SUN'S CONJECTURE ON $\det C_p(x)$: THE UNSPECIFIED COEFFICIENT d_p DETERMINED, AND BOTH HALVES VERIFIED FOR EVERY PRIME BELOW 300

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. Let $p > 3$ be a prime, $n = (p-1)/2$, and let $C_p(x) = [x + c_{ij}]_{1 \le i,j \le n}$ be the shifted Legendre-symbol matrix with $c_{1j} = \left(\frac{j}{p}\right)$ and $c_{ij} = \left(\frac{i-j}{p}\right)$ for $i \ge 2$. Ren and Sun, having evaluated the companion matrix with $\left(\frac{i+j}{p}\right)$ in place of $\left(\frac{i-j}{p}\right)$, record a conjecture of the second author on $\det C_p(x)$ and state that their method does not reach it. For $p \equiv 1 \pmod 4$ that conjecture reads $\det C_p(x) = \left(\frac{2}{p}\right)\left(a'_p - \frac{p+1}{2} b'_p\right) + d_p x$ "for some integer d_p", where $\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)} = a'_p + b'_p\sqrt{p}$; no value of d_p is proposed, there and, as far as we could find, anywhere else. We propose one: $d_p = \frac{p+1}{2} a'_p - p\, b'_p$. It carries no factor $\left(\frac{2}{p}\right)$, unlike the constant term, and the variant that does carry one is false already at $p = 13$. We verify the completed conjecture exactly for all 80 primes $p \equiv 1 \pmod 4$ with $p \le 1000$, and for the 29 such primes $p \le 293$ we prove — for all $x \in \mathbb{Z}$ at once — a restatement of it that mentions no class number and no fundamental unit, from which the conjecture with d_p named follows at those primes granting Vsemirnov's evaluation of Chapman's determinant. For $p \equiv 3 \pmod 4$ we prove the corresponding class-number-free statement for the 31 primes $7 \le p \le 283$, and Sun's conjecture follows there granting Wang and Wu's evaluation of the all-ones-row variant; together the two windows cover every prime $5 \le p \le 300$. Those two rewritings are what make the statements elementary enough to be machine-checked; the checking is done in Lean 4 against Mathlib. Outside the formal development we record what we believe to be the first verification range for this conjecture: all 166 primes $5 \le p \le 1000$, no exceptions. We also observe that $\det C_p(0)$ is a single cofactor of Chapman's matrix, hence a product of two Pfaffians when $p \equiv 3 \pmod 4$, and offer that as a route to a proof.

1. INTRODUCTION

1.1. **The matrix.** Let $p > 3$ be a prime, let $\left(\frac{\cdot}{p}\right)$ be the Legendre symbol with $\left(\frac{0}{p}\right) = 0$, and put

$$n = \frac{p-1}{2}, \qquad m = n + 1 = \frac{p+1}{2}.$$

The matrix of this paper is

$$C_p(x) = \big[x + c_{ij}\big]_{1 \le i,j \le n}, \qquad c_{ij} = \begin{cases} \left(\frac{j}{p}\right), & i = 1, \\ \left(\frac{i-j}{p}\right), & i \ge 2, \end{cases}$$

an $n \times n$ matrix over $\mathbb{Z}[x]$ whose entries are x plus a Legendre symbol. It is a member of a family of determinants going back to Chapman [3]: the matrix

$$V_p = \Big[\left(\frac{i-j}{p}\right)\Big]_{0 \le i,j \le n},$$

of side m, is Chapman's "evil determinant", and $C_p(0)$ is built from the same symbols with the index range shifted by one and the first row replaced by $\left(\left(\frac{1}{p}\right), \ldots, \left(\frac{n}{p}\right)\right)$. Adding x to every entry means adding xJ with J the all-ones matrix, so $\det C_p(x)$ is a polynomial in x of degree at most one; which is why the conjecture below has exactly two coefficients to name.

1.2. **The source, and the two things it leaves open.** Ren and Sun [1] evaluate the matrix $A_p(x) = [x + a_{ij}]_{1\le i,j\le n}$ with $a_{1j} = \left(\frac{j}{p}\right)$ and $a_{ij} = \left(\frac{i+j}{p}\right)$ for $i \ge 2$ — the same shape with $i + j$ in place of $i - j$ — completely, in both residue classes. Immediately after that theorem they write, verbatim:

> However, our method to prove Theorem 1.1 does not work for the following conjecture made by the second author.

and then state, with ε_p the fundamental unit of $\mathbb{Q}(\sqrt{p})$, $h(p)$ the class number of $\mathbb{Q}(\sqrt{p})$ and $h(-p)$ that of $\mathbb{Q}(\sqrt{-p})$:

> **Conjecture 1.1 (Sun, 2024)** [1]**.** Let $p > 3$ be a prime and let $C_p(x) = [x + c_{ij}]_{1\le i,j\le (p-1)/2}$, where $c_{ij} = \left(\frac{j}{p}\right)$ if $i = 1$ and $c_{ij} = \left(\frac{i-j}{p}\right)$ if $i > 1$. If $p \equiv 1 \pmod 4$, then
>
> $$\det C_p(x) = \left(\frac{2}{p}\right)\left(a'_p - \frac{p+1}{2}b'_p\right) + d_p x$$
>
> for some integer d_p, where we write $\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)}$ as $a'_p + b'_p\sqrt{p}$ with $a'_p, b'_p \in \mathbb{Q}$. When $p \equiv 3 \pmod 4$, we have
>
> $$\det C_p(x) = (-1)^{(p-3)/4} + \left(2\left(\frac{2}{p}\right)(-1)^{(h(-p)-1)/2} - \frac{p-1}{2}\right)x.$$

Two different things are open in that one display. The whole conjecture is open — its proof is precisely what [1] says their method cannot deliver. And inside the $p \equiv 1 \pmod 4$ half, the coefficient d_p is not even conjectured: the source writes "for some integer d_p" and never returns to it, so the first half of the conjecture, read literally, asserts only that $\det C_p(x)$ is affine in x with a named constant term. Naming d_p is the main contribution of this paper.

