The order generated by a column of the $SU(n)_k$ S-matrix is locally a numerical semigroup ring (Part II)

Algebraic number theory · orders and discriminants of fusion rings

Carles Marín

Statements

Proposition 1 4
Observation 2 4
Corollary 3 4
Lemma 4 5
Theorem 5 7
Lemma 6 8
Remark 7 8
Theorem 8 8
Theorem 9 9
Proposition 10 11
Proposition 11 12

At a glance

What the paper contributes

Part I turned one column of the $SU(n)_k$ S-matrix into an order whose defect $\delta(T)$ is the number of gaps of a numerical semigroup S_T. This note asks how the columns fit together: the p-adic valuation of the discriminant of the fusion ring splits into ramification, defects and a gluing term whose only unknown piece is $\Delta(n,p) = \Sigma\, \delta$ over orbits. **That splitting is verified computationally, not proved**, as the paper says.

- **Small defects by vanishing moments** (Proposition 1, Corollary 3, Lemma 4): with trivial stabiliser, $\delta \geq 2 \Leftrightarrow M_2M_3 = 0$, and $\delta = 3$ happens in exactly four ways, one per numerical semigroup of genus three; $\delta = 2$ never occurs at $n = 4$. Observation 2 refines this and is measured.
- **The distribution law** (Theorem 5, Lemma 6, Theorem 8): for fixed $n \geq 5$ the proportion of columns with $\delta \geq 2$ is $2/p - 1/p^2$ up to an explicit error, with no factorial threshold; the mean defect per orbit is $1 + 2/p + 3/p^2$ for $n \geq 7$.
- **Uniformity in the central range** (Theorem 9, proof sketched): both expansions hold for $\varepsilon p \leq n \leq (1-\varepsilon)p$.
- **The two ends** (Propositions 10–11, §4): totally split trinomials $X^n + aX + b$ at the top (counted at $n = 5$ by an elliptic curve of conductor 50, measured); Gauss's half-systems in the middle, whose even moments vanish exactly and which give an infinite family of non-Gorenstein orders with semigroup $\langle 3,5,7\rangle$.

🚀 **Start here: Corollary 3**: with trivial stabiliser, $\delta \geq 2$ if and only if $M_2M_3 = 0$.

Main results:

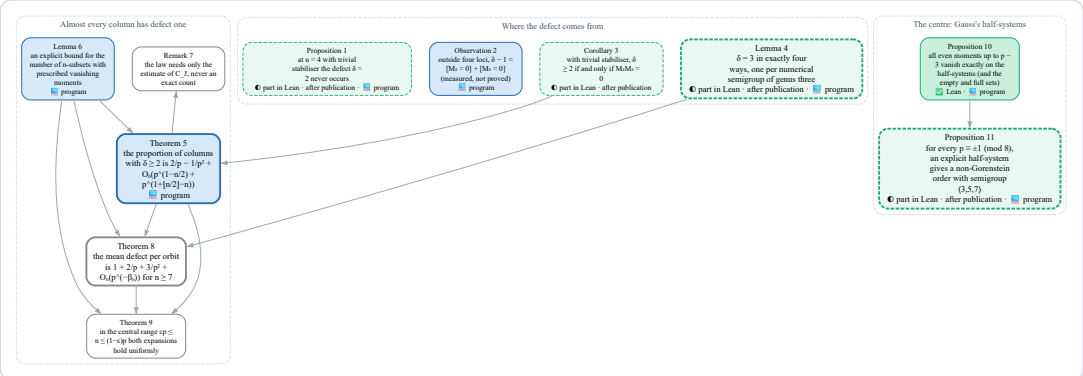
- **Lemma 4**: $\delta = 3$ in exactly four ways, one per numerical semigroup of genus three
- **Theorem 5**: the proportion of columns with $\delta \geq 2$ is $2/p - 1/p^2 + O_n(p^{(1-n/2)} + p^{(1+\lfloor n/2\rfloor - n)})$
- **Theorem 8**: the mean defect per orbit is $1 + 2/p + 3/p^2 + O_n(p^{(-\beta_n)})$ for $n \geq 7$
- **Proposition 11**: for every $p \equiv \pm 1 \pmod 8$, an explicit half-system gives a non-Gorenstein order with semigroup $\langle 3,5,7\rangle$

11 results | ✅ **1** entirely in Lean | ◐ **4** partly in Lean | 💻 **7** 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, §1–§3)

(§1) Let A_j be the order generated by the j-th Galois orbit of columns, in the étale algebra K_j, and $\mathcal{O}_j$ its normalisation. The fusion ring sits in a chain $R \subseteq \prod_j A_j \subseteq \prod_j \mathcal{O}_j$. The last index is the gluing, $G(n,p) := v_p[\prod_j A_j : R]$. Writing $\mathcal{O}$ for an orbit of centred spectra under $\mathbb{F}_p^\times$ and $h_\mathcal{O}$ for its stabiliser order,

$$D=\sum_{\mathcal{O}}\frac{p-1}{h_{\mathcal{O}}},\qquad b=\sum_{\mathcal{O}}1,\qquad \Delta=\sum_{\mathcal{O}}\delta_{\mathcal{O}},\qquad F_n(p)=\frac{1}{D}\sum_{\mathcal{O}}\frac{p-1}{h_{\mathcal{O}}}\,[\delta_{\mathcal{O}}\geq 2].$$

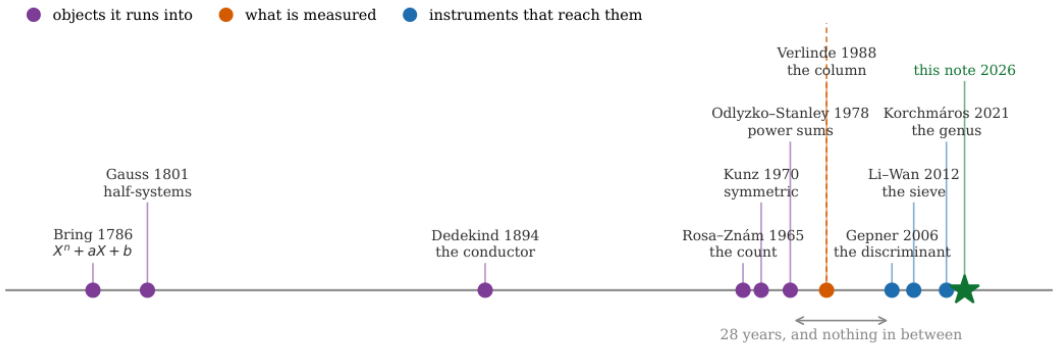
(§2) Part I reads the semigroup off the spectrum: with h the order of the multiplicative stabiliser of T and $e=(p-1)/h$ the ramification index, S_T is generated by e together with those $j<e$ for which $M_{hj}(T)\neq 0$. The defect $\delta(T)=\#(\mathbb{N}_0\setminus S_T)$ is therefore a function of one thing only: *which power sums of T vanish*. *(§3)* For $J\subseteq\{1,2,3\}$ with $1\in J$ write $C_J(n,p)$ for the number of centred T with $M_j(T)=0$ for every $j\in J$. *(§5)* A subset of $\mathbb{F}_p^{\times}$ containing exactly one of each pair $\{a,-a\}$ is a *half-system*.

