hexagon:2611.01164v1

THE ALON–TARSI (1992) CONJECTURE: FOR $n > 2$, CONGRUENCES MODULO DIVISORS OF $(n!)^3$ CAN PROVE IT ONLY AT DRISKO'S ORDERS

DAVE GOEL

Abstract. A Latin square of even order is even or odd according to the product of the signs of its rows and columns, read as permutations. The Alon–Tarsi conjecture (1992) says that for every even n the numbers L_n^e and L_n^o of even and odd Latin squares of order n are different. Drisko proved it for $n = p + 1$, p an odd prime (Drisko's orders), by showing that p^3 does not divide $L_n^e - L_n^o$; here p^3 divides $(n!)^3$, the order of the group that renames the rows, the columns and the symbols. Stones and Wanless observed that a congruence modulo a divisor of $(n!)^3$ can prove the conjecture at order n only through a prime factor of $c_n = (n!)^3/\gcd\big(L_n^e - L_n^o, (n!)^3\big)$. They found c_n for $n \le 9$, and their results show that no prime q with $n/2 < q < n-1$ divides it. We determine c_n for every even $n \ge 8$: $c_n = n-1$ if $n-1$ is prime, and $c_n = 1$ otherwise. So, for $n > 2$, such congruences can prove the conjecture at Drisko's orders and only there, and the smallest open order, 26, needs a different method. The main tool is an exact identity expressing $L_n^e - L_n^o$, up to sign, as $(n-1)!$ times a circuit-partition-polynomial value for the complete directed graph with two loops at each vertex. Successive vertex removals give a quadratic lower bound for the exponent of each fixed prime. A separate signed count of fixed Latin squares handles $q = n/2$. These results are verified in Lean.[1]

1. Introduction

A *Latin square* of order n is an $n \times n$ array filled with the symbols $1, \dots, n$ so that every symbol occurs exactly once in each row and exactly once in each column. Read from left to right, each row is a permutation of the symbols, and read from top to bottom, so is each column. A Latin square is *even* if the product of the signs of these $2n$ permutations is $+1$, and *odd* if it is -1 (Figure 1). Let L_n^e and L_n^o be the numbers of even and odd Latin squares of order n. For odd $n > 1$ these numbers are equal: exchanging the first two rows of a square leaves the set of row permutations unchanged and composes every column permutation with a transposition, so it changes the sign of the square by $(-1)^n = -1$ and pairs the even squares with the odd ones. For even n no such pairing is known, and Alon and Tarsi conjectured that none exists.

The Alon–Tarsi conjecture (1992 [2]). *For every even n, $L_n^e \neq L_n^o$.*

For more than three decades the Alon–Tarsi conjecture has stood among the central open problems in combinatorics; it carries the highest importance rating in the Open Problem Garden [21]. Alon and Tarsi showed that it implies Dinitz's conjecture on list colorings of the $n \times n$ array for even n (Galvin later proved Dinitz's conjecture by other means [12], a proof featured in Aigner and Ziegler's *Proofs from THE BOOK* [1, Chapter 38]). Huang and Rota [16] showed that the Alon–Tarsi conjecture implies Rota's basis conjecture (1989) in even dimension over characteristic 0 (the subject of the collaborative Polymath 12 project [22] and active recent work [23]). Beyond combinatorics, Kumar and Landsberg [18] linked the conjecture to a case of the Hadamard–Howe conjecture and to non-vanishing $\mathrm{SU}(n)$ integrals in geometric complexity theory, while Bürgisser and Ikenmeyer [9]

First version: November 26, 2026. This version (1.60): November 26, 2026.

2020 *Mathematics Subject Classification.* Primary 05B15; Secondary 05C45, 11A07, 20D20.

Key words and phrases. Latin squares, Alon–Tarsi conjecture, even and odd Latin squares, circuit partition polynomial, Sylow subgroups, congruences.

[1]Theorems A, B, and C are proved in Lean 4 from Lean's three standard axioms alone, and checked with `lake comparator`: https://github.com/david44hello/paper_alon-tarsi-1992-congruences/tree/v1.60/lean

TABLE 1. The best results before this paper and the new results. Here D_n is the number of even minus odd Latin squares whose first row and first column are $1, \dots, n$. For a prime q, $v_q(x)$ is its exponent in a nonzero integer x, with $v_q(0) = \infty$.

Best result before this paper	New result
c_n for $n \le 9$ [24, Section 5] and $n = 10$ (from [7]); for all even n: $n-1 \mid c_n$ when $n-1$ is prime [10], and no prime q with $n/2 < q < n-1$ divides c_n [24, Theorem 3.5].	c_n for every even $n \ge 8$: $c_n = n-1$ if $n-1$ is prime, and $c_n = 1$ otherwise (Theorem A).
$q^{v_q((n/2)!)} \mid D_n$, from $(n/2)! \mid D_n$ [7, Theorem 2.14]; one more factor q for some n and q [24, Theorem 3.4 and Table 4]; $q \mid D_n$ for every prime $q \le n-2$ [24, Theorem 3.5].	$M_q(n) = q^{v_q(n!)+v_q(n)}$ divides D_n for every even $n \ge 8$ and every prime $q \le n-2$ (Theorem B).
Linear in n: $v_q(L_n^e - L_n^o) \ge v_q(n!\,(n-1)!) + v_q((n/2)!)$ [7, Theorem 2.14], plus 1 in the cases above [24]; $2^{10} \mid D_{26}$ [24, Theorem 3.2].	A lower bound for $v_q(L_n^e - L_n^o)$ that is quadratic in n for every fixed prime q; for $q = 2$ it is at least $v_2((n-1)!) + n^2/4$ (Theorem C). At $n = 26$ the exact bound gives $2^{181} \mid D_{26}$.

and Amanov and Yeliussizov [4] connected it to fundamental invariants of tensors and rectangular Kronecker coefficients.

Despite this attention, the conjecture is known only for two infinite families of even orders: when $n-1$ is prime, by Drisko [10], and when $n+1$ is prime, by Glynn [13]. These two results cover every even order below 26, so 26 is the smallest open order. (A proof for $n = 2^r p$ [11] rests on a result of Zappa that Glynn found to be unreliable [13]. That case therefore remains open [24, p. 7].)

Drisko's proof, a congruence, is the starting point of this paper. Renaming the rows, the columns and the symbols of a Latin square gives another Latin square. These renamings form the *isotopy group* S_n^3, of order $(n!)^3$. For even n they do not change the sign of a square. Put $\Delta_n = L_n^e - L_n^o$. When a group G whose order is a power of a prime q acts on the Latin squares by isotopies, the squares fall into orbits, and the squares in one orbit have the same sign. A free orbit has $|G|$ squares of the same sign and contributes $\pm|G|$ to Δ_n, so

$$\Delta_n \equiv (\text{signed number of squares in the smaller orbits}) \pmod{|G|}. \tag{1.1}$$

The squares on the right are fixed by some element of G other than the identity. Their nontrivial symmetries make the smaller-orbit contributions accessible to counting in the cases below. For $n = p+1$, p an odd prime, Drisko took for G a Sylow p-subgroup of S_n^3, of order p^3, counted these squares and found $\Delta_n \equiv \pm p^2 \pmod{p^3}$. This shows $L_n^e \ne L_n^o$. We call the orders $n = p+1$, p an odd prime, *Drisko's orders*. (Glynn's congruence for $n = p-1$ is modulo $p = n+1$. It is not of this kind, because p does not divide $(n!)^3$.)

Can such a congruence decide the conjecture at other orders? Stones and Wanless examined this question in their paper "How not to prove the Alon–Tarsi conjecture" [24]. A congruence modulo a divisor m of $(n!)^3$ can show $\Delta_n \ne 0$ only if m does not divide Δ_n, and then some prime divides m to a higher power than it divides Δ_n. So the primes that can be used are those dividing

$$c_n = \frac{(n!)^3}{\gcd(\Delta_n, (n!)^3)} \qquad (n \text{ even}).$$

In particular, if $c_n = 1$, then $(n!)^3$ divides Δ_n, every congruence modulo a divisor of $(n!)^3$ reads $\Delta_n \equiv 0$, and no such congruence can prove the conjecture at order n. This is compatible with both $\Delta_n = 0$ and a nonzero multiple of $(n!)^3$. (Stones and Wanless write b_n for this number and c_n for an equal one defined through reduced squares; see (2.4).) They found c_n for $n \le 9$. At the even orders, $c_2 = 4$, $c_4 = 24$, $c_6 = 15$ and $c_8 = 7$. Their theorem [24, Theorem 3.5] also implies that no prime q with $n/2 < q < n-1$ divides c_n, and Drisko's congruence shows that $p = n-1$ divides c_n

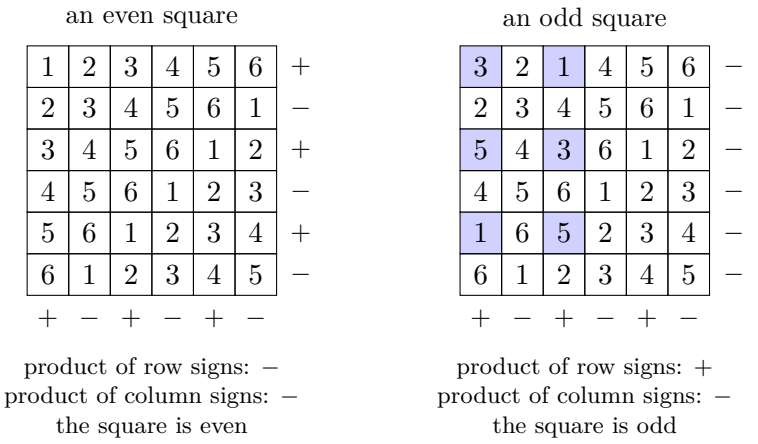

FIGURE 1. An even and an odd Latin square of order 6, with the sign of each row and each column (6 is the smallest even order with an odd square: every square of order 2 or 4 is even). The right square is the left one with two entries exchanged in each row that has blue shaded cells. The three row transpositions contribute -1, whereas the two column 3-cycles contribute $+1$; hence the sign of the square changes.

whenever it is prime. Berndsen's computation of the case $n = 10$ [7, Table 2.2] gives $c_{10} = 1$. Our main result determines c_n for every even $n \geq 8$.

Theorem A. *For every even $n \geq 8$,*

$$c_n = \begin{cases} n-1 & \text{if } n-1 \text{ is prime,} \\ 1 & \text{otherwise.} \end{cases}$$

Equivalently, $(n!)^3$ divides $L_n^e - L_n^o$ when $n-1$ is not prime, and $(n!)^3/(n-1)$, but not $(n!)^3$, divides it when $n-1$ is prime.

The orders 4 and 6 are Drisko's orders: $c_4 = 24$ is divisible by 3, and $c_6 = 15$ by 5. So, for every even $n > 2$, a congruence modulo a divisor of $(n!)^3$ can prove the Alon–Tarsi conjecture at order n exactly when $n-1$ is prime (Figure 2).

We prove Theorem A one prime at a time. For a prime q let $v_q(x)$ be the exponent of q in a nonzero integer x, with $v_q(0) = \infty$. By the definition of c_n, $q \nmid c_n$ means that $q^{3v_q(n!)}$, the full power of q in $(n!)^3$, divides Δ_n. It is convenient to divide out a known factor: let D_n be the number of even minus the number of odd *reduced* Latin squares of order n, those whose first row and first column are $1, 2, \ldots, n$ in this order. For even n, $\Delta_n = n!\,(n-1)!\,D_n$ (see (2.3)), so $q \nmid c_n$ exactly when D_n is divisible by

$$M_q(n) = q^{\,v_q(n!)+v_q(n)},$$

which we call the *natural modulus* of D_n at the prime q. A Sylow q-subgroup G of S_n^3 has order $q^{3v_q(n!)}$, so (1.1) determines Δ_n only modulo $q^{3v_q(n!)}$. After normalization, this is precisely the residue of D_n modulo $M_q(n)$. Thus, for congruences modulo divisors of $(n!)^3$, the available q-adic information about D_n is its residue modulo $M_q(n)$. Table 1 compares our three theorems with what was known before.

For even $n \geq 8$, our second theorem gives divisibility by the natural modulus at every prime $q \leq n-2$.

Theorem B. *For every even $n \geq 8$ and every prime $q \leq n-2$, the natural modulus $M_q(n) = q^{\,v_q(n!)+v_q(n)}$ divides D_n.*

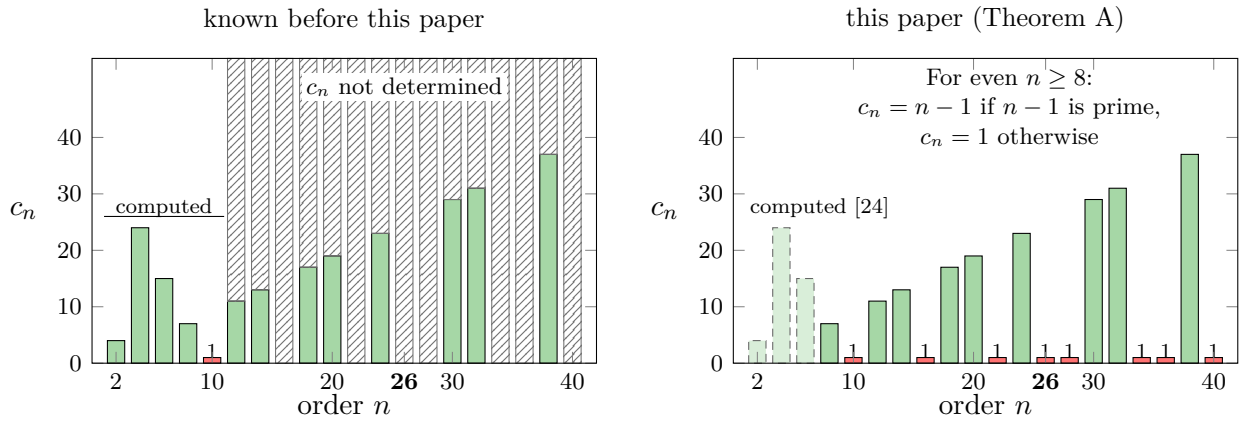

FIGURE 2. Green marks a known usable prime for the specified congruence method; red marks its failure; grey hatching marks an undetermined value of c_n. Here $c_n = (n!)^3/\gcd(\Delta_n, (n!)^3)$ for even $n \leq 40$; $c_n = 1$ blocks congruences modulo divisors of $(n!)^3$, not the Alon–Tarsi conjecture. Left: the computed values through $n = 10$, and the known divisor $n - 1$ at Drisko's orders. Right: Theorem A gives $c_n = n - 1$ at Drisko's orders and $c_n = 1$ otherwise, for even $n \geq 8$; the pale dashed bars at $n = 2, 4, 6$ are the computed values of Stones and Wanless. The smallest open order, 26, is marked in bold in both panels; $c_{26} = 1$.

Every prime factor of $(n!)^3$ is at most $n - 1$ when $n > 2$ is even. Theorem B therefore leaves only the prime $p = n - 1$, when it is prime. There Drisko's congruence shows that p exactly divides c_n. This is how Theorem A follows (Section 7).

For $q = 2$ and the odd primes $q \leq n/3$ we prove Theorem B through an exact identity instead of a congruence. For each fixed prime q, the bound we obtain, Theorem C, grows quadratically in n. Let $f_q(n, N)$ be the least value of $v_q(m_1! \cdots m_N!)$ over all ways of writing $n = m_1 + \cdots + m_N$ with positive integers m_i.

Theorem C. *For every even n and every prime q,*

$$v_q(L_n^e - L_n^o) \;\geq\; v_q((n-1)!) + \sum_{N=1}^{n-1} f_q(n, N).$$

The right side is at least $v_q(n!\,(n-1)!) + a(a-1)/2$ with $a = \lfloor n/q \rfloor$, a bound that is quadratic in n for every fixed q. For $q = 2$ it is at least $v_2((n-1)!) + n^2/4$.

For example, the exact sum in Theorem C gives $2^{181} \mid D_{26}$ (the form $n^2/4$ alone gives 2^{146}). Before, only $2^{10} \mid D_{26}$ was known [24, Theorem 3.2] (also from $13! \mid D_{26}$ [7, Theorem 2.14]), and the natural modulus is only $M_2(26) = 2^{24}$. So the 2-part of D_n lies far beyond what any congruence modulo a divisor of $(n!)^3$ can see. Theorem C is Theorem 4.1(a), (b) and Corollary 4.2 below.

The ideas of the proofs. The proof of Theorem B splits the primes $q \leq n - 2$ into four ranges, each with its own argument (Figure 3).