We also note that [1] attaches no verification range to the conjecture, and indeed prints no numerical range anywhere: in the whole e-print the word "verify" occurs exactly twice, both times inside a proof and both times about an algebraic identity; the words "check", "compute" and "numerical" do not occur, and no range of primes over which anything was tested is named. Nor does the conjecture appear in Sun's problem list [2], in any of the eight versions of it: every one of them defines a different matrix under the same name $C_p(x)$, namely $\left[x + \left(\frac{j+k-1}{p}\right)\right]$, and none contains a matrix of Legendre symbols with its first row replaced by another vector. So neither the value of d_p nor a range of primes for which the conjecture has been tested is on record. We searched for both; see §8.1.

1.3. **Results.** Write a'_p, b'_p for the two components of $\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)} = a'_p + b'_p\sqrt{p}$ as in the conjecture.

(1) *The coefficient.* We propose $d_p = \frac{p+1}{2}a'_p - p\,b'_p$ (Conjecture 3.2), and prove a class-number-free form of the completed conjecture — constant term and x-coefficient together, for every $x \in \mathbb{Z}$ — for all 29 primes $p \equiv 1 \pmod 4$ with $5 \le p \le 293$ (Theorem 6.1); granting Vsemirnov's theorem, the conjecture with d_p named holds at those primes (Corollary 6.2). The formula carries no factor $\left(\frac{2}{p}\right)$, in contrast with the constant term, and the version that carries one is false at $p = 13$ (Theorem 7.1).

(2) *The other half.* For $p \equiv 3 \pmod 4$ we prove the corresponding class-number-free statement, for every $x \in \mathbb{Z}$, for all 31 primes $7 \le p \le 283$ (Theorem 6.3); granting Wang and Wu's theorem, Sun's conjecture holds at those primes (Corollary 6.4). Together with (1) this covers every prime p with $5 \le p \le 300$: 60 primes, matrices of side up to 147.

(3) *Elementary form.* Both windows are proved in a form in which no class number and no fundamental unit occurs: a'_p is replaced by $-\det V_p$, which is Vsemirnov's theorem [4, 5], b'_p is pinned by $a'^2_p - p\,b'^2_p = -1$, and $(-1)^{(h(-p)-1)/2}$ is replaced by $\det M_p$, which is Wang and Wu's theorem [6], where M_p is V_p with its first row replaced by all ones (§3). Given those two

published evaluations, what we prove is the conjecture's second display as it stands, and its first display with d_p named.

(4) *Structure and controls.* The reduction from a polynomial identity in x to two integer determinants is a rank-one determinant identity (Lemma 4.1), and the exact determinants are certified by triangular products (Proposition 5.1). Four controls show that the hypotheses are load-bearing and that the statements are not vacuous (Theorem 7.1).

(5) *A verification range.* Outside the formal development, an independent exact computation confirms both halves of the conjecture, the proposed d_p, and the three published evaluations it rests on, for every prime $5 \le p \le 1000$ — 166 primes, no exceptions (§8).

(6) *A route.* $\det C_p(0)$ equals $-\left(\frac{-1}{p}\right)$ times a single cofactor of Chapman's matrix V_p; for $p \equiv 3 \pmod 4$ that matrix is skew-symmetric of even order, so the conjecture's constant term is a product of two Pfaffians (§9). This is offered as a route to a proof, not as a result.

The statements of §§4–7 are machine-checked; §10 says exactly which of them rest on exhaustive computation and how large each computation is, and §11 says what the machine checks. The material of §§8–9 is outside the formal development and is labelled as such. A companion manuscript [11] treats a different determinant of Legendre symbols from the same circle of questions; the background common to both is not repeated here.

2. Notation, and the published evaluations

Throughout, $p > 3$ is prime, $n = (p-1)/2$, $m = (p+1)/2$, and J denotes the all-ones matrix of whatever size the context requires. Besides $C_p(x)$ and Chapman's matrix $V_p = \left[\left(\frac{i-j}{p}\right)\right]_{0\le i,j\le n}$ we use

$$M_p = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \left(\frac{1-0}{p}\right) & \left(\frac{1-1}{p}\right) & \cdots & \left(\frac{1-n}{p}\right) \\ \vdots & & & \vdots \\ \left(\frac{n-0}{p}\right) & \left(\frac{n-1}{p}\right) & \cdots & \left(\frac{n-n}{p}\right) \end{bmatrix},$$

that is, V_p with its first row replaced by all ones. Both V_p and M_p have side m. Note $\left(\frac{-1}{p}\right) = (-1)^n$, so V_p is symmetric with zero diagonal when $p \equiv 1 \pmod 4$ and skew-symmetric when $p \equiv 3 \pmod 4$.

Three evaluations from the literature are used, all of them as *inputs*: we do not reprove them, and the machine-checked statements of §§6–7 are so phrased that they do not need them.