1 The term without a closed form

No numbered statement in this section.

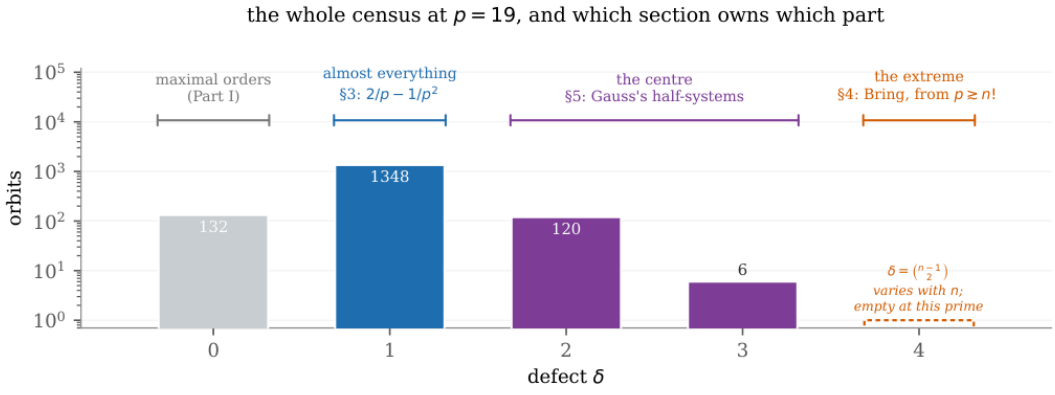
Its figures and tables are below; its text is in the paper, p. 1.

Figure 1



Everything this note runs into, on one axis, and the dashed line is the object it measures. To the left of it, in purple, the objects: Bring's trinomial, Gauss's half-system, Dedekind's conductor, Rosa and Znám's count, Kunz's criterion, Odlyzko and Stanley's enumeration of power sums. To the right, in blue, the instruments that reach them: Gepner's discriminant, the Li–Wan sieve, the generalised Bring curve. The split is clean — the last object is from 1978 and the first instrument from 2006, with nothing in between — and it is the point: nothing here was invented for the purpose.

Figure 2



The map, drawn on the object rather than tabulated. Every orbit at $p=19$, placed by its defect: $\delta=0$ are the maximal orders settled in Part I (132 orbits); $\delta=1$ is almost everything (1348) and is governed by the law of §3; the rare $\delta\geq 2$ (120 and 6) cluster at the centre, and the half-systems of §5 live in the second of those two columns. The last column is drawn detached and dashed on purpose: the maximal stratum of §4 sits at $\delta=\binom{n-1}{2}$, which is not a single value once n varies; the comparison with Bring is about $n\geq 5$, where at this prime that stratum is empty, and not about $n=3$, where the maximum is $\delta=1$ and is reached. §2 is what assigns an orbit to a column of this picture at all.

2 Where the defect comes from

Proposition 1. p. 5

> *At $n = 4$ and $h = 1$ the value $\delta = 2$ does not occur.*

Lean · ours, in part show

added to the Lean repository after publication (23-oct-2026): Covers the algebraic content of the n = 4 proposition over any field of char != 2, 3, with h = 1 entering as e_3 != 0; the generating rule of Part I is the definition genSet.

- `P3b.pow4_five_eq_zero`
- `P3b.pow4_three_eq`
- `P3b.genus_ne_two_of_four`

✅ Checked when this page was built: FourMoments.lean compiles with Lean 4.35.0, no errors, no sorry. Axioms — pow4_five_eq_zero, pow4_three_eq, genus_ne_two_of_four: propext, Classical.choice, Quot.sound.
Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean FourMoments.lean` (SHA-256 of the compiled file: `32919c3df5664506`…; 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: 3 results, standard axioms only

Proof: in this note · **Formalized:** Lean 4, by the author (public formalizations repository) · **Covers:** part: added to the Lean repository after publication (23-oct-2026): Covers the algebraic content of the n = 4 proposition over any field of char != 2, 3, with h = 1 entering as e_3 != 0; the generating rule of Part I is the definition genSet. · **Cite:** Proposition 1, p. 5, doi:10.5281/zenodo.22864267

↳ Not used by another result of the paper.

Proof

> First, $h = 1$ forces $e_3 \neq 0$: if $e_3 = 0$ then the centred quartic $X^4 + e_2X^2 - e_3X + e_4$ is even, so its root set is stable under $t \mapsto -t$ and $h \geq 2$. Hence $M_3 = 3e_3 \neq 0$ and $3 \in S_T$. Now if $M_2 \neq 0$ then $2 \in S_T$ too, so $S_T \supseteq \langle 2, 3\rangle$, whose only gap is 1, and $\delta = 1$. If $M_2 = 0$ then $e_2 = 0$, and by the cascade $M_5 = 0$ as well; hence $1, 2, 5 \notin S_T$ and $\delta \geq 3$. No spectrum is left for $\delta = 2$.

Evidence & scope

- **Program:** Newton recurrence, the cascade $M_2 = 0 \Rightarrow M_5 = 0$ at n = 4, and zero orbits with n = 4, δ = 2, over 7935 orbits, p ≤ 31, 3 ≤ n ≤ 7. `cascada_newton.py`

Observation 2. p. 5

> Let $h = 1$. Outside the four loci on which (M_2, M_3), (M_2, M_4), (M_2, M_5) or (M_3, M_5) vanish simultaneously, we find
>
> $$\delta - 1 \;=\; [\,M_2 = 0\,] + [\,M_3 = 0\,].$$
>
> This is measured, not proved, and everything below that rests on it inherits that status.

🆕 **Classical and new:** the paper labels it measured, not proved, and says nothing below depends on it.

↳ Not used by another result of the paper.

