puts it as "Its standard specialization recovers the asserted square class". The proof of the congruence is Euler's criterion followed by a two-antidiagonal determinant lemma; Vsemirnov's factorisation [7] of Chapman's matrix is used for their other result, on Sun's Conjecture 4.8(i). They also record that the square-class assertion of Conjecture 4.10(i) already follows from Sun's evaluation in [5] of the symbol of $T(d,p)=\det[\left(\frac{j^2+dk^2}{p}\right)]_{0\le j,k\le (p-1)/2}$, their own contribution being the exact congruence and its uniformity in the half system. For the record, [1] does not cite [3]: the bibliography of arXiv:2606.03970v1 — the only version — has six items, none of them [3], and neither author's name occurs anywhere in its e-print source.

The two halves are not interchangeable, and the reason is visible in the shape of the matrix. For $p\equiv 1 \pmod 4$ the exponent $n=(p-1)/2$ is even; both $\left(\frac{j+k}{p}\right)+\left(\frac{j-k}{p}\right)$ and $\left(\frac{j^2+\delta_2 k^2}{p}\right)$ then expand, after Euler's criterion, in even powers of $j$, the whole matrix sits in a single Vandermonde basis in $j^2$, and the determinant collapses. For $p\equiv 3 \pmod 4$ the exponent $n$ is odd, $(j+k)^n$ contributes odd powers of $j$, the monomial set overflows the $n+1$ available basis elements, and no such collapse is

[1] The abstract of [1] states the theorem in the form "$2\det[a_{jk}]_{0\le j,k\le (p-1)/2}$ is congruent to a square modulo $p$", which is literally what is proved, the zero square being allowed.

available. Part (ii) is the hard half, which is consistent with [1] obtaining the square class for it but not the nonvanishing.

1.4. **Results.** We settle $p \nmid \det A(p)$ on a finite window, with a proof that is checked by machine rather than reported.

(1) $p \nmid \det A(p)$ for *every* prime $p \equiv 3 \pmod 4$ with $p \le 1500$: 122 primes, the largest being $p = 1499$ with $A(p)$ of side 750 (Theorem 4.1). With Theorem 1.1 of [1] this gives Conjecture 4.10(ii) for those 122 primes (Corollary 4.2).
(2) The certificate behind (1) is a right inverse over $\mathbb{F}_p$, and its soundness is a short lemma (Proposition 3.1) in which nothing about the procedure that *produces* the inverse is assumed. The check is not vacuous: it succeeds at $p = 7$ and fails at $p = 5$ and $p = 13$, the two primes where the matrix really is singular (Proposition 3.2).
(3) The hypothesis $p \equiv 3 \pmod 4$ is not removable, and Theorem 1.1 of [1] does not imply Conjecture 4.10(ii): $5 \mid \det A(5)$ and $13 \mid \det A(13)$, each certified by an explicit kernel vector, while at $p = 5$ the conclusion $\left(\frac{2 \det A(p)}{p}\right) \ne -1$ still holds (Theorem 5.1).
(4) Outside the formal development, an independent implementation confirms Conjecture 4.10(ii) in full for all 399 primes $p \equiv 3 \pmod 4$ below 6000, and records the behaviour of the same matrix at $p \equiv 1 \pmod 4$ (§6).
(5) Jiang and Sun's own displayed identity contains a Vandermonde determinant that is invertible modulo $p$ for trivial reasons, so their identity reduces $p \nmid \det A$ to $p \nmid \det C_2$ on a matrix of side $(p+1)/4$ (Remark 2.1). We record this because it is the natural next target, both for a proof and for an eightfold cheaper verification.

Every numbered statement of §§3–5 is machine-checked in Lean 4 [10] against Mathlib [11]; §8 says precisely what the machine checks, and §7 says precisely which claims rest on exhaustive computation and how large each computation was. The material of §6 is *not* machine-checked and is labelled as such throughout.

