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

Carles Marín

Statements

Lemma 1 — the singular locus; the case $k = 3$ is Segre's 8
Proposition 2 — the invariant is $\gcd(m, 6)$ 9
Remark 3 — the minimality hypothesis is where the work is 10
Theorem 4 — the trichotomy 10
Proposition 5 — the converse fails at $k = 5$, $n = 6$ 15
Remark 6 — the higher strata still contribute nothing of weight one, and why 16
Remark 7 — "no weight one" does not mean "Artin–Tate" 16
Theorem 8 — all k, all n 17
Theorem 9 19
Remark 10 — the case $k = 4$ has a name, and is classified 20
Proposition 11 22
Theorem 12 — the column $n = 3$ 23
Proposition 13 — an S_3-fibre exists 24
Lemma 14 — the nonabelian part cannot cancel 25
Proposition 15 — the degree of Q_k 28
Proposition 16 — the degree is a dimension of modular forms 30
Corollary 17 — the criterion is a dimension 31
Remark 18 — what the column is really counting 33
Remark 19 — a null that a short window would have manufactured 34
Observation 20 — the two failures are not the same failure; cf. [17] 34
Lemma 21 — the real roots form a factor 44

At a glance

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

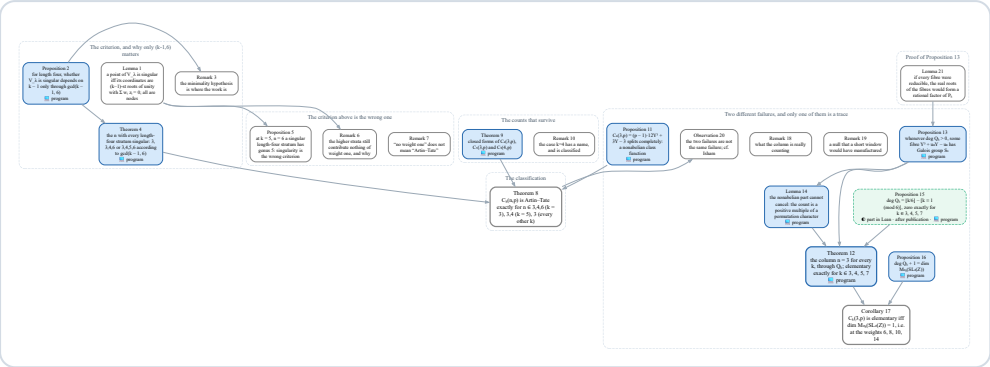
21 results | ✅ **0** entirely in Lean | ◐ **1** partly in Lean | 💻 **9** checked by a program | written proof only

(a result can carry several tags)

🗺️ Map of the results (click a box to go to it)

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.



📐 Setting (copied from the paper, abstract, §1–§6)

(Abstract) Fix $k \geq 3$ and an odd prime p, and let $C_k(n,p)$ count the n-subsets $T \subseteq \mathbb{F}_p$ with $\sum_{t\in T} t = \sum_{t\in T} t^k = 0$. *(§1)* The Li–Wan partition sieve attaches to each partition $\lambda = (w_1, \dots, w_l) \vdash n$ the variety

$$V_\lambda \;=\; \Big\{ \textstyle\sum_i w_i x_i = 0, \;\; \sum_i w_i x_i^k = 0 \Big\} \;\subset\; \mathbf{P}^{\,l-1}.$$

(§2) Throughout, write $m = k-1$ and μ_m for the m-th roots of unity. *(§3)* For $\lambda = (w_1, \dots, w_l) \vdash n$ put

$$A_\lambda = \Big\{ x \in \mathbf{A}^{\,l} : \;\; \textstyle\sum_i w_i x_i = 0, \;\; \sum_i w_i x_i^k = 0 \Big\}, \qquad z_\lambda = \textstyle\prod_j j^{m_j}\, m_j!\,,$$

with m_j the number of parts of λ equal to j, so that A_λ is the affine cone over V_λ. *(§5)* Write $\chi_p(a) = \left(\frac{a}{p}\right)$. *(§6)* Under $e_1 = 0$ Newton’s recursion reads $s_k = -e_2 s_{k-2} + e_3 s_{k-3}$ with $s_1 = 0$, $s_2 = -2e_2$, $s_3 = 3e_3$, so each s_k is a polynomial in e_2, e_3. […] every factor of s_k other than e_2 and e_3 is a polynomial Q_k in $u = e_2^3/e_3^2$.

$$f_u(Y) \;=\; Y^3 + uY - u, \qquad \text{so that} \qquad e_2 = e_3 = u, \quad \frac{e_2^3}{e_3^2} = u, \quad \text{disc } f$$

$$\mathfrak{D}_k \;=\; \mathrm{lc}(Q_k)\cdot \mathrm{disc}(Q_k)\cdot \mathrm{Res}\big(Q_k,\; u(4u+27)\big) \;\in\; \mathbb{Z}\smallsetminus\{0\}.$$

Abstract.

Fix $k \geq 3$ and an odd prime p, and let $C_k(n,p)$ count the n-subsets $T \subseteq \mathbb{F}_p$ with $\sum_{t\in T} t = \sum_{t\in T} t^k = 0$. The companion note [37] evaluates $C_3(n,p)$ and shows it is elementary — a polynomial in p with coefficients in quadratic characters of fixed integers — exactly for $n = 3, 4, 6$. We settle every k. Three things happen, and only the first is what $k = 3$ would lead

one to expect. First, the criterion for the deciding stratum to be singular depends on k only through $\gcd(k-1,6)$, by Mann's theorem on relations between roots of unity, and takes exactly three values. Second, that criterion is *not* the right one: for plane cubics, singularity forces a genus-zero normalisation, which is why it controls the answer when $k=3$, and the correct condition in general is that the normalisation have genus zero. Third, with the corrected criterion the classification collapses: $C_k(n,p)$ is Artin–Tate precisely for $n\in\{3,4,6\}$ when $k=3$, for $n\in\{3,4\}$ when $k=5$, and for $n=3$ alone in every other k. We give the closed forms that survive, and we describe the column $n=3$ completely: writing $u=e_2^3/e_3^2$, the count is governed by the roots of an explicit polynomial $Q_k(u)$ together with the cubic Y^3+uY-u attached to each root, and it is expressible in quadratic characters if and only if Q_k is constant, which happens exactly for $k\in\{3,4,5,7\}$. That list is not accidental: $\deg Q_k+1=\dim M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, so the count is elementary exactly when that space of modular forms is one-dimensional, which happens at the weights $6,8,10,14$; the exceptional return at weight 14 reflects the gap $M_2=0$ after the first cusp form appears in weight 12. Where it is not elementary, some fibre of Q_k has Galois group S_3, and a permutation-character identity shows the nonabelian part cannot cancel, so the count is not PORC. Finally we observe that the two ends of this classification fail to be polynomial on residue classes for *different* reasons: at $n=3$, $k=6$ the obstruction is a nonabelian Artin-type class function and the count takes two values, so it is polynomial on Frobenius sets; for $n\geq 4$ the obstruction is a surviving weight-one Frobenius trace coming from a positive-genus curve, and there the count is not even POFS.

Keywords: moment subset sum; finite fields; prescribed moments; Li–Wan sieve; vanishing sums of roots of unity; Mann's theorem; PORC; POFS; Artin–Tate counts; modular forms; elliptic curves; Mirimanoff's conjecture; Cauchy–Liouville–Mirimanoff polynomials.

MSC 2020: 11T06, 11T24, 11G20, 14G15, 11R18.

1 What changes when the exponent changes

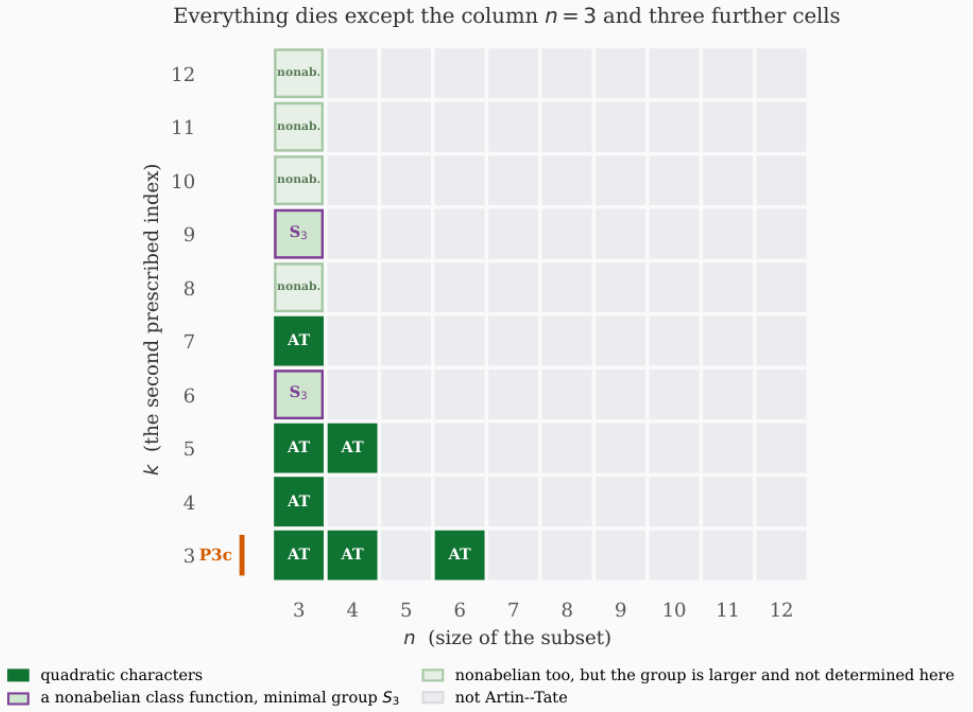
The counts $C_J(n,p)$ for a general index set J were introduced in Part II of the separate S-matrix series [38] , which proves the estimate $C_J(n,p)=p^{-|J|}\binom{p}{n}+O_n(p^{n/2})$ and leaves the closed form open; the companion note [37] closes the pair $\{1,3\}$. Nothing in its mechanism used the number 3: the Li–Wan partition sieve [21] attaches to each partition $\lambda=(w_1,\dots,w_l)\vdash n$ the variety

$$V_\lambda \;=\; \Big\{ \textstyle\sum_i w_i x_i = 0,\;\; \sum_i w_i x_i^{k} = 0 \Big\} \;\subset\; \mathbf{P}^{\,l-1}, \quad (1) \quad (1)$$

and a point of V_λ is singular exactly when its coordinates are $(k-1)$-st roots of unity with $\sum_i w_i \zeta_i = 0$. For $k = 3$ those roots are signs, the condition reads “the weights split into two blocks of equal sum”, and that is a statement about partitions. For general k it is a statement about vanishing weighted sums of roots of unity, which is a different and much better-studied kind of object.

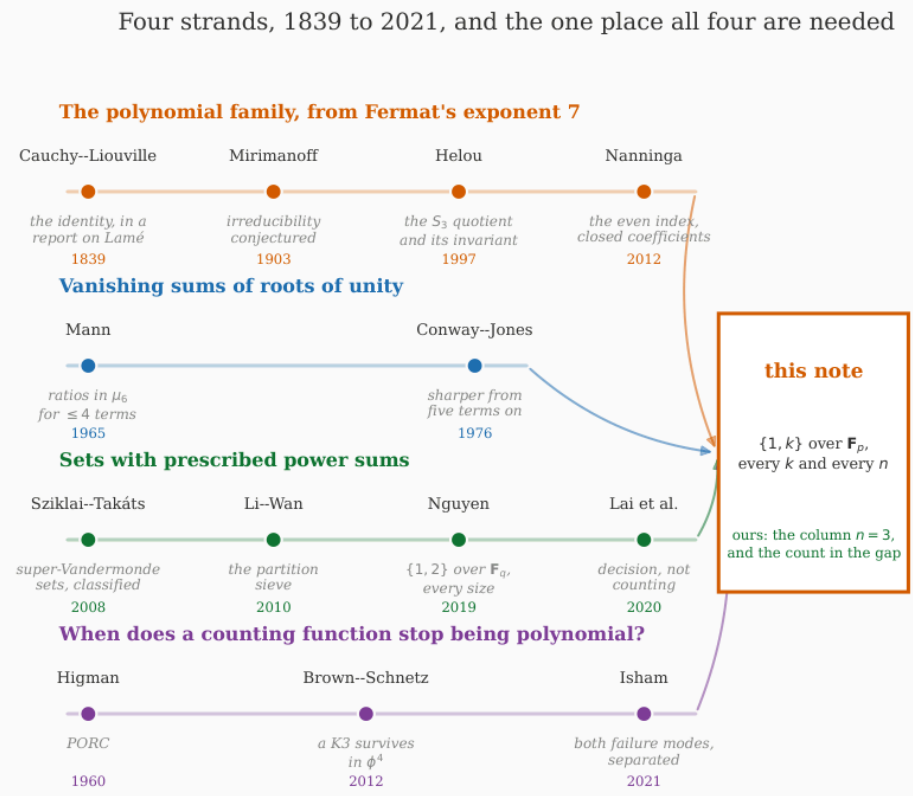
So the natural question is whether the answer for general k is the $k = 3$ answer with the signs replaced by roots of unity. It is not, and it fails twice — once in the arithmetic and once in the geometry. The arithmetic failure is mild and pleasant: the answer turns out to depend on k only through $\gcd(k-1, 6)$, so there are three cases and not infinitely many (Section 2). The whole answer is Figure 1, and the rest of this note is its proof. The geometric failure is the interesting one: the criterion “every length-four curve is singular”, which is what the $k = 3$ argument literally proves, is *the wrong criterion*, and it happens to be equivalent to the right one only when $k = 3$ (Section 3). Once corrected, the classification is short (Section 4) and the surviving counts can all be written down (Section 5).

Figure 1



The result of this note. A cell is live when $C_k(n, p)$ is Artin–Tate. The column $n = 3$ never dies, because a zero-dimensional variety always contributes an Artin character; but the class function is expressible in quadratic characters only for $k \in \{3, 4, 5, 7\}$ (Theorem 12), so "Artin–Tate" and "elementary" part company from $k = 6$ on. Among the nonabelian cells the two shades are not decoration: the darker ones, $k = 6$ and $k = 9$, are those where the group of the class function is exactly S_3, and the paler ones those where it is larger: $S_3 \times C_2$ for $k = 8, 10, 11$, and not determined here for $k = 12$. Which cells are which, and why, is settled after Theorem 12; Proposition 13 gives one S_3 *fibre* whenever $\deg Q_k > 0$, which is weaker than either and is all Lemma 14 needs. Everything else is dead, and the row $k = 3$ of the companion note is the only one with more than two live cells.

Figure 2



Where this note sits, and what it owes. Four strands of work that do not otherwise meet: the Cauchy–Liouville–Mirimanoff family, the arithmetic of vanishing sums of roots of unity, the counting of subsets with prescribed power sums, and the question of when a counting function stops being polynomial — in the order drawn. The argument below needs a piece from each — Helou and Tzermias for the family our polynomials turn out to be, Mann for the criterion, Li–Wan for the sieve, and the PORC/POFS vocabulary to say what the failure is — and the box on the right marks the part we claim, which is the smallest of the four.

What is ours

Figure 2 is the map. The singular locus of a weighted hyperplane section of a diagonal form is classical; we claim no part of it, and Section 2 says whose it is. Mann's theorem is Mann's. The vanishing of H^1 in dimension at least two is Ghorpade–Lachaud's. The sieve is Li–Wan's.

What the note establishes is Theorem 4, the corrected criterion of Proposition 5, the classification of Theorem 8 with the closed forms of Theorem 9 and Proposition 11 that it leaves standing, the arithmetic of the column $n = 3$ in Theorem 12 and its reading as a dimension of modular forms in Corollary 17, Proposition 13 with the certificates behind it and Lemma 14, which is what carries it to a failure of PORC, and Remark 3.

Some things in this note are not new and we say so where they appear. The coexistence of the two failure modes of Section 6 is in Isham [17] , whose separation of a bounded zero-dimensional contribution from a surviving

Frobenius trace is the same distinction and is load-bearing in her argument; we add only the identification of the bounded mode as POFS. And neither the polynomials Q_k nor the reduction that produces them is ours: both are in [16 , 41 , 33] , as Section 6 sets out where they first appear. What we claim there is the arithmetic consequence over $\mathbb{F}_p$, not the polynomials. Every theorem, proposition, corollary and observation below carries a card saying which of the two it is, except Proposition 2, a step towards Theorem 4; so do Lemmas 1 and 14 and Remarks 3 and 10. Figure 2 says the same thing in one picture.

2 The criterion, and why only $\gcd(k-1,6)$ matters

Throughout, write $m = k-1$ and μ_m for the m-th roots of unity.

Lemma 1. (the singular locus; the case $k=3$ is Segre's) p. 4

> *Let $\lambda = (w_1, \dots, w_l)$ with w_i positive and $\sum_i w_i = n$, and let V_λ be as in (1) over an algebraically closed field of characteristic 0 or $p > \max(n,k)$. A point $z \in V_\lambda$ is singular if and only if, after scaling, $z_i \in \mu_m$ for every i and $\sum_i w_i z_i = 0$. All such singularities are ordinary double points.*

🆕 **Classical and new:** not ours, cited: for k = 3 Segre; Elsenhans–Jahnel [EJdisc, Fact 2.8]; for arbitrary degree Dimca–Sticlaru [DS, Thm. 2.4].

