PRINCIPAL MINORS OF FOURIER MATRICES AT SQUARE-FREE ORDER: THE CARAGEA–LEE–MALIKIOSIS–PFANDER LIFTING HYPOTHESIS, DECIDED AT 452 SPLITS

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $F_N = (\omega_N^{ij})_{0\le i,j<N}$ with $\omega_N = e^{-2\pi i/N}$. A conjecture recorded by Caragea, Lee, Malikiosis and Pfander asserts that all principal minors of F_N are non-zero precisely when N is square-free. Their lifting theorem reduces the order $N = pn$, p prime, to a statement in characteristic p about the smaller matrix F_n; the hypothesis of that theorem is the finite condition $p \nmid \mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\big(\det(\zeta_n^{ij})_{i,j\in S}\big)$ for every $S \subseteq \mathbb{Z}/n\mathbb{Z}$. We decide this hypothesis at 452 splits $N = pn$: at the eleven moduli $n \in \{3, 5, 6, 7, 11, 13, 17, 19, 21, 22, 23\}$ for every prime $p \le 59$, and at the three further moduli $n \in \{10, 14, 15\}$ for every prime $p \le 499$. Of these, 384 certify the hypothesis and 68 refute it. Together with the split $(89, 11)$ and three splits certified in the weaker, per-prime-ideal form of the hypothesis, the positive ones settle 368 square-free orders, of which 215 are orders for which we know no published proof; the smallest are 154, 187, 209, 221, 238, 247, 253, 255, 266, 286. Among the consequences: every order $N = pq$ with distinct primes $p, q \le 23$ is settled, which answers a question of Caragea–Lee–Malikiosis–Pfander in that range, the last undecided case being $N = 253 = 11 \cdot 23$; the first of their four published "bad pairs", $(11, 89)$, is not an obstruction at the level of principal minors and settles $N = 979$; and the route settles no square-free order with four prime factors below 870, each such order being either out of reach or explicitly refuted. The certification is carried out entirely over the prime field $\mathbb{F}_p$, by replacing $\mathbb{Z}[\zeta_n]/(p)$ with its regular representation, so that no field extension, primitive root or irreducibility test enters. All statements are machine-checked in Lean 4.

1. Introduction

For $N \ge 1$ let $\omega_N = e^{-2\pi i/N}$ and let

$$F_N = \big(\omega_N^{ij}\big)_{0\le i,j\le N-1}$$

be the Fourier matrix of order N; it is the character table of $\mathbb{Z}/N\mathbb{Z}$. For $S \subseteq \{0, 1, \dots, N-1\}$ we write $F_N[S]$ for the submatrix of F_N on the rows and columns indexed by S; its determinant is the *principal minor* of F_N at S.

When N is prime, a classical theorem of Chebotarëv says that *every* minor of F_N is non-zero. For composite N this fails badly, and the pattern of failure is conjectured to be governed by square-freeness alone.

Conjecture 1.1 ([1, Conjecture 1.2])**.** All principal minors of F_N are non-zero if and only if N is square-free.

The conjecture is attributed in [1] to Caragea and Lee and, independently, to Cabrelli, Molter and Negreira. One direction is elementary: if $p^2 \mid N$, say $N = p^2 m$, then the p indices $0, pm, 2pm, \dots, (p-1)pm$ span a principal submatrix all of whose entries equal 1, so the corresponding principal minor vanishes. We record this as Proposition 2.2 below. The other direction — that square-free N has no vanishing principal minor — is open, and the difficulty is that F_N has 2^N principal minors, so that no order of interest can be attacked by listing them.

1.1. **What is known.** Caragea, Lee, Malikiosis and Pfander [1] prove Conjecture 1.1 for the orders $N = 2p,\ 3p,\ 5p,\ 6p,\ 7p$ with p prime [1, Theorem 1.3], and, for products of larger primes, only under a rapidly growing gap condition: their Theorem 1.5 asks $p_{j+1} > (P_j/2)^{P_j \varphi(P_j)/4}$, where P_j is the product of the primes already used. For two prime factors $N = pq$ the available criteria, going back to Zhang's finite-field form of Chebotarëv's theorem [7] — which we have consulted only through the statement of its Theorem A as quoted in [4, 5] — and refined in [6, 4, 5], all have the shape *"q generates $(\mathbb{Z}/p\mathbb{Z})^*$ and $q > \Gamma_p$"* for a constant Γ_p that is either left unquantified or very large: the smallest prime q for which the literature records that all minors of F_p are non-vanishing in characteristic q is 193 for $p = 11$ and 1619 for $p = 13$ [5, Table 4.1], against 105 863 and 11 709 007 for [1] and 105 871 and 11 709 007 for [7]. That table has columns only for the

bases $p = 2, 3, 5, 7, 11, 13$, so no threshold of this shape is published for a base above 13 at all; and Loukaki records that Γ_r grows at least exponentially in r, with $\Gamma_r \geq 2^{\binom{(r-1)/2}{2}}$, which is 2^{55} at $r = 23$ [6].

Consequently [1] names the smallest orders that its results leave open, one for each number of prime factors: $143 = 11 \cdot 13$ with two factors, $70 = 2 \cdot 5 \cdot 7$ with three, and $210 = 2 \cdot 3 \cdot 5 \cdot 7$ with four. Gu, Zhou and Wang [2] have recently settled the first two of these by computer-assisted proofs. Wang and Zhang [3] have since classified the prime multipliers of the single base 10, proving that F_{10p} has no vanishing principal minor for every prime $p \notin \{2, 5, 11\}$.

1.2. **The lifting hypothesis.** Both [2] and the present paper rest on the induction step of [1].

Theorem 1.2 ([1, Theorem 1.4])**.** *Let $N = pn$ be square-free with p prime. If all principal minors of F_n are non-zero in characteristic p, then every principal minor of F_N is non-zero.*

Section 3.2 of [1] makes "non-zero in characteristic p" precise: a minor $\Delta \in \mathbb{Z}[\zeta_n]$ is zero in characteristic p when it lies in some prime ideal of $\mathbb{Z}[\zeta_n]$ above p, and, the Galois group acting transitively on those primes, this happens if and only if p divides $\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Delta)$. Writing

$$\Delta_S = \det\big(\zeta_n^{ij}\big)_{i,j\in S} \in \mathbb{Z}[\zeta_n], \qquad S \subseteq \mathbb{Z}/n\mathbb{Z}, \tag{1}$$

the hypothesis of Theorem 1.2 is therefore the finite, prime-independent condition

$$\mathbf{(H}_{p,n}\mathbf{)} \qquad p \nmid \mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Delta_S) \quad \text{for every } S \subseteq \mathbb{Z}/n\mathbb{Z}. \tag{2}$$

This is exactly the form in which it is stated in [2, Proposition 2.1], with a citation to [1, Theorem 1.4 and §3.2]. We call a factorisation $N = pn$ with p prime, $p \nmid n$ and N square-free a *split* of N, and we say the split *certifies* N when $(\mathrm{H}_{p,n})$ holds, in which case Theorem 1.2 gives F_N no vanishing principal minor. Section 7 takes up the weaker, per-prime-ideal form $(\mathrm{H}'_{p,n})$ that Theorem 1.2 is literally stated with.

1.3. **Results.** We decide $(\mathrm{H}_{p,n})$ at 452 splits: at the eleven moduli $n = 3$, 5, 6, 7, 11, 13, 17, 19, 21, 22, 23 for every prime $p \leq 59$ with $p \nmid n$, and at $n = 10$, 14, 15 for every prime $p \leq 499$ with $p \nmid n$. Of these 384 certify the hypothesis and 68 refute it. Tables 1 and 2 give the complete outcome below 60, in the form of the number

$$\sigma(p, n) = \#\big\{\, S \subseteq \mathbb{Z}/n\mathbb{Z} \;:\; p \mid \mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Delta_S) \,\big\}, \tag{3}$$

so that $(\mathrm{H}_{p,n})$ is the assertion $\sigma(p, n) = 0$.

Together with the split $(89, 11)$ of §6 the certifying splits settle 365 distinct square-free orders, and the per-prime form of §7 adds 310, 377 and 885: 368 orders in all, of which 215 are orders for which we know no published proof. The smallest ten of those are

$$154, \quad 187, \quad 209, \quad 221, \quad 238, \quad 247, \quad 253, \quad 255, \quad 266, \quad 286,$$

and the largest is $7485 = 3 \cdot 5 \cdot 499$. Four consequences deserve to be stated separately.

