Nagoya Math. J. **205** (2012), 1–24
DOI 10.1215/00277630-1543769

HOW *NOT* TO PROVE THE ALON-TARSI CONJECTURE

DOUGLAS S. STONES AND IAN M. WANLESS

Abstract. The sign of a Latin square is -1 if it has an odd number of rows and columns that are odd permutations; otherwise, it is $+1$. Let L_n^{E} and L_n^{O} be, respectively, the number of Latin squares of order n with sign $+1$ and -1. The Alon-Tarsi conjecture asserts that $L_n^{\mathrm{E}} \neq L_n^{\mathrm{O}}$ when n is even. Drisko showed that $L_{p+1}^{\mathrm{E}} \not\equiv L_{p+1}^{\mathrm{O}} \pmod{p^3}$ for prime $p \geq 3$ and asked if similar congruences hold for orders of the form $p^k + 1$, $p + 3$, or $pq + 1$. In this article we show that if $t \leq n$, then $L_{n+1}^{\mathrm{E}} \not\equiv L_{n+1}^{\mathrm{O}} \pmod{t^3}$ only if $t = n$ and n is an odd prime, thereby showing that Drisko's method cannot be extended to encompass any of the three suggested cases. We also extend exact computation to $n \leq 9$, discuss asymptotics for $L^{\mathrm{O}}/L^{\mathrm{E}}$, and propose a generalization of the Alon-Tarsi conjecture.

§1. Introduction and basic properties

Alon and Tarsi are responsible for several fascinating conjectures. The one we will refer to as the *Alon-Tarsi conjecture* asserts that for any even order, the number of even Latin squares differs from the number of odd Latin squares. This conjecture was made in [1, p. 132], where it was shown to imply the even case of a conjecture attributed to Dinitz [6, p. 157]. The Dinitz conjecture (Theorem 1.1) was subsequently proved by Galvin [7] and Slivnik [20] (see also [3], [10], [13], [28]).

THEOREM 1.1. *Given any n^2 sets $\mathcal{S}_{ij}$ of cardinality n with $0 \leq i, j \leq n-1$, there exists an $n \times n$ matrix (l_{ij}) with each $l_{ij} \in \mathcal{S}_{ij}$ without repeated symbols in any row or column.*

This result can be interpreted in terms of partial Latin squares or list colorings of complete bipartite graphs.

Received May 14, 2010. Revised May 17, 2011. Accepted June 29, 2011.
2010 Mathematics Subject Classification. Primary 05B15; Secondary 11B50.
Authors' work partially supported by ARC grants DP0662946 and DP1093320. Stone's work also supported by the Monash Faculty of Science Postgraduate Publications Award.

Huang and Rota [12] showed that the Alon-Tarsi conjecture is equivalent to a certain conjecture for supersymmetric bracket algebras. They also showed that this conjecture in turn implies a tantalizing conjecture now commonly known as *Rota's basis conjecture*, also referred to as *Rota's colorful conjecture* (see [18]). (For further reading on the Alon-Tarsi conjecture, see [1], [8], [12], [18].) This conjecture can be stated as follows.

CONJECTURE 1.2. *Let $B_1, B_2, \ldots, B_n$ be bases for an n-dimensional vector space (or, more generally, for a rank n matroid). Then each basis can be linearly ordered, say, $B_1 = \{b_{11}, b_{12}, \ldots, b_{1n}\}$, $B_2 = \{b_{21}, b_{22}, \ldots, b_{2n}\}, \ldots,$ $B_n = \{b_{n1}, b_{n2}, \ldots, b_{nn}\}$, in such a way that each of the sets $\{b_{11}, b_{21}, \ldots, b_{n1}\}$, $\{b_{12}, b_{22}, \ldots, b_{n2}\}, \ldots, \{b_{1n}, b_{2n}, \ldots, b_{nn}\}$ is also a basis.*

The aim of this paper is to prove a number of results about the parity of Latin squares, including congruences that show that a method employed by Drisko [4] for a partial solution has little hope of being extended. First we must set up our definitions and notation.

A *Latin square* of order n is an $n \times n$ array $L = (l_{ij})$ of n symbols such that each symbol occurs exactly once in each row and exactly once in each column. We will take the symbol set of L to be $\mathbb{Z}_n$, matching the row and column indices. A Latin square is *normalized* if the first row is $(0, 1, \ldots, n-1)$. A Latin square is *reduced* if the first row is $(0, 1, \ldots, n-1)$ and the first column is $(0, 1, \ldots, n-1)^T$. A Latin square $L = (l_{ij})$ is *unipotent* if $l_{00} = l_{11} = \cdots = l_{(n-1)(n-1)}$.