↳ Used in: Proposition 5 (p. 15), 6 (p. 16)

Proof

> V_λ is cut by a hyperplane H and the hypersurface $F = \sum_i w_i x_i^k$. A point is singular iff the two differentials are proportional, i.e. $k w_i z_i^{k-1} = \mu w_i$ for all i and some μ; since $w_i \neq 0$ this says $z_i^{k-1} = \mu/k$ is the same for all i, and rescaling makes it 1. The point must also lie on H, which is $\sum_i w_i z_i = 0$.
>
> For the second statement, restrict to H the bilinear form $B(u,v) = \sum_i (w_i/z_i) u_i v_i$, which is the Hessian of F at z up to a nonzero scalar because $z_i^{k-2} = z_i^{-1}$. It is nondegenerate on the ambient space, and $B(z,u) = \sum_i w_i u_i$, so the B-orthogonal of H is $\langle z \rangle$. Since $\sum_i w_i z_i = 0$ we have $z \in H$, whence

$\operatorname{rad}(B|_H) = \langle z \rangle$; modulo the radial direction the Hessian is nondegenerate, which is an ordinary double point.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fajeno!4,colframe=fajeno!55, fontupper=,before skip=6pt,after skip=8pt] fajeno**Lemma 1**fajenonot ours — cited

For $k = 3$ the base case is Segre (1887); the statement in the pentahedral coordinates used here is Elsenhans–Jahnel [6 , Fact 2.8] , whose Examples 2.9 are three of our V_λ with their node counts printed; for arbitrary degree and coefficients it is Dimca–Sticlaru [4 , Thm. 2.4] . The proof is reproduced because the note needs the ordinary-double-point half explicitly for every k, not because anything is claimed.

The condition $\sum_i w_i\zeta_i = 0$ with $\zeta_i \in \mu_m$ is a *vanishing sum of roots of unity with positive rational weights*. For a stratum of length four — the only length that will matter — there are four terms, and that is exactly the regime that Mann settled.

Proposition 2. (the invariant is $\gcd(m, 6)$) p. 4

> *Let λ have length four. Whether V_λ is singular depends on m only through $\gcd(m, 6)$.*

🆕 **Classical and new:** a step towards Theorem 4, resting on Mann's theorem [Mann, Thm. 1].

↳ Used in: 3 (p. 10), Theorem 4 (p. 10)

Proof

Decompose a vanishing relation $\sum_{i=1}^{4} w_i\zeta_i = 0$ into minimal vanishing subsums, a decomposition that never splits an individual term. A singleton cannot vanish, because $|w_i\zeta_i| = w_i > 0$; and a block of three would leave a singleton. So the only possibilities are that the relation is itself minimal, or that it splits as $2 + 2$.

If it is minimal then, by Mann [24] , all ratios of participating roots have order dividing $\prod_{q \le 4 \text{ prime}} q = 6$; rotating one root to 1 puts the rest in $\mu_m \cap \mu_6 = \mu_{\gcd(m,6)}$, and whether such a relation exists is then a condition on $\gcd(m, 6)$ alone. If instead it splits as $2 + 2$, each pair satisfies $w_i\zeta_i = -w_j\zeta_j$, so taking absolute values gives $w_i = w_j$ and then $\zeta_i = -\zeta_j$; this requires $-1 \in \mu_m$, that is $2 \mid m$, which is again a condition on $\gcd(m, 6)$ alone.

Evidence & scope

- **Program:** the witness $1 + (-1) + \zeta_7 + (-\zeta_7) = 0$ in μ_{14}; vanishing pairs for $m \le 24$, weights ≤ 5; ten length-four partitions depend only on $\gcd(m,6)$ for $m \le 24$. `gates/P3d_mann_minimalidad.py`

Remark 3. (the minimality hypothesis is where the work is) p. 5

It is worth saying why the second case must be treated separately rather than absorbed into the first. Mann's theorem bounds the ratios *inside* a minimal subsum, not between two of them, and four terms splitting as $2 + 2$ can have ratios of arbitrarily large order:

$$1 + (-1) + \zeta_7 + (-\zeta_7) = 0$$

is a vanishing sum of four roots of unity with positive rational weights in which one ratio has order 7. A proof of Proposition 2 that decomposed into minimal subsums and then applied Mann to the whole relation would be answering a different question. For four terms Mann's bound is already sharp — the relation $2 \cdot 1 + (-1) + \omega + \omega^2 = 0$ realises a ratio of order exactly 6 — and the sharper bound of Conway and Jones [23 , Thm. 5] , which requires $l \ge \sum_{q|r}(q-2) + 2$, agrees with it here and only improves on it from five terms onwards.

↳ Not used by another result of the paper.

Measured: The witness above verified exactly in μ_{14}, together with the assertion that its subsum $\{1, -1\}$ vanishes so that it is not minimal; the claim that a vanishing pair forces $w_i = w_j$ and $\zeta_i = -\zeta_j$ checked exhaustively for $m \le 24$ and weights up to 5; and the singularity pattern of ten length-four partitions verified to depend only on $\gcd(m, 6)$ for $m \le 24$. See `gates/P3d_mann_minimalidad.py`.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Remark 3**fnuestroours — it isolates a hypothesis the proof needs

The witness $1 + (-1) + \zeta_7 + (-\zeta_7) = 0$ refutes a step that is natural to take and easy to take wrongly: decomposing into minimal subsums and then applying Mann to the whole relation. It leaves Proposition 2 standing — the $2 + 2$ case costs two lines — but the hypothesis it isolates is the one the length-four argument rests on.

Theorem 4. (the trichotomy) p. 5

> *For $m \ge 1$ let S_m be the set of $n \ge 3$ such that every $\lambda \vdash n$ of length four has V_λ singular. Then*

$$\boxed{S_m = \begin{cases} \{3\} & \text{if } m \text{ is odd,} \\ \{3,4,6\} & \text{if } 2 \mid m,\ 3 \nmid m, \\ \{3,4,5,6\} & \text{if } 6 \mid m. \end{cases}}$$

🆕 **Classical and new:** ours — an elementary consequence of Mann [Mann] and the triangle inequality (the paper's card).

↳ Used in: Theorem 8 (p. 17)

Proof

There are no partitions of 3 of length four, so $3 \in S_m$ always. The remaining content is which of $(2,1,1,1)$, $(3,1,1,1)$, $(2,2,1,1)$ and $(1,1,1,1)$ admit a relation.

For $(1,1,1,1)$ the relation $1+1-1-1=0$ works as soon as $-1 \in \mu_m$, i.e. $2 \mid m$; and for m odd no relation exists, since by Proposition 2 we may take $m \in \{1,3\}$, and four unit-weight terms in μ_3 sum to zero only if each cube root of unity occurs equally often, which four terms cannot do. This is the condition $4 \in S_m$. The partition $(2,2,1,1)$ has the same relation when $2 \mid m$, and also $2+2\omega+\omega^2+\omega^2=0$ when $3 \mid m$; that changes nothing, because whether $6 \in S_m$ is decided by $(3,1,1,1)$ below, which needs $2 \mid m$.

For $(2,1,1,1)$ there can be no proper vanishing subsum, because the weight 2 has no equal-weight partner; so the whole relation is minimal and, by Proposition 2, lives in μ_6 after normalising $\zeta_1 = 1$. Inspection gives $(\zeta_2,\zeta_3,\zeta_4)$ a permutation of $(-1,\omega,\omega^2)$ with ω a primitive cube root, and indeed $2-1+\omega+\omega^2 = 2-1-1 = 0$. Equivalently, in the polynomial form of the criterion, Φ_6 divides the weight polynomial:

$$2+X^2+X^3+X^4 = (X^2-X+1)(X^2+2X+2).$$

So $(2,1,1,1)$ is singular exactly when $6 \mid m$, and then carries exactly six geometric singular points. Since $(2,1,1,1)$ is the only length-four partition of 5, this is precisely the condition $5 \in S_m$.

For $(3,1,1,1)$, equality in $|3\zeta_1| = |\zeta_2+\zeta_3+\zeta_4|$ forces $\zeta_2=\zeta_3=\zeta_4=-\zeta_1$, which needs $-1 \in \mu_m$; so $(3,1,1,1)$ is singular exactly when $2 \mid m$, with exactly one singular point. Since $(2,2,1,1)$ is singular whenever $2 \mid m$, this gives $6 \in S_m \iff 2 \mid m$.

> Finally, for $n \geq 7$ the partition $(n-3,1,1,1)$ has $n-3>3$, so $|(n-3)\zeta_1|>|\zeta_2+\zeta_3+\zeta_4|$ and no relation can exist for any m; hence no $n \geq 7$ lies in S_m.

Evidence & scope

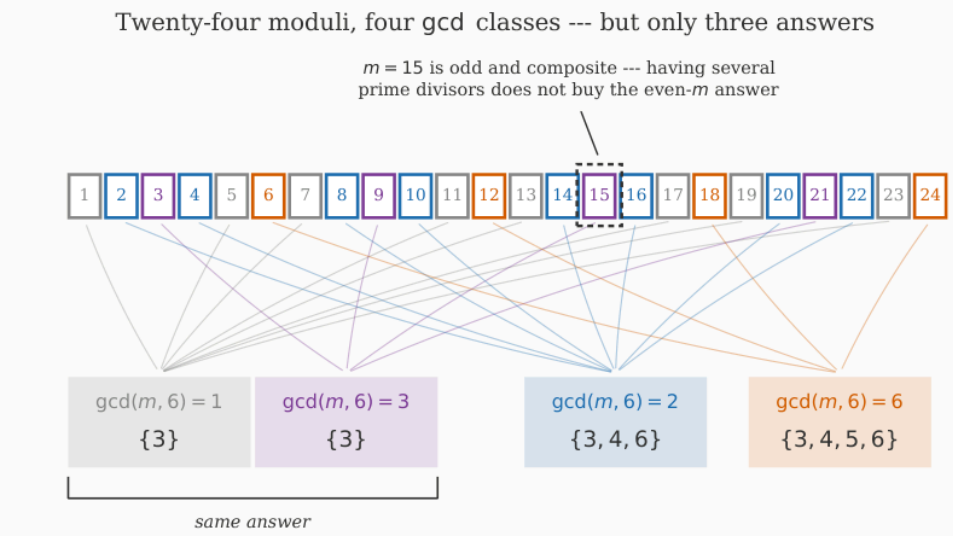
- **Program:** S_m from the definition by exhaustive enumeration over μ_m⁴, 1 ≤ m ≤ 18, 3 ≤ n ≤ 10; the factorisation by Φ₆ exactly. `gates/P3d_tricotomia_Sm.py`

$m = k-1$	$\gcd(m,6)$	S_m	**certificate**
odd	1 or 3	$\{3\}$	—
$2 \mid m$, $3 \nmid m$	2	$\{3,4,6\}$	$1+1-1-1=0$ in μ_2
$6 \mid m$	6	$\{3,4,5,6\}$	$2+X^2+X^3+X^4=\Phi_6\cdot(X^2+$

Table 1: Theorem 4 in three rows. The tinted rows are the two where something beyond $n=3$ is singular; the bottom one is where $n=5$ enters, and the certificate is the divisibility by Φ_6 that puts it there. Note that this table answers the *singularity* question, which Section 3 shows is not the same as the Artin–Tate question.

Colour: grey = nothing.

Figure 3



Proposition 2 and Theorem 4 together. What the picture shows and the statement does not is that the collapse is not injective: four gcd classes produce only three answers, because gcd $= 1$ and gcd $= 3$ agree. The circled $m = 15$ is the case that kills the natural guess — having several prime divisors is not what buys the even-m answer. The sets drawn here are the S_m of the trichotomy — which n have a *singular* length-four stratum — and not the live cells of Figure 1: the two coincide only at $k = 3$, and Section 3 is about why.

3 The criterion above is the wrong one

Theorem 4 is a complete answer to the question "for which n is every length-four stratum singular?". That question is the right one for $k = 3$ and the wrong one in general, and it is worth being precise about why.

We first fix the notation the rest of this section uses. For $\lambda = (w_1, \dots, w_l) \vdash n$ put

$$A_\lambda = \left\{ x \in \mathbf{A}^l : \ \textstyle\sum_i w_i x_i = 0, \ \sum_i w_i x_i^k = 0 \right\}, \qquad z_\lambda = \textstyle\prod_j j^{m_j} \, m_j!\,,$$

with m_j the number of parts of λ equal to j, so that A_λ is the affine cone over V_λ. The Li–Wan sieve [21] is then the exact identity

$$C_k(n,p) \ = \ \sum_{\lambda \vdash n} \frac{(-1)^{\,n-l(\lambda)}}{z_\lambda} \, \#A_\lambda(\mathbb{F}_p), \quad (2) \qquad (5)$$

counting each unordered n-subset once by inclusion–exclusion over the coincidence patterns of its elements. What obstructs an elementary formula is weight one surviving in the corresponding motivic sum,

$$\mathcal{M}_{n,k} = \sum_{\lambda \vdash n} \frac{(-1)^{\,n-l(\lambda)}}{z_\lambda}\, e_c(A_\lambda),$$

whose Frobenius trace is the right-hand side of (2). For a length-four stratum, V_λ is a plane curve C, and the cone over it satisfies $e_c(A_C) = 1 + (\mathbb{L}-1)e(C)$. Here C need not be irreducible — the witness of (6) is a union of three lines and a residual curve — so we keep track of its components. If C is reduced with r geometric components, then $e(C) = 1 - [H^1(C)] + [\Pi_C]\mathbb{L}$, where Π_C is the permutation representation of $G_{\mathbb{Q}}$ on those components, of dimension r, and hence

$$e_c(A_C) = [\Pi_C]\,\mathbb{L}^2 + (1-[\Pi_C])\,\mathbb{L} + (1-\mathbb{L})\,[H^1(C)]. \quad (3)(6)$$

The first two terms are Artin–Tate and carry only even weights, so they cannot contribute weight one; taking $r = 1$ recovers the familiar $\mathbb{L}^2 + (1-\mathbb{L})[H^1(C)]$, and nothing below depends on which case we are in.

What does need care is $[H^1(C)]$ itself. For a nodal curve, *reducible or not*, $H^1(C)$ may carry weight zero as well, coming from the dual graph Γ_C: irreducibility does not prevent it, as a nodal plane cubic shows: its normalisation is $\mathbf{P}^1$, yet the node closes a loop in Γ_C, and

$$\#C(\mathbb{F}_p) = p + 1 - \operatorname{Tr}\!\big(\mathrm{Frob}_p \mid H^1(\Gamma_C)\big),$$

which is p for a split node and $p+2$ for a non-split one — in either case not $p+1$. The two graded pieces are

$$\operatorname{gr}^W_0 H^1(C) \simeq H^1(\Gamma_C), \qquad \operatorname{gr}^W_1 H^1(C) \simeq H^1(\widetilde{C}),$$

so “the weight-one part is $[H^1(C)]$” would not be literally true; the statement that holds in both cases is

$$\operatorname{gr}^W_1 H^1(C) = H^1(\widetilde{C}),$$

$\widetilde{C}$ the normalisation: the difference between $e(C)$ and $e(\widetilde{C})$ is supported on the finite sets of nodes and branches, hence Artin of weight zero. Therefore

$$\boxed{\operatorname{gr}^W_1 e_c(A_C) = [H^1(\widetilde{C})]} \quad (4) \qquad (7)$$

and singularity is not what kills weight one — rationality of the normalisation is.

For $k = 3$ the two coincide, because every geometric component of the normalisation of a reduced singular plane cubic has genus zero — the irreducible case is the usual rational parametrisation, and a reducible one splits into lines and conics. For $k \geq 4$ they do not, and the smallest discrepancy is small enough to write out.

Proposition 5. (the converse fails at $k = 5$, $n = 6$) p. 8

> *Let $k = 5$, so $m = 4$, and $\lambda = (3, 1, 1, 1)$. Then V_λ is a geometrically irreducible plane quintic with exactly one node, its normalisation has genus 5, and consequently $C_5(6, p)$ is not elementary — although $\lambda = (3, 1, 1, 1)$ and the other length-four partition $(2, 2, 1, 1)$ of 6 are both singular, so that $6 \in S_4$.*

🆕 **Classical and new:** ours, and load-bearing (the paper's card); it does not affect Part I, which is the case k = 3.

↳ Not used by another result of the paper.

Proof

> The singular-point equation is $3z_1 + z_2 + z_3 + z_4 = 0$ with $z_i \in \mu_4$; equality in the triangle inequality forces $[z_1 : z_2 : z_3 : z_4] = [1 : -1 : -1 : -1]$, so there is exactly one singular point, a node by Lemma 1. The quintic is geometrically irreducible: two groups of components of degrees a and $5 - a$ would meet in $a(5 - a) \geq 4$ points counted with multiplicity, and with all singularities ordinary nodes those intersections cannot be concentrated in the single available node. Hence $g(\widetilde{V}_\lambda) = \frac{(5-1)(5-2)}{2} - 1 = 5$, and $[H^1]$ has dimension 10. Since $z_{(3,1,1,1)} = 3 \cdot 3! = 18$, the summand $\frac{1}{18}[H^1(\widetilde{V}_\lambda)]$ appears in (4) with the sign common to the whole length-four stratum, so it cannot cancel; and an expression polynomial in p with fixed-character coefficients is Artin–Tate and has only even weights.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Proposition 5**fnuestroours — and it is load-bearing

This is why "every four-part curve is singular" must be replaced by "every four-part curve has genus-zero normalisation". For plane cubics, singularity forces a genus-zero normalisation; in higher degree singularity alone no longer does, which is the whole content of the correction —

not that a node can never destroy weight one there, since a three-nodal plane quartic has geometric genus zero too, but that one has to count the singularities to know. It does not affect [37] , which is the case $k = 3$; it does mean that the trichotomy of Theorem 4, taken alone, would predict $6 \in S_4$ and hence a closed form for $C_5(6, p)$ that does not exist.