Evidence & scope

- **Program:** 438 orbits with h = 1 outside the loci, p ≤ 19, 3 ≤ n ≤ 7, no exception. `tricotomia.py`

Corollary 3. p. 5

> *For $h = 1$, $\delta \geq 2 \iff M_2M_3 = 0$.*

Lean · ours, in part show

added to the Lean repository after publication (21-oct-2026): δ ≥ 2 ↔ $M_2M_3 = 0$ from the generating rule (moments abstracted to a predicate), and g_i ≤ 2i − 1

- `P3b.two_le_genus_iff`
- `P3b.gap_le_two_mul_index_sub_one`
- `P3b.gap_le_two_mul_genus_sub_one`

✅ Checked when this page was built: GapBound.lean compiles with Lean 4.35.0, no errors, no sorry. Axioms — two_le_genus_iff, gap_le_two_mul_index_sub_one, gap_le_two_mul_genus_sub_one: propext, Classical.choice, Quot.sound.

Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean GapBound.lean` (SHA-256 of the compiled file: `f7f979544891ccc9…`; 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: 3 results, standard axioms only

Proof: in this note · **Covers:** not formalized · **Cite:** Observation 2, p. 5, doi:10.5281/zenodo.22864267

↳ Used in: Theorem 5 (p. 7)

Proof

The corollary does not need the Observation; it follows from the generating rule alone. Since T is centred, $M_1 = 0$, so $1 \notin S_T$. If $M_2M_3 \neq 0$ then $2, 3 \in S_T$, hence $S_T \supseteq \langle 2, 3\rangle$, whose only gap is 1, and $\delta = 1$. If $M_2 = 0$ then $2 \notin S_T$: it is not a generator, and it cannot be a sum of smaller positive elements because the only candidate is 1, which is absent. So 2 is a second gap and $\delta \geq 2$. If $M_3 = 0$ the same argument applies to 3, whose only decomposition by smaller indices would use 1.

Lemma 4. p. 6

Let T be centred with $h = 1$ and $p>7$. Then $\delta(T) = 3$ if and only if one of

$$\begin{array}{llll} S_T = \langle 4,5,6,7\rangle, & \text{gaps } \{1,2,3\}, & M_2 = M_3 = 0, & M_4M_5M_6M_7 \neq 0; \\ S_T = \langle 3,5,7\rangle, & \text{gaps } \{1,2,4\}, & M_2 = M_4 = 0, & M_3M_5M_7 \neq 0; \\ S_T = \langle 3,4\rangle, & \text{gaps } \{1,2,5\}, & M_2 = M_5 = 0, & M_3M_4 \neq 0; \\ S_T = \langle 2,7\rangle, & \text{gaps } \{1,3,5\}, & M_3 = M_5 = 0, & M_2M_7 \neq 0. \end{array}$$

Lean · ours, in part **show**

added to the Lean repository after publication (23-oct-2026): numerical semigroups of genus 3: the gap set is {1,2,3}, {1,2,4}, {1,2,5} or {1,3,5}. Not formalized: the translation into the vanishing and non-vanishing of the moments M_i for a centred T with h = 1

- `P3a.gaps_of_genus_eq_three`

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

Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean GenusThree.lean` (SHA-256 of the compiled file: `73567854f46d0932…`; 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: 1 result, standard axioms only

Proof: in this note · **Formalized:** Lean 4, by the author (public formalizations repository) · **Covers:** part: added to the Lean repository after publication (23-oct-2026): numerical semigroups of genus 3: the gap set is {1,2,3}, {1,2,4}, {1,2,5} or {1,3,5}. Not formalized: the translation into the vanishing and non-vanishing of the moments M_i for a centred T with h = 1 · **Cite:** Lemma 4, p. 6, doi:10.5281/zenodo.22864267

NEW **Classical and new:** that there are exactly four semigroups of genus three is classical [RG09]; the paper claims the vanishing-moment half of each row.

↳ Used in: Theorem 8 (p. 8)

Proof

That there are exactly four numerical semigroups of genus three, and that they are the ones listed, is classical and not ours; the count by genus is catalogued [6] . For completeness: the

> multiplicity is at most four; if it is four the gaps are $1, 2, 3$; if three, the gaps include $1, 2$ and one more, which must be 4 or 5 because $\langle 3, 4, 5\rangle$ contains every integer ≥ 3; if two, the gaps are the odd numbers below the smallest odd element, which must then be 7. What is ours is the second half of each row. The stated conditions are the generating rule read off each case: a minimal generator below e comes from a non-vanishing moment and a gap below e from a vanishing one, and the generators listed already produce every remaining index, so no further moment is constrained.

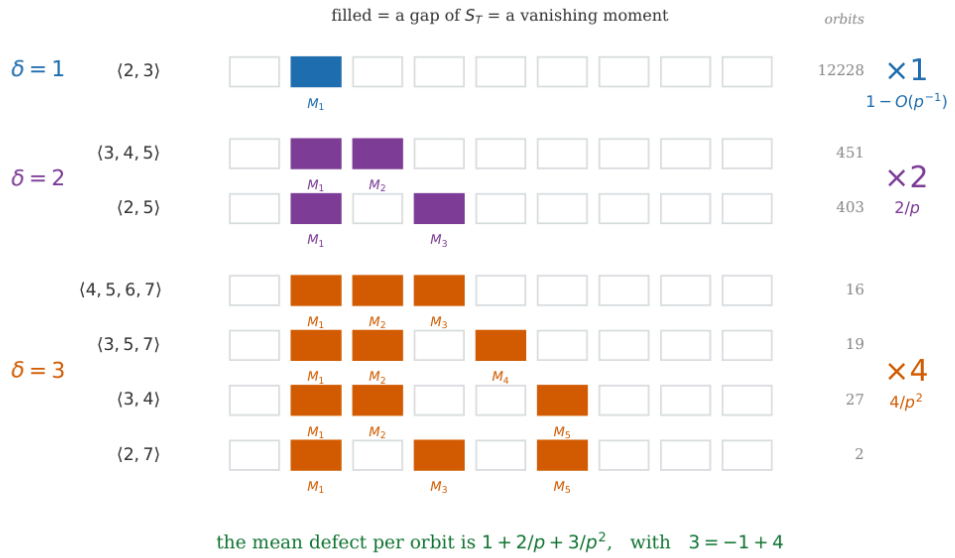
In plain words (commentary, not part of the paper)

1. For a centred spectrum with trivial stabiliser and $p>7$, defect three happens in exactly four ways, one for each numerical semigroup of genus three: $\langle 4, 5, 6, 7\rangle$, $\langle 3, 5, 7\rangle$, $\langle 3, 4\rangle$ and $\langle 2, 7\rangle$. Each way is a pair of vanishing power sums ($M_2 = M_3 = 0$, $M_2 = M_4 = 0$, $M_2 = M_5 = 0$ or $M_3 = M_5 = 0$) together with a few that must not vanish. 2. Why: by the generating rule of Part I a minimal generator below e comes from a nonzero moment and a gap below e from a vanishing one, so each semigroup of genus three translates into conditions on the moments; the generators of each row already produce every other index, so no further moment is constrained. 3. New and not new, as the paper says: that there are exactly four numerical semigroups of genus three is classical [RG09]; what the paper claims is the second half of each row, the vanishing moments. The consequence it uses later is that $\delta \geq 3$ (with $h = 1$) is governed by four *pairs* of vanishing conditions, and this is where the coefficient 4 in Theorem 8 comes from.