Theorem (Vsemirnov [4, 5]). For a prime $p \equiv 1 \pmod 4$, $\det V_p = -a'_p$; for $p \equiv 3 \pmod 4$, $\det V_p = 1$.

Theorem (Wang and Wu [6]). For a prime $p \equiv 1 \pmod 4$, $\det M_p = (-1)^{(p-1)/4}$; for $p \equiv 3 \pmod 4$, $\det M_p = (-1)^{(h(-p)-1)/2}$.

Theorem (Wang, Wu and Ni [7]). For a prime $p \equiv 1 \pmod 4$, $\det(V_p + xJ) = \left(\frac{2}{p}\right) p\, b'_p x - a'_p$; for $p \equiv 3 \pmod 4$, $\det(V_p + xJ) = 1$.

The last of these is Theorem 1.1 of [7], read there and not in quotation. It is stated in [7] for the matrix $\left[x + \left(\frac{j-i}{p}\right)\right]_{0\le i,j\le n}$, which is $V_p^{\mathsf T} + xJ$ and so has the determinant written above. It is used only in §9, as a possible input to a proof.

Finally we record the arithmetic of the pair (a'_p, b'_p) that we shall use. For $p \equiv 1 \pmod 4$ prime, the norm of ε_p is -1 and $h(p)$ is odd, so the exponent $(2 - \left(\frac{2}{p}\right))h(p)$ — an odd number times an odd number — is odd and

$$a'^2_p - p\, b'^2_p = -1. \tag{1}$$

Both facts are classical, and together they are exactly what [5] uses at the corresponding point of its own argument: that $\varepsilon_p^{h(p)}$ is a unit of norm -1, equivalently that $N(\varepsilon_p) = -1$ and $h(p)$ is odd. For

them that paper (v2) refers to [8, Ch. 4, §18.4] and [9, Ch. 5, Sec. 4, Ex. 5], and we take the same route rather than reproving anything. Moreover $\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)} > 1$ has conjugate $-\varepsilon_p^{-(2-\left(\frac{2}{p}\right))h(p)} \in (-1,0)$, so $a'_p > 0$ and $b'_p > 0$. Relation (1) was confirmed for every prime $p \equiv 1 \pmod 4$ with $p \le 1000$ (§8). It matters because it makes b'_p a function of a'_p: for a fixed real a there is exactly one $b > 0$ with $a^2 - pb^2 = -1$, namely $b = \sqrt{(a^2+1)/p}$.

3. The class-number-free form

Sun's conjecture as stated mentions ε_p, $h(p)$ and $h(-p)$. None of the three is available to a formal proof assistant as a computable object, and none of the three is needed: the two published evaluations above remove all of them, at the cost of naming two more determinants. This is the form we shall prove on a window.

Proposition 3.1 (Elementary restatement)**.** *Grant the theorems of Vsemirnov and of Wang and Wu quoted in §2, and let $p > 3$ be a prime.*

(1) *Suppose $p \equiv 3 \pmod 4$. Then the second display of Sun's conjecture holds at p if and only if*

$$\det C_p(x) = (-1)^{(p-3)/4} + \Big(2\left(\frac{2}{p}\right)\det M_p - \frac{p-1}{2}\Big)x \qquad \text{for all } x. \tag{2}$$

(2) *Suppose $p \equiv 1 \pmod 4$ and put $a = -\det V_p$. If b is a positive integer with $a^2 - pb^2 = -1$ and*

$$\det C_p(x) = \left(\frac{2}{p}\right)\Big(a - \frac{p+1}{2}b\Big) + \Big(\frac{p+1}{2}a - p\,b\Big)x \qquad \text{for all } x, \tag{3}$$

then the first display of Sun's conjecture holds at p with $d_p = \frac{p+1}{2}a'_p - p\,b'_p$.

Proof. (1) is Wang and Wu's evaluation $\det M_p = (-1)^{(h(-p)-1)/2}$ substituted into the conjecture's second display; nothing else changes. For (2), Vsemirnov's evaluation gives $a = -\det V_p = a'_p$. By (1) and $b'_p > 0$, b'_p is the unique positive real solution of $a'^2_p - pt^2 = -1$, and b is a positive solution of the same equation with the same a; hence $b = b'_p$. Substituting $a = a'_p$ and $b = b'_p$ in (3) turns its constant term into $\left(\frac{2}{p}\right)(a'_p - \frac{p+1}{2}b'_p)$, which is the conjecture's constant term, and its x-coefficient into $\frac{p+1}{2}a'_p - p\,b'_p$, an integer. □

Conjecture 3.2 (the coefficient d_p)**.** For every prime $p \equiv 1 \pmod 4$, the integer d_p left unspecified in Sun's conjecture is

$$d_p = \frac{p+1}{2}\,a'_p - p\,b'_p.$$

Remark 3.3 (both coefficients from one product). With $m = (p+1)/2$, Conjecture 3.2 and the conjecture's constant term are the two components of a single product in $\mathbb{Q}(\sqrt{p})$:

$$\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)} \cdot \big(m - \sqrt{p}\big) \;=\; d_p - \left(\frac{2}{p}\right)\det C_p(0)\cdot\sqrt{p}.$$

Indeed the left side is $(ma'_p - p\,b'_p) + (mb'_p - a'_p)\sqrt{p}$, and by the conjecture $\left(\frac{2}{p}\right)\det C_p(0) = a'_p - mb'_p$. Taking norms, and using $N(\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)}) = -1$ and $N(m-\sqrt{p}) = m^2 - p = n^2$, gives the coefficient-free identity

$$d_p^2 - p\,\big(\det C_p(0)\big)^2 = -\Big(\frac{p-1}{2}\Big)^2, \tag{4}$$

in which $\left(\frac{2}{p}\right)$ has disappeared. At $p = 13$, for instance, $61^2 - 13\cdot 17^2 = -36 = -6^2$. Identity (4) is a formal consequence of the completed conjecture together with (1); it therefore holds at every prime where those were verified, that is, at all 80 primes $p \equiv 1 \pmod 4$ below 1000 (§8). It is not part of the machine-checked development.