Two remarks are worth recording, because both bound what the method can claim.

Remark 6.

(the higher strata still contribute nothing of weight one, and why)

p. 9

For $l \geq 5$ the variety V_λ has dimension $d = l - 3 \geq 2$ and is cut in $\mathbf{P}^{l-1}$ by $r = 2$ forms, so Ghorpade–Lachaud [7 , Prop. 3.2] gives $H^i(\mathbf{P}^{l-1}) \to H^i(V_\lambda)$ an isomorphism for $i \leq l - 1 - 2 - 1 = l - 4$; taking $i = 1$ needs exactly $l \geq 5$, and yields $H^1(V_\lambda) = 0$. Blowing up the nodes, the exceptional fibres are smooth quadrics of dimension $d - 1 \geq 1$, connected and with vanishing H^1, so proper base change gives $H^1(Y_\lambda) = 0$ on the resolution as well; the quadrics contribute only even weights. What must be stressed is that this uses that the singularities are *nodes*, supplied by Lemma 1; it is not an assertion about singular hypersurfaces in general.

↳ Not used by another result of the paper.

Remark 7. (“no weight one” does not mean “Artin–Tate”)

p. 9

At the same parameters $k = 5$, $n = 6$, take $\lambda = (2, 1, 1, 1, 1)$. Then V_λ is a nodal quintic surface in $\mathbf{P}^3$; its dualising sheaf is $\mathcal{O}(1)$ and resolving ordinary double points preserves the geometric genus, so the resolution has $h^{2,0} = 4$. Its H^2 is genuinely not Artin–Tate, even though H^1 vanishes. The weight-one argument is therefore an *obstruction* and not a converse theorem: it can prove that a count fails to be elementary, never that it succeeds. Every positive statement below is proved by exhibiting the formula.

↳ Not used by another result of the paper.

4 The classification

Theorem 8. (all k, all n) p. 9

⚠ Erratum (2026-11-10): Editorial: in the bibliography, the first author of [GMPP] (Smooth symmetric systems over a finite field and applications) is N. Giménez, not «J. Giménez». No statement is affected.

⚠ Erratum (2026-11-10): Editorial: the legend drawn inside Figure 1 calls the paler nonabelian cells «nonabelian too, but the group is larger and not determined here»; the caption and the text determine the group, $S_3 \times C_2$, for $k = 8, 10, 11$, and only $k = 12$ is left undetermined. No statement is affected.

> *Say $C_k(n,p)$ is Artin–Tate if there are a number field $L/\mathbb{Q}$ finite Galois with group Γ, a number field E splitting Γ, and class functions $\alpha_0, \dots, \alpha_d$ on Γ with values in E — equivalently, E-linear combinations of Artin characters — such that*
>
> $$C_k(n,p) \;=\; \sum_{j=0}^{d} p^{\,j}\, \alpha_j(\mathrm{Frob}_p) \qquad (8)$$
>
> *for all but finitely many p. Then*
>
> $$\boxed{\{\, n \geq 3 :\ C_k(n,p) \text{ is Artin--Tate} \,\} = \begin{cases} \{3,4,6\}, & k = 3, \\ \{3,4\}, & k = 5, \\ \{3\}, & k \neq 3, 5. \end{cases}}$$

🆕 **Classical and new:** ours — proved, not extrapolated (the paper's card); the case $k = 3$ is Part I [P3c, Thm. 6 and Remark 7].

↳ Used in: 20 (p. 34)

Proof

> The case $k = 3$ is [37 , Thm. 6 and Remark 7] : Theorem 6 there excludes elementary expressions for $n \notin \{3,4,6\}$, and Remark 7 notes that the same weight-one argument excludes coefficients given by arbitrary Artin-type class functions of finite image, which is the class (5); for $n = 3, 4, 6$ the closed forms there are elementary, hence Artin–Tate. For $n = 3$ there are no length-four strata and every V_λ with $\lambda \vdash 3$ is zero-dimensional, so the cones over them contribute only Artin–Tate classes and the count is an Artin-type class function in the sense of (5). It need not be a character: Proposition 11 produces the indicator of a conjugacy class, which is why (5) was stated for combinations rather than for traces. This is the column $n = 3$ of Figure 1, and Section 6 shows the class function need not be abelian. It remains to kill every $n \geq 4$ when $k \neq 3$, and every $n \geq 5$ when $k = 5$.

Two uniform witnesses do it, and Figure 4 is the bookkeeping.

Figure 1: The proof of Theorem 8 as an accounting. A node removes exactly one unit of genus, so past $k = 3$ the nodes are never enough. The two shaded columns are the two where a witness happens to be rational; $k = 5$ is shaded because its $n = 4$ witness degenerates to a conic, which is why $C_5(4, p)$ exists at all.

The witness at $n = 4$. Here $\lambda = (1, 1, 1, 1)$ and, eliminating x_4, the curve is $F_k(x, y, z) = x^k + y^k + z^k - (x + y + z)^k$. If k is even then m is odd, the curve is smooth by Theorem 4, and its genus is $\binom{k-1}{2} \geq 3$. If k is odd then, up to a nonzero scalar,

$$F_k = (x + y)(x + z)(y + z)\, R_{k-3}, \tag{12}$$

with R_{k-3} of degree $k - 3$. Every singular point of F_k corresponds to four unit roots summing to zero, hence lies on one of the three pairing lines; since all singularities are nodes, R_{k-3} can have no singularity — off the lines it would give an unaccounted singular point of F_k, on a line it would give multiplicity at least three — and it cannot be reducible, by Bézout. So R_{k-3} is smooth of genus $\binom{k-4}{2}$. This is positive for odd $k \geq 7$ and zero exactly for $k = 3$ (no residual curve at all) and $k = 5$ (a conic). Hence $n = 4$ dies for every $k \neq 3, 5$, and survives for $k = 3, 5$.

The witness at $n \geq 5$. For $n \geq 7$ take $\lambda = (n - 3, 1, 1, 1)$, smooth for every m by the last paragraph of Theorem 4, of genus $\binom{k-1}{2} > 0$ for $k \geq 4$. For $n = 6$ take $\lambda = (3, 1, 1, 1)$: smooth when k is even and carrying exactly one node when k is odd, so its normalisation has genus $\binom{k-1}{2}$ or $\binom{k-1}{2} - 1$, positive for every $k \geq 4$. For $n = 5$ take $\lambda = (2, 1, 1, 1)$: smooth unless $6 \mid m$, and when $6 \mid m$ it carries exactly six nodes, so with r geometric components $\sum_j g(\widetilde{C}_j) = \binom{k-1}{2} - 6 + r - 1 \geq 9$ because $6 \mid m$ forces $k \geq 7$.

In each case a length-four stratum has normalisation of positive genus, so by (4) the class $\operatorname{gr}_1^W \mathcal{M}_{n,k}$ is a sum of effective classes with one common sign and is nonzero.

To conclude, fix an embedding $\iota \colon E \hookrightarrow \overline{\mathbb{Q}}_\ell$. Read through ι, the right-hand side of (5) is not the trace of a representation — its coefficients are fractional, as $\mathbf{1}_{\{1\}} = \tfrac{1}{6}\chi_{\mathrm{reg}}$ above already shows — but it is the trace of a well-defined *virtual* one, an element of the Grothendieck group

$$K_0^{\mathrm{ss}}\big(G_{\mathbb{Q}},\overline{\mathbb{Q}}_\ell\big)\otimes_{\mathbb{Z}} E$$

of semisimple $\overline{\mathbb{Q}}_\ell$-representations with coefficients extended to E. In that group the trace still determines the class, irreducible characters being E-linearly independent. Chebotarev gives agreement of traces at a set of primes of density one, so Brauer–Nesbitt forces agreement of the two classes there; and every weight occurring on the Artin–Tate side is even, while $\mathrm{gr}_1^W \mathcal{M}_{n,k} \neq 0$. The comparison is thus between virtual representations throughout, which is all the weight argument needs. The positive direction for $k=5$, $n\in\{3,4\}$ is Section 5.

5 The counts that survive

Theorem 8 asserts three closed forms beyond those of [37] . Here they are; Table 2 collects them together with those of the companion note and records, for each, the reason the length-four obstruction failed to appear. Write $\chi_p(a)=\left(\frac{a}{p}\right)$.

Theorem 9. p. 11

For $p>3$,

$$\boxed{C_4(3,p)=\frac{(p-1)\big(1+\chi_p(-3)\big)}{6}},\qquad \boxed{C_5(3,p)=\frac{(p-1)\big(4}{6}}$$

and

$$\boxed{C_5(4,p)=\frac{p-1}{24}\Big(4p-17-6\chi_p(-2)-3\chi_p(-1)\Big)}.$$

At $p=3$ the three counts are 0, 1 and 0; the two formulas for $k=5$ also hold at $p=5$, where they give 2 and 1.

🆕 **Classical and new:** ours — identities, not fits; the first recovers the size-three super-Vandermonde sets of Sziklai and Takáts [ST, Thm. 1.12].

↳ Used in: Theorem 8 (p. 17)

Proof

Write e_j for the elementary symmetric functions of the elements of T and s_j for the power sums. Under $e_1 = 0$, Newton's identities give $s_4 = 2e_2^2$ and $s_5 = -5e_2e_3$.

For three elements and $s_4 = 0$ one gets $e_2 = 0$, and the distinct triples with $e_1 = e_2 = 0$ are exactly the sets $a\{1, \omega, \omega^2\}$ with ω a primitive cube root, which exist iff $\chi_p(-3) = 1$; there are $(p-1)/3$ of them in that case and 0 otherwise, which is the first formula.

For three elements and $s_5 = 0$, away from characteristic 5, either $e_2 = 0$ or $e_3 = 0$. The triples with $e_3 = 0$ and $e_1 = 0$ are $\{0, a, -a\}$, of which there are $(p-1)/2$; the two families are disjoint, giving the second formula.

For four elements with $e_1 = 0$ the identity $s_5 = -5e_2e_3$ still holds. Let A be the family with $e_2 = 0$ and B the family with $e_3 = 0$. Vanishing of e_3 together with $e_1 = 0$ makes the root polynomial even, so $B = \{\{\pm a, \pm b\} : a, b \neq 0,\ b \neq \pm a\}$ and $|B| = (p-1)(p-3)/8$. The condition $e_2 = 0$ is the quadratic moment condition $s_2 = 0$, whose distinct-coordinate sieve gives $|A| = (p-1)\big(p - 5 - 6\chi_p(-2)\big)/24$. The intersection consists of the sets $\{a, -a, ia, -ia\}$ with $i^2 = -1$, so $|A \cap B| = (p-1)\big(1 + \chi_p(-1)\big)/8$. Inclusion and exclusion give the third formula.

At $p = 5$ the argument for the two counts with $k = 5$ does not apply, since $s_5 = -5e_2e_3$ vanishes identically; but $x^5 = x$ on $\mathbb{F}_5$, so $s_5 = s_1$ and the only condition is $s_1 = 0$. Translation by t shifts the sum of an n-subset by nt, and $n = 3, 4$ are invertible mod 5, so the $\binom{5}{n}$ subsets are spread evenly over the five sums: 2 for $n = 3$ and 1 for $n = 4$, which are the values of the two formulas.

Evidence & scope

- **Program:** against exhaustive enumeration over F_p: 16, 15 and 12 primes; |B| and |A ∩ B| separately. `gates/P3d_tricotomia_Sm.py`
- **Program:** the k = 4 triples are the sets a1, ω, ω², 28 primes 5 ≤ p ≤ 113. `gates/literatura_super_vandermonde.py`

Remark 10. (the case $k = 4$ has a name, and is classified)

p. 12

For $n = 3$ and $k = 4$, Newton under $e_1 = 0$ gives $s_4 = 2e_2^2$, so the condition $s_1 = s_4 = 0$ is $s_1 = s_2 = 0$; a triple of distinct elements with $s_1 = s_2 = 0$ and $s_3 \neq 0$ is precisely a *super-Vandermonde set* of size three in the sense of Sziklai–Takáts [45

] , whose Theorem 1.12 shows that such a set of size $t<p$ is a coset of a multiplicative subgroup — for $t = 3$, exactly the sets $a\{1, \omega, \omega^2\}$ that the proof above produces. Our first formula therefore *recovers* a classification that has been available since 2008, by a different route; we claim nothing for it, and Blokhuis et al. [22] is the current state of that line. What is not in that literature is our actual object: the invariant w_T there is by construction the first non-vanishing moment, so the prescribed condition is always an initial segment $s_1 = \cdots = s_{t-1} = 0$, whereas we prescribe $s_1 = s_k = 0$ and leave everything between them free. Already at $p = 19$ and $k = 6$, all eighteen triples with $s_1 = s_6 = 0$ have $s_2 \neq 0$ and are therefore not Vandermonde sets of any kind.

↳ Not used by another result of the paper.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fajeno!4,colframe=fajeno!55, fontupper=,before skip=6pt,after skip=8pt] fajeno**Remark 10**fajenonot ours — Sziklai–Takáts have it

The structure of the $k = 4$ triples is their Theorem 1.12, and the count $(p - 1)/3$ is a one-line consequence of it. Our first closed form recovers both by a different route, and we say so where the formula appears rather than in a footnote. The remark earns its place for the second half: it identifies, in their own terms, why our object is not in their literature.

Measured: The identification $\{s_1 = s_4 = 0,\ s_3 \neq 0\} = \{s_1 = s_2 = 0,\ s_3 \neq 0\}$ verified in the 28 primes $5 \leq p \leq 113$, together with the description of those triples as $a\{1, \omega, \omega^2\}$ and the count $(p - 1)/3$ when $p \equiv 1 \pmod 3$. See `gates/literatura_super_vandermonde.py`.

Measured: All three identities checked against exhaustive enumeration over $\mathbb{F}_p$: the first in the 16 primes $5 \leq p \leq 61$, the second in the 15 primes $7 \leq p \leq 61$, the third in the 12 primes $7 \leq p \leq 47$, in every case with no exception; and the two auxiliary counts $|B|$ and $|A \cap B|$ checked separately by enumeration. See `gates/P3d_tricotomia_Sm.py`.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Theorem 9**fnuestroours — identities, not fits

Three inclusion–exclusion computations off Newton's identities $s_4 = 2e_2^2$ and $s_5 = -5e_2e_3$. They are here because Theorem 8 asserts that they exist and a classification that cannot exhibit its own positive cases is not one. What the note adds is the control: each identity is checked against exhaustive enumeration over $\mathbb{F}_p$, which is the strongest test available and the one that would catch a slip in any of them.

count	closed form	why no obstruction	checke
$C_3(n,p)$, $n=3,4,6$	see [37]	rational, or none	11/33 primes
$C_4(3,p)$	$\frac{p-1}{6}\big(1+\chi_p(-3)\big)$	no length-four stratum	16 primes
$C_5(3,p)$	$\frac{p-1}{6}\big(4+\chi_p(-3)\big)$	no length-four stratum	15 primes
$C_5(4,p)$	$\frac{p-1}{24}\big(4p-17-6\chi_p(-2)-3\chi_p(-1)\big)$	the witness is a conic	12 primes
$C_7(3,p)$	$\frac{p-1}{6}\big(4+\chi_p(-3)\big)$	s_7 is a monomial	53 primes
$C_6(3,p)$	$(p-1)\cdot\mathbf{1}\{2Y^3+3Y-3 \text{ splits}\}$	*a nonabelian class function*	17 primes

Table 2: Every count this note and its companion put in closed form, with the reason the length-four obstruction failed to appear in each. The last row is tinted differently because it is closed but not in quadratic characters — it is the subject of Section 6.

Colour: red = no / fails.

6 Two different failures, and only one of them is a trace

The column $n=3$ of Figure 1 survives for every k, because a zero-dimensional variety contributes an Artin character — a genuine one, H^0 of a finite scheme being a permutation representation. That is a weaker statement than it looks, because the count is a *combination* of such characters and combinations need not be characters; the first place it bites is $k=6$.

Proposition 11. p. 13

> *For $p \nmid 66$,*

$$C_6(3,p) = (p-1)\cdot \mathbf{1}\{\, 2Y^3+3Y-3 \text{ splits completely over } \mathbb{F}$$

The cubic $2Y^3+3Y-3$ is irreducible over $\mathbb{Q}$ with discriminant $-1188 = -36\cdot 33$, so its Galois group is S_3 and complete splitting is not determined by any congruence on p.

🆕 **Classical and new:** ours (the paper's card).

↳ Used in: Theorem 8 (p. 17)

Proof

Newton with $e_1 = 0$ gives $s_6 = -2e_2^3 + 3e_3^2$, and a solution with distinct entries has $e_2 e_3 \neq 0$. So $s_6 = 0$ says exactly

$$\frac{e_2^3}{e_3^2} = \frac{3}{2},$$

a condition on the scaling invariant alone. Scaling the three roots by t sends $e_j \mapsto t^j e_j$, so $t = e_2/e_3$ makes e_2 and e_3 equal, and their common value is $e_2^3/e_3^2 = \frac{3}{2}$: the normalised polynomial is $Y^3 + \frac{3}{2}Y - \frac{3}{2}$, one half of $2Y^3+3Y-3$. When that splits, its nonzero scalings give exactly $p-1$ distinct subsets. The discriminant is computed directly; it is not a square, so the Galois group is S_3 and not C_3, and Chebotarev distinguishes the identity class from a 3-cycle inside any fixed cyclotomic congruence condition.