Suppose that P is a property of Latin squares of order n. Let L_n^P be the number of Latin squares of order n that satisfy P. Let K_n^P, R_n^P, and U_n^P be, respectively, the number of normalized, reduced, and normalized unipotent Latin squares of order n that satisfy P. Let T_n^P be the number of unipotent Latin squares of order n with the first column $(0, 1, \ldots, n-1)^T$ that satisfy P. If P is omitted, we can assume that P "is a Latin square" (i.e., the trivial property). It follows that $R_n = U_n = T_n$ and that

$$L_n = n!(n-1)!R_n \tag{1.1}$$

for all n.

Let α be a permutation of $\mathbb{Z}_n$. If α can be produced by the composition of an even number of transpositions, then α is called an *even* permutation; otherwise, α is an *odd* permutation. Define the *sign* of α, denoted $\epsilon(\alpha)$, as $+1$ if α is an even permutation and -1 if α is an odd permutation.

Given a Latin square $L = (l_{ij})$ of order n, we can identify the following $3n$ permutations of $\mathbb{Z}_n$. For all $i \in \mathbb{Z}_n$ define σ_i^{row} by $\sigma_i^{\text{row}}(j) = l_{ij}$. For all $j \in \mathbb{Z}_n$ define σ_j^{col} by $\sigma_j^{\text{col}}(i) = l_{ij}$. For all $\ell \in \mathbb{Z}_n$ define σ_ℓ^{sym} such that $\sigma_\ell^{\text{sym}}(i)$ is equal to the j for which $l_{ij} = \ell$. We call $\epsilon_{\text{row}}(L) := \prod_i \epsilon(\sigma_i^{\text{row}})$, $\epsilon_{\text{col}}(L) := \prod_j \epsilon(\sigma_j^{\text{col}})$, and $\epsilon_{\text{sym}}(L) := \prod_\ell \epsilon(\sigma_\ell^{\text{sym}})$ the *row-sign*, *column-sign*, and *symbol-sign* of L, respectively. The product $\epsilon(L) := \epsilon_{\text{row}}(L)\epsilon_{\text{col}}(L)$ is called the *sign* of L.

A Latin square is called *even* or *odd* if $\epsilon(L) = +1$ or $\epsilon(L) = -1$, respectively. A Latin square is called *row-even* or *row-odd* if $\epsilon_{\text{row}}(L) = +1$ or $\epsilon_{\text{row}}(L) = -1$, respectively. A Latin square is called *column-even* or *column-odd* if $\epsilon_{\text{col}}(L) = +1$ or $\epsilon_{\text{col}}(L) = -1$, respectively. A Latin square is called *symbol-even* or *symbol-odd* if $\epsilon_{\text{sym}}(L) = +1$ or $\epsilon_{\text{sym}}(L) = -1$, respectively. We define the following properties.

- E = "is an even Latin square"
- O = "is an odd Latin square"
- RE = "is a row-even Latin square"
- RO = "is a row-odd Latin square"
- CE = "is a column-even Latin square"
- CO = "is a column-odd Latin square"
- SE = "is a symbol-even Latin square"
- SO = "is a symbol-odd Latin square"

A theorem of Janssen [14, Theorem 3.2] (see also [25], [26]) states that, for any Latin square L of order n,

$$\epsilon_{\text{row}}(L)\epsilon_{\text{col}}(L)\epsilon_{\text{sym}}(L) = \begin{cases} +1 & \text{if } n \equiv 0 \text{ or } 1 \pmod 4, \\ -1 & \text{if } n \equiv 2 \text{ or } 3 \pmod 4. \end{cases} \tag{1.2}$$

In particular, we can use (1.2) to find $\epsilon_{\text{sym}}(L)$ from $\epsilon_{\text{row}}(L)$, $\epsilon_{\text{col}}(L)$ and the value of $n \pmod 4$. We define the *parity* of a Latin square L to be the ordered triplet

$$\pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}} \in \{\overbrace{000, 011, 101, 110}^{n\equiv 0 \text{ or } 1 \bmod 4}, \overbrace{111, 100, 010, 001}^{n\equiv 2 \text{ or } 3 \bmod 4}\} \tag{1.3}$$

such that $\pi_x = 0$ when $\epsilon_x(L) = +1$ and $\pi_x = 1$ when $\epsilon_x(L) = -1$ for $x \in \{\text{row}, \text{col}, \text{sym}\}$. We call π_{row}, π_{col}, and π_{sym} the *row-parity*, *column-parity*, and *symbol-parity* of L, respectively. We will use L_n^π and R_n^π to denote, respectively, the number of all Latin squares and the number of reduced Latin squares of order n with given parity $\pi = \pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$. By considering