The prime 2 and the odd primes $q \leq n/3$ (Section 4). Here Theorem C implies Theorem B. It rests on an exact identity (Section 3): $L_n^e - L_n^o$ is, up to sign, $(n-1)!$ times the value at $x = -n$ of the circuit partition polynomial of the directed graph on $n - 1$ vertices with one arc from each vertex to each other vertex and two loops at each vertex. This polynomial counts the ways of splitting the arcs into closed trails. A vertex can be removed by joining its incoming arcs to its outgoing ones (Figure 4). At $x = -n$ each removal writes the value as the product of the factorials of the numbers of arcs into the removed vertex, times an integer combination of values for the smaller

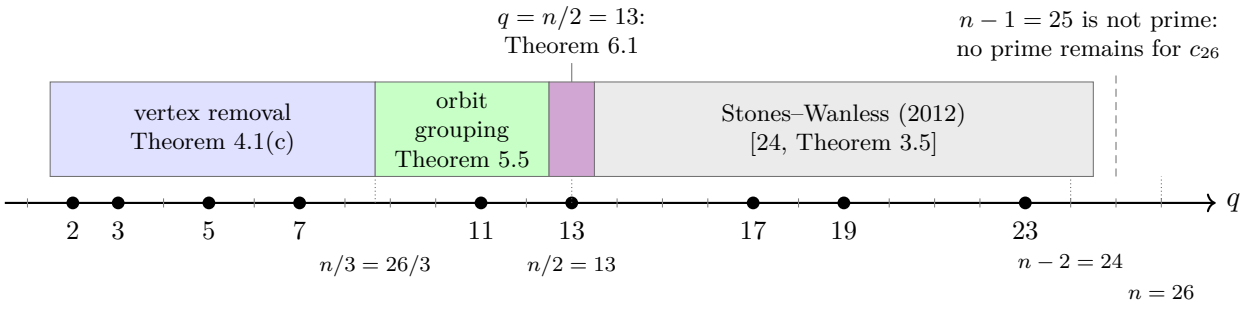

FIGURE 3. Shading separates the four prime ranges; the violet block highlights the case $q = n/2$. Each range names the argument that proves Theorem B for its primes, shown here for $n = 26$. All four ranges occur at $n = 26$, and the only candidate left over, $n - 1 = 25$, is not prime. Hence $c_{26} = 1$, and no congruence modulo a divisor of $(n!)^3$ can decide the order 26.

graphs. Removing the vertices one at a time collects one such product of factorials per step, and their exponents of q add up to the quadratic bound.

The odd primes q with $n/3 < q < n/2$ (Section 5). For $n = 3q - 1$ vertex removal already suffices; for $2q < n \leq 3q - 3$, it falls short by one factor of q. We remove all vertices but $2q$ at once and group the resulting terms under the symmetric group of the remaining $2q$ vertices: a term with a small stabilizer comes in an orbit whose size is divisible by q, and in a term fixed by a q-cycle the q walks that leave one vertex all end at one vertex w, so column w of the smaller matrix has an entry at least $q + 1$. This gives the extra factor q.

The prime $q = n/2$ (Section 6). Here we return to Drisko's method, with a Sylow q-subgroup $\mathbb{F}_q^6$ of S_n^3. A Möbius inversion over its subgroups expresses Δ_n modulo q^6 through the signed numbers of squares fixed by its subgroups of rank 1, 2 and 3. Together, the subgroups of rank two and three contribute a multiple of q^6. Individual rank-one contributions are divisible by q^4; to determine their sum modulo q^6 we must retain their cancellation. The sum gives $\Delta_{2q} \equiv q^5 \sum_{m=1}^{q-1} m^{-2} \pmod{q^6}$, and $\sum_{m=1}^{q-1} m^{-2} \equiv 0 \pmod{q}$ for $q \geq 5$.

The primes q with $n/2 < q \leq n - 2$. Here $M_q(n) = q$, and $q \mid D_n$ is due to Stones and Wanless [24, Theorem 3.5].

Section 2 fixes notation and recalls the known facts we use. Sections 3 and 4 prove Theorem C, Section 5 the case $n/3 < q < n/2$, and Section 6 the case $q = n/2$. Section 7 assembles the proofs of Theorems A and B, and Section 8 discusses implications and open directions.

2. Notation and known facts

We index rows, columns and symbols by $[n] = \{1, \ldots, n\}$, and view a Latin square L as a map $[n]^2 \to [n]$, $(r, c) \mapsto L(r, c)$. Its row r is the permutation $\rho_r = L(r, \cdot)$, which sends a column to a symbol, and its column c is the permutation $\gamma_c = L(\cdot, c)$, which sends a row to a symbol. For a symbol s let ζ_s be the permutation that sends a row r to the column c with $L(r, c) = s$. Put

$$\operatorname{sgn}_{\mathrm{row}}(L) = \prod_r \operatorname{sgn} \rho_r, \qquad \operatorname{sgn}_{\mathrm{col}}(L) = \prod_c \operatorname{sgn} \gamma_c, \qquad \operatorname{sgn}_{\mathrm{sym}}(L) = \prod_s \operatorname{sgn} \zeta_s,$$

and let $\varepsilon(L) = \operatorname{sgn}_{\mathrm{row}}(L) \operatorname{sgn}_{\mathrm{col}}(L)$ be the *sign* of L. Thus L is even if $\varepsilon(L) = 1$ and odd if $\varepsilon(L) = -1$. Then

$$\Delta_n = \sum_L \varepsilon(L) = L_n^e - L_n^o,$$

the sum over all Latin squares of order n. A Latin square is *reduced* if its first row and its first column are $1, 2, \dots, n$ in this order, and D_n is the sum of $\varepsilon(L)$ over the reduced squares. As in the introduction, $v_q(x)$ is the exponent of the prime q in x, with $v_q(0) = \infty$.

An *isotopy* is a triple $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in S_n^3$ of permutations of the rows, the columns and the symbols. It acts on Latin squares by $(\sigma L)(\sigma_1(r), \sigma_2(c)) = \sigma_3(L(r, c))$. So row $\sigma_1(r)$ of σL is $\sigma_3 \circ \rho_r \circ \sigma_2^{-1}$, and column $\sigma_2(c)$ is $\sigma_3 \circ \gamma_c \circ \sigma_1^{-1}$. An isotopy that fixes L is an *autotopism* of L. We use three known facts.

- *Janssen's identity* [17, Theorem 3.2], first proved by Richard Wilson [7, p. 12] (see also [24, (1.2)]): for every Latin square L of order n,

$$\operatorname{sgn}_{\mathrm{row}}(L)\, \operatorname{sgn}_{\mathrm{col}}(L)\, \operatorname{sgn}_{\mathrm{sym}}(L) = (-1)^{n(n-1)/2}. \tag{2.1}$$

- *Isotopy invariance* [24, (1.4)]: by the formulas for the rows and columns of σL, $\operatorname{sgn}_{\mathrm{row}}(\sigma L) = \operatorname{sgn}_{\mathrm{row}}(L)\,(\operatorname{sgn}\sigma_2 \operatorname{sgn}\sigma_3)^n$ and $\operatorname{sgn}_{\mathrm{col}}(\sigma L) = \operatorname{sgn}_{\mathrm{col}}(L)\,(\operatorname{sgn}\sigma_1 \operatorname{sgn}\sigma_3)^n$. Hence, for even n,

$$\varepsilon(\sigma L) = \varepsilon(L) \qquad (\sigma \in S_n^3). \tag{2.2}$$

- *Normalization* [24, (1.5), (1.8)]: for even n,

$$\Delta_n = n!\,(n-1)!\,D_n. \tag{2.3}$$

Stones and Wanless's b_n [24, Section 5] is our c_n. They also define $n!\,n/\gcd(D_n, n!\,n)$, denoted c_n in [24]. For even n the two agree: as $(n!)^3 = n!\,(n-1)! \cdot n!\,n$, the normalization (2.3) gives

$$c_n = \frac{n!\,n}{\gcd(D_n,\, n!\,n)} = \frac{(n!)^3}{\gcd(\Delta_n, (n!)^3)}. \tag{2.4}$$

As the exponent of a prime q in $n!\,n$ is $v_q(n!) + v_q(n)$, this is the statement of the introduction: $q \nmid c_n$ exactly when the natural modulus $M_q(n)$ divides D_n.

3. The circuit partition polynomial and vertex removal

This section writes $L_n^e - L_n^o$ as a value of a graph polynomial (Proposition 3.6) and proves the rule that removes one vertex of the graph at a time (Lemma 3.3). Propositions 3.5 and 3.6 apply the rule $n-1$ times in all. Section 4 reads off the bounds.

A *multidigraph* H has a finite vertex set and a finite set of labeled arcs. Each arc goes from its tail to its head. Loops and parallel arcs are allowed. Its matrix $M = M(H)$ has entry M_{uv} equal to the number of arcs from u to v. We call H *d-regular* if every vertex has d arcs coming in and d arcs going out. A *transition system* π of H chooses at each vertex v a bijection π_v from the arcs into v to the arcs out of v. The map $a \mapsto \pi_{\mathrm{head}(a)}(a)$, which follows each arc by the next, is a permutation of the arcs. Its cycles are closed trails (closed walks that use no arc twice), which together use every arc of H exactly once. Let $\mathrm{cyc}(\pi)$ be the number of these closed trails. The *circuit partition polynomial* of H is

$$j(H; x) = \sum_{\pi} x^{\mathrm{cyc}(\pi)},$$

the sum over all transition systems. (It is closely related to the Martin polynomial, introduced by Martin and studied by Las Vergnas [19]; see also [8].) Let K_n° be the complete digraph with loops on $[n]$. It has one arc from every vertex to every vertex, including one loop at each vertex. Thus $M(K_n^\circ) = J_n$, where J_N denotes the all-ones matrix of size N. We write J when the size is clear. We write I for the identity matrix, $X = (x_{uv})$ for a square matrix of independent indeterminates, and $[x^M]F$ for the coefficient of the monomial $x^M = \prod_{u,v} x_{uv}^{M_{uv}}$ in a polynomial F. The link with Latin squares goes through the value of j at $x = -d$: the next lemma expresses it through a coefficient of $\det(X)^d$, and Lemma 3.2 identifies that coefficient with $\pm\Delta_n$.

Lemma 3.1. *If H is d-regular on N vertices and $M = M(H)$, then*

$$j(H;-d) = (-1)^{Nd}\Big(\prod_{u,v} M_{uv}!\Big)[x^M]\det(X)^d.$$

Proof. We give each arc a its own variable y_a and let $Y = \sum_a y_a E_{\mathrm{tail}(a),\mathrm{head}(a)}$, where E_{uv} is the matrix unit. There are Nd arcs. We compute the coefficient of $\prod_a y_a$ in $\det(Y)^d$ in two ways.

First, in the ring of formal power series in t over $\mathbb{Q}[y_a]$,

$$\det(I+tY)^d = \exp\Big(d\sum_{k\ge1}\frac{(-1)^{k-1}t^k}{k}\operatorname{tr}(Y^k)\Big).$$

The polynomial $\det(I+tY)$ has degree at most N in t, with leading coefficient $\det Y$. Therefore the coefficient of t^{Nd} on the left is $\det(Y)^d$. On the right, $\operatorname{tr}(Y^k)$ is the sum of $\prod_i y_{a_i}$ over the rooted closed walks $(a_1,\dots,a_k)$ of length k. When we expand the exponential, the coefficient of $t^{Nd}\prod_a y_a$ becomes a sum over the partitions λ of Nd. If λ has m_k parts equal to k, its term is

$$\prod_k \frac{1}{m_k!}\Big(\frac{d(-1)^{k-1}}{k}\Big)^{m_k}\cdot\Big[\prod_a y_a\Big]\prod_i \operatorname{tr}(Y^{\lambda_i}).$$

The last factor counts the ordered tuples of rooted closed walks, of lengths $\lambda_1,\lambda_2,\dots$, that together use every arc exactly once. Each of these walks uses no arc twice and is therefore a closed trail. A closed trail of length k has exactly k rootings, because a rotation that fixed it would repeat an arc. Trails of equal length can fill their m_k places in $m_k!$ orders. So the last factor is $z_\lambda W_\lambda$, where $z_\lambda = \prod_k k^{m_k}m_k!$ and W_λ is the number of ways to split the arcs into closed trails of lengths given by λ. The term of λ is therefore $(-1)^{Nd-c}d^cW_\lambda$ with $c=\sum_k m_k$ the number of trails. A splitting of the arcs into closed trails is the same thing as a permutation $a\mapsto a'$ of the arcs with $\mathrm{tail}(a') = \mathrm{head}(a)$, that is, a transition system. Summing over λ,

$$\Big[\prod_a y_a\Big]\det(Y)^d = \sum_\pi (-1)^{Nd-\mathrm{cyc}(\pi)}d^{\mathrm{cyc}(\pi)} = (-1)^{Nd}j(H;-d).$$

Second, $\det Y = \det X$ under the substitution $x_{uv} = \sum_{a:\,u\to v} y_a$. A monomial $x^{M'}$ becomes a polynomial in which $\prod_a y_a$ occurs only if $M' = M$. In that case its coefficient is $\prod_{u,v} M_{uv}!$. Comparing the two computations proves the lemma. □

Lemma 3.1 may be compared with the known evaluations of the circuit partition polynomial and of the Martin polynomial at negative integers [8, 19]. For $d=2$ compare Martin's theorem [5, Theorem 26], and see also [20]. Since parallel arcs are interchangeable, $j(H;x)$ depends only on the matrix $M = M(H)$. When H is d-regular we write $j(M)$ for $j(H;-d)$.

Lemma 3.2. *For even n, $j(K_n^\circ;-n) = [x^J]\det(X)^n = (-1)^{n/2}\Delta_n$.*

Proof. The first equality is Lemma 3.1 with $M = J$ and $N = d = n$ (the sign $(-1)^{n^2}$ is 1 as n is even). For the second, we expand $\det(X)^n = \prod_{k=1}^n \sum_{\sigma_k\in S_n}\operatorname{sgn}(\sigma_k)\prod_i x_{i\sigma_k(i)}$. A term contributes to the coefficient of x^J, in which every variable occurs exactly once, when the graphs of $\sigma_1,\dots,\sigma_n$ partition $[n]^2$, that is, when $L(i,\sigma_k(i)) = k$ defines a Latin square L. Then σ_k sends a row to the column that holds the symbol k. Thus $\sigma_k = \zeta_k$, and the term is $\operatorname{sgn}_{\mathrm{sym}}(L)$. By Janssen's identity (2.1), $\operatorname{sgn}_{\mathrm{sym}}(L) = (-1)^{n(n-1)/2}\varepsilon(L)$. Finally, $n(n-1)/2 \equiv n/2 \pmod 2$ for even n. □

The second equality is the classical expression of $L_n^e - L_n^o$ as a coefficient of $\det(X)^n$ (see, for example, [3]). The divisibility results below use only $|j(K_n^\circ;-n)| = |\Delta_n|$.

The next lemma removes one vertex w. A closed trail that passes through w enters along an arc into w, perhaps runs around some loops at w, and leaves along an arc out of w. When we remove w, each such passage becomes one *virtual* arc (Figure 4).

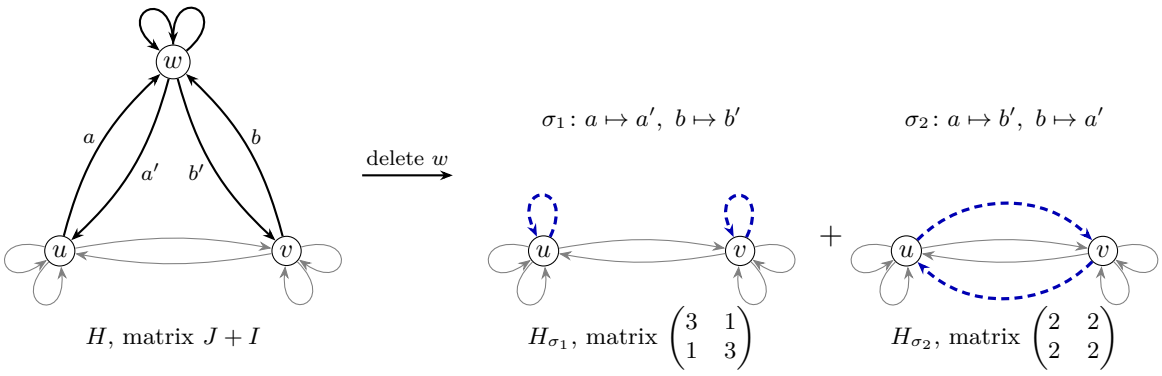

FIGURE 4. Removing a vertex w (Lemma 3.3). Black arcs are the arcs at w, gray arcs are not at w and do not change, and blue dashed arcs are virtual arcs. Here H is the graph of Proposition 3.6 for $n = 4$, with $d = 4$ and $k = 2$. Left: the arcs at w, with two loops. Middle and right: the two bijections σ_1, σ_2 from the arcs into w (other than loops) to the arcs out of w join each incoming arc to an outgoing one. Each joined pair becomes one virtual arc of the smaller graph H_σ. The k loops at w contribute only the factor $(x+d-k)\cdots(x+d-1)$ in front of the sum over σ. In this example, (E) is $j(H;x) = (x+2)(x+3)\big(j(H_{\sigma_1};x) + j(H_{\sigma_2};x)\big)$.