4. The affine structure in x

Since $C_p(x) = C_p(0) + xJ$ and J has rank one, $\det C_p(x)$ is affine in x. We use this in the following explicit form, which names the two coefficients by two values of the determinant and so replaces the polynomial identity by two integer identities. Ren and Sun use the same fact, in the shape of the matrix-determinant lemma $\det(H + uv^{\mathsf{T}}) = \det H + v^{\mathsf{T}} \operatorname{adj}(H)u$ [1, Lemma 2.1].

Lemma 4.1 (affine expansion)**.** *Let $N \geq 0$, let M be an $N \times N$ matrix over $\mathbb{Z}$ and let J be the all-ones $N \times N$ matrix. Then for every $x \in \mathbb{Z}$,*

$$\det(M + xJ) = (1 - x) \det M + x \det(M + J).$$

In particular, for every prime $p > 3$ and every $x \in \mathbb{Z}$,

$$\det C_p(x) = \det C_p(0) + x\big(\det C_p(1) - \det C_p(0)\big).$$

Proof. Subtract the first row from every other row of $M + xJ$: this leaves the determinant unchanged and removes x from all rows but the first, producing the matrix N_0 with first row $M_{0\bullet} + x\mathbf{1}$ and i-th row $M_{i\bullet} - M_{0\bullet}$ for $i \geq 1$. Expanding by linearity in the first row, $\det(M + xJ) = \det N + x \det N'$ where N is N_0 with first row $M_{0\bullet}$ and N' is N_0 with first row $\mathbf{1}$; both are independent of x. Evaluating at $x = 0$ gives $\det N = \det M$ and at $x = 1$ gives $\det N' = \det(M + J) - \det M$. The displayed identity follows, and the statement for C_p is the case $M = C_p(0)$, $N = n$, together with $C_p(x) = C_p(0) + xJ$, which holds entrywise by the definition of C_p. (The case $N = 0$ is the empty determinant, $1 = (1-x)+x$.) □

Lemma 4.1 is elementary and we claim no novelty for it; we state it because everything below is an application of it, and because it is the step that turns each prime into exactly two integer determinants, $\det C_p(0)$ and $\det C_p(1)$.

5. Certified integer determinants

The determinants at stake are exact integers, some of them large: $\det C_{293}(1)$ has six digits, and the leading principal minors met during an elimination reach 43 digits already at $p = 199$. We therefore verify each determinant by a certificate whose correctness needs no assumption about the procedure that produced it.

Proposition 5.1 (certificate soundness)**.** (1) (Legendre table.) *Let $p \geq 5$ be a prime and suppose that for every integer a with $0 \leq a < p$ the residue $r_a = a^{(p-1)/2} \bmod p$ lies in $\{0, 1, p-1\}$. Define $\ell(a) = 0, 1, -1$ according as $r_a = 0$, $r_a = 1$, or otherwise. Then $\ell(a) = \left(\frac{a}{p}\right)$ for all such a.*

(2) (Triangular product.) *Let Y, R, U, M, M' be $N \times N$ integer matrices such that Y is upper triangular with all diagonal entries 1, $YM = M'$, R is lower triangular, U is upper triangular, $RM' = U$, and $\prod_i R_{ii} \neq 0$. If $d \in \mathbb{Z}$ satisfies $\big(\prod_i R_{ii}\big)d = \prod_i U_{ii}$, then $\det M = d$.*

Proof. (1) Euler's criterion gives $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$, and by hypothesis $\ell(a) \equiv r_a \equiv a^{(p-1)/2} \pmod p$ as well, the case $r_a = p - 1$ being $\ell(a) = -1 \equiv p - 1$. So $p \mid \ell(a) - \left(\frac{a}{p}\right)$; both values lie in $\{-1, 0, 1\}$, so the difference has absolute value at most $2 < p$ and is therefore 0. (2) The determinant of a triangular matrix is the product of its diagonal, so $\det Y = 1$ and hence $\det M' = \det Y \det M = \det M$. Multiplicativity applied to $RM' = U$ gives $\big(\prod_i R_{ii}\big) \det M = \prod_i U_{ii} = \big(\prod_i R_{ii}\big)d$, and $\prod_i R_{ii} \neq 0$ cancels in $\mathbb{Z}$. □

Three remarks on how Proposition 5.1 is used. First, part (1) is the only place where the Legendre symbol is interpreted: after it, every matrix in the argument is a table of integers in $\{-1, 0, 1\}$ (or, for $C_p(x)$, in $\{x-1, x, x+1\}$). The hypothesis of part (1) is itself checked, prime by prime, for every $a < p$; nothing about Euler's criterion is assumed beyond the congruence it states. Second, the pair (R, U) in part (2) is produced by an unverified fraction-free (Bareiss) elimination on the augmented matrix $[M' \mid I]$; a wrong output makes one of the hypotheses false and proves nothing, and cannot make a

false conclusion provable. Third, the auxiliary matrix Y is needed for V_p, which has no unpivoted LU factorisation at all: V_p is symmetric or skew-symmetric with zero diagonal, so *every* leading principal minor of odd order vanishes. Taking $Y = I + E$ with E the superdiagonal of ones — determinant 1, entries of YM still bounded by 2 — clears all leading principal minors at every prime of our window, and avoids carrying a permutation sign. For $C_p(x)$ and for M_p the transform is not needed and $Y = I$ is used; M_p carries a row of ones on top, and at no prime of our window did its leading principal minors vanish.