Evidence & scope

- **Program:** against exhaustive enumeration in the 17 primes $5 \le p \le 71$ with $p \nmid 66$; density of split primes 0.160 below 400. `gates/P3d_tricotomia_Sm.py`

Theorem 12. (the column $n = 3$) p. 14

For every prime $p \nmid 6k\mathfrak{D}_k$,

$$\frac{6\,C_k(3,p)}{p-1} = \big[e_2 \mid s_k\big]\big(1+\chi_p(-3)\big) + 3\big[e_3 \mid s_k\big] + 6\,\#\{u_0 \in \mathbb{F}_p :\ Q_k(u_0) = 0,\ f_{u_0} \text{ splits compl}$$

with f_u as in (7). Consequently $C_k(3,p)$ is elementary — expressible in quadratic characters of fixed integers — if and only

if Q_k is constant, that is, if and only if s_k is a monomial in e_2 and e_3. That happens exactly for

$$\boxed{k \in \{3, 4, 5, 7\}}.$$

🆕 **Classical and new:** ours — the count, not the polynomials: Q_k and the reduction to u are in Helou, Tzermias and Nanninga [Helou; Tzermias; NanA].

↳ Used in: Corollary 17 (p. 31)

Proof

The factor e_2 contributes the triples with $e_1 = e_2 = 0$, which are the sets $a\{1, \omega, \omega^2\}$ and number $(p-1)(1+\chi_p(-3))/6$; the factor e_3 contributes $\{0, a, -a\}$, of which there are $(p-1)/2$; and the two families meet only in the zero triple. Each root u_0 of Q_k is an invariant of the scaling action, and the subsets realising it form a single orbit of $\mathbb{F}_p^\times$: if T has invariant $u_0 \neq 0$ and $tT = T$ then $t^2 e_2 = e_2$ and $t^3 e_3 = e_3$, and $e_2 e_3 \neq 0$ forces $t^2 = t^3 = 1$, hence $t = 1$. The action is therefore free and the orbit has exactly $p-1$ elements, so u_0 contributes $p-1$ subsets when f_{u_0} splits into three distinct factors over $\mathbb{F}_p$ and none otherwise. This proves the displayed identity. For the criterion, one direction is immediate: if Q_k is constant the identity has only the two character terms. The other is not, and it is where the work is: if $\deg Q_k > 0$ then Proposition 13 and Lemma 14 show the fibre contribution is not PORC, so *a fortiori* it cannot be written in quadratic characters. For the list $\{3, 4, 5, 7\}$, the four monomials are $s_3 = 3e_3$, $s_4 = 2e_2^2$, $s_5 = -5e_2 e_3$ and $s_7 = 7e_2^2 e_3$; that no other k joins them is not a computation but Proposition 15 below, which gives $\deg Q_k$ in closed form for every k and shows it vanishes exactly there.

🛡️ **Evidence & scope**

- **Program:** the identity against exhaustive enumeration for 3 ≤ k ≤ 14 and primes 5 ≤ p ≤ 257 with p ∤ 6kD_k (620 pairs), with two failing controls. `gates/P3d_columna_n3.py`

Proposition 13. (an S_3-fibre exists) p. 14

If $\deg Q_k > 0$ then Q_k has a root u_0 for which $f_{u_0}(Y) = Y^3 + u_0 Y - u_0$ has Galois group S_3 over $\mathbb{Q}(u_0)$.

🆕 **Classical and new:** unconditional, for every k (the paper's card): the inequality A < 2^d for k ≥ 38 and forty printed certificates for 6 ≤ k ≤ 46.

↳ Used in: Theorem 12 (p. 23), Lemma 14 (p. 25)

🛡️ **Evidence & scope**

- **Program:** for 6 ≤ k ≤ 46 with d > 0: roots of Q_k real, positive and simple (Sturm), P_k irreducible modulo the printed prime (Table 3). `gates/P3d_s3_certificados.py`
- **Program:** the raw leading coefficient 2 or k and A | k, by a separate route for 3 ≤ k ≤ 400. `gates/P3d_lc_Qk.py`

Lemma 14. (the nonabelian part cannot cancel) p. 15

> *Let $L/\mathbb{Q}$ be a finite Galois extension containing the roots of Q_k and of every f_{u_0} for u_0 a root of Q_k, and let $G = \mathrm{Gal}(L/\mathbb{Q})$. Fix a G-orbit $\mathcal{O}$ of roots of Q_k, let H be the stabiliser of one of them, and let $K = \ker\big(H \to S_3\big)$ for the action of H on the three roots of that fibre's cubic. For p unramified in L and $p \nmid 6k\mathfrak{D}_k$, let $N_{\mathcal{O}}(p)$ be the number of roots of Q_k in $\mathcal{O}$ that lie in $\mathbb{F}_p$ and whose cubic splits completely. Then*
>
> $$\boxed{|H/K|\; N_{\mathcal{O}}(p) \;=\; \chi_{E[G/K]}(\mathrm{Frob}_p)}, \qquad \text{so} \qquad 6\,N_{\mathcal{O}}(p) = \frac{6}{|H/}$$
>
> *with E a splitting field for G as in (5), the factor $6/|H/K|$ being a positive rational. If moreover $H/K \simeq S_3$ — which Proposition 13 provides for some orbit, and where the factor is 1 — then $E[G/K]$ has an irreducible constituent of dimension greater than one. Since the orbits enter Theorem 12 with coefficient $+1$ each, that constituent cannot cancel, and $C_k(3,p)$ is not PORC.*

🆕 **Classical and new:** ours (the paper's card).

↳ Used in: Theorem 12 (p. 23)

Proof

> A coset gK is determined by the pair consisting of the root $g(u_0) \in \mathcal{O}$ and the labelling of the three roots of $f_{g(u_0)}$ induced by g; the fibre of this correspondence over a root is H/K, of size 6 exactly when $H/K \simeq S_3$. Now Frob_p fixes gK exactly when it fixes $g(u_0)$ and acts trivially on the three roots of its cubic, that is, exactly when that root lies in $\mathbb{F}_p$ and its cubic splits completely. Each such root therefore contributes $|H/K|$ fixed cosets and no other coset is fixed, which is the displayed

identity, the character of a permutation representation being the number of fixed points.

For the second claim, H/K acts on the subset $\{hK\} \subseteq G/K$ by left translation, and that action is regular, so the image of G in $\mathrm{Sym}(G/K)$ contains a subgroup isomorphic to $H/K \simeq S_3$ and is not abelian. A representation all of whose irreducible constituents are one-dimensional has abelian image; hence $E[G/K]$ has a constituent of dimension at least two. The coefficient field must be E and not $\mathbb{Q}$ here: over E every irreducible of an abelian group is one-dimensional, whereas over $\mathbb{Q}$ an abelian group can have irreducibles of larger dimension — already $\mathbb{Q}[C_3] = \mathbb{Q} \times \mathbb{Q}(\zeta_3)$ has one of dimension two — so over $\mathbb{Q}$ the dimension alone would not exclude an abelian quotient. A PORC function is, by (5), one whose coefficients factor through an abelian quotient, and no such coefficient contains that constituent.

Evidence & scope

- **Program:** the identity 6N = χ_E[G/K](Frob_p) at k = 6 in 75 primes below 400, both sides computed independently, with a cyclic decoy. `gates/P3d_caracter_regular_S3.py`

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Lemma 14**fnuestroours

The lemma is the step from "some fibre has group S_3" to "the count is not PORC". The intuition that a nonabelian fibre cannot be cancelled by the others is right, but turning it into a proof needs two things: the fibres organised as one permutation representation $E[G/K]$, and the orbits entering with one sign, which is what Theorem 12 supplies. Nothing in the argument is deep, and the lemma is short.

Measured: The identity $6N_{\mathcal{O}}(p) = \chi_{E[G/K]}(\mathrm{Frob}_p)$ in the case $k = 6$, where it can be checked and not merely argued: $\deg Q_6 = 1$, its root $3/2$ is rational, so $H = G$, $K = 1$ and $E[G/K]$ is the regular representation of S_3 — a group already split by $E = \mathbb{Q}$, so that the check is a check over $\mathbb{Q}$. Both sides agree in all 75 primes $5 \le p < 400$ with $p \nmid 66$, with no exception, and neither is computed from the other: the left from a direct count of $C_6(3, p)$ over $\mathbb{F}_p$, the right from the factorisation type of the cubic modulo p. A decoy replacing the cubic by $Y^3 - 3Y - 1$, of square discriminant and cyclic group, correctly fails to support the argument. See `gates/P3d_caracter_regular_S3.py`.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Proposition 13**fnuestrounconditional, for every k

The "only if" half of Theorem 12 is not immediate: it needs some fibre to have group S_3, and that is a statement about Q_k, not about the sieve. Appendix A proves it: all roots of Q_k real, positive and simple; no irreducible C_3-fibres; the divisibility $\mathrm{lc}(Q_k) \mid k$, which is Waring's formula read at the extreme monomial and gives $A \le k$; the inequality $A < 2^{\deg Q_k}$, which $A \le k$ secures for every k except the twenty-nine values $k \le 37$ with $\deg Q_k > 0$ and $k \ge 2^{\deg Q_k}$; and exact irreducibility certificates for P_k covering all $6 \le k \le 46$, which contains them. No step is left measured. The classification of Theorem 8 for $n \ge 4$ does not depend on any of this.

Appendix A carries the proof in full, with its certificates; Section 8 says what about the family Q_k remains open, and it is not this. *Measured*: The identity checked against exhaustive enumeration for every $3 \le k \le 14$ and every prime $5 \le p \le 257$ with $p \nmid 6k\mathfrak{D}_k$ — between 50 and 53 of the 53 primes in that range for each k, 620 pairs (k, p) in all — with no exception; replacing f_u by $Y^3 - uY - u$, or dropping the splitting condition, makes it fail. The factorisations of s_k, the degree of Q_k and $\mathfrak{D}_k \neq 0$ computed exactly for $k \le 30$. Note in particular $C_7(3, p) = (p-1)(4 + \chi_p(-3))/6$, the same closed form as $C_5(3, p)$. See `gates/P3d_columna_n3.py`.

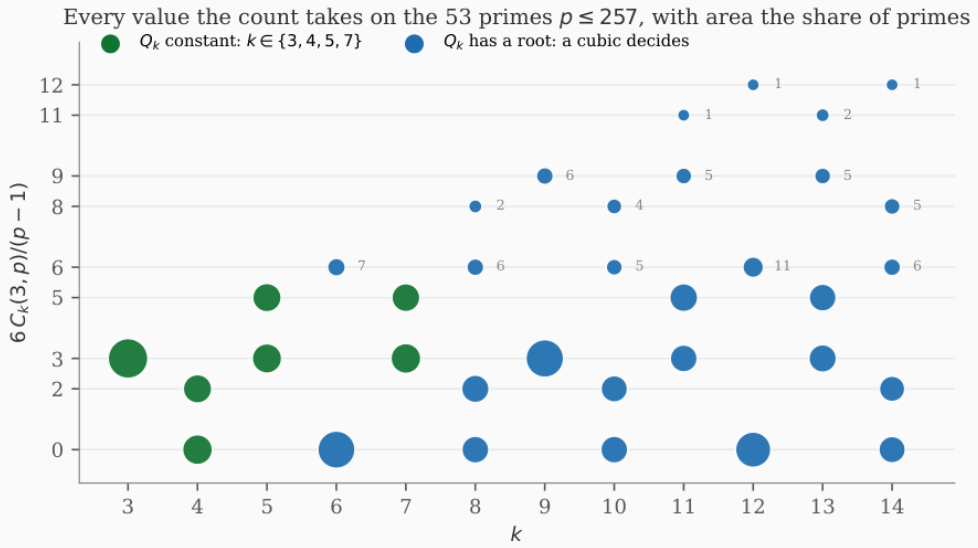
[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Theorem 12**fnuestroours — the count, not the polynomials

The polynomials and the reduction to u are Helou's [16] and are cited above. What is stated here is arithmetic over $\mathbb{F}_p$: that the subset count decomposes with no remainder into the two character families and one term of size $p-1$ per split fibre, and that it is expressible in quadratic characters exactly when Q_k is constant. That question is not the one [16 , 41 , 33] ask — they work over $\mathbb{Q}$ and towards Fermat — and the list $\{3, 4, 5, 7\}$ is the answer to ours.

Figure 5 is that measurement rather than the statement: it shows every value the count takes, and the decomposition can be read off it directly — the elementary k occupy one or two levels, and every other k climbs in steps of six, one step per root of Q_k whose cubic splits.

The list $\{3, 4, 5, 7\}$ looks accidental. It is not: it is the zero set of a formula.

Figure 5



Theorem 12 measured rather than stated: every value $6C_k(3,p)/(p-1)$ takes on the 53 primes $p \le 257$ (omitting $p \mid k$), with the area of each disc the share of primes giving it and the count printed for the rare ones. The green columns are the four elementary k; everywhere else the values climb in steps of 6, one step per root of Q_k whose cubic splits, on top of the 0 or 2 contributed by e_2 and the 3 contributed by e_3.

Proposition 15. (the degree of Q_k) p. 16

> *For every $k \ge 3$,*
>
> $$\boxed{\deg Q_k = \left\lfloor \frac{k}{6} \right\rfloor - \left[\, k \equiv 1 \pmod 6 \,\right]}.$$
>
> *In particular $\deg Q_k = 0$ exactly for $k \in \{3,4,5,7\}$, and since the degree is nondecreasing along each residue class modulo 6, no further k can return to zero.*

Lean · ours, in part **show**

added to the Lean repository after publication (21-oct-2026): the count #{(a, b) : 2a + 3b = k} = ⌊k/6⌋ + 1 − [k ≡ 1 mod 6] for every k

- `P3d.card_degreePairs`
- `P3d.card_degreePairs_eq_one_iff`

✅ Checked when this page was built: DegreeCount.lean compiles with Lean 4.35.0, no errors, no sorry. Axioms — card_degreePairs, card_degreePairs_eq_one_iff: propext, Classical.choice, Quot.sound.

Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean DegreeCount.lean` (SHA-256 of the compiled file: `55e85b8ae935ef0d`…; a source page on this site may show it with comments edited, under its own hash).

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Lean: 2 results, standard axioms only

Proof: in this note · **Covers:** not formalized · **Cite:** Lemma 1, p. 4, doi:10.5281/zenodo.22886543

🆕 **Classical and new:** for odd k the number is Helou's r_k [Helou]; the paper claims neither, only a self-contained proof for all k.

↳ Used in: Theorem 12 (p. 23)

Proof

Newton–Waring at $e_1 = 0$ is (9) below, and no coefficient there vanishes, so the monomials of s_k are exactly the pairs $(a, b) \geq 0$ with $2a + 3b = k$. Those pairs form a chain: b runs over the integers with $b \equiv k \pmod 2$ and $0 \leq b \leq k/3$, and a is determined. Dividing out the common monomial leaves consecutive powers of $u = e_2^3/e_3^2$, whence

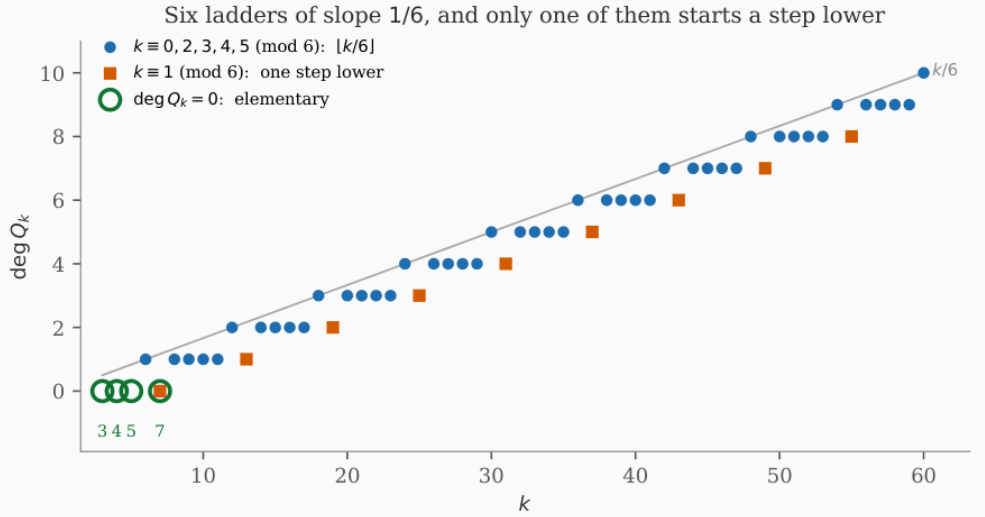
$$\deg Q_k = \#\{(a, b) \geq 0 : \ 2a + 3b = k\} - 1.$$

Counting the admissible b gives $\lfloor k/6 \rfloor + 1$ in every residue class except $k \equiv 1 \pmod 6$, where the parity constraint costs one, and subtracting 1 is the formula.

Evidence & scope

- **Program:** both sides independently for 3 ≤ k ≤ 90, and every proper factor of s_k homogeneous in u. `gates/P3d_grado_Qk.py`

Figure 6



Proposition 15. The grey line is $k/6$. What the picture adds to the formula is that the exceptional class is a single ladder rather than a scatter of exceptions, and that the four circled points are the only ones that will ever touch zero.