Lemma 3.3. *Let H be d-regular on a vertex set V with $|V| \geq 2$, let $w \in V$, and let $k = M_{ww}$ be the number of loops at w. For each bijection σ from the $d-k$ non-loop arcs into w to the $d-k$ non-loop arcs out of w, let H_σ be the multidigraph on $V \setminus \{w\}$ obtained by deleting w and adding, for every non-loop arc $e = (u \to w)$, a virtual arc from u to the head of $\sigma(e)$. Then every H_σ is d-regular,*

$$j(H;x) = (x+d-k)(x+d-k+1)\cdots(x+d-1)\sum_{\sigma} j(H_\sigma;x) \tag{E}$$

as polynomials, and

$$j(M) = (-1)^k k! \sum_{R} \operatorname{count}(R)\, j(M' + R), \qquad \operatorname{count}(R) = \frac{\prod_{u\neq w} M_{uw}! \prod_{v\neq w} M_{wv}!}{\prod_{u,v\neq w} R_{uv}!}, \tag{E$'$}$$

where M' is the restriction of M to $V \setminus \{w\}$ and R runs over the matrices of nonnegative integers on $(V \setminus \{w\})^2$ with row sums M_{uw} and column sums M_{wv}.

Proof. (i) *Strands.* We fix transitions π_v at all $v \neq w$ and π_w at w. Start from a non-loop arc e into w and apply π_w repeatedly: the walk runs through loops at w (each loop is an arc out of w and then an arc into w) until it reaches a non-loop arc out of w. It cannot repeat an arc. Indeed, e is not an arc out of w, hence not a value of π_w, and π_w is injective. As there are finitely many loops, the walk ends. The same argument for π_w^{-1} gives, from each non-loop arc out of w, a walk that ends at a non-loop arc into w. Therefore distinct walks end at distinct arcs, and π_w maps the set of loops that lie on no walk onto itself. Thus π_w splits the arcs at w into $d-k$ *strands* (a non-loop arc in, some loops, a non-loop arc out) and cyc_w cycles made of loops only. The map $\sigma(\pi_w)$ that sends the first arc of each strand to its last arc is a bijection.

(ii) *The loops.* For fixed σ, $\sum_{\pi_w:\,\sigma(\pi_w)=\sigma} x^{\mathrm{cyc}_w} = \prod_{i=0}^{k-1}(x+d-k+i)$. To see this, we place the k labeled loops one at a time. Loop $i+1$ goes directly after one of the $d-k$ strand starts or directly after one of the i loops already placed ($d-k+i$ choices, no new cycle), or it opens a new cycle of loops (weight x). Each π_w arises exactly once, as removing the loops in reverse order shows.

(iii) *The smaller graph.* At a vertex $v \neq w$, the arcs into v in H_σ are those in H, with each arc $w \to v$ replaced by the virtual arc that ends in it. The arcs out of v change in the same way. So the

transitions π_v, $v \neq w$, form a transition system of H_σ. The closed trails of H are the cyc_w cycles of loops together with, bijectively, the closed trails of H_σ (contract each strand to its virtual arc). Summing over the π_v and over π_w gives (E). A vertex $v \neq w$ gains M_{wv} virtual arcs in and loses its M_{wv} arcs from w. The same holds for the outgoing arcs. So H_σ is d-regular.

(iv) *At $x = -d$.* The factor in front becomes $(-k)(-k+1)\cdots(-1) = (-1)^k k!$. Let the profile R of σ be the matrix with R_{uv} equal to the number of arcs e from u into w for which $\sigma(e)$ goes to v. The number of σ with profile R is $\mathrm{count}(R)$. To build such a bijection, we split the M_{uw} arcs from each u by their targets ($M_{uw}!/\prod_v R_{uv}!$ ways) and the M_{wv} arcs to each v by their sources ($M_{wv}!/\prod_u R_{uv}!$ ways). Then we match the two parts of each block ($\prod_{u,v} R_{uv}!$ ways). Finally, $M(H_\sigma) = M' + R$. □

Identity (E) is a vertex recursion of the circuit partition polynomial of the kind in [19].

Corollary 3.4. *In Lemma 3.3, for every prime q,*

$$v_q(j(M)) \geq v_q\Big(\prod_{u\in V} M_{uw}!\Big) + \min_R v_q(j(M' + R)).$$

Proof. We write $\mathrm{count}(R) = \prod_{u\neq w} M_{uw}! \cdot \prod_{v\neq w}[M_{wv}!/\prod_{u\neq w} R_{uv}!]$. Each bracket is a multinomial coefficient, because column v of R sums to M_{wv}. Together with $k! = M_{ww}!$, (E′) writes $j(M)$ as $\pm\prod_{u\in V} M_{uw}!$ times an integer combination of the integers $j(M' + R)$. □

So removing w gains the factorials of the entries of column w. If all entries of M are positive and its line sums are n, these are N positive numbers with sum n. By its definition in the introduction, $f_q(n, N)$ is the least possible exponent of q in the product of their factorials.

Proposition 3.5. *Let H be n-regular on $N \geq 1$ vertices, with $M_{uv} \geq 1$ for all u, v (loops included). Then $v_q(j(M)) \geq \sum_{N'=1}^{N} f_q(n, N')$ for every prime q.*

Proof. Since the entries of a row are at least 1 and sum to n, we have $N \leq n$. We use induction on N. If $N = 1$, H is one vertex with n loops. A transition system is then a permutation of the loops, and $j(H; x) = x(x+1)\cdots(x+n-1)$. Thus $j(M) = (-1)^n n!$ and $v_q(j(M)) = v_q(n!) = f_q(n, 1)$. If $N \geq 2$, we pick any vertex w. Column w of M has N entries, each at least 1, with sum n. Therefore $v_q(\prod_u M_{uw}!) \geq f_q(n, N)$. Every $M' + R$ is $(N-1)\times(N-1)$, has all entries at least $M'_{uv} \geq 1$, and has all line sums n (row u: $(n - M_{uw}) + M_{uw}$, column v: $(n - M_{wv}) + M_{wv}$). Corollary 3.4 and the induction hypothesis finish the proof. □

Removing one vertex of K_n° gives the exact identity behind Theorem C.

Proposition 3.6. *For even n, $\Delta_n = (-1)^{n/2+1}(n-1)!\, j(J+I)$, where $J + I$ is of size $n-1$. That is, $L_n^e - L_n^o$ is, up to sign, $(n-1)!$ times the value at $x = -n$ of the circuit partition polynomial of the n-regular digraph on $n-1$ vertices with one arc from each vertex to each other vertex and two loops at each vertex.*

Proof. By Lemma 3.2, $\Delta_n = (-1)^{n/2} j(J_n)$, with $d = n$. We apply (E′) at any vertex w. There $k = 1$. Every R has all line sums 1 and is therefore a permutation matrix P of size $n-1$, with $\mathrm{count}(R) = 1$. Thus $j(J_n) = -\sum_P j(J_{n-1} + P)$. We show that the $(n-1)!$ terms are equal. By Lemma 3.1, $j(J_{n-1} + P) = 2^{n-1}[x^{J_{n-1}+P}]\det(X)^n$, since $J_{n-1} + P$ has $n-1$ entries equal to 2 and $(-1)^{(n-1)n} = 1$. If $P_{u,p(u)} = 1$ for a permutation p, the substitution $X \mapsto XP$, that is $x_{uv} \mapsto x_{u,p^{-1}(v)}$, multiplies $\det(X)^n$ by $\det(P)^n = 1$ (n is even) and carries the monomial $x^{J_{n-1}+P}$ to $x^{J_{n-1}+I}$. Hence $j(J_{n-1} + P) = j(J_{n-1} + I)$ for every P, so $j(J_n) = -(n-1)!\, j(J_{n-1} + I)$, and therefore $\Delta_n = (-1)^{n/2} j(J_n) = (-1)^{n/2+1}(n-1)!\, j(J_{n-1} + I)$. □

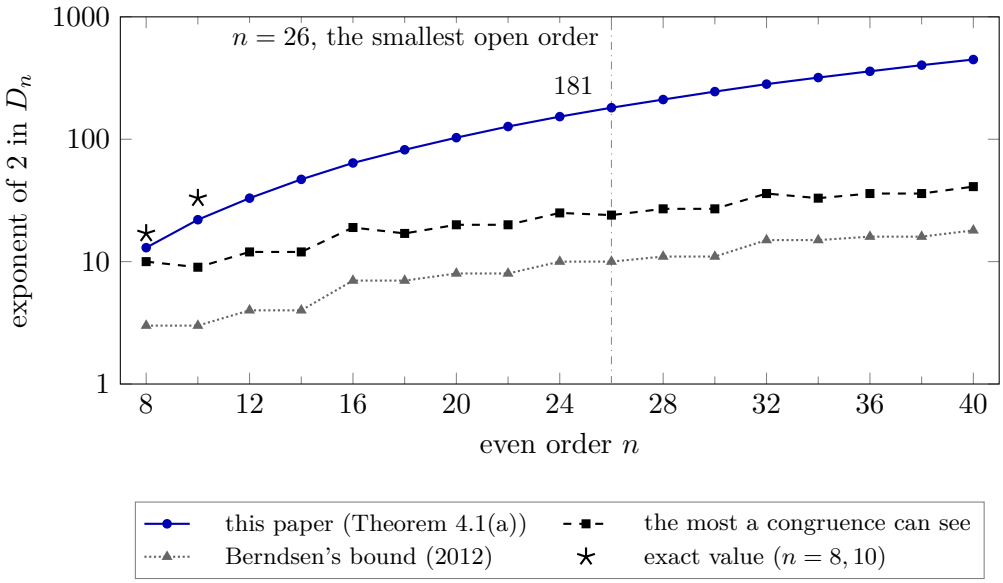

FIGURE 5. How far the 2-part of the count lies beyond what a congruence can see. For each even order n from 8 to 40, the solid line shows the exponent e for which this paper proves that 2^e divides D_n (Theorem 4.1(a)). The dashed line shows $v_2(n!)+v_2(n)$: a congruence modulo a divisor of $(n!)^3$ determines D_n at most modulo $2^{v_2(n!)+v_2(n)}$. The dotted line shows Berndsen's bound, and the stars show the exact exponents at $n = 8$ and $n = 10$, from the computed D_8 and D_{10}. The exponent axis is logarithmic: at $n = 8$ the three bounds are 13, 10 and 3, and the exact exponent is 17. At $n = 26$, the smallest order at which the conjecture is open, we prove that 2^{181} divides D_{26}, while a congruence sees at most 2^{24} and 2^{10} was known.

4. A QUADRATIC BOUND

We now read off the bounds, by applying Proposition 3.5 to the matrix $J + I$ of Proposition 3.6.

Theorem 4.1. *Let $n \geq 2$ be even.*

(a) *For every prime q, $v_q(\Delta_n) \geq v_q((n-1)!) + \sum_{N=1}^{n-1} f_q(n, N)$.*
(b) *$v_2(\Delta_n) \geq v_2((n-1)!) + n^2/4$.*
(c) *If $q = 2$ and $n \geq 8$, or if q is an odd prime with $3q \leq n$, then $v_q(\Delta_n) \geq 3v_q(n!)$; that is, the natural modulus $M_q(n)$ divides D_n.*

Part (c) is Theorem B for $q = 2$ and for the odd primes $q \leq n/3$. For $q = 2$ the right side of (a) is $1, 6, 13, 24, 37$ at $n = 2, 4, 6, 8, 10$, while the true values of $v_2(\Delta_n)$, from the computed values of D_n [24, 7], are $1, 6, 15, 28, 48$.

Proof. (a) By Proposition 3.6, $\Delta_n = \pm(n-1)!\, j(J + I)$. Here $J + I$ (of size $n - 1$) is the matrix of an n-regular multidigraph with all entries at least 1. Proposition 3.5 with $N = n - 1$ gives (a).

(b) For $m \geq 1$, $v_2(m!) \geq \lfloor m/2 \rfloor \geq (m-1)/2$. Hence $f_2(n, N) \geq (n-N)/2$, and since $f_2(n, N)$ is an integer, $f_2(n, N) \geq \lceil (n-N)/2 \rceil$. For even n, $\sum_{N=1}^{n-1} \lceil (n-N)/2 \rceil = \sum_{i=1}^{n-1} \lceil i/2 \rceil = 2\binom{n/2}{2} + \frac{n}{2} = \frac{n^2}{4}$.

(c) By (2.3) the two statements in (c) are equivalent. We prove the first. As $f_q(n, 1) = v_q(n!)$ and $v_q((n-1)!) = v_q(n!) - v_q(n)$, part (a) shows that it suffices to prove

$$Q := \sum_{N=2}^{n-1} f_q(n, N) \;\geq\; v_q(n!) + v_q(n). \tag{4.1}$$

For $m \geq 0$, $v_q(m!) \geq \lfloor m/q \rfloor \geq (m - q + 1)/q$, so $f_q(n, N) \geq \lceil (n - N(q-1))/q \rceil$.

The prime $q = 2$, $n \geq 8$. Here $Q \geq \sum_{i=1}^{n-2} \lceil i/2 \rceil = n^2/4 - n/2$, while $v_2(n!) \leq n-1$ and $v_2(n) \leq n/2$. Finally, $n^2/4 - n/2 \geq (n-1) + n/2$, because $n^2 - 8n + 4 \geq 0$ for $n \geq 8$.

Odd primes q with $3q \leq n$. Write $n = aq + b$ with $0 \leq b < q$, so that $3 \leq a \leq n/3$. For $2 \leq N \leq a$,

$$\Big\lceil \frac{n - N(q-1)}{q} \Big\rceil = \Big\lceil a - N + \frac{b+N}{q} \Big\rceil \geq a - N + 1,$$

so $Q \geq \sum_{N=2}^{a} (a - N + 1) = a(a-1)/2$ (the terms with $N > a$ are at least 0). We now compare this with $v_q(n!) + v_q(n)$ in three cases.

- If $a < q$, then $n < q^2$, $v_q(n!) = a$, and $v_q(n) \leq 1$, with equality only if $b = 0$. For $a \geq 4$, $a(a-1)/2 \geq a+1$. For $a = 3$, $b \neq 0$ because n is even and $3q$ is odd. Thus $v_q(n) = 0$ and $a(a-1)/2 = 3 = v_q(n!)$.
- If $a \geq q$, then $v_q(n!) = a + v_q(a!) \leq a + (a-1)/2$ by Legendre's formula, and $v_q(n) < 1 + \log_q(a+1) \leq 1 + \log_3(a+1)$, because $n < (a+1)q$. For $a \geq 5$, $a(a-1)/2 - a - (a-1)/2 - 1 = (a^2 - 4a - 1)/2 > \log_3(a+1)$: this holds at $a = 5$, and from a to $a+1$ the left side grows by $(2a-3)/2 \geq 7/2$, while the right side grows by less than 1.
- The remaining cases have $q \leq a \leq 4$, so $q = 3$, $a \in \{3, 4\}$, and $n \in \{10, 12, 14\}$. There the bounds $f_3(n, N) \geq \lceil (n - 2N)/3 \rceil$ and $f_3(n, N) \geq 0$ give $Q \geq 5, 8, 12$, against $v_3(n!) + v_3(n) = 4, 6, 5$.

In all cases (4.1) holds. □

The bound $Q \geq a(a-1)/2$ in the proof of (c) uses only $n = aq + b$ with $0 \leq b < q$. It therefore holds for every prime q and every even n, with $a = \lfloor n/q \rfloor$ (the sum is empty when $a \leq 1$). With $f_q(n, 1) = v_q(n!)$ it gives the following.

Corollary 4.2. *For every prime q and every even n, with $a = \lfloor n/q \rfloor$,*

$$v_q(\Delta_n) \geq v_q(n!\,(n-1)!) + \frac{a(a-1)}{2},$$

which is quadratic in n for every fixed prime q.

Figure 5 compares the bound (a) for $q = 2$ with the natural modulus and with Berndsen's bound.

5. The odd primes q with $n/3 < q < n/2$

Let q be an odd prime with $2q < n < 3q$. Then $v_q(n!) = v_q((n-1)!) = 2$ and $q \nmid n$. The natural modulus is therefore $M_q(n) = q^2$. By Proposition 3.6 we need $v_q(j(J+I)) \geq 4$, with $J + I$ of size $n - 1$. For $n = 3q - 1$, Theorem 4.1(a) already gives $v_q(\Delta_n) \geq 7$, more than needed (there $v_q((n-1)!) = f_q(n, 1) = f_q(n, 2) = 2$ and $f_q(n, 3) \geq 1$). For $2q < n \leq 3q - 3$, which occurs only for $q \geq 5$, vertex removal gives only $v_q(j(J+I)) \geq 3$ (Lemma 5.3 below). We therefore remove all but $2q$ of the vertices at once and use the symmetries of the remaining $2q$ vertices.