6. The two windows

Theorem 6.1 (Sun's conjecture with d_p determined, $p \equiv 1 \pmod 4$, $p \le 293$)**.** *Let p be one of the 29 primes $p \equiv 1 \pmod 4$ with $5 \le p \le 293$. Put $a = -\det V_p$. Then there is a positive integer b with $a^2 - pb^2 = -1$ such that*

$$\det C_p(x) = \left(\frac{2}{p}\right)\left(a - \frac{p+1}{2}b\right) + \left(\frac{p+1}{2}a - p\,b\right)x \qquad \text{for every } x \in \mathbb{Z}.$$

Corollary 6.2. *Granting Vsemirnov's theorem, Sun's conjecture holds for those 29 primes, with $d_p = \frac{p+1}{2}a'_p - p\,b'_p$ as in Conjecture 3.2.*

Proof. Proposition 3.1(2) applied to Theorem 6.1. □

Theorem 6.3 (Sun's conjecture, $p \equiv 3 \pmod 4$, $p \le 283$)**.** *Let p be one of the 31 primes $p \equiv 3 \pmod 4$ with $7 \le p \le 283$. Then*

$$\det C_p(x) = (-1)^{(p-3)/4} + \left(2\left(\frac{2}{p}\right)\det M_p - \frac{p-1}{2}\right)x \qquad \text{for every } x \in \mathbb{Z}.$$

Corollary 6.4. *Granting Wang and Wu's theorem, Sun's conjecture holds for those 31 primes.*

Proof. Proposition 3.1(1) applied to Theorem 6.3. □

Together the two windows cover every prime p with $5 \le p \le 300$; there are 60 of them, and the largest matrices involved are $C_{293}(x)$ of side 146 and V_{293} of side 147. We stress that Corollaries 6.2 and 6.4 are the only statements here that use the literature: Theorems 6.1 and 6.3 are self-contained assertions about integer determinants, and it is they, not the corollaries, that are machine-checked.

Proof of Theorems 6.1 and 6.3. Fix p in the relevant list. By Lemma 4.1 the assertion for all $x \in \mathbb{Z}$ is equivalent to the two integer identities obtained at $x = 0$ and $x = 1$, namely

$$\det C_p(0) = (\text{constant term}), \qquad \det C_p(1) - \det C_p(0) = (x\text{-coefficient}).$$

So it suffices to know the exact values of $\det C_p(0)$, $\det C_p(1)$ and, according to the residue class, $\det V_p$ or $\det M_p$, together with $\left(\frac{2}{p}\right)$. Each of those determinants is obtained from Proposition 5.1: the Legendre table of p is verified by the criterion of part (1), the matrix is assembled from that table, an unverified fraction-free elimination produces a candidate pair (R, U), and the four hypotheses of part (2) are checked entrywise in integer arithmetic. The symbol $\left(\frac{2}{p}\right)$ is read off the same verified table. With the four integers in hand, the two identities are verified by integer arithmetic; for instance at $p = 13$ they read $17 = \left(\frac{2}{13}\right)(18 - 7 \cdot 5)$ and $78 - 17 = 7 \cdot 18 - 13 \cdot 5$, and at $p = 23$ they read $-1 = (-1)^5$ and $-14 - (-1) = 2 \cdot 1 \cdot (-1) - 11$. This is done once for each of the 60 primes; nothing in the argument is uniform in p. □

The proof is exhaustive computation organised by Lemma 4.1 and Proposition 5.1; §10 states its size. Table 1 lists the data for the first primes of each class.

p	a'_p	b'_p	$\det C_p(0)$	d_p	$\frac{p+1}{2}a'_p - p\,b'_p$
5	2	1	1	1	1
13	18	5	17	61	61
17	4	1	−5	19	19
29	70	13	125	673	673
37	882	145	1873	11393	11393
41	32	5	−73	467	467
53	182	25	493	3589	3589
61	29718	3805	88237	689153	689153

p	$\det M_p$	$\det C_p(0)$	d_p
7	1	−1	−1
11	1	1	−7
19	1	1	−11
23	−1	−1	−13
31	−1	−1	−17
43	1	1	−23
47	1	−1	−21
59	−1	1	−27

TABLE 1. Left: $p \equiv 1 \pmod 4$; $d_p = \det C_p(1) - \det C_p(0)$ is the observed coefficient and the last column is the proposed formula. Right: $p \equiv 3 \pmod 4$; here d_p denotes the x-coefficient, which the conjecture predicts to be $2\left(\frac{2}{p}\right)\det M_p - \frac{p-1}{2}$.

7. Controls

A window theorem is worth only as much as the sharpness of the statement it verifies. We record four checks that the statements above are neither vacuous nor true for a cruder reason.