The order 253, and a classification. Every square-free order $N = pq$ with distinct primes $p, q \leq 23$ is now settled (Theorem 6.2). Caragea, Lee, Malikiosis and Pfander ask, verbatim, "For which pairs of distinct primes (p, q) do we have that $\mathcal{F}_p$ has the q-Chebotarev property or that $\mathcal{F}_q$ has the p-Chebotarev property?"; in the range $p, q \leq 23$ the answer at the level of principal minors is that at least one direction always holds. The last case to fall is $N = 253 = 11 \cdot 23$ (Theorem 6.1), whose only usable split is $(11, 23)$, since the other one is among our refutations. The published frontier for two-prime orders was 143 [2].

A published "bad pair" that is not an obstruction. [1] exhibit four pairs $(p, q) = (11, 89)$, $(13, 53)$, $(17, 953)$, $(19, 457)$ at which the Chebotarëv property — a statement about *all* minors — fails in both directions. Theorem 1.2 needs only *principal* minors, and at the first of the four that weaker hypothesis holds: $\sigma(89, 11) = 0$, so $N = 979 = 11 \cdot 89$ is settled by their own theorem (Theorem 6.3). The other three are genuine obstructions in the tested direction.

Four prime factors. The order 210 is not expensive but impossible for this route: all four of its splits are refuted, by five explicit determinants of size at most 240 (Theorems 7.1 and 7.2). The same holds at every reachable split of the next five four-factor orders, so no square-free order with four prime factors below 870 is settled by this route (Theorem 8.4 and the discussion after it).

The negative splits remain theorems about the lifting method rather than about Conjecture 1.1: a positive value of $\sigma(p, n)$ says that this route cannot decide F_{pn}, and nothing more. We make the distinction concrete

(§8) with eighteen orders that are *known* to have no vanishing principal minor and whose route through some split nevertheless fails.

1.4. **Method.** The usual way to decide $(\mathrm{H}_{p,n})$ reduces modulo one prime ideal above p and works in $\mathbb{F}_{p^k}$ with $k = \mathrm{ord}_n(p)$, which needs an irreducible factor of Φ_n modulo p of degree k, a primitive n-th root of unity inside the resulting field, and a sweep over the Galois conjugates, since the individual primes above p genuinely give different answers. We avoid all three: working with the whole quotient $R = \mathbb{Z}[\zeta_n]/(p) = \mathbb{F}_p[x]/(\Phi_n)$ and its regular representation over $\mathbb{F}_p$ turns $(\mathrm{H}_{p,n})$ into the non-singularity of 2^n explicit matrices over the *prime* field $\mathbb{F}_p$ (§3), and the Φ_n are computed from $x^n - 1$ rather than tabulated. Two reductions cited from [1] then cut the 2^n matrices down to what the moduli $n \le 23$ can afford (§4): the affine group of $\mathbb{Z}/n\mathbb{Z}$, of order $n\varphi(n)$, leaves $\mathrm{N}(\Delta_S)$ unchanged, and complementation $S \mapsto \mathbb{Z}/n\mathbb{Z} \setminus S$ preserves the verdict, so only orbits of subsets of size at most $n/2$ need be visited. The computation is a Lean 4 program, and each value of $\sigma(p,n)$ is a theorem of the Lean kernel rather than the output of an external program; see §10.

2. The Fourier matrix and the lifting hypothesis

Throughout, p denotes a prime and n a positive integer with $p \nmid n$; ζ_n is a primitive n-th root of unity, φ is Euler's function, $\Phi_n \in \mathbb{Z}[x]$ is the n-th cyclotomic polynomial, and $\mathrm{N} = \mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}$. Subsets $S \subseteq \mathbb{Z}/n\mathbb{Z}$ are identified with subsets of $\{0, 1, \dots, n-1\}$ and are always listed in increasing order, which makes Δ_S of (1) well defined; note $\Delta_\emptyset = 1$.

Definition 2.1. For a square-free N and a factorisation $N = pn$ with p prime, the pair (p, n) is a *split* of N. The split *certifies* N if $(\mathrm{H}_{p,n})$ of (2) holds, and *fails* otherwise, i.e. if $\sigma(p,n) > 0$ in the notation of (3).

An order can have several splits, and, as §8 shows, some of them may certify it while others fail.

We begin with the elementary direction of Conjecture 1.1, which explains why only square-free orders are in play. It is the necessity remark following Conjecture 1.2 of [1]; we include the proof because it is two lines and because it is the negative control for everything that follows.

Proposition 2.2. *Let $p \ge 2$ and $m \ge 1$ be integers, and let $\omega \in \mathbb{C}$ satisfy $\omega^{p^2 m} = 1$. Then the $p \times p$ matrix $\big(\omega^{(i\cdot pm)(j\cdot pm)}\big)_{0 \le i,j < p}$ is the all-ones matrix and its determinant is 0. In particular, if $p^2 \mid N$ then the principal minor of F_N at $S = \{0, pm, 2pm, \dots, (p-1)pm\}$, where $N = p^2 m$, vanishes; so no N divisible by a square has all principal minors non-zero.*

Proof. For $0 \le i, j < p$ one has $(i \cdot pm)(j \cdot pm) = (p^2 m) \cdot (ijm)$, so $\omega^{(i\cdot pm)(j\cdot pm)} = (\omega^{p^2 m})^{ijm} = 1$. A square matrix of size at least two with all entries equal has two equal rows, hence determinant 0. □

The smallest instances are $N = 4$ with $S = \{0, 2\}$ and $N = 9$ with $S = \{0, 3, 6\}$.

For the converse direction the only general tool at present is Theorem 1.2, and it is its hypothesis $(\mathrm{H}_{p,n})$ — not Conjecture 1.1, and not the non-vanishing of the minors of F_{pn} — that everything below decides. Keeping the two implications apart is the whole discipline of the subject: if $\sigma(p,n) = 0$ then every principal minor of F_{pn} is non-zero, while if $\sigma(p,n) > 0$ then this route fails at (p,n) and nothing whatsoever follows about F_{pn}.

3. Reduction to prime-field linear algebra

Fix $p \nmid n$ and put

$$R = \mathbb{F}_p[x]/\big(\Phi_n(x)\big) \;\cong\; \mathbb{Z}[\zeta_n]/(p),$$

a free $\mathbb{F}_p$-algebra of rank $d = \varphi(n)$ with basis $1, x, \dots, x^{d-1}$; the isomorphism is the reduction of the $\mathbb{Z}$-basis $1, \zeta_n, \dots, \zeta_n^{d-1}$ of $\mathbb{Z}[\zeta_n]$. Multiplication by x on that basis is the companion matrix $C \in M_d(\mathbb{F}_p)$ of Φ_n, so the class of ζ_n^m acts as C^m. Let

$$\rho\colon M_k(R) \longrightarrow M_{kd}(\mathbb{F}_p)$$

be the block map that replaces each entry of a $k \times k$ matrix over R by its $d \times d$ matrix of multiplication. It is a homomorphism of $\mathbb{F}_p$-algebras.

Lemma 3.1. *For every $M \in M_k(R)$ one has $\det_{\mathbb{F}_p}\big(\rho(M)\big) = \mathrm{N}_{R/\mathbb{F}_p}\big(\det_R M\big)$; and for $\alpha \in \mathbb{Z}[\zeta_n]$ the element $\mathrm{N}_{R/\mathbb{F}_p}(\alpha \bmod p)$ is the reduction modulo p of $\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\alpha)$.*

The lemma is classical — the first identity is the compatibility of the determinant with restriction of scalars along a finite free extension, the second holds because $\mathbb{Z}[\zeta_n]$ is free over $\mathbb{Z}$ on the basis defining ρ — and we use it as a cited result, outside the formal development (§10). It was checked numerically before anything was built on it, at $(7, 10)$, where $R = \mathbb{F}_{7^4}$ is a field and the norm can be computed independently as $\alpha \mapsto \alpha^{(7^4-1)/6}$: forty random subsets, forty agreements.