Table 1: Table of identities

If $n \equiv 0$ *or* $1 \pmod 4$	*If* $n \equiv 2$ *or* $3 \pmod 4$
$R_n^{\mathrm{E}} = R_n^{\mathrm{SE}} = R_n^{000} + R_n^{110}$ $R_n^{\mathrm{O}} = R_n^{\mathrm{SO}} = R_n^{011} + R_n^{101}$	$R_n^{\mathrm{E}} = R_n^{\mathrm{SO}} = R_n^{111} + R_n^{001}$ $R_n^{\mathrm{O}} = R_n^{\mathrm{SE}} = R_n^{100} + R_n^{010}$
$U_n^{\mathrm{E}} = R_n^{\mathrm{CE}} = R_n^{000} + R_n^{101}$ $U_n^{\mathrm{O}} = R_n^{\mathrm{CO}} = R_n^{011} + R_n^{110}$	$U_n^{\mathrm{E}} = R_n^{\mathrm{CO}} = R_n^{111} + R_n^{010}$ $U_n^{\mathrm{O}} = R_n^{\mathrm{CE}} = R_n^{100} + R_n^{001}$
$T_n^{\mathrm{E}} = R_n^{\mathrm{RE}} = R_n^{000} + R_n^{011} = U_n^{\mathrm{E}}$ $T_n^{\mathrm{O}} = R_n^{\mathrm{RO}} = R_n^{101} + R_n^{110} = U_n^{\mathrm{O}}$	$T_n^{\mathrm{E}} = R_n^{\mathrm{RO}} = R_n^{111} + R_n^{100} = U_n^{\mathrm{E}}$ $T_n^{\mathrm{O}} = R_n^{\mathrm{RE}} = R_n^{010} + R_n^{001} = U_n^{\mathrm{O}}$
$R_n^{111} = R_n^{100} = R_n^{010} = R_n^{001} = 0$ $R_n^{011} = R_n^{101}$ $R_n^{011} = R_n^{101} = R_n^{110}$ when n is even	$R_n^{000} = R_n^{011} = R_n^{101} = R_n^{110} = 0$ $R_n^{100} = R_n^{010}$ $R_n^{100} = R_n^{010} = R_n^{001}$ when n is even

the effect of matrix transposition, it can easily be seen that, for all n, $U_n^{\mathrm{E}} = T_n^{\mathrm{E}}$, $U_n^{\mathrm{O}} = T_n^{\mathrm{O}}$, $R_n^{100} = R_n^{010}$, and $R_n^{011} = R_n^{101}$. Consequently, we can deduce all but the last row of Table 1. The last row of Table 1 will be proved separately in Lemma 1.8 but is appended for the sake of completeness.

In Section 2 we describe an algorithm which we used to compute the values of R_n^{π} for $n \leq 9$ listed in Table 2.

Let $\mathcal{I}_n = S_n \times S_n \times S_n$, where S_n is the symmetric group acting on $\mathbb{Z}_n$. Then $\mathcal{I}_n$ acts on the set of Latin squares $L = (l_{ij})$ in the following way. For each $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$, we define $\theta(L)$ to be the Latin square formed from L by permuting the rows according to α, permuting the columns according to β, and permuting the symbols according to γ. To be precise, $\theta(L) = (l'_{ij})$ is the Latin square defined by $l'_{ij} = \gamma(l_{\alpha^{-1}(i)\beta^{-1}(j)})$ for all $i, j \in \mathbb{Z}_n$. Any $\theta \in \mathcal{I}_n$ is called an *isotopism*, and L and $\theta(L)$ are said to be *isotopic*. Isotopisms of the form (α, α, α) are called *isomorphisms*. If $\theta(L) = L$, then θ is said to be an *autotopism* of L. The group of all autotopisms of L is called the *autotopism group* of L, denoted $\mathrm{Atp}(L)$. If θ is an isomorphism and $\theta \in \mathrm{Atp}(L)$, then θ is said to be an *automorphism* of L. The identity permutation will be denoted ε. Any autotopism other than $(\varepsilon, \varepsilon, \varepsilon)$ is *nontrivial*.