Theorem 7.1 (controls)**.** (1) (The residue class is load-bearing.) $\det C_{13}(0) = 17 \neq \pm 1$, *so the constant term* $(-1)^{(p-3)/4}$ *of the* $p \equiv 3 \pmod 4$ *half fails at* $p \equiv 1 \pmod 4$.

(2) (The term $2\left(\frac{2}{p}\right)\det M_p$ is needed.) *At* $p = 23$ *the* x*-coefficient of* $\det C_{23}(x)$ *is* -13, *not* $-\frac{p-1}{2} = -11$.

(3) (No factor $\left(\frac{2}{p}\right)$ in d_p.) *At* $p = 13$,

$$\det C_{13}(1) - \det C_{13}(0) = 61 \neq \left(\frac{2}{13}\right)\Big(\frac{13+1}{2}\big(-\det V_{13}\big) - 13\cdot 5\Big) = -61.$$

So the constant term of the conjecture carries $\left(\frac{2}{p}\right)$ *and* d_p *does not: the variant of Conjecture 3.2 with that factor inserted is false.*

(4) (Nothing is constant.) $\det C_{23}(1) = -14 \neq -1 = \det C_{23}(0)$, *so* $\det C_p(x)$ *genuinely depends on* x; *and* $\det M_7 = 1$ *while* $\det M_{71} = -1$, *so replacing* $(-1)^{(h(-p)-1)/2}$ *by* $\det M_p$ *in Theorem 6.3 does not hide a constant sign. Finally the certificate of Proposition 5.1 rejects wrong values: it returns false for the assertions* $\det C_7(0) = 5$, $\det C_{23}(0) = 1$ *and* $\det C_{13}(0) = -17$.

Proof. Each item is a finite evaluation of the determinants named, certified as in §5, followed by an integer comparison; the matrices involved have side at most 36, that being the side of M_{71}. Item (3) uses $\det V_{13} = -18$, $b = 5$ and $\left(\frac{2}{13}\right) = -1$. □

Item (3) is the most informative of the four. The asymmetry it records — a factor $\left(\frac{2}{p}\right)$ on the constant term but not on the x-coefficient — is what makes Conjecture 3.2 a statement one has to find rather than guess: the $\left(\frac{2}{p}\right)$ in the source's display invites the guess that d_p carries it too, and that guess is wrong. In the form of Remark 3.3 the asymmetry becomes natural: it is $\left(\frac{2}{p}\right)\det C_p(0)$, not $\det C_p(0)$, that is a component of a product in $\mathbb{Q}(\sqrt{p})$.

8. Computations outside the formal development

The statements of this section were obtained with exact integer linear algebra in PARI/GP, from the definitions of §1, and are *not* machine-checked.

(A) *The verification range.* For every prime p with $5 \le p \le 1000$ — 166 primes, 80 with $p \equiv 1 \pmod 4$ and 86 with $p \equiv 3 \pmod 4$ — all of the following hold, with no exception: $\det C_p(x)$ is affine in x (tested at $x = 0, 1, 2$); the constant term of Sun's conjecture, in both residue classes; the x-coefficient for $p \equiv 3 \pmod 4$; the formula $d_p = \frac{p+1}{2}a'_p - p\,b'_p$ of Conjecture 3.2 for $p \equiv 1 \pmod 4$; the relation (1); Vsemirnov's evaluation of $\det V_p$ in both classes; and Wang and Wu's evaluation of $\det M_p$ for $p \equiv 3 \pmod 4$, which is the case the rewriting of §3 uses. Here a'_p and b'_p are computed from ε_p and $h(p)$ directly, not from $\det V_p$, so this is an independent check of the class-number-free rewriting of §3 as well. The whole ladder took about 26 minutes of wall time. We did not find a verification range recorded for this conjecture — [1] prints none, and the conjecture is absent from [2] — so we believe this to be the first.

(B) *Reproduction of the framing evaluations.* Before any of the above, the published results that frame the problem were recomputed from their own definitions as a check that we had read them correctly: Ren and Sun's Theorem 1.1, in both residue classes, for every prime $5 \le p \le 200$; Vsemirnov's $\det V_p$ and Wang and Wu's $\det M_p$ for every prime $p \le 1000$; and Wang, Wu and Ni's $\det(V_p + xJ)$ for every prime $p \le 60$. All agree. We record one near-miss: our first implementation of $\varepsilon_p^{(2-\left(\frac{2}{p}\right))h(p)}$ disagreed with Ren and Sun's Theorem 1.1 at every $p \equiv 1 \pmod 4$ while agreeing at every $p \equiv 3 \pmod 4$. The fault was ours — a component of the quadratic unit was being read as 0 — and the published theorem is correct as stated.

8.1. **What we searched.** We report a search, not a conclusion. For the value of d_p: it is not in [1]; it is in none of the eight versions of Sun's problem list [2], which do not contain this conjecture at all; and [1] has, at the time of writing, exactly one citing work on record, [10], which treats a different determinant $\det[x+\chi(i^2-aj)]$, settles a different conjecture of Sun, and cites [1] only in a list of related work. A bibliographic database consulted the same day reports zero citations of [1]. We searched the on-line encyclopedia of integer sequences for the sequence of values $1, 61, 19, 673, 11393, 467, 3589$ of d_p and for the sequence $-1, -7, -11, -13, -17, -23, -21$ of x-coefficients at $p \equiv 3 \pmod 4$, in both cases without result. Read all of this as "not found", not as "new".