## 2. Notation and the shape of Jiang and Sun's argument

Throughout, $p$ is an odd prime, $n = (p-1)/2$, $m = n+1 = (p+1)/2$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Matrices indexed $0 \le j, k \le n$ are $m \times m$. For an integer matrix $M$ we write $\overline{M}$ for its entrywise reduction modulo $p$; since reduction is a ring homomorphism, $\overline{\det \overline{M}} = \det \overline{M}$, and $p \mid \det M$ if and only if $\det \overline{M} = 0$ in $\mathbb{F}_p$.

We recall the structure of the proof of Theorem 1.1 of [1], because Remark 2.1 and §9 refer to it. Assume $p \equiv 3 \pmod 4$, so that $n$ is odd. Let $r_i(x)$ be the remainder of $x^i$ modulo $\prod_{k=0}^{n}(x-k)$ and put

$$f(x,y) = (x+y)^n + \sum_{l=0}^{(n-1)/2} \binom{n}{l} x^{2l} r_{2n-2l}(y) + \sum_{l=(n+1)/2}^{n} \binom{n}{l} r_{2l}(x) y^{2n-2l},$$

a polynomial of degree at most $n$ in each variable, so that $f(x,y) = \sum_{u,v=0}^{n} b(u,v) x^u y^v$. For $0 \le j, k \le n$ one has $f(j,k) = (j+k)^n + (j^2+k^2)^n \equiv \left(\frac{j+k}{p}\right) + \left(\frac{j^2+k^2}{p}\right) \pmod p$ by Euler's criterion, so with $B = [b(u,v)]_{0 \le u,v \le n}$ and the Vandermonde matrix $H = [j^u]_{0 \le j,u \le n}$ one has $\overline{A} = \overline{H}\,\overline{B}\,\overline{H}^{\mathsf{T}}$ and hence

$$\det A \equiv \det(H)^2 \det(B) \pmod p. \tag{1}$$

Since $n$ is odd, $b(u,v) = 0$ whenever $u$ and $v$ are both odd; moving the rows of even index, and then the columns of even index, to the front turns $B$ into a block matrix $C_0 = \left[\begin{smallmatrix} C_1 & C_2 \\ C_3 & C_4 \end{smallmatrix}\right]$ with $\det B \equiv \det C_0 \pmod p$, $C_4 = 0$ and $C_3 = C_2^{\mathsf{T}}$, where $C_2$ has side $(n+1)/2 = (p+1)/4$. Therefore

$$\det A \;\equiv\; (-1)^{(p+1)/4} \det(H)^2 \det(C_2)^2 \pmod p, \tag{2}$$

and since $\left(\frac{-1}{p}\right) = -1$ and $\frac{p^2-1}{8} \equiv \frac{p+1}{4} \pmod 2$ for $p \equiv 3 \pmod 4$, the two sign contributions cancel and $\left(\frac{2\det A}{p}\right) = \left(\frac{\det(H)\det(C_2)}{p}\right)^2 \in \{0,1\}$. This is Theorem 1.1, and (2) shows why the argument is silent about nonvanishing: it computes a square class, and a square class cannot distinguish 0 from a nonzero residue.

*Remark* 2.1. The identity (2) does, however, localise the open statement. The matrix $H$ is the Vandermonde matrix on the nodes $0, 1, \ldots, n$, so $\det H = \prod_{0 \le i < j \le n}(j-i)$, a product of integers $j-i$ with $1 \le j-i \le n < p$; hence $p \nmid \det H$. With (2) this gives, for every prime $p \equiv 3 \pmod 4$,

$$p \nmid \det A(p) \quad \Longleftrightarrow \quad p \nmid \det C_2,$$

where $C_2$ is the block of side $(p+1)/4$ described above. This is an immediate consequence of the identity displayed in [1], which that paper does not state explicitly, and we did not find it stated elsewhere — a report of a search, not a claim of novelty. It is a paper argument and is *not* part of the machine-checked development below.

## 3. Certificates for nonvanishing

Everything we prove about $A(p)$ goes through one elementary observation: a right inverse over $\mathbb{F}_p$ certifies nonvanishing, and it certifies it without any assumption about how the inverse was found.