For a vertex set $V = S \sqcup T$ of H, an *exit* is an arc from S to T and an *entry* is an arc from T to S.

Lemma 5.1. *Let H be d-regular on $V = S \sqcup T$ with $S \neq \emptyset$. Then $j(H; x) = \sum_{\pi_T} x^{\mathrm{cyc}_T} j(H_{\pi_T}; x)$, the sum over the families π_T of transitions at the vertices of T. Here cyc_T is the number of closed trails inside T, and H_{π_T} is the d-regular multidigraph on S formed by the arcs inside S and, for each exit e, a virtual arc from the tail of e to the head of the entry that ends the walk from e by π_T. Its matrix is $M_S + R$, where M_S is the restriction of M to S, row u of R sums to the number of exits from u, and column v of R sums to the number of entries into v.*

Proof. From an exit a_0, put $a_{i+1} = \pi_{\mathrm{head}(a_i)}(a_i)$ as long as a_i ends in T. This step is injective, and its values start in T. Suppose that $a_i = a_l$ with $i < l$ is the first repetition. Then $i = 0$, since otherwise $a_{i-1} = a_{l-1}$. But a_l starts in T and a_0 in S. Thus the arcs of the walk are distinct, and the walk stops at an entry. By the same injectivity two walks cannot reach the same entry. By

d-regularity there are as many entries as exits, so the walks pair the exits with the entries bijectively. An arc inside T lies on such a walk or on a closed trail that never meets S. Therefore cyc_T depends only on π_T. A closed trail that meets S becomes, after its walks through T are contracted to virtual arcs, one closed trail of H_{π_T}. The transitions at the vertices of S are the same objects in H and in H_{π_T}. Summing over them and over π_T gives the claim. □

Lemma 5.1 is the vertex recursion behind (E), applied to all the vertices of T at once.

Remark 5.2. An *automorphism* g of H is a permutation of the arcs that comes from a permutation of the vertices and preserves tails and heads. If $g(T) = T$, it acts on the families π_T by $(g\pi_T)_{gw}(ge) = g(\pi_{T,w}(e))$. The walks of $g\pi_T$ are the g-images of those of π_T. So cyc_T is constant on orbits. Moreover g maps H_{π_T} onto $H_{g\pi_T}$ (the virtual arc of an exit e goes to the virtual arc of ge). Therefore $j(H_{\pi_T}; x)$ is constant on orbits, and if $g\pi_T = \pi_T$, then g is an automorphism of H_{π_T}.

Lemma 5.3. *Let q be a prime and $n > 2q$. If H is n-regular on at least two vertices, with all $M_{uv} \geq 1$, then $v_q(j(M)) \geq 3$.*

Proof. Here $f_q(n, 1) = v_q(n!) \geq 2$. Also $f_q(n, 2) \geq 1$, because two parts smaller than q sum to at most $2q - 2 < n$. Now we apply Proposition 3.5. □

Lemma 5.4. *Let q be an odd prime and $n > 2q$. Let H be n-regular on $S_0 \sqcup S_1$, $|S_0| = |S_1| = q$, with all $M_{uv} \geq 1$ and $M_{ab} = 1$ for $a \in S_0$, $b \in S_1$, and let g be an automorphism of H of order q that is a q-cycle on S_1 and fixes S_0 pointwise. Then $v_q(j(M)) \geq 4$.*

Proof. We apply Lemma 5.1 with $(S, T) = (S_0, S_1)$ at $x = -n$ and group the families π_{S_1} into $\langle g\rangle$-orbits, of size q or 1. An orbit of size q contributes q times $(-n)^{\mathrm{cyc}_{S_1}} j(H_{\pi_{S_1}}; -n)$. Here $H_{\pi_{S_1}}$ lives on the $q \geq 3$ vertices of S_0 with all entries at least 1. By Lemma 5.3, the contribution of such an orbit is therefore divisible by q^{1+3}.

Now let $g\pi_{S_1} = \pi_{S_1}$, and let $a \in S_0$. The exits from a are the q arcs $a \to b$, $b \in S_1$. The g-image of the walk from $a \to b$ is the walk of π_{S_1} from $g(a \to b) = (a \to gb)$, the only arc from a to gb. This walk ends at the g-image of the last arc $b' \to a'$ of the first walk, that is, at the vertex $ga' = a'$. As g is transitive on S_1, the q walks from a all end at one vertex $w \in S_0$. So column w of the matrix of $H_{\pi_{S_1}}$ has an entry at least $q+1$, and Corollary 3.4 at w gains a factor q. On the remaining $q-1 \geq 2$ vertices, every $M' + R$ is n-regular with all entries at least 1, as in the proof of Proposition 3.5. There Lemma 5.3 gives $v_q \geq 3$. Hence $v_q(j(H_{\pi_{S_1}})) \geq 1 + 3$, and the contribution of every orbit is divisible by q^4. □

Theorem 5.5. *Let q be an odd prime and n an even integer with $2q < n < 3q$. Then q^2 divides D_n. As $v_q(n!) = 2$ and $q \nmid n$, this is $M_q(n) \mid D_n$.*

Proof. By (2.3) and $v_q(n!\,(n-1)!) = 4$ we need $v_q(\Delta_n) \geq 6$. By Proposition 3.6, $\Delta_n = \pm(n-1)!\, j(J + I)$ with $J + I$ of size $n - 1$. So it suffices to show $v_q(j(J + I)) \geq 4$. We write the $n - 1$ vertices as $S \sqcup T$ with $|S| = 2q$ and $|T| = t = n - 1 - 2q$. As n is even, $1 \leq t \leq q - 2$. By Lemma 5.1, $j(J + I) = \sum_{\pi_T} (-n)^{\mathrm{cyc}_T} j(H_{\pi_T}; -n)$, where H_{π_T} has the matrix $J + I + R$ of size $2q$, with all line sums of R equal to t.

The group $G = \mathrm{Sym}(S)$ acts on the multidigraph of $J + I$ (loop number i at v goes to loop number i at gv) and fixes T pointwise. We group the families π_T into G-orbits. An orbit has size $(2q)!/|\operatorname{Stab}(\pi_T)|$, where $v_q((2q)!) = 2$. If $v_q|\operatorname{Stab}(\pi_T)| \leq 1$, the orbit size is divisible by q. By Lemma 5.3, the contribution of the orbit is then divisible by q^{1+3}. Otherwise $\operatorname{Stab}(\pi_T)$ contains a Sylow q-subgroup of $\mathrm{Sym}(S)$, which is generated by two disjoint q-cycles. In particular it contains a q-cycle g with support S_1 that fixes $S_0 = S \setminus S_1$ pointwise. As g fixes π_T, it is an automorphism of H_{π_T} (Remark 5.2), of order q as $g^q = 1$ and $g \neq 1$. Consequently $R_{a,gb} = R_{ga,gb} = R_{a,b}$ for $a \in S_0$ and $b \in S_1$. Thus row a of R is constant on S_1, and $qR_{a,b} \leq t < q$ gives $R_{a,b} = 0$. So H_{π_T} has exactly one arc $a \to b$ for $a \in S_0$, $b \in S_1$. Lemma 5.4 then gives $v_q \geq 4$. As the contribution of every orbit is divisible by q^4, we obtain $v_q(j(J + I)) \geq 4$. □

6. The prime $q = n/2$

In this section q is an odd prime and $n = 2q$. We prove:

Theorem 6.1. *For every odd prime q, q^2 divides D_{2q}, and for every prime $q \geq 5$, q^3 divides D_{2q}.*

Here $v_q(n!) = 2$ and $v_q(n) = 1$, so the natural modulus is $M_q(2q) = q^3$. Theorem B assumes $n \geq 8$, so there $q \geq 5$, and Theorem 6.1 is Theorem B for $q = n/2$. Before this paper, $q \mid D_{2q}$ was known for every odd prime q [24, Theorem 3.5], and the full statement for $q = 3, 5$ followed from the computed values of D_6 and D_{10} [24, 7]. Since $v_q(n!\,(n-1)!) = 3$, we need Δ_n modulo q^6. The arguments of Sections 4 and 5 do not supply the required additional q-divisibility when $n = 2q$: Theorem 4.1(a) gives only $v_q(\Delta_{2q}) \geq 1 + 2 + 1 = 4$. Meanwhile, the grouping in Section 5 needs $2q$ vertices, whereas the matrix $J + I$ of Proposition 3.6 has only $2q - 1$. We therefore follow Drisko's method. The proof proceeds from Möbius reduction (Section 6.1) to the rank-two and rank-three terms (Section 6.3), then to rank-one strata (Section 6.4), layers and traces (Section 6.5), and their evaluation modulo q (Section 6.6).

A Sylow q-subgroup $P \cong \mathbb{F}_q^6$ of S_n^3 acts on the Latin squares, and a Möbius inversion over its subgroups expresses Δ_n modulo q^6 through the signed numbers $S(H)$ of squares fixed by the subgroups H of rank 1, 2 and 3 (Section 6.1). Many of these numbers vanish (Lemma 6.6(i)). The subgroups of rank three contribute a multiple of q^6, and the sum over rank two, which we compute in closed form, is divisible by q^5 and therefore contributes a multiple of q^6 (Section 6.3).

Only the rank-one sum can contribute modulo q^6 after the rank-two and rank-three terms are removed. Individual rank-one subgroups contribute multiples of q^4, so to determine their sum modulo q^6 we must retain cancellation across subgroups. Their fixed squares split into *strata*. The homogeneous strata and the squares fixed by the subgroups that fix every symbol together contribute a multiple of q^6, by Wilson's theorem, Babbage's congruence and a congruence for complete maps, while the mixed strata form orbits of size q^5 (Section 6.4).

The signed numbers of these orbits turn out to be traces of products of matrices built from the coefficients of minors of a generic circulant matrix (Section 6.5), and we compute these traces modulo q in a basis in which every circulant matrix is triangular (Section 6.6). The result is $\Delta_{2q} \equiv q^5 \sum_{m=1}^{q-1} m^{-2} \pmod{q^6}$, and the sum vanishes modulo q for $q \geq 5$.

6.1. The Möbius reduction.

Lemma 6.2. *Let a finite q-group G act on a finite set $\mathcal{X}$, with a G-invariant sign $\varepsilon : \mathcal{X} \to \{\pm 1\}$. For $H \leq G$ put $S_{\mathcal{X}}(H) = \sum \varepsilon(x)$, the sum over the $x \in \mathcal{X}$ fixed by every element of H. Then*

$$\sum_{x \in \mathcal{X}} \varepsilon(x) \;\equiv\; - \sum_{\substack{1 \neq H \leq G \\ \text{elementary abelian}}} (-1)^{r(H)}\, q^{\binom{r(H)}{2}}\, S_{\mathcal{X}}(H) \pmod{|G|},$$

where $r(H)$ is the rank of H.

Proof. A free G-orbit has $|G|$ points of the same sign. The free points therefore contribute a multiple of $|G|$. For the other points we use the Möbius function μ of the subgroup lattice of G. It satisfies $\sum_{H \leq K} \mu(1, H) = [K = 1]$ for every $K \leq G$, and therefore

$$\sum_{1 \neq H \leq G} \mu(1, H)\, S_{\mathcal{X}}(H) = \sum_{x \in \mathcal{X}} \varepsilon(x) \sum_{1 \neq H \leq \mathrm{Stab}(x)} \mu(1, H) = - \sum_{x\colon \mathrm{Stab}(x) \neq 1} \varepsilon(x).$$

For a q-group, $\mu(1, H) = (-1)^r q^{\binom{r}{2}}$ if H is elementary abelian of rank r, and $\mu(1, H) = 0$ otherwise (P. Hall [14]). Adding the free points, which contribute a multiple of $|G|$, gives the lemma. □

The Sylow subgroup. We index the rows, the columns and the symbols each by $\{0, 1\} \times \mathbb{F}_q$, identified with $[n]$ in the same way for all three, and call the sets $\{a\} \times \mathbb{F}_q$ *blocks*. In particular, the

symbol blocks are $\Sigma_c = \{c\} \times \mathbb{F}_q$, $c \in \{0,1\}$. The group $P = \mathbb{F}_q^6$ of elements $g = (u_0, u_1; v_0, v_1; w_0, w_1)$ acts on Latin squares by translating within the blocks:

$$(gL)((a, x + u_a), (b, y + v_b)) = g_\Sigma(L((a, x), (b, y))), \qquad g_\Sigma(c, z) = (c, z + w_c).$$

Since $v_q(n!) = 2$, P is a Sylow q-subgroup of S_n^3, and it preserves ε by (2.2). For $H \le P$ let $\mathrm{Fix}(H)$ be the set of Latin squares fixed by H and $S(H) = \sum_{L \in \mathrm{Fix}(H)} \varepsilon(L)$, which is $S_{\mathcal{X}}(H)$ of Lemma 6.2 for $\mathcal{X}$ the set of all Latin squares and $G = P$. The coordinates u_a, v_b, w_c restrict to linear forms $\alpha_a, \beta_b, \gamma_c$ on H, its row, column and symbol *characters* (in this section γ_c is a character, not the column permutation of Section 2). A block is fixed pointwise by H if its character is 0; otherwise it is one H-orbit, and we call it *moving*. For a symbol (c, z) we call $z \in \mathbb{F}_q$ its *phase*.

Lemma 6.3. *A subgroup of P that fixes a Latin square has rank at most* 3*, and*

$$\Delta_{2q} \equiv \sum_{r(H)=1} S(H) - q \sum_{r(H)=2} S(H) + q^3 \sum_{r(H)=3} S(H) \pmod{q^6}.$$

Proof. Let $\mathcal{K}$ be the kernel of the projection $(\sigma_1, \sigma_2, \sigma_3) \mapsto \sigma_1$ on the autotopism group $\mathrm{Atp}(L)$ of a Latin square L. If $(1, \sigma_2, \sigma_3) \in \mathcal{K}$ and $\sigma_2(j) = j$ for some column j, then σ_3 fixes every symbol of column j. Thus $\sigma_3 = 1$, and then $\sigma_2 = 1$. Hence $\mathcal{K}$ acts semiregularly on the columns, and $|\mathcal{K}|$ divides n. Consequently $|\mathrm{Atp}(L)|$ divides $n! \cdot n$, and $v_q|\mathrm{Atp}(L)| \le v_q(n!) + v_q(n) = 3$: the elementary abelian group $\mathrm{Atp}(L) \cap P$ has rank at most 3, and the subgroups of rank at least 4 fix no square. The congruence is now Lemma 6.2, whose coefficients $-(-1)^r q^{\binom{r}{2}}$ are $1, -q, q^3$ for $r = 1, 2, 3$. □

6.2. **Signs and complete maps.** The sign of a bijection between two ordered sets of the same size is the sign of the permutation obtained from the order-preserving identifications. Signs multiply under composition. We order $\mathbb{F}_q$ as $0 < 1 < \cdots < q-1$ and list every subset in increasing order. If $X = X_1 \sqcup X_2$ is ordered with X_1 first and $f : X \to Y$ maps X_i onto Y_i, then $\operatorname{sgn} f = \theta(Y_1, Y_2) \operatorname{sgn}(f|_{X_1}) \operatorname{sgn}(f|_{X_2})$, where $\theta(Y_1, Y_2)$ is the sign of the list "Y_1, then Y_2" relative to the order of Y. Put $\theta(I) = \theta(I, I^c)$ for $I \subseteq \mathbb{F}_q$. As $|I|\,|I^c|$ is even, $\theta(I) = \theta(I^c, I) = \theta(I^c)$. Counting inversions, we find $\theta(I) = (-1)^{\iota(I) - \binom{|I|}{2}}$, where $\iota(I)$ is the sum of the representatives of the elements of I in $\{0, \dots, q-1\}$. Let χ be the Legendre symbol modulo q, with $\chi(0) = 0$.