We also looked for the 2024 record that the label "Sun, 2024" on the conjecture in [1] presumably points to, and did not find one. The bibliography of [1] contains no 2024 item at all; the conjecture is in none of the eight versions of [2], the natural place for it; and it is in none of Sun's other e-prints of that year on determinants of Legendre symbols that we read (arXiv:2401.14301, 2404.11547, 2407.04642, 2408.07034, 2408.14401, 2409.08213), each of which concerns a different matrix. We therefore cite the conjecture where we found it, as Conjecture 1.1 of [1], and repeat the attribution that [1] makes rather than a source of our own.

9. A structural reduction, and a route to a proof

The following identity is elementary and was verified numerically for all 44 primes $5 \le p \le 200$; it is a paper argument and is not part of the machine-checked development. For a matrix A we write $\mathrm{cof}_{i,j}(A)$ for the (i,j) cofactor, indices starting at 0.

Proposition 9.1. *For every prime $p > 3$, $\det C_p(0) = -\left(\frac{-1}{p}\right)\mathrm{cof}_{1,0}(V_p)$.*

Proof sketch. Row 1 of $C_p(0)$ (in the paper's 1-based indexing, the row $\left(\left(\frac{1}{p}\right), \ldots, \left(\frac{n}{p}\right)\right)$) is $\left(\frac{-1}{p}\right)$ times row 0 of V_p restricted to columns $1, \ldots, n$, since $\left(\frac{0-j}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j}{p}\right)$; and rows $2, \ldots, n$ of $C_p(0)$ are rows $2, \ldots, n$ of V_p restricted to the same columns. So $C_p(0)$ is V_p with row 1 and column 0 deleted, with one row scaled by $\left(\frac{-1}{p}\right)$. Comparing with the definition of the cofactor gives the sign -1. □

Two consequences are worth chasing. First, for $p \equiv 3 \pmod 4$ the matrix V_p is skew-symmetric of even order $m = (p+1)/2$ with $\det V_p = 1$ by Vsemirnov, so $\mathrm{Pf}(V_p) = \pm 1$ and $\mathrm{cof}_{1,0}(V_p) =$

$\pm \operatorname{Pf}(V_p) \operatorname{Pf}(V_p^{\widehat{01}})$, where the second Pfaffian is that of V_p with rows and columns 0 and 1 deleted. The conjecture's constant term $(-1)^{(p-3)/4}$ would then be a Pfaffian sign — exactly the kind of statement proved for a neighbouring family of Legendre-symbol matrices in [10]. Second, Proposition 9.1 and Jacobi's identity together express the cofactors of $C_p(0)$ — whose sum is, by Lemma 4.1, the x-coefficient of $\det C_p(x)$ — through the 2×2 minors of $\operatorname{adj}(V_p)$, a setting in which $\det V_p$ (Vsemirnov), $\det M_p$ (Wang and Wu) and the cofactor sum of V_p (Wang, Wu and Ni) are all known. Whether that route closes — whether the x-coefficient can be written in terms of those three and $\det C_p(0)$ — is a finite question with a definite answer, and we have not settled it. The case $p \equiv 1 \pmod 4$ looks harder in either route: there V_p is symmetric rather than skew, and Vsemirnov's evaluation of $\det V_p$ in that class is the one he settled second, in a separate paper [5] after [4] had done $p \equiv 3 \pmod 4$.

10. The extent of the computation

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

- Lemma 4.1 and Proposition 5.1 rest on no computation. They are uniform in p and in the matrix.
- Theorem 6.1 is exhaustive over the 29 primes $p \equiv 1 \pmod 4$ with $5 \le p \le 293$. For each, three determinants are certified — $\det C_p(0)$, $\det C_p(1)$ of side n, and $\det V_p$ of side $n+1$ — and one Legendre table of length p is verified by Euler's criterion. The dominant cost is the fraction-free elimination and the entrywise product check behind Proposition 5.1(2), $\Theta(n^3)$ integer operations per determinant on integers of several dozen digits.
- Theorem 6.3 is exhaustive over the 31 primes $p \equiv 3 \pmod 4$ with $7 \le p \le 283$, with $\det M_p$ in place of $\det V_p$ and otherwise the same work.
- The two windows together are 60 primes and 180 certified determinants. The primes are handled in four blocks (5–199, 211–241, 251–271, 277–293) of roughly equal cost; the four compiled evaluations that certify them cost 417 seconds of processor time, and the development as a whole, reasoning layer included, about 7.5 minutes.
- Theorem 7.1 is a fixed finite computation at the four primes $7, 13, 23$ and 71: seven certified determinants and three certificate refusals, on matrices of side at most 36.
- §8 is outside the formal development. Item (A) is 166 primes, four determinants each for $p \equiv 1 \pmod 4$ and five for $p \equiv 3 \pmod 4$, about 26 minutes of wall time; item (B) is three further reproductions, over the primes $5 \le p \le 200$, the primes $p \le 1000$ and the primes $p \le 60$ respectively.
- Proposition 9.1 is a paper argument, checked numerically at the 44 primes $5 \le p \le 200$; it is not machine-checked.

Neither window is claimed to be a proof of the conjecture, and the computations of §8 are evidence, not proof. What the windows do settle is that no counterexample to either display, nor to Conjecture 3.2, exists below 300; and the ladder extends that to 1000 modulo the reliability of the computation.