Proposition 3.2. *Let $S = \{s_1 < \cdots < s_k\} \subseteq \mathbb{Z}/n\mathbb{Z}$ and $d = \varphi(n)$. Then $p \mid \mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(\Delta_S)$ if and only if the $kd \times kd$ matrix over $\mathbb{F}_p$ with $d \times d$ blocks*

$$B_{uv} = C^{\,s_u s_v \bmod n}, \qquad 1 \le u, v \le k,$$

is singular. Consequently $(\mathrm{H}_{p,n})$ holds if and only if all 2^n of these matrices, one for each $S \subseteq \mathbb{Z}/n\mathbb{Z}$, are non-singular.

Proof. The matrix in question is $\rho(M)$ for $M = (\zeta_n^{s_u s_v})_{u,v}$ read in $M_k(R)$, and $\det_R M = \Delta_S \bmod p$. By Lemma 3.1, $\det_{\mathbb{F}_p} \rho(M) = \mathrm{N}_{R/\mathbb{F}_p}(\Delta_S \bmod p) = \mathrm{N}(\Delta_S) \bmod p$, which vanishes exactly when $p \mid \mathrm{N}(\Delta_S)$. □

Three features of this formulation matter for a computation that has to be believed. No extension of $\mathbb{F}_p$ is constructed, so no irreducible factor of $\Phi_n \bmod p$ has to be found — a reducible modulus accepted by a weak irreducibility test yields a ring that passes every superficial check while producing wrong determinants. No primitive n-th root of unity has to be searched for. And the criterion is prime-independent: it sees all the primes of $\mathbb{Z}[\zeta_n]$ above p at once, whereas a computation in a single residue field sees one of them and under-reports. The difference is real, and §7 is about it: at $(p, n) = (11, 10)$ the four primes above 11 individually kill $40, 40, 80, 80$ subsets, whose union has 240 elements — the value $\sigma(11, 10) = 240$ of Theorem 8.1.

4. Two reductions of the search

At $n = 23$ a sweep over all 2^{23} subsets, with matrices of size up to $23\varphi(23) = 506$, is about $5 \cdot 10^{13}$ field operations, out of reach. Two propositions of [1], neither of them proved here, cut that by three orders of magnitude.

The first is affine invariance [1, Proposition 3.7]: for $n \ge 3$, every map $\psi(x) = ax + b$ with $a \in (\mathbb{Z}/n\mathbb{Z})^*$ satisfies $\mathrm{N}(D_{K,L}) = \mathrm{N}(D_{\psi(K),L}) = \mathrm{N}(D_{K,\psi(L)})$ for minors $D_{K,L}$ of F_n with $|K| = |L|$. Applying it to rows and then to columns gives $\mathrm{N}(\Delta_{\psi(S)}) = \mathrm{N}(\Delta_S)$, so "$p \mid \mathrm{N}(\Delta_S)$" is constant on the orbits of the affine group A_n, of order $n\varphi(n)$, and one representative decides a whole orbit.

The second is complementation [1, Proposition 3.3]: for a unitary A and $|K| = |L|$, $A[K, L]$ is invertible if and only if $A[K^c, L^c]$ is, and the remark following that proposition transfers the equivalence to a cyclotomic field reduced modulo a prime above q, provided $\det A$ is non-zero in characteristic q. For $A = F_n$ one has $|\det F_n|^2 = n^n$, so the proviso is exactly $p \nmid n$, our standing hypothesis; running over all primes above p gives $p \mid \mathrm{N}(\Delta_S)$ if and only if $p \mid \mathrm{N}(\Delta_{\mathbb{Z}/n\mathbb{Z}\setminus S})$. Complementation commutes with every affine map, so the affine orbit of S^c is the set of complements of the orbit of S and has the same size; of each such pair only the member of smaller cardinality need be visited, its two orbit sizes credited together. The saving exceeds a factor 2 because the discarded representatives are the large ones: one costs about $(|S|\varphi(n))^3/3$ field operations and every $|S| > n/2$ disappears. Both proposition numbers are those of v3 of [1]; earlier versions of that preprint number them differently.

Proposition 4.1. *The two reductions are implemented and validated as follows.*

1. *The affine-orbit sweep agrees with the exhaustive sweep of Proposition 3.2 on the exact value of $\sigma(p, n)$ — not merely on whether it vanishes — at 73 splits: $n \in \{6, 10, 11, 14\}$ at every prime $p \le 59$ with $p \nmid n$, $n = 13$ at every prime $p \le 29$, and the three cells $(61, 15)$, $(151, 15)$, $(199, 15)$. Sixteen of those splits are failures, with counts including 1196, 2352, 1260, 3840 and 1680; at three further failing splits, $(7, 15)$, $(11, 15)$ and $(2, 15)$, the affine-orbit sweep returns 30, 1080 and 3120, the values the exhaustive sweep gives there.*
2. *The complement-folded sweep, whose orbit representatives are recognised by a local test rather than by a 2^n-bit table of visited masks, agrees with the exhaustive sweep on the exact value of $\sigma(p, n)$ at 74 splits — $n \in \{6, 10, 11, 14\}$ at every prime $p \le 59$ with $p \nmid n$ and $n = 13$ at every prime $p \le 43$ — and at the three further cells $(7, 15)$, $(11, 15)$, $(17, 15)$. It reproduces the affine-orbit sweep at $(17, 21)$ and returns the four values $\sigma(2, 21) = 112\,840$, $\sigma(17, 21) = 0$, $\sigma(3, 22) = 38\,654$, $\sigma(31, 22) = 0$ that the affine engine had produced.*

(3) *Every sweep reports, besides $\sigma(p,n)$, the number of subsets its visited orbits accounted for, and every theorem below pins that number to 2^n; an incomplete enumeration cannot report a zero. At $n = 23$ the 8 388 608 subsets fall into 16 770 affine orbits, of which the fold visits 8385; the affine group of $\mathbb{Z}/n\mathbb{Z}$ is checked to have $n\varphi(n)$ elements, each a permutation of $\mathbb{Z}/n\mathbb{Z}$, at $n = 15, 21, 22, 23$; and splitting the mask range into eight pieces and adding the results reproduces the undivided sweep at $(7,15)$, $(17,15)$ and $(17,21)$.*

(4) *The hypothesis $p \nmid n$ of the complement fold is load-bearing. Violating it deliberately, the affine reduction — whose justifying proposition carries no such hypothesis — still returns the exhaustive count while the fold returns a strictly smaller one: at $(5,10)$, $(2,14)$, $(3,6)$, $(2,6)$ the exhaustive and affine values are 988, 14 533, 48, 37 and the folded ones are 952, 12 810, 32, 18.*

The measured effect at $(p,n) = (11,23)$: the exhaustive sweep is about $5.1\cdot10^{13}$ field operations (modelled, never run), the affine-orbit sweep $4.96\cdot10^{10}$ and the folded sweep $1.17\cdot10^{10}$ (both measured) — a factor 4.2 on top of the group's 506, and about 4.5 CPU-minutes of compiled evaluation per cell. Because representatives are recognised locally, the working state is a set of byte-sliced image tables of size 6.8 MB at $n = 33$, against the 1 GB a table of visited masks would need there.

TABLE 1. $\sigma(p,n)$ for the six moduli treated in the previous version of this work, at every prime $p \le 59$ with $p \nmid n$. A zero certifies $N = pn$ through Theorem 1.2; a positive entry refutes the lifting hypothesis at that split and says nothing about F_{pn}. A dash marks $p \mid n$, where pn is not square-free.

p	$n=6$	$n=10$	$n=11$	$n=13$	$n=14$	$n=15$
2	—	—	0	0	—	3120
3	—	30	44	1196	140	—
5	0	—	0	156	14	—
7	0	0	0	0	—	30
11	0	240	—	0	0	1080
13	0	0	0	—	210	60
17	0	0	0	0	0	0
19	0	0	0	0	0	720
23	0	0	880	0	0	0
29	0	0	0	104	2352	720
31	0	80	0	0	0	4920
37	0	0	0	0	0	0
41	0	0	0	0	84	480
43	0	0	0	0	1260	0
47	0	0	0	0	0	0
53	0	0	0	1716	0	0
59	0	0	0	0	0	120

Every theorem in §§5–8 is proved by running the search of Proposition 3.2 in the reduced form of Proposition 4.1: enumerate the orbit representatives, build for each the block matrix over $\mathbb{F}_p$, decide non-singularity by Gaussian elimination, and sum the orbit sizes over the failing ones. The arithmetic is exact and there is no probabilistic step. The Φ_n are computed by dividing $x^n - 1$ successively by the Φ_d with $d \mid n$, $d < n$, and the resulting constants are verified rather than assumed (Proposition 9.1).