**Proposition 3.1** (Soundness of the certificate)**.** *Let $p$ be a prime and let $T = [t_{jk}]_{0 \le j,k \le n}$ be the table of natural numbers defined by*

$$t_{jk} = \Big( (j+k)^{\,n} \bmod p \;+\; (j^2+k^2)^{\,n} \bmod p \Big) \bmod p, \qquad n = \tfrac{p-1}{2}.$$

*Then $\overline{T} = \overline{A(p)}$ in $M_m(\mathbb{F}_p)$. Consequently, if there exists a matrix $Y \in M_m(\mathbb{F}_p)$ with $\overline{T}\,Y = I_m$, then $p \nmid \det A(p)$.*

*Proof.* The first assertion is Euler's criterion entry by entry: for every integer $a$ one has $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$, so $\overline{t_{jk}} = \overline{(j+k)^n} + \overline{(j^2+k^2)^n} = \overline{\left(\frac{j+k}{p}\right)} + \overline{\left(\frac{j^2+k^2}{p}\right)}$, which is the reduction of the $(j,k)$ entry of $A(p)$. For the second, a right inverse forces $\det \overline{T} \cdot \det Y = 1$, so $\det \overline{A(p)} = \det \overline{T} \neq 0$; as reduction commutes with det, this says $\overline{\det A(p)} \neq 0$, i.e. $p \nmid \det A(p)$. □

Two features of Proposition 3.1 matter for what follows. First, the hypothesis is the existence of $Y$, so a candidate produced by any procedure whatsoever — in our case by an unverified Gauss–Jordan elimination — can be used: a wrong candidate makes the equation $\overline{T}Y = I_m$ false and proves nothing, it cannot make a false conclusion provable. Second, the identification $\overline{T} = \overline{A(p)}$ is the only place where the Legendre symbol appears; after it, the argument is linear algebra over $\mathbb{F}_p$ on a table of residues. We write $\mathrm{cert}(p)$ for the Boolean value of the test "$\overline{T}Y = I_m$" where $Y$ is the output of that fixed elimination procedure applied to $T$.

A certificate predicate that were true by construction would prove nothing, so we record that it is not.

**Proposition 3.2** (The test is not vacuous)**.** $\mathrm{cert}(5)$ *and* $\mathrm{cert}(13)$ *are false, and* $\mathrm{cert}(7)$ *is true.*

*Proof.* Three evaluations of a fixed finite computation, on matrices of side 3, 7 and 4. □

The two failures are not accidents of the elimination: by Theorem 5.1 the matrices $A(5)$ and $A(13)$ really are singular modulo 5 and 13, so no right inverse exists and no procedure could return one.

## 4. The window

**Theorem 4.1** (Sun's Conjecture 4.10(ii), nonvanishing half, for $p \le 1500$)**.** *Let $p$ be a prime with $p \equiv 3 \pmod 4$ and $p \le 1500$. Then*

$$p \nmid \det A(p),$$

*equivalently, $\overline{A(p)}$ is invertible in $M_{(p+1)/2}(\mathbb{F}_p)$. There are 122 such primes, from $p = 3$ to $p = 1499$; the largest matrix involved has side 750.*

*Proof.* For each of the 122 primes the elimination procedure of §3 is run on the table $T$ of that prime and the resulting $m \times m$ candidate $Y$ is multiplied back against $T$ modulo $p$; every entry of the product is compared with the corresponding entry of $I_m$. All 122 tests return true, so Proposition 3.1 applies at each of them. Two finite verifications are involved and both are exhaustive: the 122 certificate checks themselves, and a separate check that the list of 122 primes contains every prime $q \le 1500$ with $q \equiv 3 \pmod 4$, so that no prime in the range can have been silently omitted. The arithmetic is described in §7 and its machine verification in §8. □

**Corollary 4.2.** *Granting Theorem 1.1 of* [1]*, Conjecture 4.10(ii) of* [2] *holds for every prime $p \equiv 3 \pmod 4$ with $p \le 1500$: for those $p$ the integer $2 \det A(p)$ is a quadratic residue modulo $p$.*