Evidence & scope

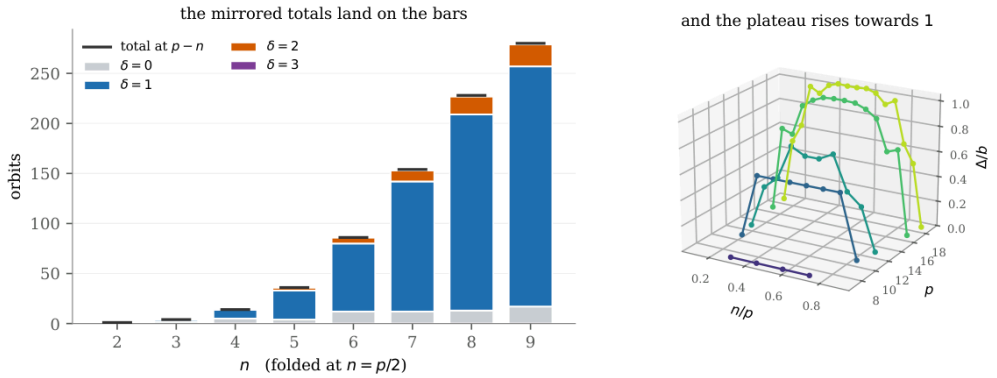
- **Program:** the four rows in both directions over every centred orbit with h = 1: p ≤ 19 all n, p = 23 with 4 ≤ n ≤ 9, p = 29 with 5 ≤ n ≤ 8; no fifth gap set. `familias_delta3.py`
- **Program:** the ladder of small defects (Figure 3). `escalera_defectos.py`

Figure 3



The small defects, and where the coefficients come from. One row per numerical semigroup of genus δ; a filled cell is a gap of S_T, and the same filled cell is the index of a moment that vanishes — the comb is read twice, which is what Lemma 4 says. The cell at 1 is filled in every row because T is centred, so every row starts from the same condition and only the rest distinguishes them. The number of rows in a band is the coefficient of the corresponding term: one semigroup of genus one, two of genus two, four of genus three, giving $2/p$ and $4/p^2$ and hence $3 = -1 + 4$ in Theorem 8. The counts on the right are orbits with $h = 1$ measured over $p \leq 29$; all four genus-three rows occur, the rarest twice.

Figure 4



Left: the census at $p = 19$ *folded* at $n = p/2$. The bars are the orbit counts by defect for $n \le p/2$; the dashes are the *totals* at the mirrored index $p - n$, plotted on top. They land on the bars — all eight pairs, exactly. What the dashes display is the equality of the totals; the stronger statement, that the whole distribution by defect agrees term by term, is the measurement recorded below the figure and is not something the dashes alone can show. Right: the mean defect Δ/b against n/p, which is a third quantity again — neither F_n, the proportion of *spectra* with $\delta \ge 2$, nor the unweighted proportion of orbits — one ridge per prime, with nothing interpolated between them: each ridge is symmetric, and the plateau rises towards 1 as p grows. The plateau sits at $n \asymp p/2$, which is outside the reach of Theorem 5; what governs it is Theorem 9, visible here before it is proved. Both from the archived output of `nivel_rango.py`.

3 Almost every column has defect one

Theorem 5. p. 8

For every fixed $n \ge 5$,

$$\boxed{F_n(p) \;=\; \frac{2}{p} - \frac{1}{p^2} \;+\; O_n\!\left(p^{1-n/2} + p^{1+\lfloor n/2\rfloor - n}\right)}$$

and in particular $F_n(p) = 2/p + O_n\!\left(p^{-\min(2,\, n/2-1)}\right)$.

Classical and new: the sieve over partitions is that of Li and Wan [LW], as in Lai, Marino, Robinson and Wan [LMRW20]; only the estimate is used, never an exact count [GMPP23].

↳ Used in: 7 (p. 8), Theorem 8 (p. 8), Theorem 9 (p. 9)

In plain words (commentary, not part of the paper)

1. Almost every column has defect one. For each fixed $n \ge 5$, the proportion $F_n(p)$ of centred spectra (equivalently, of columns at prime height) with $\delta \ge 2$ is $2/p - 1/p^2$ up to an error $O_n(p^{1-n/2} + p^{1+\lfloor n/2\rfloor - n})$; for $n \ge 7$ that error is $o(p^{-2})$, so the coefficient -1 is identified as a theorem. No factorial threshold in n is needed. 2. Why, in four steps: there are exactly $\binom{p}{n}/p$ centred spectra (translation has no fixed points); the number C_J of centred sets with prescribed vanishing moments is $\binom{p}{n}/p^{|J|} + O_n(p^{n/2})$ by additive characters, a sieve over partitions and Weil's bound (Lemma 6); by Corollary 3, with trivial stabiliser $\delta \ge 2$ means $M_2 M_3 = 0$, counted by inclusion–exclusion as $C_{\{1,2\}} + C_{\{1,3\}} - C_{\{1,2,3\}}$; and the spectra with a nontrivial stabiliser are only $O_n(p^{\lfloor n/2\rfloor})$. 3. The paper says plainly that the coefficient -1 is not visible numerically in the computed range ($n = 8$, $p \le 97$): a stabiliser correction of about $-8!/(384\,p)$ is still of size one there. Only the estimate of C_J is used, never an exact count (Remark 7). The sieve over partitions is that of Li and Wan, as in Lai, Marino, Robinson and Wan.