5. The complete rows

Proposition 5.1. *$\sigma(p,6) = 0$ for every prime p with $5 \le p \le 59$; that is, all fifteen splits $(p,6)$ certify the orders $N = 6p$.*

This row is a reproduction, not a new result: [1, Theorem 1.3] covers $N = 6p$ for all primes p, and its proof proceeds precisely by asserting that all principal minors of F_6 are non-zero in every characteristic $p > 3$. Proposition 5.1 confirms fifteen instances of that assertion, and its role here is as a positive control: a defect in the arithmetic would have to survive fifteen cases whose answer is known in advance.

TABLE 2. $\sigma(p,n)$ at the eight moduli added here, again for every prime $p \le 59$ with $p \nmid n$. The moduli $3,5,7$ are small enough to sweep exhaustively; $17,19,21,22,23$ are the ones the reductions of §4 make affordable.

p	$n=3$	$n=5$	$n=7$	$n=17$	$n=19$	$n=21$	$n=22$	$n=23$
2	0	0	28	748	76	112840	—	12236
3	—	0	0	0	0	—	38654	92
5	0	—	0	0	76	3192	3608	0
7	0	0	—	0	21774	—	0	0
11	0	0	0	0	2166	378	—	0
13	0	0	0	272	0	83454	0	0
17	0	0	0	—	0	0	0	0
19	0	0	0	0	—	168	0	0
23	0	0	0	0	0	0	1562308	—
29	0	0	0	0	0	18900	0	0
31	0	0	0	0	0	84	0	0
37	0	0	0	0	11970	1008	0	0
41	0	0	0	0	0	12222	0	0
43	0	0	0	0	0	499212	19800	0
47	0	0	0	0	0	0	0	3196402
53	0	0	0	0	0	0	0	0
59	0	0	0	0	0	0	0	0

Proposition 5.2. *For $n=10$ the values of $\sigma(p,10)$ at the fifteen primes $p \le 59$ with $p \ne 2,5$ are those of the column $n=10$ of Table 1: zero except at $p=3,11,31$, where they are $30, 240, 80$. At all 78 primes $61 \le p \le 499$ the value is 0, so the orders $610,\dots,4990$ of that range are certified.*

This row is entirely contained in [3, Theorem 1.1], which settles $N=10p$ for every prime $p \notin \{2,5,11\}$; it is kept as an independent exact check of that classification at 93 multipliers, and, at the 78 above 59, as evidence for the computation their theorem rests on, namely that the rational primes dividing $\prod_S |\mathrm{N}(\Delta_S)|$ at $n=10$ are exactly $\{2,3,5,11,31\}$.

Theorem 5.3. *For $n=11$ and the sixteen primes $p \le 59$ with $p \ne 11$, the values of $\sigma(p,11)$ are those of the column $n=11$ of Table 1: zero except at $p=3$ and $p=23$, where they are 44 and 880. In particular the fourteen orders*

$$22,\ 55,\ 77,\ 143,\ 187,\ 209,\ 319,\ 341,\ 407,\ 451,\ 473,\ 517,\ 583,\ 649$$

are certified, and the route fails at $(3,11)$ and $(23,11)$.

Theorem 5.4. *For $n=13$ and the sixteen primes $p \le 59$ with $p \ne 13$, the values of $\sigma(p,13)$ are those of the column $n=13$ of Table 1: zero except at $p=3,5,29,53$, where they are $1196, 156, 104, 1716$. In particular the twelve orders*

$$26,\ 91,\ 143,\ 221,\ 247,\ 299,\ 403,\ 481,\ 533,\ 559,\ 611,\ 767$$

are certified, and the route fails at $(3,13)$, $(5,13)$, $(29,13)$ and $(53,13)$.

Theorem 5.5. *For $n=14$ and the fifteen primes $p \le 59$ with $p \ne 2,7$, the values of $\sigma(p,14)$ are those of the column $n=14$ of Table 1: zero except at $p=3,5,13,29,41,43$. For the 78 primes $61 \le p \le 499$ the value is zero except at $p=71$, 83, 113, 127, 197, 281, 379, 421, 491. The certified orders are the nine $154, 238, 266, 322, 434, 518, 658, 742, 826$ below 60 and 69 further orders $854,\dots,6986$.*

Theorem 5.6. *For $n=15$ and the fifteen primes $p \le 59$ with $p \ne 3,5$, the values of $\sigma(p,15)$ are those of the column $n=15$ of Table 1: zero exactly at $p=17,23,37,43,47,53$. For the 78 primes $61 \le p \le 499$ the value is zero except at $p=61$, 79, 89, 151, 181, 211, 241, 271, 331, 421. The certified orders are the six $255, 345, 555, 645, 705, 795$ below 60 and 68 further orders $1005,\dots,7485$.*

Theorem 5.7. *For $n \in \{17,19,21,22,23\}$ and every prime $p \le 59$ with $p \nmid n$, the values of $\sigma(p,n)$ are those of Table 2. In particular:*

- *$n=17$: 14 of 16 splits certify, the exceptions being $p=2,13$; the certified orders are 51, 85, 119, 187, 323, 391, 493, 527, 629, 697, 731, 799, 901, 1003.*

- $n = 19$*: 11 of* 16 *certify, the exceptions being* $p = 2, 5, 7, 11, 37$*; the certified orders are* 57*,* 247*,* 323*,* 437*,* 551*,* 589*,* 779*,* 817*,* 893*,* 1007*,* 1121*.*
- $n = 21$*: 5 of* 15 *certify, at* $p = 17, 23, 47, 53, 59$*; the certified orders are* 357*,* 483*,* 987*,* 1113*,* 1239*.*
- $n = 22$*: 11 of* 15 *certify, the exceptions being* $p = 3, 5, 23, 43$*; the certified orders are* 154*,* 286*,* 374*,* 418*,* 638*,* 682*,* 814*,* 902*,* 1034*,* 1166*,* 1298*.*
- $n = 23$*: 13 of* 16 *certify, the exceptions being* $p = 2, 3, 47$*; the certified orders are* 115*,* 161*,* 253*,* 299*,* 391*,* 437*,* 667*,* 713*,* 851*,* 943*,* 989*,* 1219*,* 1357*.*

Proposition 5.8. *For* $n \in \{3, 5\}$ *and every prime* $p \le 59$ *with* $p \ne n$ *one has* $\sigma(p, n) = 0$*; for* $n = 7$ *the only non-zero value at such a prime is* $\sigma(2, 7) = 28$*; for* $n = 11$ *the only non-zero values are* $\sigma(3, 11) = 44$ *and* $\sigma(23, 11) = 880$*.*

Proposition 5.8 settles how much of the failure at a composite modulus is inherited from its divisors. If $m \mid n$ with n square-free and the route fails at (p, m), then it fails at (p, n): the image of a bad $S \subseteq \mathbb{Z}/m\mathbb{Z}$ under $x \mapsto (n/m)x$ is bad in $\mathbb{Z}/n\mathbb{Z}$, since $\zeta_n^{(n/m)^2 ij} = (\zeta_m^{n/m})^{ij}$ is a Galois conjugate of ζ_m^{ij} and $\mathrm{N}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = \big(\mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}\big)^{\varphi(n)/\varphi(m)}$. This predicts the failures at $(2, 21)$ and $(3, 22)$ from $(2, 7)$ and $(3, 11)$, and, by Proposition 5.8, nothing else below $p = 60$: of the ten failures in the row $n = 21$ exactly one is inherited and nine are new at the composite modulus, and of the four in the row $n = 22$ two are inherited and two are new.

