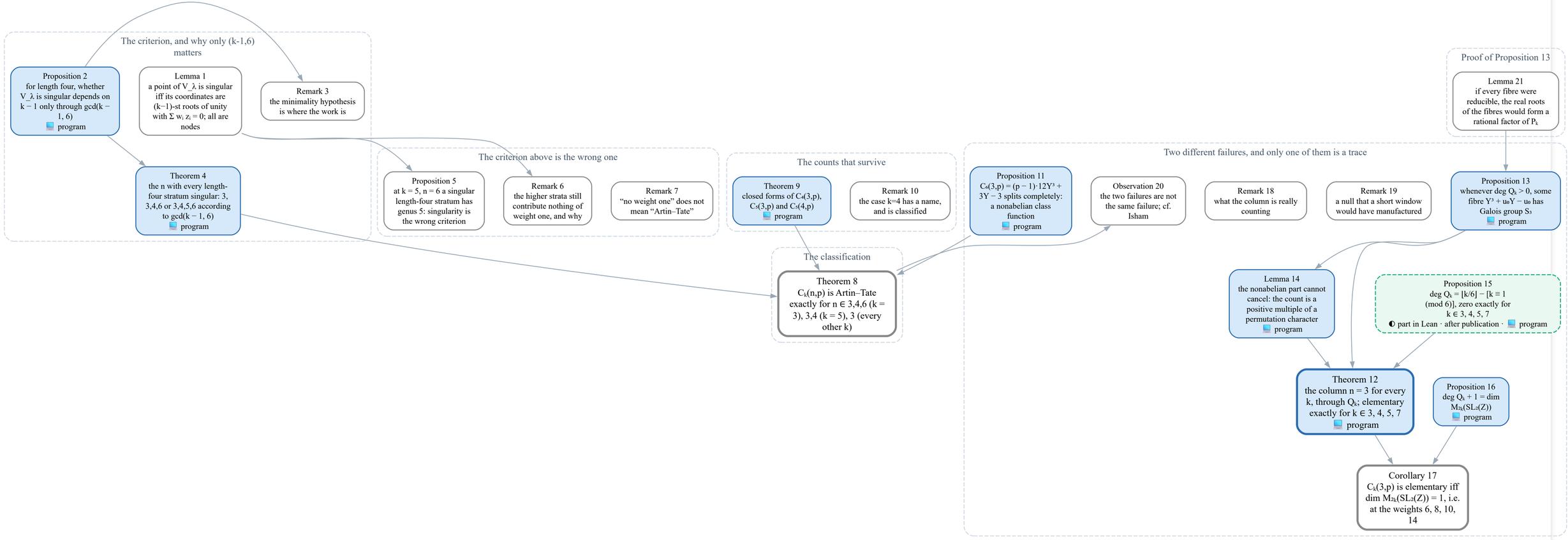
Blueprint

Map of *Subsets of F_p with two prescribed moments, Part II: every exponent — the classification, the Cauchy-Liouville-Mirimanoff polynomials that decide the column n=3, and where this moment subset sum stops being PORC*

Arithmetic geometry over finite fields · subsets with prescribed power sums

21 results | **0** entirely in Lean | **1** partly in Lean | **9** checked by a program | written proof only | (a result can carry several tags)

Dependencies in the written proof: an arrow A → B means that this proof of B uses A. Every result rests on its written proof; the tags record what was checked besides, and each statement's "Evidence & scope" block says how far. The colour of a box is its strongest tag, in the order above; the tags in the box give the rest. Boxes with a thick border are the main results; click a box to read the statement.



What the paper contributes

$C_k(n,p)$ counts the n-subsets of $\mathbb{F}_p$ with $\Sigma t = \Sigma t^k = 0$. Part I settled $k = 3$; this note settles every $k \geq 3$.

- **The singularity criterion** (Proposition 2, Theorem 4): for a length-four stratum, singularity depends on k only through $\gcd(k-1, 6)$, by Mann's theorem, and the set of n with all length-four strata singular takes exactly three values.
- **…is the wrong criterion** (Proposition 5): what kills weight one is a genus-zero normalisation; at $k = 5$, $n = 6$ a singular stratum has genus 5. With the corrected criterion, $C_k(n,p)$ is Artin–Tate exactly for $n \in \{3,4,6\}$ ($k = 3$), $\{3,4\}$ ($k = 5$) and $n = 3$ otherwise (Theorem 8), and the surviving counts are written down (Theorem 9, Proposition 11).
- **The column n = 3** (Theorem 12, Propositions 15–16, Corollary 17): one term per root of Q_k whose cubic $Y^3 + uY - u$ splits; elementary exactly for $k \in \{3, 4, 5, 7\}$, because $\deg Q_k + 1 = \dim M_{2k}(SL_2(\mathbb{Z}))$.
- **Not PORC** (Proposition 13, Lemmas 14 and 21): some fibre has group S_3 — unconditionally, with forty printed certificates for $6 \leq k \leq 46$ — and a permutation-character identity shows it cannot cancel. Observation 20 separates the two failures of PORC by weight (Isham has the coexistence).
- The polynomials Q_k and the reduction to u are Helou's, Tzermias's and Nanninga's; the paper claims the arithmetic over $\mathbb{F}_p$.

🚀 **Start here:** **Theorem 8**: $C_k(n,p)$ is Artin–Tate exactly for $n \in 3,4,6$ ($k = 3$), $3,4$ ($k = 5$), 3 (every other k).

Main results:

- **Theorem 8**: $C_k(n,p)$ is Artin–Tate exactly for $n \in 3,4,6$ ($k = 3$), $3,4$ ($k = 5$), 3 (every other k)
- **Theorem 12**: the column $n = 3$ for every k, through Q_k; elementary exactly for $k \in 3, 4, 5, 7$
- **Corollary 17**: $C_k(3,p)$ is elementary iff $\dim M_{2k}(SL_2(Z)) = 1$, i.e. at the weights 6, 8, 10, 14

🧭 Fields: where the paper lives and what it connects

Tools taken from other branches

- **Vanishing sums of roots of unity** → Mann's theorem on minimal relations with at most four terms (and Conway–Jones), applied with positive weights — Proposition

2, Theorem 4

- **ℓ-adic cohomology and weights** → weight one of the sieve class, normalisations of plane curves, Ghorpade–Lachaud, Chebotarev and Brauer–Nesbitt for virtual representations — Proposition 5, Theorem 8
- **Cauchy–Liouville–Mirimanoff polynomials** → the reduction of x^k + y^k + z^k on x + y + z = 0 to the invariant $u = e_2^3/e_3^2$ (Helou, Tzermias, Nanninga), Newton–Waring at $e_1 = 0$ — Theorem 12, Proposition 15
- **Galois theory of cubics** → total reality of the roots of Q_k, discriminants of the fibre cubics, permutation characters, irreducibility certificates modulo one prime — Proposition 13, Lemma 14, Lemma 21
- **Modular forms** → M_*($SL_2(Z)$) = C[E_4, E_6]: the monomials of s_k index a basis of M_{2k} — Proposition 16, Corollary 17

What the results serve

- **Moment subset sum problem** ← which (n, k) admit a closed form in characters, for every exponent k, and the closed forms that survive — Theorem 8, Theorem 9, Proposition 11
- **PORC and POFS counting functions** ← two failures of PORC separated by weight: a nonabelian class function at n = 3 (still POFS) and a surviving Frobenius trace for n ≥ 4 — Lemma 14, Proposition 11, Theorem 8