Evidence & scope

- **Program:** the four steps of the proof, each against the census (Step 3 exact for $5 \le n \le 8$, $p \le 43$). `ley_2p.py`

- **Numerical illustration (not a proof):** the three-moment census at n = 8 up to p = 97: the coefficient −1 is not yet visible, as the paper says. `ley_2p_largo.py`, `ley_2p_estabilizadores.py`

Lemma 6. p. 8

Let $n<p$, let J be a set of positive integers with $1 \in J$ and $d = \max J<p$, and let $C_J(n,p)$ be the number of n-subsets of $\mathbb{F}_p$ with $M_j = 0$ for every $j \in J$. Then

$$\boxed{\left| C_J(n,p) - p^{-|J|}\binom{p}{n} \right| \;\le\; \left(1 - p^{-|J|}\right) \frac{1}{n!} \prod_{r=0}^{n-1} \left((d-1)\sqrt{p} + r \right).} \qquad (1)$$

↳ Used in: Theorem 5 (p. 7), Theorem 8 (p. 8), Theorem 9 (p. 9)

Proof

Expand the $|J|$ conditions by additive characters. A frequency $(a_j)_{j\in J}$ contributes the sum of $e_p\big(\sum_{t\in T} f(t)\big)$ over n-subsets T, with phase polynomial $f(X) = \sum_{j\in J} a_j X^j$. The zero frequency gives $\binom{p}{n}/p^{|J|}$ exactly. On a non-zero frequency f is non-constant of degree at most d, so each character sum over $\mathbb{F}_p$ is at most $(d-1)\sqrt{p}$ by Weil. Expanding the n-subsets by cycle type contributes one such factor per cycle, and the identity $\sum_{\sigma\in S_n} x^{c(\sigma)} = x(x+1)\cdots(x+n-1)$ sums those contributions over S_n; dividing by $n!$ and summing the $p^{|J|} - 1$ non-zero frequencies gives the stated bound.

Evidence & scope

- **Program:** the bound holds in all 48 cases of the three-moment census, n = 8, 29 ≤ p ≤ 97 (ratio bound/error 57 to 2.4·10⁵). `cota_CJ.py`

Remark 7. p. 11

Theorem 5 needs only the estimate (4), never an exact formula for $C_{\{1,2\}}$, so it is unaffected by however the exact count of those subsets is settled [17] . The estimate is the whole of what the argument uses.

NEW **Classical and new:** the paper: «it is unaffected by however the exact count of those subsets is settled [GMPP23]».

↳ Not used by another result of the paper.

Theorem 8. p. 11

For every fixed $n \ge 7$, with $\beta_n = \min(3, n/2 - 1)$,

$$\boxed{\frac{\Delta(n,p)}{b(n,p)} \;=\; 1 + \frac{2}{p} + \frac{3}{p^2} + O_n\big(p^{-\beta_n}\big),}$$

and in the uniform measure on centred spectra $\mathbb{P}(\delta = 3) = 4/p^2 + O_n(p^{-\beta_n})$.

↳ Used in: Theorem 9 (p. 9)

Proof

The inclusion–exclusion is over the four *loci* $L_{ab} = \{M_a = M_b = 0\}$ with $ab \in \{23, 24, 25, 35\}$, not over the four rows of Lemma 4: the rows carry non-vanishing conditions as well and describe four different semigroups, so as events they are *disjoint* and there is nothing to include or exclude. It is the loci that overlap, and by the consequence recorded after that lemma their union is exactly $\{h = 1,\ \delta \ge 3\}$. Note that lying in L_{ab} is weaker than realising the corresponding semigroup: further moments may vanish and the defect may be larger.

Each locus imposes two vanishing conditions beyond $M_1 = 0$, so each has probability $p^{-2} + O_n(p^{1-n/2})$ by Lemma 6 with $d \le 5$. Any two of them together impose at least three — the six pairwise unions are $\{2,3,4\}$, $\{2,4,5\}$, $\{2,3,4,5\}$ and $\{2,3,5\}$ three times — so each intersection is $O_n(p^{-3} + p^{1-n/2})$, where the second term must be kept: at $n = 7$ it is $p^{-5/2}$, which is larger than p^{-3}. Inclusion–exclusion gives $\mathbb{P}(\delta \ge 3) = 4p^{-2} + O_n(p^{-\beta_n})$, and (7) with $r = 4$ gives $\mathbb{P}(\delta \ge 4) = O_n(p^{-3} + p^{1-n/2})$. Since T is centred, $1 \notin S_T$ whenever $h = 1$, so $\delta = 0$ forces $h>1$ and $\mathbb{P}(\delta = 0) = O_n(p^{-3})$ for $n \ge 7$. Now

$$\mathbb{E}\,\delta = \big(1 - \mathbb{P}(\delta = 0)\big) + \mathbb{P}(\delta \ge 2) + \mathbb{P}(\delta \ge 3) + \sum_{r \ge 4} \mathbb{P}(\delta \ge r),$$

the last sum being at most $\binom{n-1}{2}\mathbb{P}(\delta \ge 4)$. Substituting Theorem 5 for the second term and the above for the third gives $1 + 2/p + (-1+4)/p^2$, and the change of measure adds nothing at this order.

In plain words (commentary, not part of the paper)

1. The mean defect per orbit is $1 + 2/p + 3/p^2$ up to $O_n(p^{-\beta_n})$, $\beta_n = \min(3, n/2 - 1)$, for every fixed $n \ge 7$; and in the uniform measure on centred spectra, $\mathbb{P}(\delta = 3) = 4/p^2$ up to the same error. Since $\Delta(n,p)$ is the one term of the gluing formula without a closed form, this gives (granting the measured splitting of the discriminant) an estimate for the gluing $G(n,p)$ itself. 2. Why: write the mean as $1 - \mathbb{P}(\delta = 0) + \mathbb{P}(\delta \ge 2) + \mathbb{P}(\delta \ge 3) + \sum_{r \ge 4} \mathbb{P}(\delta \ge r)$. Theorem 5 gives $\mathbb{P}(\delta \ge 2) = 2/p - 1/p^2 + \dots$. By Lemma 4 the event $\delta \ge 3$ (with $h = 1$) is the union of four loci, each two vanishing moments beyond M_1; each has probability p^{-2} up to error (Lemma 6) and their pairwise intersections impose at least three conditions, so inclusion–exclusion gives $4/p^2$. The higher tails are bounded through the gap bound $g_i \le 2i - 1$. 3. So the coefficient 3 is $-1 + 4$: the -1 of Theorem 5 and one unit for each row of Lemma 4. The paper says the computed range ($p \le 19$, $n \le 8$) is nowhere near the asymptotic regime and neither confirms nor contradicts the theorem, which rests on its proof.

Evidence & scope

- **Numerical illustration (not a proof):** at p ≤ 19, n ≤ 8 the ratio Δ/b is still between 0.50 and 1.01: the computed range neither confirms nor contradicts the theorem, which rests on its proof. `censo_delta.py`

Theorem 9. p. 12

Fix $0<\varepsilon<1/2$. There is $c_\varepsilon>0$ such that, uniformly for $\varepsilon p \le n \le (1-\varepsilon)p$,

$$\boxed{F_n(p) = \frac{2}{p} - \frac{1}{p^2} + O_\varepsilon\big(e^{-c_\varepsilon p}\big)}, \qquad \frac{\Delta(n,p)}{b(n,p)} = 1 + \frac{2}{p} + \frac{3}{p^2} + O_\varepsilon\big(p^{-3}\big).$$

Classical and new: the paper gives the proof as a sketch and says so.