*Proof.* By Theorem 1.1 of [1], $\left(\frac{2 \det A(p)}{p}\right) \neq -1$; by Theorem 4.1, $p \nmid \det A(p)$ and hence $p \nmid 2 \det A(p)$, so $\left(\frac{2 \det A(p)}{p}\right) \neq 0$. The only remaining value is 1. □

We stress that Corollary 4.2 is *not* part of the machine-checked development. It combines Theorem 4.1, which is checked, with the published Theorem 1.1 of [1], which we take from the literature and have not formalised; only the nonvanishing half is machine-checked here.

The smallest case is instructive. At $p = 3$ we have $n = 1$ and $A(3) = \left[\begin{smallmatrix} 0 & 2 \\ 2 & -2 \end{smallmatrix}\right]$, so $\det A(3) = -4 \equiv 2 \pmod 3$ and $\left(\frac{2 \cdot (-4)}{3}\right) = \left(\frac{1}{3}\right) = 1$.

## 5. The hypothesis, and the gap between Theorem 1.1 and the conjecture

The matrix $A(p)$ is defined for every odd prime, and Theorem 4.1 carries the hypothesis $p \equiv 3 \pmod 4$. The next theorem shows that the hypothesis is doing real work, and — more to the point — that the published Theorem 1.1 of [1] cannot be upgraded to Conjecture 4.10(ii) by any argument that uses only its conclusion.

**Theorem 5.1.** (1) *It is* not *the case that $p \nmid \det A(p)$ for every prime $p$: indeed $5 \mid \det A(5)$ and $13 \mid \det A(13)$.*

(2) *At $p = 5$ one has both $\left(\frac{2 \det A(5)}{5}\right) \neq -1$ and $5 \mid \det A(5)$.*

*Proof.* For (1) it suffices to exhibit nonzero kernel vectors of the reduced matrices. Over $\mathbb{F}_5$, with $A(5)$ of side 3, the vector $(3, 0, 1)^{\mathsf{T}}$ satisfies $\overline{A(5)}\, v = 0$; over $\mathbb{F}_{13}$, with $A(13)$ of side 7, the vector $(12, 0, 6, 0, 0, 9, 1)^{\mathsf{T}}$ satisfies $\overline{A(13)}\, v = 0$. Both verifications are finite evaluations of the matrix–vector product, using the identification $\overline{T} = \overline{A(p)}$ of Proposition 3.1. A square matrix over a field with a nonzero kernel vector has vanishing determinant, so $\det \overline{A(p)} = 0$ and therefore $p \mid \det A(p)$ for $p = 5, 13$. For (2), 5 divides $\det A(5)$ by (1), hence also $2 \det A(5)$, so $\left(\frac{2 \det A(5)}{5}\right) = 0 \neq -1$. □

Part (2) is the point of the section. The conclusion of Theorem 1.1 of [1] is the inequality $\left(\frac{2 \det A}{p}\right) \neq -1$, and at $p = 5$ that inequality is *true* while $\det A(5)$ is divisible by 5. So the conclusion of Theorem 1.1 is strictly weaker than Conjecture 4.10(ii) as a statement about a given prime, and no purely formal strengthening of it — no rearrangement of the symbol identity — can close the gap. Closing the gap requires an input that sees the difference between 0 and a nonzero square, which is exactly what a certificate provides at one prime and what §9 discusses in general.

*Remark* 5.2. Outside the formal development, exact integer elimination shows that $\det A(5)$ and $\det A(13)$ are not merely divisible by 5 and 13 but equal to 0 in $\mathbb{Z}$.

## 6. Computations outside the formal development

The statements of this section were obtained with an independent implementation in C (Gaussian elimination over $\mathbb{F}_p$) and are *not* machine-checked. We report them because they extend the certified window considerably and because we did not find a verification range recorded for Conjecture 4.10, in either part: in v8 of [2] the eight remarks that record one — "We have verified this conjecture for odd primes $p < 2000$" and its variants — are attached to conjectures of its §5, and none to any conjecture of its §4; [1] prints no numerical value at all; and [3] prints tables only for its other determinant. We searched the papers citing [2] as well. That is a "not found", not a claim that no range exists.