Proof of Propositions 5.1, 5.2, 5.8 and Theorems 5.3–5.7. Each statement is one row of exhaustive searches in the sense of Propositions 3.2 and 4.1: for the modulus n and each admissible prime p in the stated range the orbit representatives are enumerated, the block matrix over $\mathbb{F}_p$ is formed, and the orbit sizes of the singular ones are summed; each row also asserts that the visited orbits accounted for all 2^n subsets. The rows at $n \in \{6, 10, 11, 13, 14, 15\}$ with $p \le 59$ and at $n \in \{3, 5, 7, 11\}$ are run in the unreduced form as well. The largest matrices have size $\lfloor n/2 \rfloor \varphi(n) = 242$ at $n = 23$; the most expensive single cell is a base-23 one, at about 4.5 CPU-minutes and $1.17 \cdot 10^{10}$ field operations. □

Adding the 92 splits of Table 1, the 234 splits with $61 \le p \le 499$ at $n \in \{10, 14, 15\}$, the 78 splits of Table 2 at $n \in \{17, 19, 21, 22, 23\}$, and the 48 splits at $n = 3, 5, 7$ of Proposition 5.8 — whose row $n = 11$ is already in Table 1 — gives 452 splits in all, of which 384 certify and 68 refute.

6. Orders settled here for the first time

6.1. The order 253, and the two-prime classification.

Theorem 6.1. $\sigma(11, 23) = 0$*: every principal minor of* F_{23} *is non-zero in characteristic* 11*. Hence* $N = 253 = 11 \cdot 23$ *has no vanishing principal minor.*

Proof. One complement-folded sweep at $(11, 23)$, in the sense of Proposition 4.1: the visited orbits account for all $2^{23} = 8\,388\,608$ subsets of $\mathbb{Z}/23\mathbb{Z}$ and none of them is singular; the matrices have size at most $11\varphi(23) = 242$ over $\mathbb{F}_{11}$. □

The order 253 has exactly two splits, and the other one, $(23, 11)$, is one of our refutations: $\sigma(23, 11) = 880$ by Theorem 5.3. So $(11, 23)$ is the only route to 253 through Theorem 1.2, and it needs the modulus 23. No published result reaches the order: $253/11 = 23$ and $253/23 = 11$ are primes above 7, so [1, Theorem 1.3] misses it; the gap condition of [1, Theorem 1.5] asks with $P_1 = 11$ for a second prime above $5.5^{27.5} \approx 2 \cdot 10^{20}$; [2] closes exactly 70 and 143 and [3] is about $10p$; and of the two directions in which a two-prime criterion could apply, $(23, 11)$ fails the generating hypothesis outright ($23 \equiv 1 \bmod 11$ has order 1) while $(11, 23)$ satisfies it — 11 is a primitive root modulo 23 — and fails the threshold, no threshold being published at base 23 and Loukaki's bound giving $\Gamma_{23} \ge 2^{55}$.

Theorem 6.2. *Let* $3 \le p < q \le 23$ *be primes. Then* $\sigma(p, q) = 0$ *or* $\sigma(q, p) = 0$*; in every one of these* 28 *cases* $N = pq$ *has no vanishing principal minor. Exactly nine of the orders are certified by only one of the two splits, namely*

$$33, \quad 39, \quad 65, \quad 69, \quad 95, \quad 133, \quad 209, \quad 221, \quad 253.$$

Proof. Every one of the 56 values $\sigma(p,q)$, $\sigma(q,p)$ is an entry of Table 1, Table 2 or Proposition 5.8; the rows at the moduli $3,5,7,11,13$ restricted to $p \le 23$ are also run as a separate computation, which reproduces the entries $\sigma(3,11)=44$, $\sigma(23,11)=880$, $\sigma(3,13)=1196$ and $\sigma(5,13)=156$ of Theorems 5.3 and 5.4 through the folded enumeration. Inspection of the 28 pairs gives the assertion, the nine listed orders being those with exactly one zero. □

The eight remaining orders pq with $p,q \le 23$ distinct primes are the $2q$, instances of [1, Theorem 1.3]; so all 36 such orders are settled. Theorem 6.2 answers, for $p,q \le 23$, the question of [1, §5] quoted in §1 — with the proviso that their question is about *all* minors while our data are about principal ones, the weaker property and the one Theorem 1.2 consumes. On that reading no pair of primes ≤ 23 is bad in both directions.

6.2. **A published bad pair that is not an obstruction.**

Theorem 6.3. *For the four pairs* $(p,q) = (11,89),\ (13,53),\ (17,953),\ (19,457)$ *of* [1, §5] *one has*

$$\sigma(89,11)=0, \qquad \sigma(53,13)=1716, \qquad \sigma(953,17)=1632, \qquad \sigma(457,19)=27\,360.$$

In particular $N = 979 = 11\cdot 89$ *has no vanishing principal minor.*

Proof. Four complement-folded sweeps, over 2^{11}, 2^{13}, 2^{17} and 2^{19} subsets, with matrices of size at most $\lfloor n/2 \rfloor \varphi(n)$ over $\mathbb{F}_q$; each asserts that the visited orbits accounted for all 2^n masks. The value $\sigma(53,13)=1716$ reproduces the entry of Theorem 5.4. □

[1] obtain these four pairs from four explicit norms of *non-principal* minors — $\mathrm{N}(1+\omega_{11}+\omega_{11}^2+\omega_{11}^5)=89$ and its three analogues — and offer them as pairs at which the Chebotarëv property fails in both directions. Theorem 6.3 says the first of the four is not an obstruction to Conjecture 1.1: F_{11} does lose the 89-Chebotarëv property, but all 2^{11} of its principal minors survive in characteristic 89, which is all Theorem 1.2 asks. The order 979 is not reached by any published result: both cofactors are primes above 7, and $89 \equiv 1 \pmod{11}$ has order 1 in $(\mathbb{Z}/11\mathbb{Z})^*$, so the generating hypothesis of every two-prime criterion fails before any threshold is consulted, and the threshold 193 of [5] at base 11 would exclude 89 in any case. Independently, $\sigma(q,11)$ was recomputed for $q \in \{23,67,89,199,331\}$ by ordinary determinants over $\mathbb{F}_q$ — legitimate because $q \equiv 1 \pmod{11}$ puts a primitive 11-th root of unity in $\mathbb{F}_q$ — with no cyclotomic polynomial, companion matrix or regular representation anywhere, and the counts agree prime ideal by prime ideal. That check is not part of the formal development.

6.3. **Three prime factors, and the moduli 21 and 22.**

Theorem 6.4. $(\mathrm{H}_{p,n})$ *holds at the six splits*

$$(13,10), \quad (17,10), \quad (19,10), \quad (11,14), \quad (17,14), \quad (17,15),$$

so that every principal minor of F_N *is non-zero for* $N = 130,\ 170,\ 190,\ 154,\ 238,\ 255$.

Each of the six orders has three prime factors: $130 = 2\cdot 5\cdot 13$, $170 = 2\cdot 5\cdot 17$, $190 = 2\cdot 5\cdot 19$, $154 = 2\cdot 7\cdot 11$, $238 = 2\cdot 7\cdot 17$, $255 = 3\cdot 5\cdot 17$. None is of the shape $2p, 3p, 5p, 6p, 7p$, so [1, Theorem 1.3] does not reach them, and the criteria of [7, 6, 4, 5] are statements about orders with two prime factors. Three of the six, however, are of the form $10p$ and are covered by [3, Theorem 1.1], which appeared after the previous version of this paper; the three that are not are 154, 238 and 255.

Theorem 6.5. $\sigma(17,21)=0$ *and* $\sigma(31,22)=0$, *so* $N = 357 = 3\cdot 7\cdot 17$ *and* $N = 682 = 2\cdot 11\cdot 31$ *have no vanishing principal minor. The same two moduli are not vacuous:* $\sigma(2,21)=112\,840$ *and* $\sigma(3,22)=38\,654$.

Both orders have three prime factors, so no two-prime criterion applies; and $357/3 = 119$, $357/7 = 51$, $682/2 = 341$ are composite, so [1, Theorem 1.3] does not reach them either. The same applies to the orders $483, 987, 1113, 1239$ and $286, 374, 418, 638, 814, 902, 1034, 1166, 1298$ of Theorem 5.7, all $3\cdot 7\cdot p$ or $2\cdot 11\cdot p$ with composite cofactors.

6.4. **Two prime factors below every published threshold.**

Theorem 6.6. ($\mathrm{H}_{p,n}$) *holds at the four splits* $(17,11)$, $(19,11)$, $(17,13)$, $(19,13)$, *so that every principal minor of* F_N *is non-zero for* $N = 187 = 11\cdot 17$, $209 = 11\cdot 19$, $221 = 13\cdot 17$, $247 = 13\cdot 19$.