Two computational facts about the family are worth recording, because the criterion of Theorem 12 is only useful if Q_k can be produced. Specialising the Newton–Waring formula to $e_1 = 0$ gives

$$s_k \;=\; k \sum_{\substack{a,b\ge 0\\ 2a+3b=k}} (-1)^a \,\frac{(a+b-1)!}{a!\,b!}\, e_2^a e_3^b, \quad (9) \tag{15}$$

in which no coefficient vanishes. And writing $R_k(u) = u^{-\lceil k/3\rceil} s_k(u,u)$, so that R_k is Q_k up to the integer content, one has the two recursions

$$R_k = R_{k-3} - u^{\,[3|k]} R_{k-2}, \qquad R_{k+18} = (3-2u)R_{k+12} - (u^2+6u+3)R_{k+6} + R_k.$$

The second has coefficients independent of k and order three, which is what one should expect: if y_1, y_2, y_3 are the roots of $Y^3 + uY - u$, the three numbers $\beta_i = y_i^6/u^2$ have elementary symmetric functions $3-2u$, u^2+6u+3 and 1, and R_{k+6} is the corresponding power sum. There is no reason to look for a two-term Chebyshev-like relation.

Measured: (9) against the recursion for $2 \le k \le 60$; both recursions verified symbolically, the first for $3 \le k < 40$ and the second for $0 \le k \le 21$; and the three symmetric functions of the β_i computed from the power sums s_6 and s_{12} without extracting roots. See `gates/P3d_familia_Qk.py`.

Proposition 16. (the degree is a dimension of modular forms)

p. 18

Substitute $e_2 = -3E_4$ and $e_3 = 2E_6$, with E_4, E_6 the normalised Eisenstein series. Then $\mathcal{F}_k = s_k(-3E_4, 2E_6)$ is a modular form of weight $2k$ for $\mathrm{SL}_2(\mathbb{Z})$, and since $M_*(\mathrm{SL}_2(\mathbb{Z})) = \mathbf{C}[E_4, E_6]$ a basis of M_{2k} is indexed by the solutions of $2a + 3b = k$ — the same set that indexes the terms of s_k. Hence

$$\boxed{\dim M_{2k} = \deg Q_k + 1},$$

and $\dim M_{2k} = 1$ exactly for $k \in \{3, 4, 5, 7\}$.

Proof: in this note · **Covers:** not formalized · **Cite:** Proposition 16, p. 18, doi:10.5281/zenodo.22886543

NEW **Classical and new:** the dictionary M_* = C[E₄, E₆] is standard [Milne, Prop. 4.16]; what is used is the coincidence of index sets.

↳ Used in: Corollary 17 (p. 31)

Evidence & scope

- **Program:** dim M_2k = deg Q_k + 1 for $3 \le k \le 60$; Waring's formula against the recursions. `gates/P3d_familia_Qk.py`

This is what makes the exceptional class conceptual rather than accidental. The four weights are $6, 8, 10, 14$, and the corresponding forms are E_6, E_8, E_{10}, E_{14}: weight 14 is still one-dimensional *after* weight 12 has reached dimension two, because that is where the first cusp form Δ appears. The class $k \equiv 1 \pmod 6$ is one step behind the others in the degree for the same reason that $\dim M_{2k}$ lags there. Normalising by the constant term $2^k + 2(-1)^k$ gives those four Eisenstein series on the nose; already for $k = 6$ the form is not Eisenstein, since $\mathcal{F}_6/66 = (9E_4^3 + 2E_6^2)/11$, and Q_k records the zeros of $\mathcal{F}_k$ that survive after the elliptic points are removed.

Corollary 17. (the criterion is a dimension) p. 18

For every $k \ge 3$,

$$\boxed{C_k(3, p) \text{ is elementary} \iff \dim M_{2k}(\mathrm{SL}_2(\mathbb{Z})) = 1.}$$

Proof: in this note · **Covers:** not formalized · **Cite:** Corollary 17, p. 18, doi:10.5281/zenodo.22886543

NEW **Classical and new:** ours — but only the joining of two halves (the paper's card).

↳ Not used by another result of the paper.

Proof

> By Theorem 12, $C_k(3,p)$ is elementary if and only if $\deg Q_k = 0$, and by Proposition 16 that is $\dim M_{2k} = 1$. The one-dimensional weights are $2k \in \{4,6,8,10,14\}$, and $2k = 4$ is excluded by $k \geq 3$; the remaining four are the list of Theorem 12.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fnuestro!4,colframe=fnuestro!55, fontupper=,before skip=6pt,after skip=8pt] fnuestro**Corollary 17**fnuestroours — but only the joining of two halves

Neither half is new here: the criterion $\deg Q_k = 0$ is Theorem 12 and the dimension formula is classical. What the corollary contributes is that they are the same condition, which is what turns an arbitrary-looking list into one sentence. The proof is three lines and the content is the identification, not the argument.

Measured: $\dim M_{2k} = \deg Q_k + 1$ for $3 \leq k \leq 60$, against the degrees computed by factoring s_k, and $\dim M_{2k} = 1$ exactly on $\{2,3,4,5,7\}$ for $k<200$ — with $k = 2$ outside the range $k \geq 3$ of this note, which is why the corollary's list has four entries and not five. See `gates/P3d_familia_Qk.py`.

That is the statement to remember. The list $\{3,4,5,7\}$ looks arbitrary and is not: it is the one-dimensional weights $6,8,10,14$, read through a sieve over $\mathbb{F}_p$. The reason 6 drops out and 7 comes back is the cusp forms: $S_w = \Delta\, M_{w-12}$, so $\dim M_{12} = 2$ because Δ itself is there, while $S_{14} = \Delta M_2 = 0$ because $M_2 = 0$ — and weight 14 is one-dimensional again. It is the *gap* above the first cusp form, not a position below it.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fajeno!4,colframe=fajeno!55, fontupper=,before skip=6pt,after skip=8pt] fajeno**Proposition 16**fajenothe dictionary is standard

The structure $M_* = \mathbf{C}[E_4, E_6]$ and the resulting basis of M_{2k} are classical; see for instance [28 , Prop. 4.16] . What is used here is only the coincidence of index sets, and the consequence for $\deg Q_k$ follows from Proposition 15.

Measured: Both sides computed independently for $3 \leq k \leq 90$ — the left by factoring s_k in $\mathbb{Z}[e_2, e_3]$ and reading the degree in u, the right by the formula — with no discrepancy; and every proper factor of s_k verified to be homogeneous in u over the same range. See `gates/P3d_grado_Qk.py`.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fajeno!4,colframe=fajeno!55, fontupper=,before skip=6pt,after skip=8pt] fajeno**Proposition 15**fajenothe number is Helou's; the proof above is self-contained

For odd k this degree is Helou's $r_k = (k-3-2b)/6$ [16] , with b as in Section 6, restated in [41 , § 2] , and our closed form $\lfloor k/6 \rfloor - [k \equiv 1]$ is the same number written differently; for even k it is the construction that [34 , § 5.4] states can be carried out. We claim neither.

What the proof above adds is only that it needs neither: counting the solutions of $2a + 3b = k$ settles all k at once, which matters because Theorem 12 rests on the consequence — the degree is monotone along each residue class, so no k beyond $\{3, 4, 5, 7\}$ can return to zero.

Theorem 12 also settles the two shades of Figure 1. Call the *group of the class function* the smallest finite quotient of $G_{\mathbb{Q}}$ through which the class function above factors. A sufficient criterion for it to be exactly S_3 is that two things hold at once: Q_k has a single *rational* root, so that there is one fibre and it is defined over $\mathbb{Q}$; and $e_2 \nmid s_k$, so that the count does not also carry $\chi_p(-3)$. We do not claim the criterion is necessary for every k. The second condition is not by itself enough to force $S_3 \times C_2$, and the missing step is arithmetic rather than formal: the quadratic subfield of the fibre cubic's splitting field is generated by $\sqrt{\operatorname{disc} f_{u_0}}$, and it coincides with $\mathbb{Q}(\sqrt{-3})$ exactly when that discriminant is -3 times a square. It never does here — for $k = 8, 10, 11, 13$ the squarefree parts are $-43, -57, -31, -35$ — so the two fields are distinct, the compositum has degree twelve, and the group is $S_3 \times C_2$. In the range of Figure 1 the computation shows that the criterion is met exactly for $k = 6, 9$, and those are the cells drawn darker.

Measured: For $3 \le k \le 14$: the degree of Q_k, the rationality of its roots, whether $e_2 \mid s_k$, the discriminant of the fibre cubic and its squarefree part, each computed separately; the four discriminants above are checked not to be -3 times a square, with a control showing the check can see the case where one is. See `gates/P3d_grupo_del_caracter.py`.

Remark 18. (what the column is really counting) p. 19

Normalise the cubic attached to a root u of Q_k as $f_u(Y) = Y^3 + uY - u$, with $\operatorname{disc}(f_u) = -u^2(4u + 27)$, and let E_u be the elliptic curve $V^2 = f_u(Y)$, of j-invariant $6912u/(4u + 27)$. Then

$$\boxed{f_u \text{ splits completely over } \mathbb{F}_p \iff E_u[2] \subseteq E_u(\mathbb{F}_p)},$$

because $S_3 = \mathrm{GL}_2(\mathbb{F}_2)$ acting on the three nonzero 2-torsion points is exactly the Galois action on the roots. So at $n = 3$ the count is of fibres with fully rational 2-torsion, over a finite set of values of the modular parameter. This resolves what looks like a paradox in Observation 20: there are elliptic curves behind the zero-dimensional problem too, but what is counted there is their *torsion*, which takes finitely many states, and not their trace.

↳ Not used by another result of the paper.

Measured: $\operatorname{disc}(Y^3 + uY - u) = -u^2(4u + 27)$ and, for $k = 11$, $u = 1$ giving $Y^3 + Y - 1$ of discriminant -31 and Galois group S_3. See `gates/P3d_familia_Qk.py`.

Remark 19.

(a null that a short window would have manufactured) p. 20

For $k = 9$ one has $s_9 = -3e_3(3e_2^3 - e_3^2)$, so the count should take two values. Over the 14 primes $5 \le p \le 53$ it takes *one*: the second family first appears at $p = 71$, and then at $83, 97, 131, 193, 257$. A family of Chebotarev density $1/6$ is expected about twice in fourteen primes, so its absence there is not evidence of absence. We record this because the criterion is general: a null result on a window too short to see the predicted density is not a null result.

↳ Not used by another result of the paper.

So under the narrow reading — coefficients in quadratic characters of fixed integers — even $n = 3$ stops being elementary at $k = 6$; under the broad reading, arbitrary Artin-type class functions, $n = 3$ is elementary for every k. The classification of Theorem 8 is stated for the broad reading, and Figure 1 keeps the two apart by colour. The distinction is not a blemish: it is the reason the two halves of this note fail to be *PORC* — polynomial on residue classes, in Higman's sense [10] — for structurally different reasons.

Observation 20.

(the two failures are not the same failure; cf. [17]) p. 20

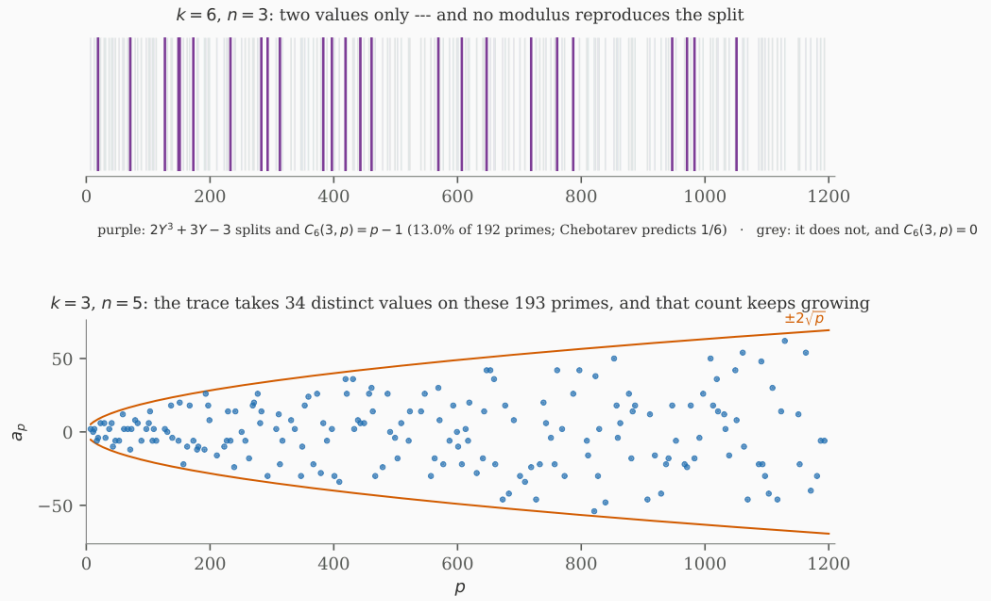
At $n = 3$, $k = 6$ the count takes exactly two polynomial values, $p - 1$ and 0, and the partition of the primes between them is a splitting condition in a nonabelian extension — the class function is the indicator of a conjugacy class, not a character. It is therefore not PORC but it *is* polynomial on Frobenius sets, POFS in the sense of Stanojkovski–Voll [47 , § 1.5.2] . For $n \ge 4$ the surviving object is the Frobenius trace of a curve of positive genus, and the count is not POFS either — not because of how many values it takes, but because a POFS function is Artin–Tate in the sense of (5) and Theorem 8 rules that out by weight one. The two failures are therefore separated by *weight*, and the numerical growth of the set of values is an illustration of the difference rather than the argument for it. The archetype usually offered for the first mode is du Sautoy–Vaughan-Lee [5] , whose non-PORC behaviour is likewise a finite-valued count partitioned by a nonabelian splitting condition rather than a surviving trace; Isham's separation [17 , § 2.4.2] is the one that already contains both.

↳ Not used by another result of the paper.

Measured: For $n = 3$, $k = 6$: exactly two values across all $p \le 2000$ with $p \nmid 66$, and no modulus among $4, 6, 8, 12, 24, 33, 36, 44, 66, 72, 99, 132, 264, 396$ and 1188 — the last being the discriminant itself — assigns a single value to every residue class. For $n = 5$, $k = 3$: the number of distinct Frobenius traces of the conductor-20 curve grows $15 \to 24 \to 31 \to 52$ as the window grows $p \le 200, 500, 1000, 2000$ ($p \nmid 20$), while the control quantity $\chi_p(-3)$ takes two values on the same window. Four windows fix no exponent and none is claimed: one quantity is bounded by a theorem, while the observed support of the other keeps growing across these windows, and that is the distinction Observation 20 draws. See `gates/P3b_pofs_vs_porc.py`.

Figure 7 puts the two measurements on one page, which is the only place in this note where the two failures can be compared directly rather than described in turn.

Figure 7



Observation 20, measured. Both panels show a failure of polynomiality on residue classes, and they are different failures: above, a two-valued count whose partition of the primes no modulus reproduces; below, a growing set of observed Frobenius traces. The “not POFS” conclusion comes from weight one and not from this numerical growth: one quantity is bounded by a theorem, while the observed support of the other keeps growing across these windows. A reader who wants a single picture of why “not PORC” is too coarse a verdict for this classification should look at these two panels together.

[enhanced,sharp corners=downhill,boxrule=0.4pt,left=5pt,right=5pt, top=3pt,bottom=3pt,colback=fajeno!4,colframe=fajeno!55, fontupper=,before skip=6pt,after skip=8pt] fajeno**Observation 20**fajenonot ours — Isham has it

The coexistence of the two modes in one classification, and their separation by the size of the contribution, is already in Isham [17 , § § 2.3.3, 2.4.2] : her Example 2.3.8 isolates a zero-dimensional stratum $z^3 - z - 1$ with Galois group S_3 and notes that a nonabelian group makes the count nonquasipolynomial, her Proposition 2.3.7 bounds all such strata by a constant independent of q, and §2.4.2 contrasts that $O(1)$ with a Frobenius trace equidistributed on $[-2\sqrt{p}, 2\sqrt{p}]$. It is the engine of her proof, not a remark. What is not in that treatment is the *positive* half — that the bounded mode is still POFS in the sense of [47 , § 1.5.2] — and that is all we add here.

7 Where this sits

Almost every ingredient of this note belongs to someone else, and the list is long enough to be worth reading as one: the polynomial family and its S_3 reduction to Cauchy and Liouville in 1839, Mirimanoff in 1903 and Helou in

1997; the criterion for four roots of unity to Mann in 1965; the vanishing of H^1 in higher dimension to Ghorpade and Lachaud; the sieve to Li and Wan; the triples of Remark 10 to Sziklai and Takáts in 2008; the coexistence of the two failure modes to Isham in 2021; and the vocabulary for that coexistence to Stanojkovski and Voll. What is left is a single question about counting over $\mathbb{F}_p$, and it is worth asking why so small a residue survives so much company.

The answer is not that nobody looked. It is that the neighbouring literature mostly cannot state the question in its own language. The exact evaluation frameworks that include the first moment — the Vandermonde sets of [45 , 22] and the consecutive pair of [36 , 35] — prescribe an *initial segment* $s_1 = \cdots = s_m = 0$; so does the decision problem of [18] , which is discussed below and which bounds rather than evaluates. Two frameworks are more general in the index set, and both stop short in a different way: they do not evaluate in the regime $d_1 = 1$ that our pairs live in, d_1 being the smallest prescribed exponent in the notation of [15] . Giménez, Matera, Pérez and Privitelli [14] allow an *arbitrary* index set $I = \{i_1 < \cdots < i_m\}$ subject to $i_m \le n - 3$, which includes our $I = \{1, k\}$ exactly in the range $k \le n - 3$, and Gottig, Pérez and Privitelli [15] allow non-consecutive exponents; both obtain bounds for each factorisation pattern — bounds, not an evaluation, and it is the evaluation that the gap between the indices governs. The hypothesis $2 \le d_1$ of [15] excludes the first moment outright. For the Vandermonde sets the initial segment is not a convention but the definition: the invariant w_T is the first non-vanishing moment, so a set with $s_1 = s_6 = 0$ and $s_2 \neq 0$ is simply not a Vandermonde set of any kind, and at $p = 19$ that is every one of the eighteen triples. The gap between the two prescribed indices is invisible there by construction.