(A) *Conjecture 4.10(ii) in full, to $p < 6000$.* For all 399 primes $p \equiv 3 \pmod 4$ with $3 \le p \le 5987$, the determinant $\det A(p)$ is nonzero modulo $p$ and $\left(\frac{2\det A(p)}{p}\right) = 1$. The matrices range from $2 \times 2$ (at $p = 3$) to $2994 \times 2994$ (at $p = 5987$).

(B) *The same matrix at $p \equiv 1 \pmod 4$.* Among the 211 primes $p \equiv 1 \pmod 4$ with $5 \le p \le 2969$, one has $p \mid \det A(p)$ at exactly two primes, $p = 5$ and $p = 13$; and $\left(\frac{2\det A(p)}{p}\right) = -1$ for 127 of the 211, $+1$ for 82, and 0 for the two singular ones. So at $p \equiv 1 \pmod 4$ both halves of the story fail: the square class fails for a majority of primes, and nonvanishing fails outright twice.

(C) *Part (i), reproduced.* For the same 211 primes and all four sign choices $(\delta_1, \delta_2) \in \{\pm 1\}^2$, the 844 determinants of Conjecture 4.10(i) are all nonzero with $2\det a$ quadratic residue. This is a reproduction of the theorem of [3], not a new result, and we record it only as a check on our implementation.

Item (B) is the reason the hypothesis $p \equiv 3 \pmod 4$ appears in Theorem 4.1 and in Theorem 1.1 of [1]: neither statement is a shadow of something true for all odd primes. Note also that the only two singular cases found in the whole $p \equiv 1 \pmod 4$ range are $p = 5$ and $p = 13$, the two primes certified in Theorem 5.1.

## 7. The extent of the computation

We state exactly which claims rest on exhaustive computation and how large each search was.

- Proposition 3.1 rests on no computation: it is Euler's criterion and two standard facts about determinants over a commutative ring, uniform in $p$. Remark 2.1 likewise is a two-line argument from the identity displayed in [1].
- Theorem 4.1 is the exhaustive claim. The search is the complete set of 122 primes $p \equiv 3 \pmod 4$ with $p \le 1500$, and for each of them two things are evaluated: the table $T$ of $m^2$ residues, each entry by two modular exponentiations with exponent $n$; and the $m \times m$ product $\overline{T}\,Y$ against $I_m$, where $Y$ is the elimination output. The dominant cost is the product, $\Theta(m^3)$ per prime; over the window this is $1.18 \times 10^{10}$ modular multiply–add operations, and about 0.8 CPU-hours of compiled arithmetic. A second exhaustive evaluation checks that the list of 122 primes contains every prime $q \le 1500$ with $q \equiv 3 \pmod 4$. The window was checked in ten independent pieces of roughly equal cost, the first holding the 77 primes $3 \le p \le 863$ and the last the single prime $p = 1499$.
- Proposition 3.2 is three evaluations of the same fixed computation, at $p = 5, 7, 13$.
- Theorem 5.1 is two matrix–vector products, of sizes 3 and 7, plus one evaluation of a Legendre symbol. No exhaustive search is involved, and no compiled evaluation either (see §8).
- The statements of §6 are outside the formal development. Item (A) is 399 determinants over $\mathbb{F}_p$, $2.43 \times 10^{12}$ modular multiply–adds; item (B) is 211 determinants, $1.62 \times 10^{11}$; item (C) is 844 determinants, $6.47 \times 10^{11}$. They were cross-checked in two independent ways: against a separate implementation in Python on the whole range $3 \le p \le 107$, agreeing digit for digit, and against a second C binary whose modular reduction uses integer division rather than

a floating-point reciprocal, on a sample of 31 primes from 3 to 5843, agreeing on both the determinant and its symbol. Independently of both, the 122 primes of Theorem 4.1 constitute a third implementation of the same predicate on a sub-range, and agree.