11. Verification

Lemma 4.1, Proposition 5.1, Theorem 6.1, Theorem 6.3 and Theorem 7.1 have been machine-checked in Lean 4 [12] against Mathlib [13]. The matrices are formalised as what they are — matrices over $\mathbb{Z}$ whose entries are values of Mathlib's `legendreSym` — and the certified statements are about `Matrix.det` over $\mathbb{Z}$, quantified over all $x : \mathbb{Z}$, not about numerical residues or about a table of integers; the passage from the integer matrix to the computed table is the formalised Euler criterion of Proposition 5.1(1). The development separates reasoning from arithmetic. The affine expansion, the certificate soundness bridge, the identification of the computed Legendre table with `legendreSym`, and the two per-prime assembly lemmas that turn certified determinant values into the statements of Theorems 6.1 and 6.3 are checked by the kernel alone, their axiom closure being the standard propositional extensionality, quotient soundness and choice. Compiled evaluation enters the two window theorems only through the certificate lists, one axiom per list: three lists (for C_p, for V_p,

for M_p) in each of the four blocks of primes named in §10, so that each per-prime theorem adds exactly the two axioms of the two lists it draws on, and the whole window rests on twelve. This was recounted from the axiom listing of the released development: every per-prime statement we printed carries the three standard axioms and exactly two compiled ones, and all twelve lists are non-empty and used. Theorem 7.1 draws on the same lists, except for its certificate refusals, which are three further compiled evaluations of their own. There is no `sorry` anywhere in the development, and the computations of §§8–9 are outside it entirely. Repository reference to be added at submission.

12. What remains

Sun's conjecture is open in both residue classes, and Conjecture 3.2 is open as well; the windows above do not suggest a proof of either. We close with what the natural next steps cost.

Proving the $p \equiv 3 \pmod 4$ half. The Pfaffian route of §9 is, as far as we know, untried. It needs two things: the sign in $\mathrm{cof}_{1,0}(V_p) = \pm \operatorname{Pf}(V_p) \operatorname{Pf}(V_p^{\widehat{01}})$, which is bookkeeping, and an evaluation of the smaller Pfaffian, which is not. Deciding whether Jacobi's identity reduces the x-coefficient to the constant term is a finite question with a definite answer, and is the concrete next task.

Enlarging the certified window. The per-prime cost of the certificate route grows like $p^{3.5}$ (measured: 0.13, 0.74, 2.73 and 4.57 seconds at $p = 47, 103, 151, 199$), so the cumulative cost to a bound P grows like $P^{4.5}/\log P$. From the 417 seconds spent certifying $p \le 300$: $p \le 500$ would cost about 1.2 processor hours and $p \le 600$ about 2.6; $p \le 700$, at about 5 hours, we did not run. The arithmetic core of the development imports nothing, so compiling it to a shared library is the way past that bound rather than more processor time.

Enlarging the exact ladder. Extending item (A) of §8 from $p \le 1000$ to $p \le 2000$ was priced at about 1.8 processor hours, from a measured 42 seconds for the pair of determinants at $p = 1499$; we did not run it. Its value would be evidential only, and the evidence for Conjecture 3.2 at 166 primes is already strong; the open problem is a proof.

References

[1] C.-K. Ren and Z.-W. Sun, *Evaluation of a determinant involving Legendre symbols*, arXiv:2507.18589 [math.NT], v1, 24 July 2025. 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 Lemma 2.1 (the matrix-determinant lemma, which that paper attributes to R. Vrabel), and Conjecture 1.1, quoted in §1, are used here.

[2] Z.-W. Sun, *Problems and results on determinants involving Legendre symbols*, arXiv:2405.03626 [math.NT]; v1, 6 May 2024 through v8, 28 July 2024. All eight versions were read, because the assertion made about this reference in §1 — that it does not contain the conjecture of [1] — is a statement about particular versions. [1] labels that conjecture "Sun, 2024" but its bibliography contains no 2024 item to which the label could point, and we found no other 2024 record of the conjecture; see §8.1.

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

[4] M. Vsemirnov, *On the evaluation of R. Chapman's "evil determinant"*, Linear Algebra Appl. **436** (2012), no. 11, 4101–4106; DOI 10.1016/j.laa.2011.08.039. This is the paper that settles $p \equiv 3 \pmod 4$.

[5] 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), whose own record carries no journal reference. The section pointers quoted from it in §2 are those of v2.

[6] L.-Y. Wang and H.-L. Wu, *On the cyclotomic field $\mathbb{Q}(e^{2\pi i/p})$ and Zhi-Wei Sun's conjecture on $\det M_p$*, Finite Fields Appl. **101** (2025), Article 102533; DOI 10.1016/j.ffa.2024.102533; e-print arXiv:2401.05853, whose record carries that journal reference.

[7] L.-Y. Wang, H.-L. Wu and H.-X. Ni, *On a generalization of R. Chapman's "evil determinant"*, arXiv:2405.02112 [math.NT], v1, 3 May 2024; the record carries no journal reference. Its Theorem 1.1 is the evaluation quoted in §2.

[8] H. Hasse, *Vorlesungen über Zahlentheorie*, Grundlehren der mathematischen Wissenschaften **59**, Springer, Berlin, 1950.

[9] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Pure and Applied Mathematics **20**, Academic Press, New York, 1966.

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

[11] Korea Superintelligence Labs, *The open half of Sun's Conjecture 4.10(ii): nonvanishing of* $\det\left[\left(\frac{j+k}{p}\right)+\left(\frac{j^2+k^2}{p}\right)\right]$ *for every prime* $p\equiv 3 \pmod 4$ *below* 1500, companion manuscript, 2026.

[12] 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.

[13] 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.