And the gap is where the arithmetic is. With consecutive indices the conditions become a congruence in a truncated unit group and the character sums are Gauss sums of known value — that is exactly why [36 , 35] close the case $\{1, 2\}$ for every subset size. Leave one index out and the coset structure goes with it: $s_1 = s_3 = 0$ forces $e_1 = e_3 = 0$ with e_2 free, the length-four strata become plane curves, and a Frobenius trace can survive. The classification of this note is, in that light, a map of where the gap bites.

The consecutive pair $\{1, 2\}$ over $\mathbb{F}_q$ with both moments zero is settled, and settled for *every* subset size: Nguyen [36 , Thm. 2.11] and Zhang, Zheng, Wang and Yuan [35 , Cor. 21] evaluate every Li–Wan stratum in closed form, uniformly in the subset size n — the pair of exponents there is fixed at $\{1, 2\}$, so the uniformity is in n and not in our second exponent k. The reason that works is structural and it is exactly the reason it does not transfer. The pair $\{1, 2\}$ makes the conditions a congruence $\prod_i (1 + x_i y) \equiv 1 \pmod{y^3}$, a coset in a truncated unit group whose characters are quadratic Gauss sums with known exact values; weight one is present but it is never unknown. Our pair $\{1, 3\}$ gives $e_1 = e_3 = 0$ with e_2

free, which is not a congruence of that shape, and the length-four strata are plane curves whose traces are not determined by anything smaller. The first non-consecutive pair is where an unknown Frobenius trace can appear, and Theorem 8 says exactly when it does.

On the decision side, Lai–Marino–Robinson–Wan [18] decide positivity of the consecutive m-th moment subset count in polynomial time for fixed m; they use the same Li–Wan sieve, but to bound each stratum by $((mn+1)\sqrt{q})^{e_i}$, and the distinction our classification turns on is precisely what such a bound discards. Their framework reaches the index set $\{1,3\}$ in one place only: they may drop the moments with $p \mid j$, and dropping $j=2$ while keeping 1 and 3 requires $p=2$. That is the characteristic in which Moisio and Ranto [27] found the same index pair producing elliptic curves for the opposite factorisation type — a second independent arrival at $\{1,3\}$ in characteristic two, and a third in all, by a route that meets neither of the others.

Exact counts for systems of two diagonal equations exist in a few families — Cao–Chou–Gu [11] for $\sum X_i = \sum X_i^{p^\ell+1} = 0$ over $\mathbb{F}_{p^{2\ell t}}$, and Castro–Rubio–Guan–Figueroa [12] for the Waring number of the same exponent family — but these count *tuples* rather than subsets of distinct elements, which is the condition that produces the partition sieve in the first place, and their exponent is tied to the characteristic: $p^\ell+1=3$ forces $p=2$, so the fixed exponent 3 over an odd prime field is not reachable there. Gottig–Pérez–Privitelli, besides the hypothesis $2 \le d_1$ already noted, work with unit coefficients rather than the repeated weights (1) produces.

Finally, the shape of this story is not new even if the object is. Kontsevich conjectured that graph hypersurfaces have (quasi-)polynomial point counts; Stembridge [46] verified it for small graphs, Belkale and Brosnan [1] disproved it in general, and Brown and Schnetz [3] exhibited explicit counterexamples whose counting functions involve a modular form of a singular K3 surface. Closed forms in the small cases, and a surviving motive after them, is a recurring pattern; what varies is the weight at which the survival happens. Here it is weight one, which is why at $k=3$, $n=5$ an elliptic curve and not a modular form of higher weight is what one meets; at $k=5$, $n=6$ it is the genus-five curve of Section 8.

One last observation belongs here rather than in the appendix, because it is about the object and not about the people. The identity behind the family E_k is not the subject of the 1839 paper that contains it: it appears inside a *referee report*, found by Liouville and Cauchy while checking Lamé’s proof of Fermat’s Last Theorem for the exponent seven, and judged by them “assez curieux pour mériter d’être indiqué dans ce rapport” [13] . The polynomial extracted in passing while auditing someone else’s argument is still, a hundred and eighty years later, the one whose irreducibility nobody can

settle — and the one our criterion evaluates. Appendix B tells that story, and the others of Figure 2, in full.

Code and data availability

Every computational claim marked *Measured* names a script, and the scripts are not internal paths: the verification code and the data behind every figure and table in this note are archived with it, at `doi:10.5281/zenodo.22886542`, so that each `gates/…` reference resolves to a file a reader can run. Nothing in the note depends on a computation that is only described. The scripts need Python with `sympy` and `numpy`; the certificates of Table 3 need neither, since each row is one irreducibility check modulo one printed prime and is verifiable in any computer algebra system.

8 What is left open

The family Q_k: what is open there is not ours either. The irreducibility of E_k over $\mathbb{Q}$ for k prime is Mirimanoff's conjecture [32] , still open; Helou [16 , Prop. 2] shows it is equivalent to the irreducibility of T_k, so it is a question about exactly the polynomial our criterion evaluates, and [20] is the current state of it. A closed coefficient formula is already known [34 , (4.4)] . The exceptional class $k \equiv 1 \pmod 6$, which looked accidental, is explained by Proposition 16: it is where $\dim M_{2k}$ lags, and the lag is the appearance of Δ in weight 12. What remains genuinely open is the arithmetic of the Q_k that our criterion evaluates, and there the question is Mirimanoff's, not ours.

Proposition 13 is proved, and the proof is in Appendix A. It is stated here because Proposition 13, with Lemma 14, gives that $k \geq 6$ and $k \neq 7$ imply $C_k(3,p)$ is not PORC, which is what closes the "only if" half of Theorem 12; what remains open about the family Q_k is Mirimanoff's question above, not ours.

The Jacobian of the genus-five curve of $k=5$, $n=6$, is not $\mathbb{Q}$-simple. It decomposes: writing $w = x_1$, $a = x_2 + w$, $b = x_3 + w$, $c = x_4 + w$ and $A = ab + ac + bc$, so that $a + b + c = 0$, the quintic C becomes $(6w^2 - A)B + 2wA(2w^2 - A) = 0$ with $B = abc$, since $3w^5 + \sum (a-w)^5 = 5\big[(6w^2 - A)B + 2wA(2w^2 - A)\big]$. Write $\widetilde{C}$ for its normalisation. The quotient of $\widetilde{C}$ by S_3 is a rational curve, and $\widetilde{C}$ is the

Galois closure of a cubic over it. Quotienting by A_3 gives the elliptic curve $E_0\colon v^2 = x^3 - 147x - 718$, of j-invariant $-235298/13$; quotienting by a transposition gives the genus-two curve $D\colon v^2 = t^6 + 12t^4 + 40t^3 + 36t^2 + 48t + 16$, whose sextic has discriminant $2^{35}3^6 \cdot 13$. The idempotent relations of Kani and Rosen [19] then give $J(\widetilde{C}) \sim_{\mathbb{Q}} E_0 \times J(D)^2$, so $a_p(\widetilde{C}) = a_p(E_0) + 2a_p(D)$; that step is quoted, not certified here.

What we do certify is that the genus-two factor does not decompose further, and the certificate is two primes, an irreducibility certificate at each, and four comparisons of integers at each. At $p = 11$ and $p = 19$ the curve D has 11 and 25 points over $\mathbb{F}_p$, and 111 and 373 over $\mathbb{F}_{p^2}$. Since $\#D(\mathbb{F}_p) = p + 1 + a_1$ and $\#D(\mathbb{F}_{p^2}) = p^2 + 1 - a_1^2 + 2a_2$, the first count fixes a_1 and only the second fixes a_2; together they give the Weil polynomials $T^4 + a_1T^3 + a_2T^2 + a_1pT + p^2$, namely

$$T^4 - T^3 - 5T^2 - 11T + 121, \qquad T^4 + 5T^3 + 18T^2 + 95T + 361,$$

with $(a_1, a_2) = (-1, -5)$ and $(5, 18)$. Both come with a certificate of the same kind as Table 3: the first polynomial is already irreducible modulo 2, the second modulo 17, which proves each irreducible over $\mathbb{Q}$ in one line, so $J(D)$ is simple at both primes. Both reductions are ordinary, since $p \nmid a_2$ in each. For a simple ordinary abelian surface, Howe and Zhu [9 , Thm. 6] show that absolute simplicity fails in exactly four cases — $a_1 = 0$, $a_1^2 = p + a_2$, $a_1^2 = 2a_2$ and $a_1^2 = 3a_2 - 3p$, splitting over an extension of degree 2, 3, 4 and 6 respectively — and neither of ours is one:

$$1 \notin \{6,\, -10,\, -48\}, \qquad 25 \notin \{37,\, 36,\, -3\},$$

with $a_1 \neq 0$ both times. So the reduction of $J(D)$ is absolutely simple at both primes, and therefore so is $J(D)$ over $\overline{\mathbb{Q}}$: a proper abelian subvariety, defined over some number field, would reduce at a prime of good reduction to a proper abelian subvariety of the reduction. Nothing here is decided numerically.

Absolute simplicity alone does not give $\mathrm{End}^0_{\overline{\mathbb{Q}}} J(D) = \mathbb{Q}$. By Albert's classification, the endomorphism algebra of a simple abelian surface is $\mathbb{Q}$, a real quadratic field, a quartic CM field or an indefinite quaternion algebra over $\mathbb{Q}$ [2] , and each of the last three contains a real quadratic field F. The bridge to the finite fields is specialisation. The endomorphisms of $J(D)$ are all defined over some number field K', and at a prime $\mathfrak{p}$ of K' above a prime p of good reduction, reduction of endomorphisms is an injective ring homomorphism $\mathrm{End}_{K'} J(D) \hookrightarrow \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(J(D) \bmod \mathfrak{p})$; tensoring with $\mathbb{Q}$, $\mathrm{End}^0_{\overline{\mathbb{Q}}} J(D)$ embeds in $\mathrm{End}^0_{\overline{\mathbb{F}}_p}(J(D) \bmod p)$. At $p = 11$ and $p = 19$ the reduction is ordinary and, as just shown, absolutely simple. Over $\mathbb{F}_{p^m}$ its endomorphism algebra is, by Tate [39] and in the ordinary case

Waterhouse [40] , commutative and equal to the Frobenius field $\mathbb{Q}(\alpha^m)$, α a root of the Weil polynomial at p; and absolute simplicity gives $\mathbb{Q}(\alpha^m) = \mathbb{Q}(\alpha)$ for every m, so the algebra does not grow with the base field and the geometric algebra $\mathrm{End}^0_{\overline{\mathbb{F}}_p}$ is the quartic CM field $\mathbb{Q}(\alpha)$. Hence F would embed in $\mathbb{Q}(\alpha)$ at both primes. Those fields are quartic CM, and the real quadratic subfield of each is read off the resolvent $T^2 + a_1 T + (a_2 - 2p)$ satisfied by $\alpha + p/\alpha$: here $T^2 - T - 27$ and $T^2 + 5T - 20$, of discriminants 109 and 105, both squarefree. The subfields are therefore $\mathbb{Q}(\sqrt{109})$ and $\mathbb{Q}(\sqrt{105})$ — distinct, so the two quartic fields are not even isomorphic, and nothing but $\mathbb{Q}$ survives. What is *not* done is assembling this into a formula for $C_5(6, p)$: the other strata, including those of higher dimension, still have to be treated.

Measured: $j(E_0) = -235298/13$; the sextic discriminant $2^{35}3^6 \cdot 13$; and $\#D(\mathbb{F}_{11}) = 11$, $\#D(\mathbb{F}_{19}) = 25$, $\#D(\mathbb{F}_{121}) = 111$ and $\#D(\mathbb{F}_{361}) = 373$, by direct enumeration, against the stated Weil polynomials, including their functional equation; and a control showing that the count over $\mathbb{F}_p$ alone leaves dozens of values of a_2 open. Separately, the two certificates of irreducibility — modulo 2 and modulo 17 — and the four Howe–Zhu comparisons at each prime, all in integer arithmetic. Two decoys, each aimed at one half of the argument: for absolute simplicity, the Weil restriction $T^4 - T^2 + 121$ at $p = 11$, which is irreducible over $\mathbb{Q}$ like ours but meets condition $a_1 = 0$ and splits over $\mathbb{F}_{p^2}$, where its Weil polynomial becomes $(T^2 - T + 121)^2$; and for the endomorphism step, a curve with complex multiplication, $v^2 = t^5 - 1$, whose two Frobenius fields give the *same* real subfield $\mathbb{Q}(\sqrt{5})$, so the criterion correctly declines to certify it. See `gates/P3d_weil_D.py`, `gates/P3d_familia_Qk.py` and `gates/P3d_jacobiana_genero5.py`.

The counting function of the non-elementary cases. Theorem 8 says what $C_k(n, p)$ is not. For $k = 3$, $n = 5$ the companion note says what it is, in terms of one elliptic curve. For $k = 5$, $n = 6$ the obstruction is the genus-five curve whose Jacobian is decomposed above as $E_0 \times J(D)^2$; what is missing there is not the curve but the assembly, since the other strata — including those of higher dimension — still have to be treated.

Whether weight one is the only obstruction. Remark 7 shows that a higher stratum can carry non-Artin–Tate H^2 while its H^1 vanishes. Our method cannot see that, so for the cases it declares Artin–Tate the proof is always by exhibiting a formula. A criterion that sees all weights at once would subsume both halves of this note.

A Proof of Proposition 13

What is proved here. Proposition 13: whenever $\deg Q_k>0$, some fibre f_{u_0} has Galois group S_3 over $\mathbb{Q}(u_0)$. Combined with Lemma 14, this is what Theorem 12 needs: *$k \geq 6$ and $k \neq 7$ imply $C_k(3,p)$ is not PORC* — and the exclusion of 7 is not a technicality, it is forced by Theorem 12, which gives $C_7(3,p)$ in quadratic characters, so any statement covering $k \geq 6$ without qualification has its counterexample printed in this same note.

The proof runs in four steps.

Step one: the roots of Q_k are real, positive and simple. One parametrisation makes the whole step visible. A triple summing to zero with two roots on the unit circle is

$$(x,y,z) = \bigl(e^{i\theta},\, e^{-i\theta},\, -2\cos\theta\bigr),$$

and then $e_2 = 1 - 4\cos^2\theta$, $e_3 = -2\cos\theta$, so that

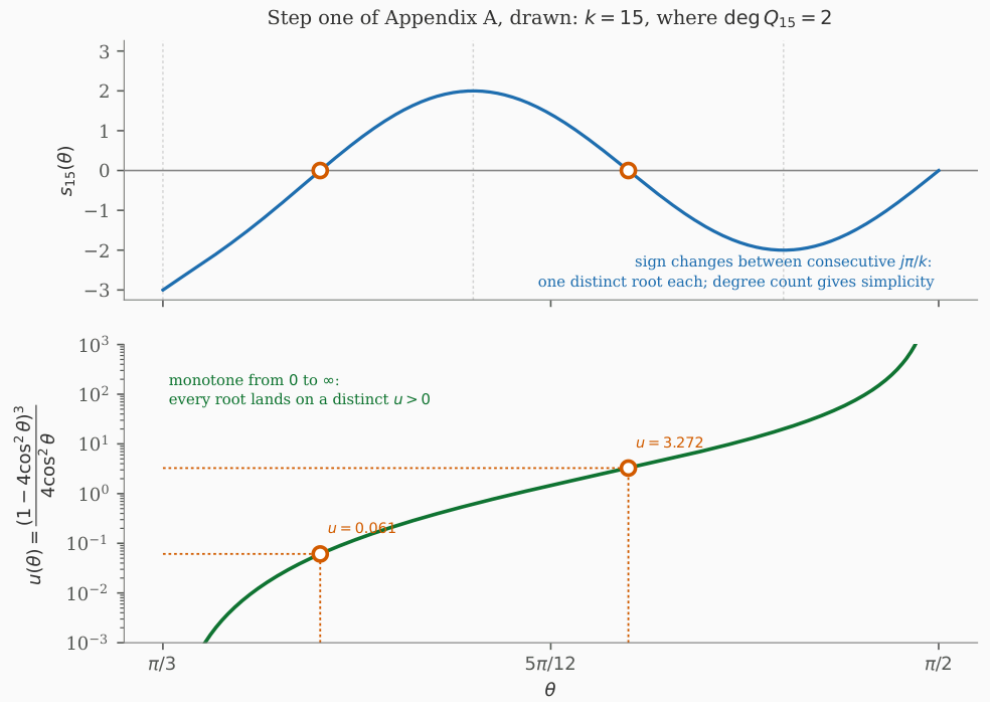
$$\boxed{u(\theta) = \frac{(1-4\cos^2\theta)^3}{4\cos^2\theta}}, \qquad s_k = (-2\cos\theta)^k + 2\cos k\theta. \tag{10}$$

On $\pi/3<\theta<\pi/2$ the numerator and denominator are both positive and u increases monotonically from 0 to ∞, so *every* positive real value of the invariant is attained exactly once on that interval, and the roots of Q_k correspond to the zeros of s_k there. Those are located by the sign alternation of $(-2\cos\theta)^k + 2\cos k\theta$ at $\theta = j\pi/k$ for $\lceil k/3\rceil \leq j \leq \lfloor k/2\rfloor$. The number of sign changes is the number of such j minus one, and that number is the degree itself:

$$\#\{\text{sign changes}\} = \left\lfloor \frac{k}{2} \right\rfloor - \left\lceil \frac{k}{3} \right\rceil = \deg Q_k =: d.$$

So the changes produce d distinct real positive roots, and since Q_k has degree exactly d these *exhaust* its roots and every one of them is simple — simplicity is a consequence of the count, not of the sign change. Figure 8 is this step.