- Before any of the above, the printed evaluations that frame the problem were reproduced from their definitions with independent code, as a check that we had read the sources correctly: Chapman's evaluation $\det\left[\left(\frac{j+k}{p}\right)\right]_{0\le j,k\le n} = 2^{(p-1)/2}$ [4] as an exact integer determinant for every prime $p \equiv 3 \pmod 4$ with $7 \le p \le 59$ (and, correctly, failing at $p = 3$, which that statement excludes); Sun's relations $S_p = \frac{2}{p-1}T_p$ and $\left(\frac{T_p}{p}\right) = \left(\frac{2}{p}\right)$ [5] for every odd prime $5 \le p \le 59$; and the whole reduction chain of [1] recalled in §2 — the polynomial $f$, the factorisation $\overline{A} = \overline{H}\,\overline{B}\,\overline{H}^{\mathsf{T}}$, the vanishing of $C_4$ and the identity (2) — rebuilt from the definitions in [1] and confirmed for every prime $p \equiv 3 \pmod 4$ with $3 \le p \le 127$.

## 8. Verification

Proposition 3.1, Proposition 3.2, Theorem 4.1 and Theorem 5.1 have been machine-checked in Lean 4 [10] against Mathlib [11]. The matrix $A(p)$ is formalised as what it is — a matrix over $\mathbb{Z}$ whose entries are values of Mathlib's `legendreSym` — and the certified statement is $\neg\,(p \mid \det A(p))$ with the divisibility taken in $\mathbb{Z}$, not a statement about a numerical residue; the passage from the integer matrix to the table of residues is the formalised Euler criterion of Proposition 3.1. The development separates the reasoning from the arithmetic: the soundness bridge, the identification of the table with the reduced matrix, and the whole of Theorem 5.1 (both kernel vectors, the failure of the unrestricted statement, and the coexistence at $p = 5$ of $\left(\frac{2\det A}{p}\right) \ne -1$ with $5 \mid \det A$) are checked by the kernel alone, with no appeal to compiled evaluation, their axiom closure being the standard propositional extensionality, quotient soundness and choice. Compiled evaluation enters the proof of Theorem 4.1 in exactly two places, each recorded by its own axiom: the ten pieces into which the 122 certificate checks are split, and the check that the list of window primes is complete — eleven such axioms in all, and nothing else. Proposition 3.2, being three evaluations of the same fixed computation, carries one such axiom for each. There is no `sorry` anywhere in the development, and the computations of §6 are outside it entirely. Repository reference to be added at submission.

## 9. What remains

Conjecture 4.10(ii) is open, and the window of Theorem 4.1 does not suggest a proof; we record what we can say about the shape of the obstruction, and what the natural next computations cost.

*Why the usual technique is unavailable.* Every nonvanishing statement we found in this literature is a corollary of an *exact evaluation*, or of an exact vanishing criterion, for the determinant in question: Vsemirnov's factorisation of Chapman's matrix [7], the evaluation of Li and Wu [6] of the determinant over multiplicative subgroups, the Pfaffian-square factorisation of Chen and Liu [8], whose $a = n!$ case settles Sun's Conjecture 4.1 and which decides exactly when that determinant vanishes, and the work of Li and Yan [9], which reduces the vanishing of such determinants to the supersingular reduction of certain CM elliptic curves. We did not find a standalone technique for proving that a Legendre-symbol determinant is nonzero; read that as "not found". For $A(p)$ the difficulty is visible in (2): modulo $p$ the target is $\left(\frac{2}{p}\right)$ times a perfect square, and a character sum or Gauss-sum estimate that sees only the square class is blind to the distinction between 0 and a nonzero value — which is precisely the content of Theorem 5.1(2).