↳ Not used by another result of the paper.

Proof

Sketch. With $x = (d-1)\sqrt{p}$ and $L = \lceil x \rceil$, the right side of Lemma 6 is at most $\binom{n+L-1}{L-1} \le (n+L)^{L-1} = \exp\big(O_d(\sqrt{p}\log p)\big)$, while $\binom{p}{n} \ge e^{pH(n/p)}/(p+1) \ge e^{pH(\varepsilon)}/(p+1)$, H the binary entropy, because n is a mode of the corresponding binomial. The relative error is therefore exponentially small, uniformly in the strip, for any fixed d; we use $d \le 11$. For the stabilisers, a spectrum fixed by an element of order $h>1$ is a union of h-cosets, so with $n = hr$ their number is $A = \binom{(p-1)/h}{r}$ and $A^h \le \binom{p-1}{n}$, whence $A \le \binom{p}{n}^{1/2}$; summing over h leaves an exponentially small proportion. A fixed spectrum may also carry 0, so the case $n = hr + 1$ has to be counted as well; there $A^h \le \binom{p-1}{n-1}$ and the same estimate applies.

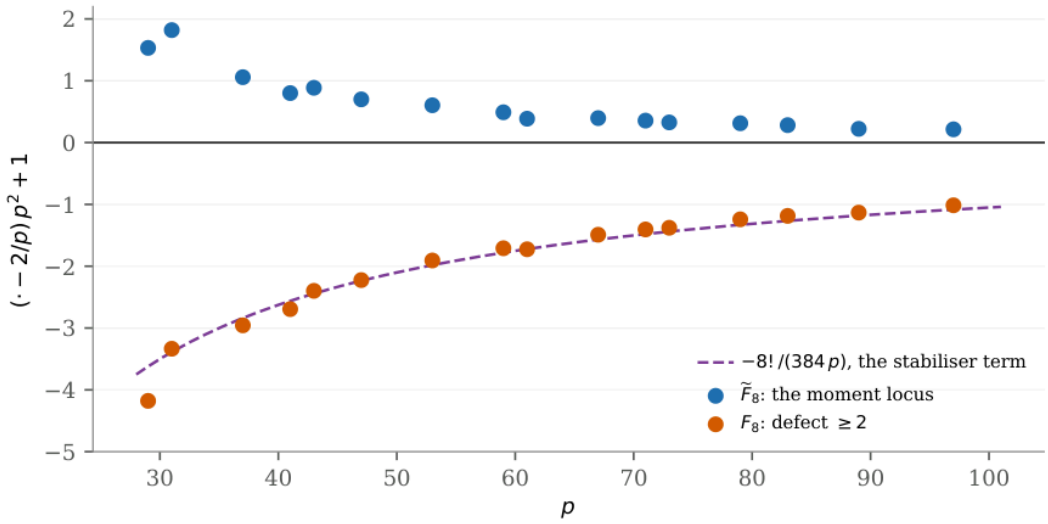
The two expansions then follow as in Theorems 5 and 8, with one change that is not cosmetic. For fixed n the higher tails were absorbed by $\sum_{r \ge 4} \mathbb{P}(\delta \ge r) \le L_n\,\mathbb{P}(\delta \ge 4)$ with $L_n = \binom{n-1}{2}$ constant. Here $n \asymp p$, so $L_n \asymp p^2$ and that step would give only $O(p^{-1})$. Instead keep the first two terms separate:

$$\boxed{\sum_{r\geq 4}\mathbb{P}(\delta\geq r)\;\leq\;\mathbb{P}(\delta\geq 4)+\mathbb{P}(\delta\geq 5)+L_n\,\mathbb{P}(\delta\geq 6)}.$$

By (7) with $d\leq 7,9,11$ the three terms are $O_\varepsilon(p^{-3})$, $O_\varepsilon(p^{-4})$ and $O_\varepsilon(p^{-5})$ up to exponentially small errors, so the sum is $p^{-3}+p^{-4}+O(p^2)p^{-5}=O_\varepsilon(p^{-3})$. This is what forces the moment of degree eleven: without the third term the factor L_n would have to multiply $\mathbb{P}(\delta\geq 4)$.

Finally the change of measure. Since $h\leq n$, every exceptional orbit has at least $(p-1)/n$ elements, which bounds their proportion among *orbits* and not merely among sets; in the strip the extra factors n and $\delta\leq\binom{n-1}{2}$ are absorbed by the exponentially small error.

Figure 5



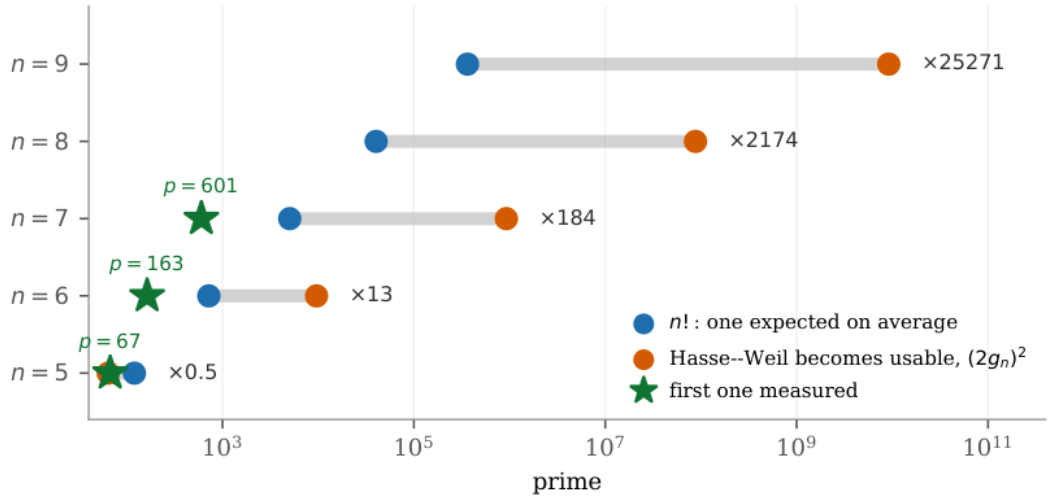
The two quantities at $n=8$ over the sixteen primes $29\leq p\leq 97$ — one more than the table above, which starts at 31 — plotted as $(\cdot-2/p)p^2+1$, which should tend to zero if the coefficient -1 is visible. Blue is the moment locus $\widetilde{F}_8$, orange is F_8 itself, and the dashed curve is not a fit but the stabiliser term $-8!/(384\,p)$ computed from the classification of the spectra with $h{>}1$. The two series approach zero from opposite sides, and neither is close to it at $p=97$: the dashed curve says why, and it is of size one over the whole range. The earlier version of this figure drew the blue points alone and labelled them F_8.