Figure 8



Step one of this appendix, for $k = 15$, an example where Q_k has two roots — with one root nothing would show that they are *simple*, which is half the statement. The smallest such k is 12, by Proposition 15; 15 is drawn because its two roots are further apart on the u-axis and the guides do not collide. Above, s_k on the interval, changing sign once between consecutive $j\pi/k$; each change is a root, and they can be counted. Below, the invariant $u(\theta)$ of (10), which climbs monotonically from 0 to ∞, so each root above lands on a positive value of u and on a different one. The two halves of "real, positive and simple" are the two properties of this curve. The lower axis is logarithmic and clipped to the band where the roots fall; the curve leaves it at both ends, which is what "from 0 to ∞" means.

Step two: no fibre is cyclic, and not every fibre is reducible. Total reality then forces the discriminant $-u^2(4u + 27)$ to be a non-square in every real embedding, so no *irreducible* fibre has cyclic Galois group C_3: every fibre is either reducible or has group S_3. What remains is to exclude the case where *every* fibre is reducible. Writing Y for the root of the fibre cubic and eliminating $u = Y^3/(1 - Y)$, the roots of all fibres at once are the roots of

$$P_k(Y) \;=\; (1-Y)^d\, Q_k\big(Y^3/(1-Y)\big) \;=\; \sum_{i=0}^{d} c_i\, Y^{3i}(1-Y)^{d-i}, \qquad Q_k =$$

a polynomial of degree $3d$ and leading coefficient $A = \mathrm{lc}(Q_k)$. Since $\mathrm{disc}\, f_u < 0$, each fibre has exactly one real root; moreover $f_u(0) = -u < 0$ and $f_u(1) = 1 > 0$, so that root lies in $(0, 1)$. Hence P_k has exactly d real roots, all in $(0, 1)$. If every fibre were reducible, those d real roots would

form a rational factor of P_k — and this needs no irreducibility of Q_k, which is Mirimanoff's question and is not assumed anywhere here.

Lemma 21. (the real roots form a factor) p. 25

> *Suppose f_u is reducible over $\mathbb{Q}(u)$ for every root u of Q_k, and let $y(u) \in (0,1)$ be the real root of f_u. Then the set $\{y(u) : Q_k(u) = 0\}$ is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and the primitive integral multiple h of $\prod_u (Y - y(u))$ lies in $\mathbb{Z}[Y]$, has degree d, divides P_k, and has leading coefficient $B \mid A$.*

Proof: in this note · **Covers:** not formalized · **Cite:** Lemma 21, p. 25, doi:10.5281/zenodo.22886543

↳ Used in: Proposition 13 (p. 24)

Proof

> Every root of Q_k is real by step one, so every conjugate of u is real and $\mathbb{Q}(u)$ is totally real. A reducible cubic f_u has a root $r \in \mathbb{Q}(u)$. For each embedding σ of $\mathbb{Q}(u)$, $\sigma(r)$ is a real root of $f_{\sigma(u)}$, whose discriminant is negative, so it is the only one: $\sigma(r) = y(\sigma(u))$. Hence $r = y(u)$, and the conjugates of $y(u)$ are the values of y at the conjugates of u. The $y(u)$ are distinct, since $u = y^3/(1-y)$ recovers u, so the product has degree d and divides P_k in $\mathbb{Q}[Y]$; by Gauss's lemma its primitive integral multiple divides P_k in $\mathbb{Z}[Y]$, whence $B \mid A$.

Then $h(0)$ and $h(1)$ are nonzero integers, and $1 \le |h(0)h(1)| = B^2 \prod y_i(1-y_i) \le A^2/4^d$, absurd once $A < 2^d$.

Conversely P_k irreducible forces every fibre to be S_3, and the degrees close it in two lines. If y is a root of P_k then $u = y^3/(1-y)$, so

$$[\mathbb{Q}(y) : \mathbb{Q}(u)] \le 3, \qquad [\mathbb{Q}(u) : \mathbb{Q}] \le d.$$

Irreducibility gives $[\mathbb{Q}(y) : \mathbb{Q}] = 3d$, so both inequalities are equalities: Q_k is the minimal polynomial of u, and f_u is irreducible over $\mathbb{Q}(u)$. Its discriminant is not a square there, by the opening of Step two, so its group is S_3 and not C_3.

Step three: $A \le k$. What is left is to bound A, and Waring's formula does it at a single monomial — equivalently, one reads the extreme term of the classical expansion of $x^k + y^k + z^k$ for $x + y + z = 0$ recalled in Section 6. Write $s_k = \sum_{2a+3b=k} \gamma_{a,b}\, e_2^a e_3^b$ with $e_1 = 0$, so that $|\gamma_{a,b}| = k\,(a+b-1)!/(a!\,b!)$, and let $\widetilde{Q}_k$ be that polynomial read in $u = e_2^3/e_3^2$, of which Q_k is the primitive part. The top coefficient of $\widetilde{Q}_k$ is the

$\gamma_{a,b}$ with b minimal, and $3b = k - 2a$ forces $b \equiv k \pmod 2$; there the factorials cancel outright,

$$k \text{ even}: \quad b = 0,\ \ a = \tfrac{k}{2}, \qquad |\gamma_{a,b}| = \frac{k\,(\frac{k}{2}-1)!}{(\frac{k}{2})!\;0!} = 2;$$

$$k \text{ odd}: \quad b = 1,\ \ a = \tfrac{k-3}{2}, \qquad |\gamma_{a,b}| = \frac{k\,(\frac{k-3}{2})!}{(\frac{k-3}{2})!\;1!} = k.$$

Passing to the primitive part divides every coefficient by one and the same content and leaves the degree alone, so A divides that number: $A \mid 2$ for k even and $A \mid k$ for k odd. Either way $A \mid k$, and in particular $A \le k$.

The inequality $A<2^d$ therefore holds whenever $k<2^d$, and that is arithmetic. Write $k = 6q + r$ with $0 \le r \le 5$, so that $d = q - [r = 1]$. For $r \neq 1$ it is enough that $6q + 5<2^q$, which holds at $q = 6$ and is stable under $q \mapsto q + 1$; for $r = 1$ it is enough that $6q + 1<2^{q-1}$, which holds at $q = 7$ and is stable likewise. So $k<2^d$ for every $k \ge 38$, and among the $k \le 37$ with $d>0$ the bound $k<2^d$ fails at twenty-nine; only at those can $A<2^d$ fail.

Step four: the remaining k, by certificate. Those twenty-nine are settled, together with every other k in the same range, by exact certificates rather than left as a finite computation not carried out: *P_k is irreducible over $\mathbb{Q}$ for all $6 \le k \le 46$ with $d>0$*, forty cases, each certified by a prime modulo which P_k is still irreducible. The certificates are printed in Table 3, because a certificate one has to take on trust is not a certificate. Proposition 13 is therefore unconditional for every k, with no measured input anywhere in the chain.

Table 3: The forty certificates behind Proposition 13. For each k with $\deg Q_k>0$ in the range, $d = \deg Q_k$, $A = \mathrm{lc}(Q_k)$, and p is a prime modulo which P_k — of degree $3d$ — remains irreducible, which proves it irreducible over $\mathbb{Q}$. Each row is checkable in one line of any computer algebra system and requires nothing of ours to be believed. Shade of A is the margin $2^d/A$ by which the inequality holds — dark where it barely does, pale where it holds by orders of magnitude — and the tinted rows are the seven where it does not hold at all. The two codes together are the shape of the argument: the margin grows exponentially in k while $A \le k$ grows at most linearly, so the tinted rows can only occur early, and they do. The table is generated by `gates/P3d_s3_certificados.py`, not typed.

Measured: For every $6 \le k \le 46$ with $\deg Q_k>0$: the d roots of Q_k real, positive and simple by Sturm sequences; $Q_k(0) \neq 0$; P_k of degree $3d$ with exactly d real roots, all in $(0, 1)$; and P_k irreducible over $\mathbb{Q}$, with the witness prime printed for each. The seven exceptions to $A<2^d$ at the *measured* value of A are $k = 6, 9, 10, 15, 21, 33, 35$, of which $k = 6, 10$ are equality cases. The proof above uses only $A \le k$, which is weaker: it leaves twenty-nine exceptions rather than seven, and those are checked to be the values $k \le 37$ with $d>0$ and $k \ge 2^d$, all inside the certified range. The two lists, the raw leading coefficient 2 or k, and the divisibility $A \mid k$ are each verified by a

separate route for $3 \le k \le 400$. See `gates/P3d_s3_certificados.py` and `gates/P3d_lc_Qk.py`.

B The four strands, told by their people

Figure 2 draws four lines of work that never meet until this note needs all four. Read by years it is a diagram; read by people it is better, and the pieces below say which section of the note each one hangs from. Nothing here is needed to follow the mathematics. Everything here has been checked against the source named with it, and four attractive stories about the same people were found to be legend or to rest on paraphrase and are excluded deliberately rather than dropped in silence.

B.1 The identity was found while refereeing (Section 6)

On Monday 16 September 1839 the Académie des sciences heard a commission report. Its heading names the commissioners and, in the French convention, which of them wrote it: “Commissaires, MM. Liouville, Cauchy rapporteur.” The subject was Lamé’s memoir proving Fermat’s Last Theorem for the exponent seven, and the report approves it — “les savants apprendront avec plaisir qu’il est parvenu effectivement au but qu’il s’était proposé d’atteindre”.

The interesting part is what the two referees did next. Rather than stop at a verdict they asked whether the lemma Lamé had used might be a special case of something more general; they found that it was; and they judged the answer worth a detour in their own report — “un théorème d’analyse qui nous semble assez curieux pour mériter d’être indiqué dans ce rapport” [13] . The theorem is the factorisation $(x+y)^n - x^n - y^n = n\,xy(x+y)(x^2+xy+y^2)^b E_n(x,y)$, with $b \in \{0,1,2\}$ as in Section 6, and E_n is the family whose S_3 quotient Section 6 evaluates. An object produced as a by-product of auditing somebody else’s proof has outlived the proof it was auditing: Lamé’s exponent seven was superseded within a year, and E_n’s irreducibility is open in 2026.

The two men return eight years later on the other side of the same subject. In March 1847 Lamé announced a general proof of Fermat’s Last Theorem by factoring into linear factors over the cyclotomic integers; the announcement did not survive the session, and both his and the competing programme foundered on the arithmetic of those integers. Lamé wrote to Dirichlet in

June of that year — “Les sages avis de Liouville m’ont désillusionné; j’ai rougi de ma folle équipée” [8] .

B.2 Mirimanoff conjectured twice, in two subjects (Section 8)

Dmitry Mirimanoff conjectured in 1903 that E_n is irreducible over $\mathbb{Q}$ for n prime [32] . That is still open, and Section 8 records why it is a question about exactly the polynomials our Theorem 12 evaluates. The same Mirimanoff, in Geneva in 1917, wrote the paper that introduced the cumulative hierarchy and the distinction between well-founded and ill-founded sets — the idea that became the axiom of foundation. Two conjectures in two subjects, one of which is now a standard axiom and the other of which is still open after a hundred and twenty years.

B.3 Mann proved his first theorem with no academic position (Section 2)

The criterion of Section 2 rests on Mann’s theorem [24] on relations between roots of unity, which he published in 1965. It is not the work he is remembered for. Mann emigrated from Vienna in 1938; in New York he earned his living for several years primarily by tutoring; and in 1941, with no academic post, he proved the Schnirelmann–Landau conjecture on the density of sums of sets of integers, a problem on which Landau, Khinchin, Besicovitch, Schur and Brauer had obtained partial results over the preceding decade. His interest in it had been aroused by Brauer’s lectures at New York University — that is, by one of the people who had nearly solved it. The American Mathematical Society gave him the Cole Prize in 1946. He is also, separately, the Mann of the Mann–Whitney test.

B.4 Higman posed the PORC question from outside the war (Section 6)

Graham Higman’s 1960 paper [10] asks whether the number of groups of order p^n is polynomial on residue classes in p — the PORC conjecture, proved for $n \le 7$ and open for $n \ge 8$, and the question Section 6 answers in the negative for our counts. His mathematical career had been interrupted: he registered as a conscientious objector and served the war in the Meteorological Office, in Northern Ireland and Gibraltar. He returned to become Waynflete Professor at Oxford from 1960 to 1984, supervised more than fifty doctoral students, and founded the *Journal of Algebra*.

B.5 The Hungarian strand, and a prize shaped like the Fano plane (Remark 10)

Vandermonde sets were introduced by András Gács and Zsuzsa Weiner in 2003, in a paper about arcs; Sziklai and Takáts classified the super-Vandermonde ones in 2008 [45] , and their Theorem 1.12 is what Remark 10 recovers by a different route. All of them belong to the finite-

geometry school built at Eötvös Loránd University in Budapest. Gács died in 2009, at forty; his family endowed a prize for young mathematics teachers in his name, whose trophy is a model of the Fano plane.

B.6 The Conway of Conway–Jones (Section 2)

The sharpening of Mann's theorem from five terms on, which we quote but do not need, is Conway–Jones [23] . It is the John Horton Conway — the paper is item 115 of his own bibliography — and the co-author is not an anonymous initial either: A. J. Jones is Antonia Jane Jones (1943–2010), who took a Cambridge doctorate on sums of roots of unity, the subject of the paper, and who signs it from Royal Holloway College while Conway signs from D. P. M. M. S. The two standard records of her thesis disagree, and we report the disagreement rather than choose: the Mathematics Genealogy Project gives *Sums of roots of unity and Diophantine approximation*, 1969, supervised by Harold Davenport and J. W. S. Cassels, and Wikipedia gives *Sums of roots of unity and cyclic overlattices*, 1968. We could not find the thesis itself, and the paper does not cite it.

The paper is worth reading to the end for a reason that has nothing to do with our use of it. Having built the machinery for vanishing sums of roots of unity, the last page spends it on a piece of elementary geometry: a triangle all of whose edges are rational and all of whose angles are rational multiples of π must be equilateral. The proof is three lines, and its engine is the step that $(k,n)=1 \Rightarrow k \equiv \pm 1 \pmod{n}$ forces $n \in \{1,2,3,4,6\}$ — bookkeeping over small cyclotomic degrees, of the same flavour as the criterion of Section 2. Jones later left number theory altogether and became Professor of Evolutionary and Neural Computing at Cardiff, with sixteen doctoral students to her name.

B.7 The gap in our list is where Δ lives (Corollary 17)

Corollary 17 says that $C_k(3,p)$ is elementary exactly when $\dim M_{2k}(\mathrm{SL}_2(\mathbb{Z})) = 1$, and the four weights are $6, 8, 10, 14$, with forms E_6, E_8, E_{10}, E_{14}. The list is easier to remember by what is *missing* from it: weight 12. And the reason weight 12 is missing is a single function.

The dimension of M_w grows by one every twelve, and the first place it reaches two is $w = 12$, because that is where the first cusp form appears:

$$\Delta(q) = q\prod_{n\ge 1}(1-q^n)^{24} = \sum_{n\ge 1}\tau(n)q^n.$$

So $\dim M_{12} = 2$ and our $k = 6$ is not elementary — it is the first k where the count needs a cubic. Weight 14 then returns to dimension one, and the reason is exact rather than approximate: every cusp form of weight w is Δ

times a form of weight $w-12$, that is $S_w = \Delta\, M_{w-12}$, and $M_2 = 0$, so $S_{14} = 0$. There is no room for a cusp form in weight 14 because there is nothing in weight 2 to multiply Δ by. That is the whole reason $k = 7$ joins $3, 4, 5$. The exceptional residue class $k \equiv 1 \pmod 6$ of Proposition 15, which looks like an arithmetic accident when one only counts solutions of $2a + 3b = k$, is that same lag seen from the other side.

Ramanujan wrote the coefficients $\tau(n)$ down in 1916 and conjectured, on the evidence of a table, that they are multiplicative and satisfy $|\tau(p)| \le 2p^{11/2}$ [29]. Mordell proved the multiplicativity the following year [30]. The bound waited until Deligne derived it in 1974 from the Weil conjectures [31] — which is the same Weil-weight formalism that Section 3 uses to decide our length-four strata, at weight eleven instead of weight one: each two-dimensional weight-one pair contributes at most $2\sqrt{p}$, so for a genus-g curve the whole trace is bounded by $2g\sqrt{p}$, and the two-dimensional representation attached to Δ is bounded by $2p^{11/2}$.

B.8 Twelve edges, and then years with nothing to show (Section 7)

The story Section 7 points at is worth telling with its dates, because it is the same shape as this note at a much larger scale. Kontsevich conjectured in 1997 that the number of points of a graph hypersurface over $\mathbb{F}_q$ is a (quasi-)polynomial in q. Stembridge then verified it by computer [46], for every graph with at most twelve edges; that is the whole of what was reachable, and it all agreed. In 2003 Belkale and Brosnan [1] proved the conjecture false, and false in the strongest available sense: for large graphs the counting functions are of general type.

The part that is easy to miss is what happened next, which is nothing. Their method builds graphs with very large numbers of edges, so for years after the conjecture was known to be false, *no explicit counterexample was known*; the first ones came later, from two independent constructions, and those of [3] are graphs of ϕ^4 theory whose counting functions carry a modular form of a singular K3 surface. A statement can be refuted long before anything can be shown.