Remark 6.7. These four orders, and the two-prime orders of Theorems 5.3, 5.4, 5.7 and 6.1, are the ones for which the published two-prime criteria have to be checked explicitly. Those criteria require the characteristic to exceed a threshold: the smallest prime q for which [5] records that all minors of F_p are non-vanishing in characteristic q is 193 for $p = 11$ and 1619 for $p = 13$, and the corresponding values from [1] and [7] are larger by two or three orders of magnitude, while their table has no column for a base above 13. Every characteristic occurring in our two-prime orders is at most 59, except the 89 of Theorem 6.3. Moreover $221 = 13\cdot 17$ fails the generation hypothesis in both directions, since $\mathrm{ord}_{13}(17) = 6 \neq 12$ and $\mathrm{ord}_{17}(13) = 4 \neq 16$, so it lies outside [4, Corollary 1] whatever the constant there. One caveat: those thresholds are for *all* minors of F_p in characteristic q, a stronger property than the non-vanishing of the *principal* minors Theorem 1.2 needs, so a weaker result specific to principal minors would not appear in that table. We have not found one.

6.5. **A second route to the order 143.**

Theorem 6.8. ($\mathrm{H}_{11,13}$) *holds: every principal minor of* F_{13} *is non-zero in characteristic* 11. *Hence the split* $(11,13)$ *certifies* $N = 143$.

The order $143 = 11\cdot 13$ was settled in [2] through the split $(13,11)$; Theorem 6.8 uses the other split, which does not appear there, so the two computations share neither the modulus nor the characteristic. The same happens at $299 = 13\cdot 23$, certified by $(23,13)$ in Theorem 5.4 and by $(13,23)$ in Theorem 5.7, and at 323, 391, 437, each certified by both of its splits.

7. The per-prime hypothesis, and the order 210

Fix $N = pn$ square-free with $p \nmid n$, so that p is unramified in $\mathbb{Z}[\zeta_n]$ and $p\mathbb{Z}[\zeta_n] = Q_1\cdots Q_r$ with $r = \varphi(n)/f$, $f = \mathrm{ord}_n(p)$. Beside ($\mathrm{H}_{p,n}$) of (2), which says $\Delta_S \notin Q_j$ for *every* j and every S, stands the weaker

$$(\mathbf{H}'_{p,n}) \qquad \text{there is some } j \text{ with } \Delta_S \notin Q_j \text{ for every } S \subseteq \mathbb{Z}/n\mathbb{Z}. \tag{4}$$

($\mathrm{H}_{p,n}$) $\Rightarrow$ ($\mathrm{H}'_{p,n}$), and the converse fails. Which of the two is the hypothesis of Theorem 1.2 is a genuine question about [1]: their §3.2 defines the Fourier matrix in characteristic p by reducing modulo $Q = Q_j$ "with any $1 \le j \le r$", which is (H′), while the last step of their printed proof takes norms and consumes (H). The gap is now closed in the literature: [3] state the distinction — "a rational norm … forgets which local chart is bad" — and prove a selective lifting lemma [3, Lemma 4.1] from which the bridge under (H′) follows. We use that bridge as a citation, exactly as we use Theorem 1.2 itself.

(H′) is decided here without any field extension either. $\Phi_n \bmod p$ is square-free, so $R = \mathbb{F}_p[x]/(\Phi_n)$ is a product of r fields, one per Q_j; the $\mathbb{F}_p$-null space of the block matrix $\rho(M_S)$ of Proposition 3.2 is the R-module $\ker M_S$, and $\Delta_S \notin Q_j$ exactly when the corresponding irreducible factor of $\Phi_n \bmod p$ divides every coordinate of every null-space vector. The greatest common divisor of $\Phi_n \bmod p$ with all those coordinates, over all S, is therefore a polynomial — the *survivor* — whose irreducible factors are exactly the primes above p at which no principal minor of F_n vanishes, and ($\mathrm{H}'_{p,n}$) holds precisely when it has positive degree. No irreducible factor is ever computed and no primitive root is searched for.

Theorem 7.1. *The order* $210 = 2\cdot 3\cdot 5\cdot 7$ *has exactly four splits, namely* $(2,105)$, $(3,70)$, $(5,42)$ *and* $(7,30)$, *and* ($\mathrm{H}_{p,n}$) *fails at every one of them, with witnesses*

$$(7,30):\{0,2,6,18,22,24\},\qquad (5,42):\{0,6,18,24,30,33,36\},$$
$$(3,70):\{0,14,21,63\},\qquad (2,105):\{0,21,77,91\} \text{ and } \{0,21,49,63,91\}.$$

Theorem 7.2. ($\mathrm{H}'_{p,n}$) *fails at all four splits of* 210 *as well: the witnesses of Theorem 7.1 lie in every prime of* $\mathbb{Z}[\zeta_n]$ *above* p. *At* $(2,105)$ *one witness does not suffice — each of the two leaves a survivor of degree* 24, *that is, two of the four primes above* 2 *— and the two together leave none.*

Proof of Theorems 7.1 and 7.2. The list of splits is a finite check on the divisors of 210. Each witness is a single determinant of the form of Proposition 3.2, of size 48, 84, 96, 192 and 240 respectively; each is verified to be singular, which is (H) refuted, and the greatest common divisor of $\Phi_n \bmod p$ with the null-space coordinates is verified to be constant, which is (H′) refuted. As a control, at each of the four splits the initial

segment of $\mathbb{Z}/n\mathbb{Z}$ of the same size as the witness gives a non-singular matrix, so the checker is not one that reports singularity indiscriminately. □

So the difficulty of 210 was misplaced: not that a sweep over 2^{30} subsets of $\mathbb{Z}/30\mathbb{Z}$ is expensive — although it is, at about 3.2 CPU-hours per cell — but that its answer is negative, and five determinants of size at most 240 say so. This says nothing about F_{210}: Conjecture 1.1 there remains open, and what closes is this route to it. The tower of [1, Theorem 1.5] adjoins primes in increasing order, so its last step at 210 would be the split $(7, 30)$, one of the four.

Theorem 7.3. ($\mathrm{H}'_{p,n}$) *holds at* $(29, 13)$ *and at* $(59, 15)$*, where* ($\mathrm{H}_{p,n}$) *fails: the survivor has degree* 6 *at* $(29, 13)$ *and degree* 4 *at* $(59, 15)$*, so in each case two of the four primes above* p *carry no vanishing principal minor, while* $\sigma(29, 13) = 104$ *and* $\sigma(59, 15) = 120$*. Consequently* $N = 377 = 13 \cdot 29$ *and* $N = 885 = 3 \cdot 5 \cdot 59$ *have no vanishing principal minor.*

Neither order is reached by a published result: 377 has $\mathrm{ord}_{13}(29) = 3 \neq 12$, failing the generating hypothesis of [4, Corollary 1] in that direction, and 29 is far below the threshold 1619 of [5] in the other; 885 has three prime factors, and the classification of [3] is for the single base 10.

Proposition 7.4. ($\mathrm{H}'_{31,10}$) *holds:* $\sigma(31, 10) = 80$ *and the survivor at* $(31, 10)$ *is* $x^2 + 18x + 1$ *over* $\mathbb{F}_{31}$*, of degree* 2*, so two of the four primes above* 31 *are clean and* $N = 310 = 2 \cdot 5 \cdot 31$ *has no vanishing principal minor.*

This order is not new: it is [3, Proposition 6.1]. The agreement is exact on both sides — their count of "exactly 80 subsets" is our $\sigma(31, 10) = 80$, and the two charts they name as safe, "the roots 15 and 29", are precisely the two roots of $x^2 + 18x + 1$ over $\mathbb{F}_{31}$, since $15^2 + 18 \cdot 15 + 1 = 16 \cdot 31$ and $29^2 + 18 \cdot 29 + 1 = 44 \cdot 31$.

Proposition 7.5. (H) *and* (H′) *differ in both directions, and neither is vacuous. At the six splits* $(7, 15)$*,* $(3, 10)$*,* $(5, 14)$*,* $(11, 10)$*,* $(2, 15)$*,* $(23, 11)$ *the norm hypothesis fails and the survivor collapses to a constant, so* (H′) *fails too. At the three splits* $(17, 15)$*,* $(7, 10)$*,* $(13, 11)$ *the norm hypothesis holds and the survivor is the whole of* $\Phi_n \bmod p$*, of degree* 8*,* 4 *and* 10*.*

8. Where the route fails, and what that does not mean

Sixty-eight of the 452 splits refute ($\mathrm{H}_{p,n}$). Each such refutation is a theorem about the lifting method: it says that this particular route cannot decide the order in question, and it is consistent with the order being perfectly well behaved.