4 The extreme: Bring's quintics

No numbered statement in this section.

Its figures and tables are below; its text is in the paper, p. 13.

Figure 6



One bar per n, on a logarithmic scale: the bar *is* the gap. Its left end is $n!$, where the *expected* number of columns of maximal defect first reaches one; its right end is $(2g_n)^2$, the prime from which the Hasse–Weil bound carries any information; the ratio is printed beside it. The stars are measured first appearances — $p = 67$, 163 and 601 for $n = 5, 6, 7$ — and all three sit *left* of $n!$, by a margin that widens with n. That is the point of the figure: neither end of the bar predicts the star, but the right end misses it by a factor that grows quadratically while the left end misses it by a factor that stays small. At $n = 5$ the two ends are inverted, which is why the geometry works there and nowhere above.

5 The centre: Gauss's half-systems

Proposition 10. Lean ✓ p. 15

> *Let $T \subseteq \mathbb{F}_p^\times$ satisfy $M_r(T) = 0$ for every even r with $2 \le r \le p-3$. Then T is empty, a half-system, or all of $\mathbb{F}_p^\times$. Conversely every half-system has those moments zero. In particular a non-empty proper T with those moments zero has $|T| = (p-1)/2$: the size is forced, not assumed.*

Lean · ours show

- `HalfSystems.trichotomy`
- `HalfSystems.moments_of_halfSystem`

✅ Checked when this page was built: HalfSystems.lean compiles with Lean 4.35.0, no errors, no sorry. Axioms — trichotomy, moments_of_halfSystem: propext, Classical.choice, Quot.sound.
Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean HalfSystems.lean` (SHA-256 of the compiled file: `4e1ccb742e1cffc1…`; a source page on this site may show it with comments edited, under its own hash).

Trust base: 🔒 kernel only. Lean: 2 results, standard axioms only

Proof: in this note · **Covers:** not formalized · **Cite:** Theorem 5, p. 8, doi:10.5281/zenodo.22864267

🆕 **Classical and new:** the paper has not found the statement anywhere, under five vocabularies, and attributes it to nobody.

↳ Used in: Proposition 11 (p. 12)

Proof

For a quadratic residue q put $w(q) = \#\{t \in T : t^2 = q\} \in \{0, 1, 2\}$. For $r = 2k$ the hypothesis reads $\sum_q w(q) q^k = 0$ for $1 \le k < (p-1)/2$. The full Vandermonde matrix on the distinct values q, with rows $k = 0, \dots, m-1$, is invertible, so the rows $k = 1, \dots, m-1$ have a kernel of dimension exactly one; and the constant vector lies in it, because $\sum_{q \in \mathrm{QR}} q^k = 0$ for

$1 \le k < m$. Hence all $w(q)$ are equal, to 0, 1 or 2: T is empty, meets each pair $\{a, -a\}$ once, or is all of $\mathbb{F}_p^\times$. If $0 \in T$ the same argument applies to $T \setminus \{0\}$, which adds the half-systems with 0 adjoined, of size $(p+1)/2$.

Conversely, if T is a half-system then squaring is injective on T and T^2 runs over the quadratic residues exactly once, so for $r = 2k$ with $1 \le k < m$ one has $M_{2k}(T) = \sum_{s \in \mathrm{QR}} s^k = 0$.

Evidence & scope

- **Program:** no non-half-system with those moments over every orbit with p ≤ 19; the converse over 2924 half-systems. `semisistemas.py`

Proposition 11. p. 16

Let $p > 7$ be a prime with $(2 \mid p) = 1$ and let $m = (p-1)/2$. There is exactly one $k \in \{0, \dots, m\}$ with $8k(k+1) + 1 \equiv 0 \pmod{p}$, and for it the set

$$\boxed{T_k = \{1, \dots, k\} \cup \{-(k+1), \dots, -m\} \subset \mathbb{F}_p^\times}$$

is a centred half-system with trivial stabiliser and $S_{T_k} = \langle 3, 5, 7 \rangle$, hence $\delta(T_k) = 3$ and the order is not Gorenstein.

Lean · ours, in part show

added to the Lean repository after publication (23-oct-2026): Covers the moment computation of the family proposition for a given k with 8k(k+1)+1=0 and p>7; existence of k, centring and the semigroup <3,5,7> are not formalized.

- `P3a.moments_Tk`
- `P3a.moment_Tk_odd`

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

Reproduce: Lean 4.35.0, Mathlib f0b4c8150aa0; in that Lean project, `lake env lean FamilyMoments.lean` (SHA-256 of the compiled file: `bde3c56ef9d894d7…`; 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 · **Formalized:** Lean 4, by the author (public formalizations repository) · **Covers:** part: added to the Lean repository after publication (23-oct-2026): Covers the moment computation of the family proposition for a given k with 8k(k+1)+1=0 and p>7; existence of k, centring and the semigroup <3,5,7> are not formalized. · **Cite:** Proposition 11, p. 16, doi:10.5281/zenodo.22864267

🆕 **Classical and new:** infinite explicit non-Gorenstein families are cheap (Marseglia [Mar22]); the paper claims only that this one is natural and its semigroup does not move with p.

↳ Not used by another result of the paper.

Proof

The congruence is $(2k+1)^2 \equiv \frac{1}{2}$, which has two roots in $\mathbb{F}_p$ because $(2 \mid p) = 1$; they are k and $p-1-k$, one on each side of m, and neither equals m, so exactly one lies in $\{0, \dots, m\}$. By construction T_k contains one of each pair $\{t, -t\}$, so it is a half-system and every even moment vanishes by Proposition 10. For the odd ones put $u = k(k+1)$ and $v = m(m+1)$, so that $u \equiv -\frac{1}{8}$ and $v \equiv -\frac{1}{4}$ in $\mathbb{F}_p$. Writing $F_j(t) = \sum_{r \le t} r^j$, one has $M_j(T_k) = 2F_j(k) - F_j(m)$ for odd j, and the classical closed forms $F_3 = \frac{[t(t+1)]^2}{4}$, $F_5 = \frac{[t(t+1)]^2(2t(t+1)-1)}{12}$ and $F_7 = \frac{[t(t+1)]^2(3[t(t+1)]^2 - 4t(t+1)+2)}{24}$ give, after substituting u and v,

$$M_3(T_k) = -\tfrac{1}{128}, \qquad M_5(T_k) = \tfrac{7}{1536}, \qquad M_7(T_k) = -\tfrac{245}{49152},$$

all non-zero for $p > 7$. The same two variables give the centring, which does not follow from the three moments above: $F_1(t) = t(t+1)/2$, so

$$M_1(T_k) \;=\; 2F_1(k) - F_1(m) \;=\; u - \tfrac{v}{2} \;\equiv\; -\tfrac{1}{8} + \tfrac{1}{8} \;=\; 0.$$

> So T_k is centred, and $M_3 M_5 M_7 \neq 0$ forces $h = 1$; the displayed semigroup then follows from the previous paragraph.