Lemma 6.4. *Let $H \le P$ and $L \in \mathrm{Fix}(H)$.*

(a) *Rows of L in one H-orbit have equal signs, and so do columns. Therefore $\varepsilon(L)$ is the product of the signs of one row per row orbit and one column per column orbit (every H-orbit has* 1 *or q elements, an odd number).*

(b) *A permutation $(b, y) \mapsto (\varpi(b), \phi_b(y))$ of $\{0,1\} \times \mathbb{F}_q$ has sign $(-1)^{[\varpi \ne \mathrm{id}]} \operatorname{sgn} \phi_0 \operatorname{sgn} \phi_1$. On $\mathbb{F}_q$, translations are even and $y \mapsto \lambda y$ has sign $\chi(\lambda)$.*

(c) *Interchanging the two blocks of one coordinate (rows, columns or symbols), or rescaling a block by $(a, x) \mapsto (a, \lambda x)$, is an isotopy ψ that normalizes P, and $L \mapsto \psi L$ is a sign-preserving bijection $\mathrm{Fix}(H) \to \mathrm{Fix}(\psi H \psi^{-1})$. Transposing a square keeps ε and maps $\mathrm{Fix}(H)$ onto $\mathrm{Fix}(H^T)$, where H^T is H with its row and column components exchanged.*

Proof. (a) Let $\sigma \in H$. As $\sigma L = L$, row $\sigma_1(i)$ of L is $\sigma_3 \circ (\text{row } i) \circ \sigma_2^{-1}$, and σ_2, σ_3 are products of q-cycles, hence even. (b) A block interchange is a product of q transpositions, an odd number. The rest is Zolotarev's lemma [25]. (c) Conjugation by ψ maps block translations to block translations, and ψ preserves ε by (2.2). Transposition exchanges the rows and the columns and therefore keeps ε. □

A *complete map* of $\mathbb{F}_q$ is a map $h : \mathbb{F}_q \to \mathbb{F}_q$ such that h and $h - \mathrm{id}$ are both bijections (in the usual terms, h is an orthomorphism of $\mathbb{F}_q$ and $h - \mathrm{id}$ a complete mapping). Put $\tau_q = \sum_h \operatorname{sgn}(h) \operatorname{sgn}(h - \mathrm{id})$, the sum over all complete maps, and let t_q be the same sum over the normalized ones, those with $h(0) = 0$.

Lemma 6.5. *$\tau_q = q\,t_q$ and $t_q \equiv -1 \pmod q$. For $\delta \neq 0$, the sum of $\operatorname{sgn}(h)\operatorname{sgn}(h-\delta\,\mathrm{id})$ over all h for which h and $h-\delta\,\mathrm{id}$ are bijections is also τ_q.*

Proof. We use the classical identity

$$\sum_{x\in\mathbb{F}_q} \chi(x(x+c)) = -1 \qquad (c \neq 0), \tag{6.1}$$

which holds because $\chi(x(x+c)) = \chi(1+c/x)$ for $x \neq 0$ while $1+c/x$ runs over $\mathbb{F}_q \setminus \{1\}$. The group $\mathbb{F}_q^2$ acts on complete maps by $h \mapsto h(\cdot - a) + b$, keeping both signs. Its subgroup $\{0\} \times \mathbb{F}_q$ acts freely, and exactly one of its elements makes $h(0) = 0$. This gives $\tau_q = q\,t_q$. If $(a,b) \neq 0$ fixes h, then $a \neq 0$ and $h(x+a) = h(x) + b$ for all x, and then $h(x) = \lambda x + e$ with $\lambda = b/a \notin \{0,1\}$. The complete maps that are not affine therefore form orbits of size q^2, while for each $\lambda \notin \{0,1\}$ the maps $\lambda x + e$ form one orbit of size q and sign $\chi(\lambda(\lambda-1))$, by Lemma 6.4(b). With (6.1) this gives $\tau_q \equiv q\sum_\lambda \chi(\lambda(\lambda-1)) = -q \pmod{q^2}$, and dividing by q gives $t_q \equiv -1 \pmod q$. For the last statement, writing $h = \delta h_1$ gives $\operatorname{sgn}(h)\operatorname{sgn}(h-\delta\,\mathrm{id}) = \chi(\delta)^2\operatorname{sgn}(h_1)\operatorname{sgn}(h_1 - \mathrm{id})$. □

6.3. **Vanishing, and the ranks two and three.**

Lemma 6.6. (i) *If a nontrivial subgroup $H \leq P$ fixes some column (or some row), that is, every element of H fixes it, then $S(H) = 0$. In particular, among the subgroups of rank one only those that move both row blocks and both column blocks contribute.* (ii) *If $r(H) = 3$, then P/H acts freely on $\operatorname{Fix}(H)$, so $q^3 \mid S(H)$.* (iii) *At rank two,*

$$\sum_{r(H)=2} S(H) = 2q^4(q-1)^5(q-2)(q+1) - 8q^3(q-1)^5\tau_q + 4q^2(q-1)^4(q!)^2,$$

and q^5 divides it.

Proof of (i) *and* (ii). (i) If H fixes column j, it fixes the q columns of the block that contains j. If the row part of H is trivial, then a fixed square would have an autotopism $(1,\sigma_2,\sigma_3) \neq 1$ with $\sigma_2(j) = j$. As in the proof of Lemma 6.3, this forces $\sigma_3 = 1$ and $\sigma_2 = 1$. So $\operatorname{Fix}(H)$ is empty. Otherwise H moves a row block U, which is then one H-orbit of size q. For each column k of the block of j, the set $L(U,k)$ of symbols in the rows of U is one symbol orbit, of size q. There are at most 2 such orbits and $q \geq 3$ columns. So there is a first pair of columns $k_1 < k_2$ in the block with $L(U,k_1) = L(U,k_2)$. We exchange the entries of columns k_1 and k_2 in the rows of U. The exchange gives a Latin square, commutes with H (H fixes k_1, k_2 and maps U to itself) and keeps every set $L(U,k)$. It is therefore an involution of $\operatorname{Fix}(H)$. Being a partial column switch of odd length q, it changes the sign [24, Lemma 1.11]: each of the q rows of U changes by a transposition, while columns k_1, k_2 change by mutually inverse permutations of their common set of symbols (compare [24, proof of Theorem 3.8]). Hence $S(H) = 0$. A fixed row is handled in the same way, with rows and columns exchanged (Lemma 6.4(c)). A subgroup $\langle g\rangle$ of rank one with some $u_a = 0$ or $v_b = 0$ fixes a whole row block or column block.

(ii) For $L \in \operatorname{Fix}(H)$, $\operatorname{Stab}_P(L) \supseteq H$ has rank at most 3 by Lemma 6.3 and therefore equals H. Since P is abelian, P permutes $\operatorname{Fix}(H)$, and the quotient P/H, of order q^3, acts freely on $\operatorname{Fix}(H)$, preserving ε. □

Proof of (iii). Let $r(H) = 2$. We distinguish row/column character-span dimensions $(1,1)$, $(2,1)$, $(1,2)$ and $(2,2)$. In the $(2,2)$ case, express the column characters β_0, β_1 in the row-character basis α_0, α_1. The resulting invertible 2×2 matrix is monomial, has exactly one zero entry, or has no zero entry. For each case, R_* denotes the sum of $S(H)$ over its subgroups: the first three give R_{11}, R_{21} and R_{12}, and the three matrix types give R_{mon}, R_{one} and R_{full}. By (i) we may assume that all row and column characters are nonzero. Then $\varepsilon(L)$ is the product of the signs of the rows $(0,0),(1,0)$ and the columns $(0,0),(1,0)$ (Lemma 6.4(a)). If two of the six characters form a basis of the dual space H^*, then H is the graph of a linear map. We count the subgroups H by the coordinates of the other four characters in that basis: each choice of these coordinates gives exactly one H.

Block interchanges and rescalings of rows and columns (Lemma 6.4(c)) map the subgroups with given row and column characters bijectively onto those with normalized ones, preserving $S(H)$ and permuting the symbol characters. In each case we count the original row and column character choices before using a normalized representative to calculate their contribution. These multiplicities and signed filling sums are collected in the table at the end of this proof, with R_{21} and R_{12} combined. Normalization does not identify those subgroups in the sum: their multiplicity is retained, and the symbol characters are summed over their transported choices. Two facts hold for every $L \in \mathrm{Fix}(H)$.

Fact 1. No element $g \neq 1$ of H fixes all columns and a row: its symbol component would fix the symbols of that row, hence all symbols, and then $g = 1$. Likewise no $g \neq 1$ fixes all rows and a column.

Fact 2. If α_a, β_b are independent, H acts simply transitively on the cells of the block (a, b), and $L((a, x), (b, y)) = (c, z + \lambda x + \mu y)$, with x, y measured from a base cell and $\gamma_c = \lambda\alpha_a + \mu\beta_b$. The block is *Latin* (no symbol repeats in a row or a column of it) if and only if $\lambda\mu \neq 0$. Every filling of this form is fixed by H. We call (λ, μ) the *slopes* of the block. Suppose that all four blocks are of this kind. Each fills every row and column of its block with an entire symbol block. Adjacent blocks must use different symbol blocks to avoid a repeated symbol in a row or column. Thus they form a checkerboard: $00, 11$ use one symbol block and $01, 10$ the other. Moreover, exactly one of the rows $(0, 0), (1, 0)$ and exactly one of the columns carry a block interchange. Lemma 6.4(b) therefore gives

$$\varepsilon(L) = \textstyle\prod_{a,b} \chi(\lambda_{ab}\mu_{ab}). \tag{6.2}$$

Rows and columns each span a line. We count these subgroups H and their fixed squares. If α_0, β_0 are dependent, some $g \neq 1$ fixes all rows and columns, and then $\mathrm{Fix}(H) = \emptyset$ by Fact 1. Otherwise, in the basis α_0, β_0, we write $\alpha_1 = r\alpha_0$, $\beta_1 = s\beta_0$ and $\gamma_c = \xi_c\alpha_0 + \eta_c\beta_0$ $(rs \neq 0)$. The block (a, b) then has slopes $(\xi_c/r_a, \eta_c/s_b)$, where $(r_0, r_1) = (1, r)$ and $(s_0, s_1) = (1, s)$. Therefore $\mathrm{Fix}(H) \neq \emptyset$ if and only if all $\xi_c\eta_c \neq 0$. In that case $\mathrm{Fix}(H)$ has $2q^4$ squares (two layouts, four constants), all even, as the product of the slopes is $(\xi_0\xi_1\eta_0\eta_1/(rs))^2$. These $(q-1)^6$ subgroups give $R_{11} = 2q^4(q-1)^6$.

Rows span the plane, columns a line. Now the two row characters are independent and the column characters are proportional. In the basis $e = \alpha_0$, $f = \alpha_1$ we write $\beta_0 = k_0 e + k_1 f$ and $\beta_1 = s\beta_0$. If $k_1 = 0$ (or $k_0 = 0$), then $\ker e$ (or $\ker f$) fixes all columns and a row block, and so $\mathrm{Fix}(H) = \emptyset$ by Fact 1. For the other $(q-1)^3$ choices, rescale the row blocks and the second column block to make $\beta_0 = \beta_1 = e + f$, using Lemma 6.4(c). The $(q-1)^3$ original choices remain as a multiplicity. For $\gamma_c = \xi_c e + \eta_c f$ the blocks $(0, b)$ and $(1, b)$ have slopes $(\xi_c - \eta_c, \eta_c)$ and $(\eta_c - \xi_c, \xi_c)$. Thus $\mathrm{Fix}(H) \neq \emptyset$ if and only if $\xi_c\eta_c(\xi_c - \eta_c) \neq 0$ for both c. Then $S(H) = 2q^4\chi(\xi_0\eta_0\xi_1\eta_1)$ by (6.2). Over the admissible (ξ, η), $\sum \chi(\xi\eta) = -(q-1)$: the sum over all $\xi\eta \neq 0$ is $(\sum_\xi \chi(\xi))^2 = 0$, and the excluded diagonal $\xi = \eta$ contributes $q - 1$. Each of the $(q-1)^3$ choices of (k_0, k_1, s) therefore gives $2q^4(-(q-1))^2$. In total $R_{21} = 2q^4(q-1)^5$. By transposition, $R_{12} = R_{21}$.

Both span the plane. The remaining subgroups have independent row characters and independent column characters. We sort them by the matrix that expresses the column characters in the row basis. In the basis $e = \alpha_0$, $f = \alpha_1$ we write $\beta_b = k_{b0}e + k_{b1}f$, with (k_{bj}) invertible. There are $2(q-1)^2$ monomial matrices, $4(q-1)^3$ with exactly one zero entry, and $(q-2)(q-1)^3$ with none.

The matrix is monomial. Each column character is a multiple of one row character. We normalize $\beta_0 = e$, $\beta_1 = f$. The blocks $01, 10$ are as in Fact 2, and each of them is therefore filled from one symbol block. A row of row block 0 meets 01 in q cells, which hold all of the symbol block of 01. Its cells in 00 therefore hold the other symbol block. In the same way a column of column block 0 meets 10, and the cells of 00 therefore also avoid the symbol block of 10. Hence 01 and 10 use the same symbol block Σ_c, and 00 uses the other one, $\Sigma_{c'}$, as does 11, which shares row block 1 with 10. In the block 00 (resp. 11) the cell orbits are the diagonals $y - x = d$, and $\ker e$ (resp. $\ker f$) fixes every cell, hence every symbol of $\Sigma_{c'}$. So $\gamma_{c'}$ vanishes on $\ker e$ and on $\ker f$, which together span H, and $\gamma_{c'} = 0$. Then $\gamma_c = \xi e + \eta f$ with $\xi\eta \neq 0$, the blocks $01, 10$ have slopes $(\xi, \eta), (\eta, \xi)$, and $L((a, x), (a, y)) = \phi_{aa}(y - x)$ for arbitrary bijections $\phi_{aa} : \mathbb{F}_q \to \Sigma_{c'}$. This gives $q^2(q!)^2$ squares. For

their signs, note that a block interchange occurs in exactly one of the rows $(0,0),(1,0)$ and in exactly one of the columns $(0,0),(1,0)$. So the two rows get opposite factors $(-1)^{[\varpi\neq\mathrm{id}]}$ in Lemma 6.4(b), and so do the two columns. Write the factors for the first row and first column as $\epsilon_r,\epsilon_c\in\{\pm1\}$, respectively. The four signs are

$$\begin{aligned}\text{rows } (0,0),(1,0): &\quad \epsilon_r \operatorname{sgn}\phi_{00}\chi(\eta), \qquad -\epsilon_r \operatorname{sgn}\phi_{11}\chi(\xi),\\ \text{columns } (0,0),(1,0): &\quad \epsilon_c\chi(-1)\operatorname{sgn}\phi_{00}\chi(\eta), \qquad -\epsilon_c\chi(\xi)\chi(-1)\operatorname{sgn}\phi_{11}.\end{aligned}$$

Their product is

$$\varepsilon(L)=\epsilon_r(-\epsilon_r)\epsilon_c(-\epsilon_c)\big(\operatorname{sgn}\phi_{00}\operatorname{sgn}\phi_{11}\chi(-1)\chi(\eta)\chi(\xi)\big)^2=1.$$

The two pairs of opposite factors multiply to $(-1)(-1)=1$, and every other factor occurs twice. All these squares are therefore even. In total, $2(q-1)^2$ matrices, 2 choices of c', $(q-1)^2$ choices of (ξ,η) and $q^2(q!)^2$ squares each give $R_{\mathrm{mon}}=4q^2(q-1)^4(q!)^2$.

The matrix has exactly one zero entry. Here one block is not of the kind in Fact 2: its filling is given by a map h for which h and $h-\delta\,\mathrm{id}$ are bijections, as in Lemma 6.5. We normalize $\beta_0=e$, $\beta_1=e+f$. The blocks $01,10,11$ are as in Fact 2, while on the block 00 we have $\alpha_0=\beta_0$. Each of $01,10,11$ is filled from one symbol block. A row of row block 1 meets 10 and 11, and a column of column block 1 meets 01 and 11; as each holds every symbol once, 11 uses a different symbol block from 10 and from 01. So 01 and 10 use one symbol block Σ_c and 11 uses the other, $\Sigma_{c'}$. A row of row block 0 meets 01 in all of Σ_c, and its cells in 00 therefore hold $\Sigma_{c'}$ too. Both symbol blocks are moving, because a block as in Fact 2 has a nonzero symbol character. Since $\ker e$ fixes the cells of 00, $\gamma_{c'}=\delta e$ with $\delta\neq0$. Let $\gamma_c=\xi e+\eta f$. Then $L((0,x),(0,y))=(c',\delta x+h(y-x))$, and the block 00 is Latin if and only if h and $h_\delta=h-\delta\,\mathrm{id}$ are bijective (the entry in row x of column y has phase $\delta y+h_\delta(y-x)$). The blocks $01,10,11$ have slopes $(\xi-\eta,\eta)$, (η,ξ) and $(-\delta,\delta)$. They must be Latin, which forces $\xi\eta(\xi-\eta)\neq0$, and each of them has one free constant. Again let $\epsilon_r,\epsilon_c\in\{\pm1\}$ denote the first row and column block-order factors. Then

$$\begin{aligned}\text{rows } (0,0),(1,0): &\quad \epsilon_r \operatorname{sgn}(h)\chi(\eta), \qquad -\epsilon_r\chi(\xi\delta),\\ \text{columns } (0,0),(1,0): &\quad \epsilon_c \operatorname{sgn}(h_\delta)\chi(-1)\chi(\eta), \qquad -\epsilon_c\chi(\xi-\eta)\chi(-\delta).\end{aligned}$$

Multiplying these four signs, the block-order factors give 1, as above, and

$$\begin{aligned}\varepsilon(L)&=\operatorname{sgn}(h)\operatorname{sgn}(h_\delta)\chi\big(\eta^2(\xi\delta)(-1)(\xi-\eta)(-\delta)\big)\\ &=\operatorname{sgn}(h)\operatorname{sgn}(h-\delta\,\mathrm{id})\chi(\xi(\xi-\eta)).\end{aligned}$$

Lemma 6.5 gives $S(H)=q^3\tau_q\chi(\xi(\xi-\eta))$. With $\eta=t\xi$, $\sum\chi(\xi(\xi-\eta))=(q-1)\sum_{t\neq0,1}\chi(1-t)=-(q-1)$. In total, $4(q-1)^3$ matrices, 2 choices of c', $q-1$ choices of δ and the sum of $S(H)$ over (ξ,η), which is $-(q-1)q^3\tau_q$, give $R_{\mathrm{one}}=-8q^3(q-1)^5\tau_q$.