Theorem 8.1. *The lifting hypothesis is false at the five splits below, with the stated number of subsets* $S \subseteq \mathbb{Z}/n\mathbb{Z}$ *whose minor has norm divisible by* p*:*

$$\sigma(7, 15) = 30, \quad \sigma(11, 10) = 240, \quad \sigma(11, 15) = 1080, \quad \sigma(13, 14) = 210, \quad \sigma(13, 15) = 60.$$

In particular the splits $(7, 15)$*,* $(11, 10)$*,* $(11, 15)$*,* $(13, 14)$*,* $(13, 15)$ *of the orders* 105*,* 110*,* 165*,* 182*,* 195 *do not certify those orders.*

Theorem 8.2. *Enumerate the subsets of* $\mathbb{Z}/n\mathbb{Z}$ *by the binary expansion of* $0, 1, \ldots, 2^n - 1$*, the* i*-th bit selecting the element* i*. The first subset in this order whose minor has norm divisible by* p *is*

$$\begin{array}{llll} (p,n) = (7,15): & S = \{0,2,3,6,7,9\}, & (p,n) = (11,10): & S = \{0,1,3\}, \\ (p,n) = (11,15): & S = \{0,1,5\}, & (p,n) = (13,14): & S = \{0,1,3,4\}, \\ (p,n) = (13,15): & S = \{0,2,3,6,9\}. & & \end{array}$$

Theorem 8.3. *At the three failing splits of the modulus* 23 *the first failing orbit representative is*

$$\{0,1,2,3,4,7,13\} \text{ at } p = 2, \qquad \{0,1,2,3,5,7,8,11,12,15,17\} \text{ at } p = 3, \qquad \{0,1,3\} \text{ at } p = 47,$$

its affine orbit and the orbit of its complement together carrying 1012*,* 92 *and* 1012 *subsets. In particular the whole of the failure at* $(3, 23)$*, all* 92 *subsets of it, is a single such orbit pair. Moreover* $\{0, 1, 3\}$ *is, up to the affine group, the* only *three-element witness at* $(47, 23)$*: the* 3*-subsets of* $\mathbb{Z}/23\mathbb{Z}$ *fall into four affine orbits, represented by* $\{0, 1, 2\}$*,* $\{0, 1, 3\}$*,* $\{0, 1, 4\}$*,* $\{0, 1, 5\}$ *and of sizes* 253*,* 506*,* 506*,* 506*, and only the second fails.*

Three elements is the smallest size at which a failure can occur at a prime modulus n: for $|S| = 1$ the minor is a root of unity, and for $S = \{i, j\}$ it is $\zeta^{2ij}(\zeta^{(i-j)^2} - 1)$, whose norm is $\pm\Phi_n(1) = \pm n$. The orbit of $\{0, 1, 2\}$ could not have failed either, being an arithmetic progression and hence a generalised Vandermonde determinant — [1] make the same observation — so the other two orbits are the genuine information.

Theorem 8.4. *The lifting hypothesis fails at* $(11, 30)$, $(13, 30)$, $(17, 30)$, $(19, 30)$ *and* $(23, 30)$, *with witnesses*

$$(11,30) : \{0,1,2,4,8\}, \qquad (13,30) : \{0,2,3,4,5,8,10,11,15\},$$
$$(17,30) : \{0,3,4,6,9\}, \qquad (19,30) : \{0,2,8\},$$
$$(23,30) : \{0,1,2,3,4,6,8,10,11,14,15,16\}.$$

These are the splits of the orders 330, 390, 510, 570, 690.

Proof. Each witness is one evaluation of the folded range sweep on a single mask, which certifies both the subset and the weight its orbit pair carries: $480 = 2 \cdot |A_{30}|$ in four cases and 240 for $\{0, 2, 8\}$, whose stabiliser in A_{30} has order 2. A refutation needs one subset, where a certification would need the whole sweep at about 3.2 CPU-hours a cell. □

Corollary 8.5. *No square-free order with four prime factors below* 870 *is settled by the route of Theorem 1.2.*

Proof. Those orders are 210, 330, 390, 462, 510, 546, 570, 690, 714, 770, 798, 858. The first is refuted at all four of its splits by Theorem 7.1, and each of $330, 390, 510, 570, 690$ has exactly one split whose modulus is smaller than 42, namely the one with modulus 30, which Theorem 8.4 refutes; certifying either of their other splits would require a sweep over at least 2^{66} subsets. The remaining six — $462, 546, 714, 770, 798, 858$ — have no split at all with modulus below 42: their smallest moduli are $42, 42, 42, 70, 42, 66$. So every one of the twelve orders is either refuted or out of computational reach, with no case left in doubt. □

Proposition 8.6. $\sigma(5, 14) = 14$ *and* $\sigma(3, 10) = 30$. *Thus the split* $(5, 14)$ *of* $N = 70$ *fails, although* F_{70} *has no vanishing principal minor by* [2]*; and the split* $(3, 10)$ *of* $N = 30$ *fails, although* F_{30} *has no vanishing principal minor by* [1, Theorem 1.3], $30 = 6 \cdot 5$.

Tables 1 and 2 contain sixteen further instances. Twelve are orders covered by [1, Theorem 1.3] at which some route fails: 14 through $(2, 7)$, 33 through $(3, 11)$, 34 through $(2, 17)$, 38 through $(2, 19)$, 39 through $(3, 13)$, 42 through $(3, 14)$ and again through $(2, 21)$, 46 through $(2, 23)$, 65 through $(5, 13)$, 66 through $(3, 22)$, 69 through $(3, 23)$, 95 through $(5, 19)$ and 133 through $(7, 19)$. One is $310 = 2 \cdot 5 \cdot 31$, settled by [3, Theorem 1.1], whose only split inside our range, $(31, 10)$, refutes (H) — although not (H′), by Proposition 7.4. Three are of a sharper kind, the order being certified by *this paper's* other split: $209 = 11 \cdot 19$ is certified by $(19, 11)$ and refuted at $(11, 19)$, $221 = 13 \cdot 17$ is certified by $(17, 13)$ and refuted at $(13, 17)$, and $253 = 11 \cdot 23$ is certified by $(11, 23)$ and refuted at $(23, 11)$. The order 30 makes the point on its own: of its three splits $(5, 6)$, $(3, 10)$, $(2, 15)$, the first certifies it and the other two fail. The lifting hypothesis is a property of the split, not of the order.

Question 8.7. Which pairs (p, n) satisfy $(\mathrm{H}_{p,n})$? In the range of Tables 1 and 2 the answer depends on neither the size of p nor its class modulo n: at $n = 15$ the prime 43 succeeds while $13 \equiv 43 \pmod{15}$ fails, at $n = 13$ the prime 59 succeeds where the smaller 29 fails, and at $n = 23$ the prime 47 fails between the successes 43 and 53, on 38% of all subsets. Is there an arithmetic criterion?

A criterion would be worth more than the individual orders settled here: by Theorem 1.2 it would convert into a statement about an infinite family of square-free orders, in the direction in which Conjecture 1.1 is open. The observation below records what the data say about the shape of such a criterion. It is empirical, not a theorem: the counts it aggregates — but not the aggregation — are the machine-checked values of §5.

Remark 8.8 (an observation, not a theorem). Let $g = \varphi(n)/\mathrm{ord}_n(p)$ be the number of primes of $\mathbb{Z}[\zeta_n]$ above p. Over the 452 splits decided here the failure rate is monotone in g: it is 4 of 161 for $g = 1$, 16 of 165 for $g = 2$, 4 of 21 for $g = 3$, 13 of 66 for $g = 4$, and 31 of 39 for $g \geq 5$; over all splits it is 68 of 452. Aggregating instead by modulus and over $p \leq 499$, an inert characteristic fails in 4 of 238 cells and a totally split one in 40 of 71; at $n = 15$ every one of the nine primes $p \equiv 1 \pmod{15}$ below 500 fails, while only 3 of the 48 primes with $\mathrm{ord}_{15}(p) = 4$ do. So the variable that matters is not the size of p but its splitting type. The rule is statistical, with counterexamples in both directions ($p = 41$ at $n = 10$ is totally split and the hypothesis holds; $p = 7, 11$ at $n = 26$ are inert and it fails), and the buckets are unequally populated across moduli.