💡 **In plain words (commentary, not part of the paper)**

1. For every prime $p>7$ with $p \equiv \pm 1 \pmod 8$ there is an explicit spectrum, $T_k = \{1, \dots, k\} \cup \{-(k+1), \dots, -m\}$ with $m = (p-1)/2$ and k the unique solution in $\{0, \dots, m\}$ of $8k(k+1) + 1 \equiv 0$, whose order has value semigroup $\langle 3, 5, 7 \rangle$: defect three, gaps $\{1, 2, 4\}$, and not Gorenstein. The semigroup does not move with p. 2. Why: T_k takes one element from each pair $\{t, -t\}$, so it is one of Gauss's half-systems and all its even moments vanish (Proposition 10). The odd ones come from Faulhaber's closed forms for $\sum r^3, \sum r^5, \sum r^7$ and $\sum r$, with $k(k+1) \equiv -1/8$ and $m(m+1) \equiv -1/4$: $M_1 = 0$ (the set is centred) and $M_3 = -1/128$, $M_5 = 7/1536$, $M_7 = -245/49152$, all nonzero for $p>7$, which forces a trivial stabiliser. The generating rule then gives $\langle 3, 5, 7 \rangle$, which is not symmetric, so Kunz's criterion says the order is not Gorenstein. 3. What the paper claims and what it does not: infinite explicit families of non-Gorenstein orders are cheap (Marseglia); the point here is that this family is natural, generated by character values, and its semigroup is constant. It covers the primes $p \equiv \pm 1 \pmod 8$, half of them by density, not all.

🛡️ **Evidence & scope**

- **Program:** the 19 admissible primes p ≤ 200: half-system, $M_1 = 0$, h = 1, the three constants, gaps 1,2,4. `familia_Tk.py`

6 What is open

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper, p. 19.

Note

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper (PDF).

MSC 2020

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper (PDF).

Declaration of competing interest

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper (PDF).

Data availability

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper (PDF).

Declaration on generative AI

No numbered statement in this section.

It is prose only (no statement, figure or table): read it in the paper (PDF).

📊 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 without a number, in the text of §3 Almost every column has defect one

p	31	37	41	43	47	53	59	61	67	71	73	79
$(\widetilde{F}_8 - 2/p)p^2 + 1$	1.82	1.06	0.80	0.89	0.70	0.60	0.49	0.39	0.40	0.36	0.33	0.31
$(F_8 - 2/p)p^2 + 1$	−3.33	−2.96	−2.69	−2.40	−2.22	−1.91	−1.71	−1.73	−1.49	−1.40	−1.38	−1.2

⬇ CSV

Table without a number, in the text of §4 The extreme: Bring's quintics

n	g_n	$(2g_n)^2$	$n!$	$(2g_n)^2/n!$
5	4	64	120	0.5
6	49	9 604	720	13.3
7	481	925 444	5 040	183.6
8	4 681	87 647 044	40 320	2 173.8

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

⬇ CSV

References

1 E. S. Bring, *Meletemata quaedam mathematica circa transformationem aequationum algebraicarum*, Lund, 1786. 🔎 find it

2 C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801. 🔎 find it

3 R. Dedekind, *Supplement XI*, in P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed., Vieweg, Braunschweig, 1894. 🔎 find it

4 E. Verlinde, *Fusion rules and modular transformations in 2D conformal field theory*, Nucl. Phys. B **300** (1988), 360–376. 🔎 find it

5 A. M. Odlyzko and R. P. Stanley, *Enumeration of power sums modulo a prime*, J. Number Theory **10** (1978), 263–272. 🔎 find it

6 J. C. Rosales and P. A. García-Sánchez, *Numerical Semigroups*, Developments in Mathematics **20**, Springer, 2009. 🔎 find it

7 D. Gepner, *Galois groups in rational conformal field theory II. The discriminant*, 2006, arXiv:hep-th/0608140.

8 E. Kunz, *The value-semigroup of a one-dimensional Gorenstein ring*, Proc. Amer. Math. Soc. **25** (1970), 748–751. 🔎 find it

9 A. Rosa and Š. Znám, *On a combinatorial problem in the theory of congruences* (in Russian), Mat.-Fyz. Časopis SAV **15** (1965), 49–59. 🔎 find it

10 N. J. A. Sloane (ed.), *The On-Line Encyclopedia of Integer Sequences*, sequence A262568, https://oeis.org/A262568.

11 C. Levaillant, *Powers of two weighted sum of the first p divided Bernoulli numbers modulo p*, arXiv:2001.03471.

12 S. Marseglia, *Cohen–Macaulay type of orders, generators and ideal classes*, arXiv:2206.03758.

13 G. Korchmáros, S. Lia and M. Timpanella, *A generalization of Bring's curve in any characteristic*, arXiv:2112.10886.

14 H. W. Braden and L. Disney-Hogg, *Bring's curve: old and new*, Eur. J. Math. **10** (2024), art. 3; doi:10.1007/s40879-023-00706-0; arXiv:2208.13692.

15 J. Li and D. Wan, *Counting subset sums of finite abelian groups*, J. Combin. Theory Ser. A **119** (2012), 170–182. 🔎 find it

16 T. Lai, A. Marino, A. Robinson and D. Wan, *Moment subset sums over finite fields*, Finite Fields Appl. **62** (2020), 101607. 🔎 find it

17 N. Giménez, G. Matera, M. Pérez and M. Privitelli, *Smooth symmetric systems over a finite field and applications*, arXiv:2312.09477.

18 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.

19 C. Marín, *The order generated by a column of the* $\mathrm{SU}(n)_k$ *S-matrix is locally a numerical semigroup ring. Part I: Gauss sums, power sums of the spectrum, and Gorenstein columns*, 2026, https://doi.org/10.5281/zenodo.22848529.