The matrix has no zero entry. Here all four blocks are as in Fact 2. Every fixed square is therefore one checkerboard of four affine blocks, in one of the two layouts (the blocks $00,11$ use Σ_0 or Σ_1), and by (6.2) the count reduces to a character sum, computed below. The ratio $\nu=k_{00}k_{11}/(k_{01}k_{10})\notin\{0,1\}$ is invariant under rescaling, and each ν comes from $(q-1)^3$ matrices. We normalize $\beta_0=e+f$, $\beta_1=e+\nu f$. For $\gamma_c=\xi e+\eta f$ the slopes in $00,01,10,11$ are $(\xi-\eta,\eta)$, $((\nu\xi-\eta)/\nu,\eta/\nu)$, $(\eta-\xi,\xi)$ and $(\eta-\nu\xi,\xi)$. In either layout Σ_c contributes $\kappa(\gamma_c)=\chi(-\xi\eta(\xi-\eta)(\nu\xi-\eta))$ to (6.2) (on $01,10$ up to the square ν^{-2}). Moreover $\kappa(\gamma_0)\kappa(\gamma_1)=0$ if and only if $\mathrm{Fix}(H)=\emptyset$. The two checkerboard layouts and the independent sums over the two symbol characters give $2q^4\big(\sum_{\xi,\eta}\kappa(\xi e+\eta f)\big)^2$.

Putting $\eta=t\xi$, we get $\sum_{\xi,\eta}\kappa(\xi e+\eta f)=\chi(-1)(q-1)\varrho(\nu)$ with $\varrho(\nu)=\sum_t\chi(t(t-1)(t-\nu))$.

For the full second moment, put $\chi_t=\chi(t(t-1))$. Then

$$\sum_\nu\varrho(\nu)^2=\sum_{t,s}\chi_t\chi_s\sum_\nu\chi((t-\nu)(s-\nu))=q\sum_t\chi_t^2-\Big(\sum_t\chi_t\Big)^2=q(q-2)-1.$$

The middle step uses (6.1): $\sum_\nu \chi((t-\nu)(s-\nu))$ is $q-1$ if $t=s$ and -1 otherwise. The last step uses $\chi_t^2 = 1$ for $t \notin \{0,1\}$ and $\sum_t \chi_t = -1$, again by (6.1).

To restrict to the admissible ratios, remove $\nu = 0, 1$. Since $\varrho(0) = -\chi(-1)$ and $\varrho(1) = -1$, we have $\sum_{\nu\neq 0,1} \varrho(\nu)^2 = q^2 - 2q - 3$. In total, $(q-1)^3$ matrices for each $\nu \notin \{0,1\}$, $2q^4$ squares for each choice of the symbol characters, and the factor $(q-1)^2\varrho(\nu)^2$ from the sum over them give $R_{\text{full}} = \sum_{\nu\neq 0,1}(q-1)^3\, 2q^4(q-1)^2\varrho(\nu)^2 = 2q^4(q-1)^5(q^2-2q-3)$.

The rank-two contributions are summarized in the following table. The middle two columns separate the multiplicity of the original row and column characters from the signed sum over symbol characters and fillings for one such choice. Thus each contribution is their product. In the last row these products are also summed over $\nu \notin \{0,1\}$.

Case	Row/column choices	Symbol/filling sum	Contribution
R_{11}	$(q-1)^2$	$2q^4(q-1)^4$	$2q^4(q-1)^6$
$R_{21}+R_{12}$	$2(q-1)^3$	$2q^4(q-1)^2$	$4q^4(q-1)^5$
R_{mon}	$2(q-1)^2$	$2q^2(q-1)^2(q!)^2$	$4q^2(q-1)^4(q!)^2$
R_{one}	$4(q-1)^3$	$-2q^3(q-1)^2\tau_q$	$-8q^3(q-1)^5\tau_q$
R_{full}	$(q-1)^3$ per ν	$2q^4(q-1)^2\varrho(\nu)^2$	$2q^4(q-1)^5$ $\cdot\,(q^2-2q-3)$

The factor 2 in the second row counts the two disjoint character-span cases: rows span the plane and columns a line, or conversely. Transposition makes their signed contributions equal; it does not merge their subgroups. The symbol/filling sums include both checkerboard layouts where applicable, and retain the character-sum signs and the $q!$ or complete-map factors calculated above.

Assembly. We have $R_{11} + 2R_{21} + R_{\text{full}} = 2q^4(q-1)^5((q-1)+2+(q^2-2q-3)) = 2q^4(q-1)^5(q-2)(q+1)$, and adding R_{mon} and R_{one} gives the formula. Each term is divisible by q^4. Divided by q^4, the three terms are congruent modulo q to 4, -8 and 4, as $\tau_q/q \equiv -1$ and $(q-1)! \equiv -1$. So q^5 divides the sum. (At $q=3$, $\tau_3 = -3$ and the sum is $62208 = 2^8\,3^5$.) □

By Lemmas 6.3 and 6.6, $\Delta_{2q} \equiv \sum_{r(H)=1} S(H) \pmod{q^6}$. It remains to sum over the subgroups of rank one.

6.4. **Rank one: shapes and strata.** By Lemma 6.6(i), a subgroup $\langle g\rangle$ of rank one contributes only if $u_0, u_1, v_0, v_1 \neq 0$. Its *shape* is 0, B or C if it has 0, 1 or 2 nonzero symbol coordinates, respectively. Counting generators and dividing by $q-1$, there are $(q-1)^3$, $2(q-1)^4$ and $(q-1)^5$ such subgroups of these shapes. Rescaling blocks, and for shape B interchanging the symbol blocks, conjugates every such subgroup to one generated by

$$\ell_0 = (1,1;1,1;0,0), \qquad \ell_B = (1,1;1,1;0,1), \qquad \ell_C = (1,1;1,1;1,1);$$

so S is constant on each shape (Lemma 6.4(c)).

Fixed squares of ℓ. Let $\ell \in \{\ell_0, \ell_B, \ell_C\}$ and $L \in \mathrm{Fix}(\langle\ell\rangle)$. For each block (a,b) and each *offset* $d \in \mathbb{F}_q$ the cells $((a,x),(b,x+d))$ form one orbit. So if $L((a,0),(b,d)) = (c,z)$, then $L((a,x),(b,x+d)) = (c, z+w_c x)$, where $w_c \in \{0,1\}$ is the symbol coordinate of ℓ. Let O_{ab} be the set of offsets d with $L((a,0),(b,d)) \in \Sigma_0$. Every row and every column meets Σ_0 exactly q times. Thus $|O_{a0}| + |O_{a1}| = q = |O_{0b}| + |O_{1b}|$, and so $|O_{00}| = |O_{11}| = m$ and $|O_{01}| = |O_{10}| = q-m$ for some $m \in \{0,\dots,q\}$. We call any quadruple $O = (O_{00}, O_{01}; O_{10}, O_{11})$ of subsets of $\mathbb{F}_q$ with these sizes a *pattern of size* m, and m the *stratum* of L; the complement $O^c = (O_{ab}^c)$ of a pattern of size m is a pattern of size $q-m$. We call the stratum *mixed* if $0 < m < q$ and *homogeneous* otherwise.

For ℓ_B, m is the number of fixed symbols in the block 00. For ℓ_C, it is the number of diagonals of the block 00 that map into Σ_0.

The entries in Σ_c sit at the offsets of $E = O$ (for $c = 0$) or $E = O^c$ (for $c = 1$). If Σ_c is moving ($w_c = 1$), then $L((a, x), (b, x + d)) = (c, x + h_{ab}(d))$ for maps $h_{ab} : E_{ab} \to \mathbb{F}_q$. If it is fixed, then $L((a, x), (b, x + d)) = \phi_{ab}(d)$ for maps $\phi_{ab} : E_{ab} \to \Sigma_c$. Every row and every column of L contains each symbol exactly once if and only if, for both c:

(L1) for each a, $d \mapsto h_{ab}(d)$ (resp. $\phi_{ab}(d)$) is a bijection $E_{a0} \sqcup E_{a1} \to \mathbb{F}_q$ (resp. $\to \Sigma_c$);
(L2) for each b, $d \mapsto h_{ab}(d) - d$ (resp. $\phi_{ab}(d)$) is a bijection $E_{0b} \sqcup E_{1b} \to \mathbb{F}_q$ (resp. $\to \Sigma_c$).

Here (L2) comes from column (b, y), which meets the offset d of the block (a, b) in row $(a, y - d)$, with phase $y + h_{ab}(d) - d$. A family $h = (h_{ab})$ satisfying (L1) and (L2) on a pattern E is a *layer* on E, and a family ϕ satisfying the versions in parentheses is a *fixed layer*. Ordering $E_{a0} \sqcup E_{a1}$ and $E_{0b} \sqcup E_{1b}$ with the first set first, we give a layer h the *sign* $\omega(h)$, the product of the signs of its two (L1) bijections and its two (L2) bijections, and the *phase sums* $\Phi_{ab}(h) = \sum_{d \in E_{ab}} h_{ab}(d)$.

Lemma 6.7. *For $\ell \in \{\ell_0, \ell_B, \ell_C\}$ and $L \in \mathrm{Fix}(\langle \ell \rangle)$, $\varepsilon(L)$ is the product of $\omega(h)$ over the moving symbol blocks of L (and is 1 if there are none).*

Proof. By Lemma 6.4(a) we may use the rows $(a, 0)$ and the columns $(b, 0)$. In column $(b, 0)$ we index the rows of each block by $d = -x$, which changes its sign by $\chi(-1)^2 = 1$. Then row $(a, 0)$ sends column (b, d), and column $(b, 0)$ sends row (a, d), to the entry of offset d in the block (a, b), read as $h_{ab}(d)$, resp. $h_{ab}(d) - d$, or as $\phi_{ab}(d)$. By the rule for disjoint unions, each of these four signs is the product of its two layer parts and of the sign of the shuffle that lists the Σ_0-positions first. For a set $Y \subseteq \mathbb{F}_q$ let $\mathrm{inv}(Y)$ count the pairs $d' < d$ with $d' \notin Y \ni d$. The shuffle for row a has $\mathrm{inv}(O_{a0}) + \mathrm{inv}(O_{a1}) + |O_{a1}|\,|O^c_{a0}|$ inversions, and that for column b has $\mathrm{inv}(O_{0b}) + \mathrm{inv}(O_{1b}) + |O_{1b}|\,|O^c_{0b}|$. The total, $2\sum_{ab} \mathrm{inv}(O_{ab}) + 2(q - m)^2 + 2m^2$, is even. Finally, a fixed layer contributes $+1$. Indeed, with $Y = \phi_{00}(E_{00})$, (L1) and (L2) give $\phi_{01}(E_{01}) = \phi_{10}(E_{10}) = \Sigma_c \setminus Y$ and $\phi_{11}(E_{11}) = Y$. The rows 0 and the columns 0 each contribute $\theta(Y, \Sigma_c \setminus Y)$, the rows 1 and the columns 1 each contribute $\theta(\Sigma_c \setminus Y, Y)$, and each $\operatorname{sgn} \phi_{ab}$ occurs twice. □

Lemma 6.8. (a) $S(\langle \ell_0 \rangle) = \binom{2q}{q}(q!)^4 = (2q)!\,(q!)^2$, *and every square fixed by ℓ_0 is even.* (b) *For $\ell \in \{\ell_B, \ell_C\}$, a square $L \in \mathrm{Fix}(\langle \ell \rangle)$ of mixed stratum has $\mathrm{Stab}_P(L) = \langle \ell \rangle$. So the squares of mixed stratum m form P-orbits of size q^5, each of constant sign.* (c) *The homogeneous strata contribute exactly $2(q!)^2\tau_q^2$ to $S(\langle \ell_B \rangle)$ and $2\tau_q^4$ to $S(\langle \ell_C \rangle)$.*

Proof. (a) Here $L((a, x), (b, y)) = f_{ab}(y - x)$ with injective maps f_{ab} from $\mathbb{F}_q$ to the symbols. With $Y = f_{00}(\mathbb{F}_q)$, the rows and columns force $f_{11}(\mathbb{F}_q) = Y$ and $f_{01}(\mathbb{F}_q) = f_{10}(\mathbb{F}_q) = Y^c$. Conversely, any q-set Y of symbols and four such bijections give a fixed Latin square. This gives $\binom{2q}{q}(q!)^4$ squares. Since ℓ_0 fixes every symbol, $\varepsilon = 1$ by Lemma 6.7.

(b) Let $g = (u_0, u_1; v_0, v_1; w_0, w_1)$ fix L. It sends the cells of offset d in the block (a, b) to those of offset $d + v_b - u_a$, and Σ_0 to itself. Therefore $O_{ab} + (v_b - u_a) = O_{ab}$. For ℓ_B, g maps the block 00 to itself. The translation w_0 of Σ_0 therefore preserves the m fixed symbols of the block 00, and $w_0 = 0$ as $0 < m < q$. Each O_{ab} is a nonempty proper subset of $\mathbb{F}_q$. Since q is prime, a nonzero translation of $\mathbb{F}_q$ has the single orbit $\mathbb{F}_q$ and fixes no such subset. It follows that $v_b = u_a$ for all a, b, and all four equal some $s_0 \in \mathbb{F}_q$. A moving entry $(c, x + z)$ at $((a, x), (b, x + d))$ goes to $(c, x + z + w_c)$, which must be the entry $(c, x + s_0 + z)$ at $((a, x + s_0), (b, x + s_0 + d))$. Thus $w_c = s_0$, and $g \in \langle \ell \rangle$. As P is abelian, it permutes $\mathrm{Fix}(\langle \ell \rangle)$, keeping strata and ε.

(c) For $m = q$, $O = (\mathbb{F}_q, \emptyset; \emptyset, \mathbb{F}_q)$. By (L1) and (L2), a moving layer on O or O^c is a pair of complete maps h_{00}, h_{11} (resp. h_{01}, h_{10}), of sign $\prod \operatorname{sgn}(h_{ab}) \operatorname{sgn}(h_{ab} - \mathrm{id})$. A fixed layer on O is a pair of bijections $\mathbb{F}_q \to \Sigma_0$. By Lemma 6.7, the stratum $m = q$ contributes τ_q^4 for ℓ_C and $(q!)^2\tau_q^2$ for ℓ_B. Interchanging the symbol blocks (for ℓ_C) or the column blocks (for ℓ_B) commutes with ℓ, keeps ε, and exchanges the strata m and $q - m$. Hence the stratum $m = 0$ contributes the same. □

For $0 < m < q$ let $N_{B,m}$ (resp. $N_{C,m}$) be the signed number of P-orbits of squares of mixed stratum m fixed by ℓ_B (resp. ℓ_C), and let $N_B = \sum_{0<m<q} N_{B,m}$ and $N_C = \sum_{0<m<q} N_{C,m}$. By Lemma 6.8, as integers,

$$S(\langle \ell_B \rangle) = 2(q!)^2 \tau_q^2 + q^5 N_B, \qquad S(\langle \ell_C \rangle) = 2\tau_q^4 + q^5 N_C. \tag{6.3}$$

Proposition 6.9. $\Delta_{2q} \equiv q^5(2N_B - N_C) \pmod{q^6}$. *Hence* $q^2 \mid D_{2q}$ *and* $D_{2q}/q^2 \equiv (2N_B - N_C)/2 \pmod{q}$.