A mechanism is easy to name — $\mathrm{N}(\Delta_S)$ is, modulo p, a product over the g primes above p, so g is the number of independent chances for p to divide it, and for square-free n with two odd prime factors $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic, forcing $g \geq 2$ — but turning it into a theorem is exactly what Question 8.7 asks for. The $n = 26$ counts, and the buckets drawing on moduli beyond those of §5, are auxiliary computations outside the formal development.

9. Controls on the computation

A search that reports "no singular matrix" is only as good as its ability to report the opposite, and the constants it uses are only as good as their derivation. Both are checked, as are the two reductions of §4 (Proposition 4.1).

Proposition 9.1. *$\sigma(2,2) = 1$, and the unique subset of $\mathbb{Z}/2\mathbb{Z}$ counted is $S = \{0,1\}$, for which $\Delta_S = \zeta_2 - 1 = -2$. Moreover $\prod_{d|n} \Phi_d(x) = x^n - 1$ holds for the derived cyclotomic polynomials at every modulus used, $n \in \{6, 10, 11, 13, 14, 15\}$; and, explicitly, $\Phi_{10} = x^4 - x^3 + x^2 - x + 1$ and $\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.*

The first assertion is the non-triviality control: a procedure that always answered "non-singular" would prove every positive result in this paper, and this one does not. The second is the constants control: the product identity, together with $\Phi_1 = x - 1$, determines every Φ_d used.

Proposition 9.2. *$\sigma(5,6) = \sigma(7,6) = \sigma(11,6) = \sigma(13,6) = 0$, certifying $N = 30, 42, 66, 78$, all of which are covered by* [1, Theorem 1.3] *as $N = 6p$.*

The four splits of Proposition 9.2 are run as separate computations, one per order. Many further known-good orders occur inside the rows already reported — $22, 55, 77, 26, 91$ in Table 1, $51, 85, 119$ at $n = 17$, 57 at $n = 19$, $115, 161$ at $n = 23$, and every certified entry of the rows $n = 3, 5, 7$ — all of them instances of [1, Theorem 1.3]. Of the 368 orders settled here, 153 are covered by [1, Theorem 1.3], [2] or [3, Theorem 1.1], and each is a positive control.

Proposition 9.3. *$(\mathrm{H}_{7,10})$ and $(\mathrm{H}_{13,11})$ hold; that is, $\sigma(7,10) = 0$ and $\sigma(13,11) = 0$. These are the two hypotheses through which* [2] *settles $N = 70$ and $N = 143$.*

These two are not new: they are the content of [2], whose authors evaluate 2^{10} determinants in $\mathbb{F}_{7^4}$ and 2^{11} in $\mathbb{F}_{13^{10}}$ after realising primitive roots of unity there. Reproducing them by the route of §3, which constructs no extension field at all, calibrates the method against the two published computations of the kind.

10. Verification

Every statement of this paper has been formally verified in Lean 4 [8] against *Mathlib* [9], and the development contains no `sorry` and no hand-written axiom; the repository is currently private, and a repository reference is to be added at submission. Proposition 2.2 is proved from the definitions and is kernel-checked, depending on no axioms beyond Lean's own `propext`, `Classical.choice` and `Quot.sound`. Everything else is a finite computation — the values $\sigma(p,n)$ of Tables 1 and 2 and of the ranges $61 \leq p \leq 499$, the witnesses of Theorems 8.2, 8.3, 7.1 and 8.4, the survivor polynomials of §7, and the controls of §4 and §9 — and is discharged by compiled evaluation inside the proof assistant, through Lean's `native_decide`, so that each such value is a theorem carrying the corresponding compiled-evaluation axiom rather than the output of an external program; the enumeration procedures, the arithmetic over $\mathbb{F}_p$, the affine group and its orbit sizes, the complement pairing and the derivation of the cyclotomic polynomials are all part of the verified development, and the total is about two and a half CPU-hours (19 CPU-minutes for the exhaustive sweeps of §5, 30 for the per-prime and affine-orbit modules, 99 for the complement-folded rows). Four ingredients are cited and deliberately not formalised: Theorem 1.2 and its per-prime reading, the bridge from $(\mathrm{H}_{p,n})$ or $(\mathrm{H}'_{p,n})$ to a statement about F_{pn}; Lemma 3.1, the bridge to Proposition 3.2; and the two reductions of §4, which is why Proposition 4.1 checks them against the unreduced search on exact counts rather than on zeros. Independently, every value reported here was first obtained by separate implementations written in C — one for the unreduced sweep, one for the orbit and complement enumerations, and one, valid when $p \equiv 1 \pmod{n}$, computing ordinary determinants over $\mathbb{F}_p$ with no cyclotomic polynomial and no regular representation at all — which agree wherever they overlap.

11. Changes in this version

This is the second version of this work. The first decided ($H_{p,n}$) at the 92 splits with $n = 6$, 10, 11, 13, 14, 15 and $p \leq 59$. What is new here:

- the two reductions of §4 and their validation (Proposition 4.1), which is what makes the moduli $17, 19, 21, 22, 23$ affordable;
- the rows at those five moduli (Theorem 5.7), the small moduli $3, 5, 7$ (Proposition 5.8), and the extension of the rows $n \in \{10, 14, 15\}$ to $p \leq 499$ (Proposition 5.2 and Theorems 5.5 and 5.6);
- the order 253 (Theorem 6.1) and the classification of the two-prime orders with both primes at most 23 (Theorem 6.2);
- the four published bad pairs and the order 979 (Theorem 6.3);
- the per-prime hypothesis, the orders 377 and 885, and the verification of 310 (§7);
- the four-factor orders: 210 refuted at every split, and Corollary 8.5.

Three statements of the first version are corrected. Its theorem on the modulus 10 certified eleven orders it described as having no published proof; [3], which appeared afterwards, settles all of them, and the same applies to 130, 170, 190 in Theorem 6.4 — so the count of orders for which we know no published proof stands at 215, in a much larger total, rather than at 45. Its remark that 210 is out of reach on grounds of cost is replaced by Theorems 7.1 and 7.2, which show it is out of reach at every split; and its remark that a translation reduction "could in principle" shorten each sweep by a factor close to n understated what is available, the affine group having order $n\varphi(n)$ and complementation giving a further measured factor 4.2 at $n = 23$. Question 8.7 is unchanged as a question, but Remark 8.8 records what the enlarged data say about its answer.

What remains priced and not run: six cells at the modulus 26, about 102 CPU-minutes, which would settle $494, 962, 1066, 1118, 1222, 1534$; the modulus 30, at about 3.2 CPU-hours a cell, where the smallest four-factor order this route could still settle is $1110 = 30 \cdot 37$; and the moduli $33, 34, 35$, at about 21, 35 and 139 CPU-hours a cell in C.

References

[1] A. Caragea, D. G. Lee, R. D. Malikiosis and G. E. Pfander, *Principal minors of Fourier matrices of square-free order*, arXiv:2505.24326v3 (2025); every numbered reference to this work above is to v3.

[2] J. Gu, L. Zhou and Y. Wang, *Principal nonsingularity of the Fourier matrices of orders* 70 *and* 143, arXiv:2608.17746v1 (2026).

[3] Y. Wang and X. Zhang, *Prime multipliers of order ten: norm spectra, local charts, and selective lifting*, arXiv:2608.22119v1 (2026).

[4] W. Zhou, *Principal non-singularity of Fourier matrices on $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_2^k \times \mathbb{Z}_q$*, arXiv:2505.01189v3 (2026).

[5] T. Emmrich and S. Kunis, *Real and finite field versions of Chebotarëv's theorem*, arXiv:2506.02947v2 (2025).

[6] M. Loukaki, *Chebotarëv's theorem for cyclic groups of order pq and an uncertainty principle*, Bull. Lond. Math. Soc. **57** (2025), no. 12, 3841–3856; arXiv:2412.08600.

[7] G. Zhang, *On the Chebotarëv theorem over finite fields*, Finite Fields Appl. **56** (2019), 97–108.

[8] 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, pp. 625–635.

[9] The mathlib Community, *The Lean mathematical library*, in: CPP 2020, ACM, 2020, pp. 367–381.