That gap is the reason this note is built the way it is. Appendix A could have said that P_k is irreducible for every k it was able to test; instead it proves $A{<}2^d$ for all $k \ge 38$ and prints forty certificates for the rest, each one a prime a reader can check without believing anything of ours. And Section B.10 is the same lesson in miniature, on our own data: four values of k in a row with Q_k monic, and the fifth is not. There the counterexample was the very next case. Kontsevich's was out of reach for years.

Measured: The two dates and the twelve edges against the abstract of [3], which states them, and the absence of an explicit counterexample against its introduction, which says so in those words. Nothing here rests on a secondary account.

B.9 Four integers for every extension at once (Section 8)

Absolute simplicity is a question about infinitely many fields at once. An abelian surface that is simple over $\mathbb{F}_p$ may split over $\mathbb{F}_{p^m}$, and no search over m, however long, can show that it never does. Section 8 settles it for $J(D)$ with four comparisons of integers at each of two primes, and the theorem that makes that possible was not written for anything like our question.

Howe and Zhu [9] set out to prove that over every field, and in every dimension, there is an abelian variety that stays simple over the algebraic closure. An absolutely simple variety stays simple over every extension field, so it is enough to treat the prime fields; over $\mathbb{Q}$, as they note, examples in every dimension were already known from Mori and Zarhin, so what was left was $\mathbb{F}_p$. Their Theorem 6 is the tool for dimension two: it reads the answer off the characteristic polynomial of Frobenius of a simple ordinary surface, and it gives, in their words, “a very short proof” of that case.

The list of four conditions is short, and part of the reason is one already met at the end of [23] . Their proof takes the least d for which $\mathbb{Q}(\alpha^d)$ is a proper subfield of the quartic CM field $\mathbb{Q}(\alpha)$, α a root of the Weil polynomial, and shows that either the Weil polynomial is a polynomial in T^2 or T^4, or $\mathbb{Q}(\alpha)$ is obtained from an imaginary quadratic field by adjoining a primitive d-th root of unity. If that root of unity generated a field of degree larger than two it would have to generate all of $\mathbb{Q}(\alpha)$, which the proof rules out; so it lies in a quadratic field, and a root of unity in a quadratic field has order 1, 2, 3, 4 or 6. The splitting degrees 2 and 4 can come from the first alternative, the Weil polynomial being a polynomial in T^2 or T^4; the degrees 3 and 6 can only come from the second, as orders of roots of unity in an imaginary quadratic field. That short list is the same phenomenon, $\varphi(d) \le 2$, as the $n \in \{1,2,3,4,6\}$ that gives Conway and Jones their equilateral triangle.

Measured: The aim of [9] , the reduction to prime fields, the attribution to Mori and Zarhin, the phrase “a very short proof” and the structure of the proof of Theorem 6 read off the arXiv version of the paper, math/0002205, its introduction and Section 4; the four conditions and the splitting degrees against the statement of Theorem 6 there.

B.10 A pattern that is not one (Section 6)

The values $k = 11, 17, 23, 29$ give $Q_{11} = u - 1$, $Q_{17} = u^2 - 5u + 1$, $Q_{23} = u^3 - 12u^2 + 14u - 1$ and $Q_{29} = u^4 - 22u^3 + 66u^2 - 30u + 1$: monic, with constant term ± 1. It is tempting to read that as a property of the class $k \equiv 5 \pmod 6$. It is not: the next member is

$$Q_{35}(u) = 35u^5 - 1225u^4 + 7007u^3 - 8580u^2 + 1925u - 35,$$

primitive but not monic. Helou [16 , p. 53] explains why k prime gives a monic Q_k: T_k is monic over $\mathbb{Q}$ always, and lies in $\mathbb{Z}[X]$ when k is prime. T_k is defined for odd k, and for odd k our Q_k is its primitive integral form, so Q_k is monic exactly when T_k is already integral, and in particular whenever k is prime. That 35 breaks the pattern is measured, not explained. The converse is not a theorem we have. For odd $k \leq 400$ the monic Q_k are exactly those of prime k — for odd $k \leq 40$, $11, 13, 17, 19, 23, 29, 31, 37$ and not 35 — but that is a measurement; and for even k it is false, since Q_8, Q_{16}, Q_{32}, … are monic too. See `gates/P3d_lc_Qk.py`. Searching the leading and constant coefficients turns up no usable OEIS entry, and the variable content makes such searches fragile in any case.

Measured: Every quotation above checked against its source: the two French passages of Section B.1 and the approval of Lamé's memoir character by character against the *Comptes rendus* themselves; Lamé's letter against [8] ; the statements about Mann against the Ohio State University departmental memorial and those about Higman against his obituary and the Royal Society biographical memoir. The affiliations, submission dates and reference list of [23] , and its closing theorem on rational triangles, read off the published pages; the two conflicting records of Jones's thesis are reported as conflicting because we could not settle them. In Section B.7 the mathematics — $\dim M_{12} = 2$, $\dim M_{14} = 1$, and the product expansion of Δ — is checked in `gates/P3d_familia_Qk.py` and follows from [28] , which we have read; the three historical attributions to Ramanujan, Mordell and Deligne are cited for priority only, carry nothing the argument uses, and are not claimed as read. Four further stories about the same people are excluded as legend or as resting on paraphrase, deliberately rather than in silence.

📊 Tables

Every table of the paper, in its order: click one to unfold it, with where the paper cites it, how its numbers were checked, and its data as CSV. The typeset table is one click away, on its page of the PDF.

Table 1. Theorem 4 in three rows. The tinted rows are the two where something beyond $n = 3$ is singular; the bottom one is where $n = 5$ enters, and the certificate is the divisibility by Φ_6 that puts it there. Note that this table answers the *singularity* question, which Section 3 shows is not the same as the Artin–Tate question.

$m = k - 1$	$\gcd(m, 6)$	S_m	**certificate**
odd	1 or 3	$\{3\}$	—

$2 \mid m, 3 \nmid m$	2	$\{3,4,6\}$	$1+1-1-1=0$ in μ_2
$6 \mid m$	6	$\{3,4,5,6\}$	$2+X^2+X^3+X^4=\Phi_6\cdot(X^2+2X+2)$

Colour: grey = nothing.

p. 6 in the PDF ⬇ CSV

cited in §2 The criterion, and why only gcd(k-1,6) matters

Table 2. Every count this note and its companion put in closed form, with the reason the length-four obstruction failed to appear in each. The last row is tinted differently because it is closed but not in quadratic characters — it is the subject of Section 6.

count	closed form	why no obstruction	checked
$C_3(n,p)$, $n=3,4,6$	see [P3c]	rational, or none	11/33 primes
$C_4(3,p)$	$\frac{p-1}{6}\big(1+\chi_p(-3)\big)$	no length-four stratum	16 primes
$C_5(3,p)$	$\frac{p-1}{6}\big(4+\chi_p(-3)\big)$	no length-four stratum	15 primes
$C_5(4,p)$	$\frac{p-1}{24}\big(4p-17-6\chi_p(-2)-3\chi_p(-1)\big)$	the witness is a conic	12 primes
$C_7(3,p)$	$\frac{p-1}{6}\big(4+\chi_p(-3)\big)$	s_7 is a monomial	53 primes
$C_6(3,p)$	$(p-1)\cdot\mathbf{1}\{2Y^3+3Y-3 \text{ splits}\}$	*a nonabelian class function*	17 primes

Colour: red = no / fails.

p. 13 in the PDF ⬇ CSV cited in §5 The counts that survive

Table 3. The forty certificates behind Proposition 13. For each k with $\deg Q_k > 0$ in the range, $d=\deg Q_k$, $A=\mathrm{lc}(Q_k)$, and p is a prime modulo which P_k — of degree $3d$ — remains irreducible, which proves it irreducible over $\mathbb{Q}$. Each row is checkable in one line of any computer algebra system and requires nothing of ours to be believed. Shade of A is the margin $2^d/A$ by which the inequality holds — dark where it barely does, pale where it holds by orders of magnitude — and the tinted rows are the seven where it does not hold at all. The two codes together are the shape of the argument: the margin grows exponentially in k while $A \le k$ grows at most linearly, so the tinted rows can only occur early, and they

do. The table is generated by `gates/P3d_s3_certificados.py`, not typed.

k	d	A	p	k	d	A	p	k	d	A	p
6†	1	2	7	21†	3	21	97	35†	5	35	113
8	1	1	11	22	3	2	281	36	6	2	89
9†	1	3	2	23	3	1	23	37	5	1	31
10†	1	2	11	24	4	2	71	38	6	2	5
11	1	1	2	25	3	5	59	39	6	39	11
12	2	2	5	26	4	2	37	40	6	2	7
13	1	1	3	27	4	9	113	41	6	1	179
14	2	2	5	28	4	2	13	42	7	2	31
15†	2	15	11	29	4	1	71	43	6	1	5
16	2	1	29	30	5	2	11	44	7	2	191
17	2	1	11	31	4	1	23	45	7	45	29
18	3	2	61	32	5	1	101	46	7	2	17
19	2	1	13	33†	5	33	41				
20	3	2	29	34	5	2	29				

Colour: blue shade = the number's size within its column.

p. 28 in the PDF · ⬇ CSV · cited in §7 Where this sits · cited in §8 What is left open · cited in §A Proof of Proposition 13

References

1

P. Belkale and P. Brosnan, *Matroids, motives, and a conjecture of Kontsevich*, Duke Math. J. **116** (2003), no. 1, 147–188. 🔎 find it

2

C. Birkenhake and H. Lange, *Complex Abelian Varieties*, 2nd ed., Grundlehren der mathematischen Wissenschaften **302**, Springer, Berlin, 2004. 🔎 find it

3

F. Brown and O. Schnetz, *A K3 in ϕ^4*, Duke Math. J. **161** (2012), no. 10; arXiv:1006.4064.

4

A. Dimca and G. Sticlaru, *Waring rank of symmetric tensors, and singularities of some projective hypersurfaces*, arXiv:1902.01351, Thm. 2.4.

5

M. du Sautoy and M. Vaughan-Lee, *Non-PORC behaviour of a class of descendant p-groups*, J. Algebra **361** (2012), 287–312; arXiv:1106.5530.

6

A.-S. Elsenhans and J. Jahnel, *The discriminant of a cubic surface*, arXiv:1006.0721 (2010), Fact 2.8 and Examples 2.9.

7

S. R. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Moscow Math. J. **2** (2002), 589–631; corrected version arXiv:0808.2169, Prop. 3.2.

8

C. Goldstein, *Gabriel Lamé et la théorie des nombres: "une passion malheureuse"?*, Bulletin de la Sabix **44** (2009), 131–139. The letter to Dirichlet is in the NachlaSS Dirichlet, Staatsbibliothek zu Berlin. 🔎 find it

9

E. W. Howe and H. J. Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), no. 1, 139–163. 🔎 find it

10

G. Higman, *Enumerating p-groups. II: Problems whose solution is PORC*, Proc. London Math. Soc. (3) **10** (1960), 566–582. 🔎 find it

11

X. Cao, W.-S. Chou and J. Gu, *On the number of solutions of certain diagonal equations over finite fields*, Finite Fields Appl. **42** (2016), 225–252. 🔎 find it

12

F. N. Castro, I. Rubio, P. Guan and R. Figueroa, *On systems of linear and diagonal equation of degree $p^i + 1$ over finite fields of characteristic p*, Finite Fields Appl. **14** (2008), 648–657. 🔎 find it

13

A. Cauchy and J. Liouville, *Rapport sur un mémoire de M. Lamé relatif au dernier théorème de Fermat*, C. R. Acad. Sci. Paris **9** (1839), 359–363. 🔎 find it

14

J. Giménez, G. Matera, M. Pérez and M. Privitelli, *Smooth symmetric systems over a finite field and applications*, J. Algebra (2024); arXiv:2312.09477.

15

J. F. Gottig, M. Pérez and M. Privitelli, *An approach to the moments subset sum problem through systems of diagonal equations over finite fields*, arXiv:2401.06964 (2024).

16

C. Helou, *Cauchy–Mirimanoff polynomials*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), no. 2, 51–57. 🔎 find it

17

K. Isham, *Problems relating to arcs in projective space and subrings in* $\mathbb{Z}^n$, Ph.D. dissertation, University of California, Irvine, 2021; https://escholarship.org/uc/item/0ms4x869. See §2.3.3, Prop. 2.3.7, Ex. 2.3.8 and §2.4.2.

18

T. Lai, A. Marino, A. Robinson and D. Wan, *Moment subset sums over finite fields*, Finite Fields Appl. **62** (2020), 101607; arXiv:1910.05894.

19

E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. 🔎 find it

20

H. Karapetyan and R. Hambardzumyan, *Irreducibility and locus of complex roots of polynomials related to Fermat's Last Theorem*, arXiv:2510.00020 (2025–2026).

21

J. Li and D. Wan, *A new sieve for distinct coordinate counting*, Sci. China Math. **53** (2010), 2351–2362. 🔎 find it

22

A. Blokhuis, G. Marino, F. Mazzocca and O. Polverino, *On almost small and almost large super-Vandermonde sets in* $\mathrm{GF}(q)$, Des. Codes Cryptogr. **84** (2017), 197–201. 🔎 find it

23

J. H. Conway and A. J. Jones, *Trigonometric diophantine equations (On vanishing sums of roots of unity)*, Acta Arith. **30** (1976), 229–240, Thm. 5. 🔎 find it

24

H. B. Mann, *On linear relations between roots of unity*, Mathematika **12** (1965), 107–117, Thm. 1; DOI:10.1112/S0025579300005210. A modern statement with a full proof is Schwartz–Solymosi–de Zeeuw [26 , Thm. 3.1] .

25

P. Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer, New York, 1999, pp. 226–230. 🔎 find it

26

R. Schwartz, J. Solymosi and F. de Zeeuw, *Rational distances with rational angles*, Mathematika **58** (2012), 409–418; arXiv:1008.3671, Thm. 3.1.

27

M. Moisio and K. Ranto, *Elliptic curves and explicit enumeration of irreducible polynomials with two coefficients prescribed*, Finite Fields Appl. **14** (2008), 798–815. 🔎 find it

28

J. S. Milne, *Modular Functions and Modular Forms*, course notes, v1.31 (2017), Prop. 4.16. 🔎 find it

29

S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. **22** (1916), no. 9, 159–184. 🔎 find it

30

L. J. Mordell, *On Mr Ramanujan's empirical expansions of modular functions*, Proc. Cambridge Philos. Soc. **19** (1917), 117–124. 🔎 find it

31

P. Deligne, *La conjecture de Weil. I*, Publ. Math. IHES **43** (1974), 273–307. 🔎 find it

32

D. Mirimanoff, *Sur l'équation* $(x+1)^l - x^l - 1 = 0$, Nouv. Ann. Math. **3** (1903), 385–397. 🔎 find it

33

P. M. Nanninga, *Cauchy–Mirimanoff and related polynomials*, J. Aust. Math. Soc. **92** (2012), no. 2, 269–280. 🔎 find it

34

P. M. Nanninga, *Cauchy–Mirimanoff and related polynomials*, Ph.D. thesis, Australian National University, 2013. 🔎 find it

35

Y. Zhang, D. Zheng, X. Wang and M. Yuan, *Some new results on the second moment k-subset sum problem over finite fields*, Finite Fields Appl. **117** (2027), 102877; DOI:10.1016/j.ffa.2026.102877. 🔎 find it

36

J. Nguyen, *Higher moments subset sum problem over finite fields*, Ph.D. dissertation, University of California, Irvine, 2019; https://escholarship.org/uc/item/2cr0w697.

37

C. Marín, *Subsets of $\mathbb{F}_p$ with two prescribed moments, Part I: the pair $\{1,3\}$ — exact counts of totally split squarefree polynomials with a non-consecutive pair of prescribed coefficients, and exactly when those counts are elementary*, 2026; doi:10.5281/zenodo.22886540.

38

C. Marín, *The order generated by a column of the $\mathrm{SU}(n)_k$ S-matrix is locally a numerical semigroup ring, Part II*, 2026; doi:10.5281/zenodo.22864266.

39

J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. 🔎 find it

40

W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. 🔎 find it

41

P. Tzermias, *On Cauchy–Liouville–Mirimanoff polynomials*, Canad. Math. Bull. **50** (2007), no. 2, 313–320. 🔎 find it

42

P. Tzermias, *On Cauchy–Liouville–Mirimanoff polynomials II*, Funct. Approx. Comment. Math. **46** (2012), no. 1, 15–27; DOI:10.7169/facm/2012.46.1.2. 🔎 find it

43

I. Todhunter, *Theory of Equations*, Macmillan and Co., London, 1861. 🔎 find it

44

T. Muir, *Cauchy's theorem regarding the divisibility of* $(x+y)^n+(-x)^n+(-y)^n$, Messenger of Math. **8**(2) (1878), 119–120. 🔎 find it

45

P. Sziklai and M. Takáts, *Vandermonde sets and super-Vandermonde sets*, Finite Fields Appl. **14** (2008), 1056–1067; DOI:10.1016/j.ffa.2008.06.004. Theorem 1.12. 🔎 find it

46

J. R. Stembridge, *Counting points on varieties over finite fields related to a conjecture of Kontsevich*, Ann. Comb. **2** (1998), no. 4, 365–385. 🔎 find it

47

M. Stanojkovski and C. Voll, *Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves*, Math. Ann. **381** (2021), 593–629; arXiv:1912.09860, §1.5.2.