Proof. By the count of shapes, Lemma 6.8(a) and (6.3), the sum of $S(H)$ over the subgroups of rank one is $\Xi + q^5\big(2(q-1)^4 N_B + (q-1)^5 N_C\big)$, where

$$\Xi = (q-1)^3 \tbinom{2q}{q} (q!)^4 + 4(q-1)^4 (q!)^2 \tau_q^2 + 2(q-1)^5 \tau_q^4.$$

With $q! = q\,(q-1)!$ and $\tau_q = q\,t_q$,

$$\Xi/q^4 = (q-1)^3\Big[2\big(((q-1)!)^2 + (q-1)t_q^2\big)^2 + \Big(\tbinom{2q}{q} - 2\Big)((q-1)!)^4\Big].$$

Here $((q-1)!)^2 + (q-1)t_q^2 \equiv 1 - 1 = 0 \pmod{q}$, by Wilson's theorem and Lemma 6.5. Moreover $\binom{2q}{q} = 2\prod_{i=1}^{q-1}(1 + q/i) \equiv 2\big(1 + q\sum_{i=1}^{q-1} 1/i\big) \equiv 2 \pmod{q^2}$, because $\sum_{i=1}^{q-1} 1/i \equiv 0 \pmod{q}$ (pair i with $q - i$). This congruence for $\binom{2q}{q}$, equivalently $\binom{2q-1}{q-1} \equiv 1 \pmod{q^2}$, is due to Babbage [6]. Hence $q^6 \mid \Xi$. Also $2(q-1)^4 \equiv 2$ and $(q-1)^5 \equiv -1 \pmod{q}$, and therefore $\Delta_{2q} \equiv q^5(2N_B - N_C) \pmod{q^6}$.

Finally, $(2q)!\,(2q-1)! = q^3\Lambda$, where Λ is 2 times the product of the integers in four complete systems of nonzero residues modulo q. Thus $\Lambda \equiv 2(-1)^4 = 2 \pmod{q}$ by Wilson's theorem. By (2.3), $q^3\Lambda\, D_{2q} \equiv q^5(2N_B - N_C) \pmod{q^6}$. This gives $q^2 \mid D_{2q}$ and then $\Lambda\, D_{2q}/q^2 \equiv 2N_B - N_C \pmod{q}$. As $\Lambda \equiv 2 \pmod{q}$, this is the statement. □

6.5. **Layers and traces.** To count the mixed orbits, we choose in each of them the squares whose pattern and layers are centered. A pattern is *centered* if every O_{ab} has element sum $s(O_{ab}) = 0$ in $\mathbb{F}_q$ (then O^c is centered too). A layer is *centered* if all its phase sums vanish. For a centered pattern E let $\Omega(E) = \sum_h \omega(h)$, the sum over the centered layers h on E.

Lemma 6.10. *For* $0 < m < q$, *with sums over the centered patterns* O *of size* m,

$$N_{B,m} = (q-1)!\,m!\,(q-m)! \sum_O \Omega(O^c), \qquad N_{C,m} = \sum_O \Omega(O)\,\Omega(O^c).$$

Proof. A square of mixed stratum m fixed by ℓ_C is a pattern O of size m with layers $h^{(0)}$ on O and $h^{(1)}$ on O^c, of sign $\omega(h^{(0)})\omega(h^{(1)})$. A square fixed by ℓ_B is a pattern O with a fixed layer ϕ on O and a layer h on O^c, of sign $\omega(h)$ (Lemma 6.7). The element $g \in P$ sends these data to $O_{ab} + (v_b - u_a)$, $h_{ab}^{(c)}(\cdot - v_b + u_a) + w_c - u_a$ and $g_\Sigma \circ \phi_{ab}(\cdot - v_b + u_a)$. The elements with $u_0 = 0$ form a transversal of $\langle \ell \rangle$ in P. By Lemma 6.8(b), they act simply transitively on each mixed orbit.

We proceed in three steps: center the pattern using row and column translations with $u_0 = 0$; center each moving layer using symbol translations; then count the centered squares remaining in each orbit. There will be one for shape C and q for shape B: the residual translation w_0 of the fixed symbol block in shape B accounts for the division by q in $N_{B,m}$.

For a moving layer on E, each bijection in (L1) has image $\mathbb{F}_q$, whose element sum is 0 because q is odd. The same holds for each bijection in (L2). Thus

$$\sum_{a,b} \sum_{d \in E_{ab}} h_{ab}(d) = 0, \qquad \sum_{a,b} \sum_{d \in E_{ab}} (h_{ab}(d) - d) = 0.$$

Subtracting gives $\sum_{ab} \sum_{d \in E_{ab}} d = 0$, and therefore $\sum_{ab} s(O_{ab}) = 0$. For ℓ_C we take $E = O$, and for ℓ_B we take $E = O^c$ and use $s(O_{ab}^c) = -s(O_{ab})$. Let $\bar{o}_{ab} = s(O_{ab})/|O_{ab}|$ be the mean of O_{ab} (the sizes m and $q - m$ are nonzero in $\mathbb{F}_q$, as $0 < m < q$). Since $q - m = -m$ in $\mathbb{F}_q$, the relation

$\sum_{ab} s(O_{ab}) = 0$ reads $m(\bar{o}_{00} - \bar{o}_{01} - \bar{o}_{10} + \bar{o}_{11}) = 0$, and so $\bar{o}_{00} - \bar{o}_{01} - \bar{o}_{10} + \bar{o}_{11} = 0$. Therefore $(u_0, u_1, v_0, v_1) = (0, \bar{o}_{10} - \bar{o}_{00}, -\bar{o}_{00}, -\bar{o}_{01})$ is the unique choice with $u_0 = 0$ that centers O. For a centered pattern, (L1) and (L2) give $\Phi_{a0} + \Phi_{a1} = 0 = \Phi_{0b} + \Phi_{1b}$ for a moving layer. Its phase sums thus vanish once Φ_{00} does. Moreover, w_c adds $|E_{00}|\, w_c$ to Φ_{00}. We conclude that each mixed ℓ_C-orbit contains exactly one square with $O, h^{(0)}, h^{(1)}$ centered, and each mixed ℓ_B-orbit contains exactly q (differing in w_0).

For a centered pattern, a fixed layer is a choice of $Y = \phi_{00}(O_{00}) \subseteq \Sigma_0$ with $|Y| = m$ and of four bijections onto Y or its complement. There are $\binom{q}{m}(m!)^2((q-m)!)^2 = q!\, m!\, (q-m)!$ such choices. As each mixed ℓ_B-orbit contains exactly q centered squares, dividing by q gives $N_{B,m}$. For ℓ_C, the layers $h^{(0)}$ on O and $h^{(1)}$ on O^c can be chosen independently, which gives $N_{C,m}$. □

Trace forms. Lemma 6.10 expresses the mixed-orbit counts through signed layer counts $\Omega(E)$. We now encode the bijections of a layer by coefficients of minors, so that summing over centered patterns becomes a matrix trace. These identities are over the integers; we reduce them modulo q only in Section 6.6. For $0 < k < q$ and k-subsets Y, I, J of $\mathbb{F}_q$ let $Z_Y(I, J)$ be the sum of $\operatorname{sgn}(h)\operatorname{sgn}(h - \mathrm{id})$ over the bijections $h : Y \to I$ for which $h - \mathrm{id} : Y \to J$ is also a bijection. Let $\Gamma(x) = \sum_{d \in \mathbb{F}_q} x_d T_d$, with independent variables x_d and the $q \times q$ matrices $(T_d)_{ij} = [i - j = d]$ on $\mathbb{F}_q$. Thus $\Gamma(x)$ is a generic circulant matrix. We write $[x^Y]$ for the coefficient of $\prod_{d \in Y} x_d$, and $\Gamma(x)[I, J]$ for the submatrix with rows I and columns J.

Let $\mathcal{C}_m$ be the set of centered m-subsets of $\mathbb{F}_q$, and $K = |\mathcal{C}_m|$. A nonzero translation generates the additive group of $\mathbb{F}_q$, so it fixes no nonempty proper subset. Since $0 < m < q$, each translation orbit of m-subsets has q members. Translation changes the element sum by m times the shift, so exactly one member is centered. Hence $K = \binom{q}{m}/q$.

For $X \in \mathcal{C}_m$ let $\mathcal{A}_X$ and $\mathcal{B}_X$ be the $\mathcal{C}_m \times \mathcal{C}_m$ matrices

$$\mathcal{A}_X(I, J) = Z_X(I, J), \qquad \mathcal{B}_X(I, J) = \theta(I)\theta(J) Z_{X^c}(I^c, J^c),$$

and put $\mathcal{E} = \sum_{X \in \mathcal{C}_m} \mathcal{A}_X$ and $\mathcal{F} = \sum_{X \in \mathcal{C}_m} \mathcal{B}_X$. The matrices $\mathcal{A}_X, \mathcal{B}_X, \mathcal{E}, \mathcal{F}$ have their rows and columns indexed by $\mathcal{C}_m$, so they have size $K \times K$.

Put $\mathcal{U} = \sum_{X \in \mathcal{C}_m} \mathcal{A}_X \otimes \mathcal{B}_X$ and let $\mathcal{S}$ be the swap of the two tensor factors: $\mathcal{S}(\mathbf{e}_I \otimes \mathbf{e}_J) = \mathbf{e}_J \otimes \mathbf{e}_I$, where $\mathbf{e}_I$ is the basis vector indexed by $I \in \mathcal{C}_m$. The rows and columns of $\mathcal{U}$ and $\mathcal{S}$ are indexed by ordered pairs from $\mathcal{C}_m$, so they have size $K^2 \times K^2$.

Lemma 6.11. (a) $Z_Y(I, J) = [x^Y] \det \Gamma(x)[I, J]$. (b) *For a centered pattern O of size m put $X_1 = O_{00}$, $X_2 = O^c_{01}$, $X_3 = O^c_{10}$, $X_4 = O_{11}$, all in $\mathcal{C}_m$. Then $\Omega(O) = \operatorname{tr}(\mathcal{A}_{X_1}\mathcal{B}^T_{X_3}\mathcal{A}_{X_4}\mathcal{B}^T_{X_2})$ and $\Omega(O^c) = \operatorname{tr}(\mathcal{B}_{X_1}\mathcal{A}^T_{X_3}\mathcal{B}_{X_4}\mathcal{A}^T_{X_2})$.* (c) *$\mathcal{A}^T_X = \mathcal{A}_{-X}$ and $\mathcal{B}^T_X = \mathcal{B}_{-X}$, so $\mathcal{E}, \mathcal{F}, \mathcal{U}$ are symmetric.* (d) *As integers, $\sum_O \Omega(O^c) = \operatorname{tr}((\mathcal{E}\mathcal{F})^2)$ and $N_{C,m} = \operatorname{tr}((\mathcal{U}\mathcal{S})^4)$.*

Proof. (a) A term of $\det \Gamma(x)[I, J]$ is a bijection $f : I \to J$ of weight $\operatorname{sgn}(f) \prod_{i \in I} x_{i - f(i)}$. It gives the monomial $\prod_{d \in Y} x_d$ if and only if the differences $i - f(i)$ are distinct and form Y. Then $h(i - f(i)) = i$ defines $h : Y \to I$ with $h - \mathrm{id} = f \circ h : Y \to J$. Conversely, $f = (h - \mathrm{id}) \circ h^{-1}$. Finally, $\operatorname{sgn} f = \operatorname{sgn}(h)\operatorname{sgn}(h - \mathrm{id})$.

(b) Let E be a centered pattern, $k = |E_{00}|$, and h a centered layer on E. The images $I_{ab} = h_{ab}(E_{ab})$ and the difference sets $J_{ab} = (h_{ab} - \mathrm{id})(E_{ab})$ are centered, and (L1), (L2) say $I_{a1} = I^c_{a0}$ and $J_{1b} = J^c_{0b}$. Put $I = I_{00}$, $J = J_{00}$, $J^* = J^c_{01}$ and $I^* = I^c_{10}$, all in $\mathcal{C}_k$. By the rule for disjoint unions (Section 6.2), $\omega(h) = \theta(I)\theta(J)\theta(J^*)\theta(I^*) \prod_{ab} \operatorname{sgn}(h_{ab}) \operatorname{sgn}(h_{ab} - \mathrm{id})$. Therefore $\Omega(E)$ is the sum over $I, J, I^*, J^* \in \mathcal{C}_k$ of

$$Z_{E_{00}}(I, J)\, \big[\theta(I^*)\theta(J) Z_{E_{10}}(I^{*c}, J^c)\big]\, Z_{E_{11}}(I^*, J^*)\, \big[\theta(I)\theta(J^*) Z_{E_{01}}(I^c, J^{*c})\big].$$

For $E = O$, since $E_{00} = X_1$, $E_{11} = X_4$, $E_{10} = X^c_3$ and $E_{01} = X^c_2$, the four factors are $\mathcal{A}_{X_1}(I, J)$, $\mathcal{B}_{X_3}(I^*, J)$, $\mathcal{A}_{X_4}(I^*, J^*)$ and $\mathcal{B}_{X_2}(I, J^*)$, and the sum over I, J, I^*, J^* is the first trace. For $E = O^c$, we re-index $\mathcal{C}_{q-m}$ by $\mathcal{C}_m$ through $I \mapsto I^c$. As $\theta(I^c) = \theta(I)$, the four factors, in the order of the trace, become $\Theta\mathcal{B}_{X_1}\Theta$, $\Theta\mathcal{A}^T_{X_3}\Theta$, $\Theta\mathcal{B}_{X_4}\Theta$ and $\Theta\mathcal{A}^T_{X_2}\Theta$ with $\Theta = \operatorname{diag}(\theta(I))$, and the Θ's cancel in the trace.

(c) The map $h \mapsto (h - \mathrm{id}) \circ (-\mathrm{id})$ sends the maps counted by $Z_Y(J, I)$ bijectively to those counted by $Z_{-Y}(I, J)$, exchanging the roles of h and $h - \mathrm{id}$. The two negations of the domain have equal signs. Also $-X \in \mathcal{C}_m$ and $(-X)^c = -(X^c)$.

(d) The centered patterns correspond bijectively to the quadruples $(X_1, \ldots, X_4) \in \mathcal{C}_m^4$. Summing (b) gives $\sum_O \Omega(O^c) = \mathrm{tr}(\mathcal{F}\mathcal{E}^T\mathcal{F}\mathcal{E}^T) = \mathrm{tr}((\mathcal{E}\mathcal{F})^2)$ by (c). By Lemma 6.10, $N_{C,m} = \sum_O \Omega(O)\Omega(O^c)$. For a fixed quadruple (X_1, X_2, X_3, X_4), part (b) and the identity $\mathrm{tr}(P)\mathrm{tr}(Q) = \mathrm{tr}(P \otimes Q)$ give

$$\Omega(O)\Omega(O^c) = \mathrm{tr}\big((\mathcal{A}_{X_1} \otimes \mathcal{B}_{X_1})(\mathcal{B}_{X_3}^T \otimes \mathcal{A}_{X_3}^T) \cdot (\mathcal{A}_{X_4} \otimes \mathcal{B}_{X_4})(\mathcal{B}_{X_2}^T \otimes \mathcal{A}_{X_2}^T)\big).$$

Since the four subsets defining a centered pattern are independent subject to their prescribed sizes and zero element sums, the four X_i range independently over $\mathcal{C}_m$. Summing each of the first and third factors over its own index gives $\mathcal{U}$; summing each of the second and fourth gives $\mathcal{S}\mathcal{U}^T\mathcal{S}$, since $\mathcal{B}^T \otimes \mathcal{A}^T = \mathcal{S}(\mathcal{A} \otimes \mathcal{B})^T\mathcal{S}$. Hence

$$N_{C,m} = \mathrm{tr}\big(\mathcal{U} \cdot \mathcal{S}\mathcal{U}^T\mathcal{S} \cdot \mathcal{U} \cdot \mathcal{S}\mathcal{U}^T\mathcal{S}\big) = \mathrm{tr}((\mathcal{U}\mathcal{S})^4),$$

using $\mathcal{U}^T = \mathcal{U}$ from (c) and $\mathcal{S}^2 = 1$. □

6.6. **Evaluation modulo q.**

Proposition 6.12. *$N_{B,m} \equiv N_{C,m} \equiv 1/m^2 \pmod q$ for $0 < m < q$.*

Proof. By Lemmas 6.10 and 6.11 we must evaluate $\mathrm{tr}((\mathcal{E}\mathcal{F})^2)$ and $\mathrm{tr}((\mathcal{U}\mathcal{S})^4)$ in $\mathbb{F}_q$.