*The natural target is $C_2$.* By Remark 2.1, the conjecture is equivalent to $p \nmid \det C_2$ on a matrix of side $(p+1)/4$, half the side of $A(p)$ and hence an eighth of the arithmetic in the certificate route. The entries of $C_2$ are binomial coefficients and coefficients of the reductions $r_i(x)$, so $C_2$ is an object of a different kind from $A(p)$: no Legendre symbols appear in it, and it might admit an evaluation of its own. We regard this as the most promising direction, both for an argument and, on the verification side, for enlarging the window: the cost of the present route is $\Theta(p^3)$ per prime, so the same window

carried to $p \le 2000$ would cost about 2.2 CPU-hours against the 0.8 spent on $p \le 1500$, and routing the certificate through $C_2$ instead would divide that by eight. The obstacle to the $C_2$ route is not compute but formalisation: it requires the Vandermonde factorisation and the even/odd permutation of §2 to be proved, not merely recomputed.

*The determinant's value.* The certificate of §3 proves $\det \overline{A(p)} \neq 0$ without ever naming $\det A(p)$. Replacing the inverse by an $LU$ factorisation of a symmetrically permuted $A(p)$ would name it, as the product of the diagonal of $U$, and would therefore certify Conjecture 4.10(ii) in full at each window prime rather than only its open half, at the same cubic cost.

*Further numerical evidence* in the style of §6 is cheap but of decreasing value: extending item (A) from $p < 6000$ to $p < 8000$ costs about 2.2 further CPU-hours, roughly twice what that sweep has already cost, for a 33% larger bound.

## References


[1] B. Jiang and Z.-W. Sun, *Some new results on determinants and permanents*, arXiv:2606.03970v1 [math.NT] (2 June 2026). Cited as an e-print: at the time of writing v1 is the only version and the record carries no journal reference and no DOI beyond the arXiv one. Theorem 1.1, its Remark, and the proof of Theorem 1.1 are used here.

[2] Z.-W. Sun, *Problems and results on determinants involving Legendre symbols*, arXiv:2405.03626v8 [math.NT] (28 July 2024). Conjecture 4.10 is the tenth and last conjecture of §4 of that version, which is why the version is pinned here. The bibliographies of [1] and of [3] both attribute the paper to *Bull. Math. Soc. Sci. Math. Roumanie*, in press; we found no published version on record — the arXiv entry carries neither a journal reference nor a DOI, and zbMATH holds the e-print only — so we cite the e-print.

[3] Y. Yang and Y. Zhang, *Two determinant evaluations in Sun's conjectures involving Legendre symbols*, e-print arXiv:2605.19517 [math.NT]; version v1 was posted on 19 May 2026 and version v3 on 27 May 2026. Corollary 1.3 of v3 is the statement of part (i) of Conjecture 4.10 of [2] used in §1; the record carries no journal reference.

[4] R. Chapman, *Determinants of Legendre symbol matrices*, Acta Arith. **115** (2004), no. 3, 231–244; DOI 10.4064/aa115-3-4.

[5] Z.-W. Sun, *On some determinants with Legendre symbol entries*, Finite Fields Appl. **56** (2019), 285–307; DOI 10.1016/j.ffa.2018.12.004.

[6] J. Li and H.-L. Wu, *A conjecture of Zhi-Wei Sun on matrices concerning multiplicative subgroups of finite fields*, Bull. Aust. Math. Soc. **111** (2025), no. 3, 490–496; DOI 10.1017/S0004972724000765; e-print arXiv:2405.08552.

[7] M. Vsemirnov, *On R. Chapman's "evil determinant": case $p \equiv 1 \pmod 4$*, Acta Arith. **159** (2013), no. 4, 331–344; DOI 10.4064/aa159-4-3; e-print arXiv:1108.4031 (v1, 19 August 2011; v2, 26 March 2012), which itself carries no journal reference.

[8] H.-G. Chen and F. Liu, *A Pfaffian proof and generalization of a conjecture of Sun Zhiwei*, arXiv:2607.01695 [math.NT] (2 July 2026).

[9] G. Li and X. Yan, *On Sun's conjectures for truncated Jacobi-symbol determinants via supersingular elliptic curves*, arXiv:2608.08509 [math.NT] (9 August 2026).

[10] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[11] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.