Full operators. We index by all m-subsets of $\mathbb{F}_q$ and let $A(x)_{I,J} = \det \Gamma(x)[I, J]$ and $B(x)_{I,J} = \theta(I)\theta(J) \det \Gamma(x)[I^c, J^c]$ (matrices of integer polynomials), and for an m-subset X let $\widehat{\mathcal{A}}_X = [x^X]A(x)$ and $\widehat{\mathcal{B}}_X = [x^{X^c}]B(x)$. By Lemma 6.11(a), a nonzero entry $\widehat{\mathcal{A}}_X(I, J)$ needs $s(I) - s(J) = s(X)$, and a nonzero entry $\widehat{\mathcal{B}}_X(I, J)$ needs $s(I^c) - s(J^c) = s(X^c)$. This is the same condition. Now we reduce modulo q. Let $V = \mathbb{F}_q^q$ with basis $(\mathbf{e}_i)_{i \in \mathbb{F}_q}$, $W = \wedge^m V$ with basis $(\mathbf{e}_I)$, and $W_s = \langle \mathbf{e}_I : s(I) = s \rangle$. For centered X both operators preserve every W_s, and their matrices on W_0 are $\mathcal{A}_X$ and $\mathcal{B}_X$. So $\widehat{\mathcal{E}} = \sum_{X \in \mathcal{C}_m} \widehat{\mathcal{A}}_X$, $\widehat{\mathcal{F}} = \sum_{X \in \mathcal{C}_m} \widehat{\mathcal{B}}_X$ and $\widehat{\mathcal{U}} = \sum_{X \in \mathcal{C}_m} \widehat{\mathcal{A}}_X \otimes \widehat{\mathcal{B}}_X$ restrict to $\mathcal{E}$, $\mathcal{F}$ on W_0 and to $\mathcal{U}$ on $W_0 \otimes W_0$, which the swap also preserves.

A triangular basis. As $T_1^q = 1$, in characteristic q we have $(T_1 - 1)^q = 0$. We fix a basis $\mathbf{b}_1, \ldots, \mathbf{b}_q$ of V in which $T_1 - 1$ is strictly upper triangular. Then every $T_d = T_1^d$ and every $T_d^T = T_{-d}$ is upper unitriangular in this basis. Here the transpose refers to the original cyclic basis. Consequently $\Gamma(x)$ and the operator with standard matrix $\Gamma(x)^T$ are upper triangular with all diagonal entries equal to $\sum_d x_d$. In particular, $\det \Gamma(x) = (\sum_d x_d)^q$ in $\mathbb{F}_q[x]$. Fix a total order $\preceq$ on the m-subsets of $\{1, \ldots, q\}$ that refines the componentwise order of their increasing lists. If an operator is upper triangular in $(\mathbf{b}_j)$, its m-th exterior power has, in the basis $\mathbf{b}_R = \wedge_{j \in R} \mathbf{b}_j$, entries only from $\mathbf{b}_R$ to $\mathbf{b}_{R'}$ with $R' \preceq R$. Indeed, the entry is the minor on the rows R' and the columns R. A nonzero term of this minor matches the elements of R with those of R' so that each element of R' is at most its partner, which forces the kth smallest element of R' to be at most the kth smallest element of R for every k. The diagonal entries are products of m diagonal entries. So $A(x) = \wedge^m \Gamma(x)$ is upper triangular with diagonal $(\sum_d x_d)^m$. By Jacobi's complementary-minor identity (see, for example, [15]), for an invertible $q \times q$ matrix Γ and m-subsets I, J, $\det\big((\Gamma^T)^{-1}\big)[I, J] = (-1)^{\iota(I)+\iota(J)} \det \Gamma[I^c, J^c] / \det \Gamma$. With $\theta(I)\theta(J) = (-1)^{\iota(I)+\iota(J)}$ (as $|I| = |J|$, this sign is the same whether the indices run over $1, \ldots, q$ or over $0, \ldots, q-1$), over $\mathbb{F}_q(x)$ we get $B(x) = \det \Gamma(x) \cdot \wedge^m\big((\Gamma(x)^T)^{-1}\big)$. Here $\Gamma(x)^T$ is upper triangular in the same basis $(\mathbf{b}_j)$ as $\Gamma(x)$, by $T_d^T = T_{-d}$. Its inverse is upper triangular there too. Thus $B(x)$ is upper triangular in $(\mathbf{b}_R)$ with diagonal $(\sum_d x_d)^q (\sum_d x_d)^{-m} = (\sum_d x_d)^{q-m}$. Let Q_0 be the constant matrix of this change of basis of W. Since Q_0 is constant, conjugation by Q_0 commutes with taking the coefficient of a monomial: $Q_0^{-1}\widehat{\mathcal{A}}_X Q_0 = [x^X](Q_0^{-1}A(x)Q_0)$. Therefore, for every m-subset X, $\widehat{\mathcal{A}}_X$ and $\widehat{\mathcal{B}}_X$ are upper triangular in $(\mathbf{b}_R)$ with constant diagonals $[x^X](\sum_d x_d)^m = m!$ and $[x^{X^c}](\sum_d x_d)^{q-m} = (q-m)!$.

Traces. The triangular basis on the whole space need not respect W_0; we therefore use nilpotence before restricting. As integers, $K\,m!\,(q-m)! = (q-1)!$. As sums over the K sets $X \in \mathcal{C}_m$, $\widehat{\mathcal{E}}$ and $\widehat{\mathcal{F}}$ are upper triangular with diagonals $K\,m!$ and $K\,(q-m)!$. Hence $\widehat{\mathcal{E}}\widehat{\mathcal{F}} - K(q-1)!\cdot\mathrm{id}$ is nilpotent. Both $\widehat{\mathcal{E}}$ and $\widehat{\mathcal{F}}$ preserve W_0, as shown above, so their product and this nilpotent difference preserve W_0 too. If a power of an operator is zero, the same power of its restriction to an invariant subspace is zero. Therefore $\mathcal{E}\mathcal{F} - K(q-1)!\cdot\mathrm{id}$ is nilpotent on W_0, of dimension K, and we get $\mathrm{tr}((\mathcal{E}\mathcal{F})^2) = K\big(K(q-1)!\big)^2$. In the basis $(\mathbf{b}_R \otimes \mathbf{b}_{R'})$ each $\widehat{\mathcal{A}}_X \otimes \widehat{\mathcal{B}}_X$ has entries from $\mathbf{b}_J \otimes \mathbf{b}_{J'}$ to $\mathbf{b}_I \otimes \mathbf{b}_{I'}$ only if $I \preceq J$ and $I' \preceq J'$, and diagonal $m!\,(q-m)!$. So $\widehat{\mathcal{U}}$ has this support and diagonal $(q-1)!$, and so does $\mathcal{S}\widehat{\mathcal{U}}\mathcal{S}$, as both tensor factors use the same basis. Such operators are closed under products, with the diagonals multiplying. Thus $(\widehat{\mathcal{U}}\mathcal{S})^2 = \widehat{\mathcal{U}}(\mathcal{S}\widehat{\mathcal{U}}\mathcal{S})$ has this support with diagonal $((q-1)!)^2$, and $(\widehat{\mathcal{U}}\mathcal{S})^4 - ((q-1)!)^4\cdot\mathrm{id}$ is nilpotent, although $\mathcal{S}$ itself need not be triangular. Restricting to $W_0 \otimes W_0$, of dimension K^2: $\mathrm{tr}((\mathcal{U}\mathcal{S})^4) = K^2((q-1)!)^4$.

Arithmetic. First, $K = \binom{q-1}{m-1}/m \equiv (-1)^{m-1}/m \not\equiv 0 \pmod q$, since $0 < m < q$. Thus division by K is valid in $\mathbb{F}_q$. Wilson's theorem gives $(q-1)! \equiv -1$, and the integer identity $K\,m!\,(q-m)! = (q-1)!$ then gives $m!\,(q-m)! \equiv -1/K$. Consequently $N_{C,m} \equiv K^2 = 1/m^2$, $\sum_O \Omega(O^c) \equiv K^3$, and by Lemma 6.10, $N_{B,m} \equiv (q-1)!\,m!\,(q-m)!\,K^3 \equiv (-1)(-1/K)K^3 = K^2 = 1/m^2$. □

Proof of Theorem 6.1. By Propositions 6.9 and 6.12, $q^2 \mid D_{2q}$ and

$$2N_B - N_C \equiv \sum_{m=1}^{q-1} \frac{1}{m^2} = \sum_{x\in\mathbb{F}_q^*} x^2 \pmod q,$$

as inversion permutes $\mathbb{F}_q^*$. For $q \geq 5$ we pick $y \in \mathbb{F}_q^*$ with $y^2 \neq 1$. Then $\sum_x x^2 = \sum_x (yx)^2 = y^2 \sum_x x^2$. So the sum is 0, and $q^3 \mid D_{2q}$. For $q = 3$ the sum is 2. Thus $D_6/9 \equiv 1 \pmod 3$ and $9 \parallel D_6$, in agreement with $D_6 = 2^8\,3^2$ [24]. □

7. Proof of Theorems A and B

Proof of Theorem B. Let $n \geq 8$ be even and $q \leq n-2$ a prime. If $q = 2$, or q is odd with $q \leq n/3$, the natural modulus $M_q(n)$ divides D_n by Theorem 4.1(c). If $n/3 < q < n/2$, it does by Theorem 5.5. If $q = n/2$, then $q \geq 5$ and $M_q(n) = q^3$ divides D_n by Theorem 6.1. If $n/2 < q \leq n-2$, then $v_q(n!) = 1$ and $q \nmid n$, so $M_q(n) = q$, and $q \mid D_n$ by Stones and Wanless [24, Theorem 3.5]. □

Proof of Theorem A. Let $n \geq 8$ be even. Every prime factor of $n!\,n$ is at most n, and it is not n, because n is even and $n > 2$. By (2.4), a prime q divides c_n if and only if $M_q(n)$ does not divide D_n. If $n-1$ is not prime, every prime factor of $n!\,n$ is at most $n-2$, and Theorem B shows that $M_q(n)$ divides D_n for each of them. Hence $n!\,n \mid D_n$ and $c_n = 1$. If $p = n-1$ is prime, then $M_p(n) = p$, as $v_p(n!) = 1$ and $p \nmid n$. The same argument shows that $n!\,n/p$ divides D_n. Therefore $c_n \mid p$. Drisko's theorem [10] (stated as [24, Theorem 1.4]) gives $L^e_{p+1} - L^o_{p+1} \equiv (-1)^{(p+1)/2}p^2 \pmod{p^3}$. Thus $v_p(\Delta_n) = 2$. Since $v_p(n!\,(n-1)!) = 2$, we get $p \nmid D_n$ and $c_n = p$. □

In both cases $n!\,n/(n-1) = n^2(n-2)!$ divides D_n, for every even $n \geq 8$. Berndsen observed that $(n-2)!$ divides D_n for even $n \leq 10$ [7, p. 20].

The smaller even orders have $c_2 = 4$, $c_4 = 24$ and $c_6 = 15$, as stated in the introduction. At $n = 6$, for example, $M_2(6) = 2^5$ divides $D_6 = 2^8\,3^2$, but $M_3(6) = 3^3$ does not.

8. Discussion

Theorem A settles the question of Stones and Wanless [24] on congruences modulo divisors of the isotopy-group order $(n!)^3$ for every even $n \geq 8$ (and hence for every even $n > 2$). Only Drisko's orders, where $n-1$ is prime, yield a nonzero residue modulo a divisor of $(n!)^3$; for every other even $n \geq 8$, the full order $(n!)^3$ divides $L^e_n - L^o_n$ and $c_n = 1$. Theorem C shows further that for every

fixed prime q, the q-adic valuation $v_q(L_n^e - L_n^o)$ grows at least quadratically in n, placing the q-part of D_n far beyond the natural modulus $M_q(n)$ accessible to Sylow q-subgroup orbit counts.

As Glynn [13] and Stones and Wanless [24, p. 7] recorded, Drisko's [11] argument for orders $n = 2^r p$ depends on an unverified lemma of Zappa and remains open. Combined with Theorem A, this means that the smallest open order $n = 26$ has $c_{26} = 1$ and cannot be resolved by any congruence modulo a divisor of $(26!)^3$.

What lies beyond isotopy-group congruences remains largely unexplored. Glynn [13] resolved the orders with $n+1$ prime through a congruence modulo $p = n+1$, which does not divide $(n!)^3$; whether congruences modulo larger primes or built from non-isotopy symmetries can reach orders where neither $n-1$ nor $n+1$ is prime, starting at $n = 26$, is unknown. Within the q-adic picture itself, Theorem C establishes the quadratic lower bound $v_q(L_n^e - L_n^o) \geq v_q(n!\,(n-1)!) + a(a-1)/2$ with $a = \lfloor n/q \rfloor$ (giving $2^{181} \mid D_{26}$ from the exact sum), yet the true asymptotic growth rate and leading constant of $v_q(D_n)$ as $n \to \infty$ are not known. Outside congruences altogether, Alpoge [3] proved square-root cancellation in the signs of Latin squares, while Kumar and Landsberg [18] and Amanov and Yeliussizov [4] recast the conjecture through $\mathrm{SU}(n)$ integrals and tensor invariants; whether analytic or representation-theoretic tools can establish $L_n^e \neq L_n^o$ directly at $n = 26$ and beyond is open.

Acknowledgments

This work was done overwhelmingly by AI models, steered by the author in a continuous critical dialogue, variously with Google's Gemini, Anthropic's Claude and OpenAI's ChatGPT. The author takes full responsibility for the paper.

References

[1] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*, 6th ed., Springer, Berlin, 2018.
[2] N. Alon and M. Tarsi, Colorings and orientations of graphs, *Combinatorica* 12 (1992) 125–134.
[3] L. Alpoge, Square-root cancellation for the signs of Latin squares, *Combinatorica* 37 (2017) 137–142.
[4] A. Amanov and D. Yeliussizov, Fundamental invariants of tensors, Latin hypercubes, and rectangular Kronecker coefficients, *Int. Math. Res. Not. IMRN* 2023 (2023) 17552–17599.
[5] R. Arratia, B. Bollobás and G. B. Sorkin, The interlace polynomial of a graph, *J. Combin. Theory Ser. B* 92 (2004) 199–233; arXiv:math/0209045 (theorem numbers refer to the arXiv version).
[6] C. Babbage, Demonstration of a theorem relating to prime numbers, *Edinburgh Philos. J.* 1 (1819) 46–49.
[7] J. Berndsen, Three problems in algebraic combinatorics, Master's thesis, Eindhoven University of Technology, 2012, https://research.tue.nl/p/en/studenttheses/three-problems-in-algebraic-combinatorics
[8] B. Bollobás, Evaluations of the circuit partition polynomial, *J. Combin. Theory Ser. B* 85 (2002) 261–268.
[9] P. Bürgisser and C. Ikenmeyer, Fundamental invariants of orbit closures, *J. Algebra* 477 (2017) 390–434.
[10] A. A. Drisko, On the number of even and odd Latin squares of order $p+1$, *Adv. Math.* 128 (1997) 20–35.
[11] A. A. Drisko, Proof of the Alon–Tarsi conjecture for $n = 2^r p$, *Electron. J. Combin.* 5 (1998) #R28.
[12] F. Galvin, The list chromatic index of a bipartite multigraph, *J. Combin. Theory Ser. B* 63 (1995) 153–158.
[13] D. G. Glynn, The conjectures of Alon–Tarsi and Rota in dimension prime minus one, *SIAM J. Discrete Math.* 24 (2010) 394–399.
[14] P. Hall, The Eulerian functions of a group, *Quart. J. Math. Oxford Ser.* 7 (1936) 134–151.
[15] R. A. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed., Cambridge University Press, Cambridge, 2013.
[16] R. Huang and G.-C. Rota, On the relations of various conjectures on Latin squares and straightening coefficients, *Discrete Math.* 128 (1994) 225–236.
[17] J. C. M. Janssen, On even and odd Latin squares, *J. Combin. Theory Ser. A* 69 (1995) 173–181.
[18] S. Kumar and J. M. Landsberg, Connections between conjectures of Alon–Tarsi, Hadamard–Howe, and integrals over the special unitary group, *Discrete Math.* 338 (2015) 1232–1238.
[19] M. Las Vergnas, Le polynôme de Martin d'un graphe eulérien, *Ann. Discrete Math.* 17 (1983) 397–411.
[20] S. Mertens and C. Moore, The complexity of the fermionant and immanants of constant width, *Theory Comput.* 9 (2013) 273–282.
[21] Open Problem Garden, Even vs. odd latin squares (N. Alon and M. Tarsi, 1992), https://www.openproblemgarden.org/op/even_vs_odd_latin_squares

[22] Polymath 12, Rota's basis conjecture (led by T. Chow, 2017), https://polymathprojects.org/2017/02/23/rotas-basis-conjecture-polymath-12/
[23] L. Sauermann, Rota's basis conjecture holds for random bases of vector spaces, *European J. Combin.* 121 (2024) 103836.
[24] D. S. Stones and I. M. Wanless, How not to prove the Alon–Tarsi conjecture, *Nagoya Math. J.* 205 (2012) 1–24.
[25] G. Zolotareff, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouv. Ann. Math. (2)* 11 (1872) 354–362.