Let $\theta = (\alpha, \beta, \gamma) \in \mathcal{I}_n$ be an isotopism. By considering the action of θ on each individual row and column, we find that

$$\begin{aligned} \epsilon\big(\theta(L)\big) &= \epsilon(L)\epsilon^n(\alpha)\epsilon^n(\beta)\epsilon^{2n}(\gamma) = \epsilon(L)\epsilon^n(\alpha)\epsilon^n(\beta), \\ \epsilon_{\mathrm{row}}\big(\theta(L)\big) &= \epsilon_{\mathrm{row}}(L)\epsilon^n(\beta)\epsilon^n(\gamma), \\ \epsilon_{\mathrm{col}}\big(\theta(L)\big) &= \epsilon_{\mathrm{col}}(L)\epsilon^n(\alpha)\epsilon^n(\gamma), \\ \epsilon_{\mathrm{sym}}\big(\theta(L)\big) &= \epsilon_{\mathrm{sym}}(L)\epsilon^n(\alpha)\epsilon^n(\beta). \end{aligned} \tag{1.4}$$

Table 2: R_n^π where $\pi = \pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$ and $1 \le n \le 9$

	Even Latin squares				*Odd Latin squares*	
	$n \equiv 0,1 \pmod 4$		$n \equiv 2,3 \pmod 4$		$n \equiv 0,1 \pmod 4$	$n \equiv 2,3 \pmod 4$
n	R_n^{000}	R_n^{110}	R_n^{111}	R_n^{001}	$R_n^{011} = R_n^{101}$	$R_n^{100} = R_n^{010}$
1	1					
2			1			
3				1		
4	4					
5	8	32			8	
6			4080	1776		1776
7			4488960	4120320		4166400
8	138478485504	132267638784			132267638784	
9	94408261830180864	94406174985682944			94391567074197504	

For example, (1.4) implies that θ preserves the parity of a Latin square if n is even or if θ is an isomorphism. So, when n is even and $P \in \{\text{E}, \text{O}, \text{RE}, \text{RO}, \text{CE}, \text{CO}, \text{SE}, \text{SO}\}$ or P is any parity,

$$L_n^P = n!(n-1)!R_n^P = n!(n-1)!U_n^P. \tag{1.5}$$

Considering the effect of swapping two rows, columns, or symbols, we find from (1.4) that for odd $n \geq 3$,

$$L_n^{000} = L_n^{011} = L_n^{101} = L_n^{110} \qquad \text{and} \qquad L_n^{111} = L_n^{100} = L_n^{010} = L_n^{001}, \tag{1.6}$$

and hence

$$L_n^{\text{E}} = L_n^{\text{O}} = \frac{1}{2}L_n = \frac{1}{2}n!(n-1)!R_n = \frac{1}{2}n!(n-1)!U_n. \tag{1.7}$$

We will see shortly that for odd n it is conjectured that $R_n^{\text{E}} \neq R_n^{\text{O}}$ and $U_n^{\text{E}} \neq U_n^{\text{O}}$, even though $L_n^{\text{E}} = L_n^{\text{O}}$ when $n \geq 3$. On the other hand, for even n, (1.5) implies that

$$R_n^{\text{E}} = R_n^{\text{O}} \iff U_n^{\text{E}} = U_n^{\text{O}} \iff L_n^{\text{E}} = L_n^{\text{O}}.$$

We now introduce the following conjecture by Alon and Tarsi [1, p. 132] and a theorem of Drisko [4], which motivate the results in Section 3.

Conjecture 1.3 (Alon-Tarsi conjecture). *When n is even, $L_n^{\text{E}} \neq L_n^{\text{O}}$.*

Theorem 1.4 (see Drisko [4]). *If p is an odd prime, then $L_{p+1}^{\text{E}} - L_{p+1}^{\text{O}} \equiv (-1)^{(p+1)/2}p^2 \pmod{p^3}$.*

Theorem 1.4 proves a special case of the Alon-Tarsi conjecture. After proving Theorem 1.4, Drisko [4, p. 34] made the following remark: "This strongly suggests that the conjecture should hold for all even integers. How might one prove the other cases? The general results and approach...could still be applied. The most promising cases seem to be p^k+1...but one might also try $p+3$ or even $pq+1$, where $p \neq q$ are odd primes."

In Corollary 3.7, we will prove that $L_{n+1}^{\text{E}} \equiv L_{n+1}^{\text{O}} \pmod{t^3}$ for all $1 \leq t \leq n$ except when $t = n$ and n is an odd prime. This rules out an analogue of Theorem 1.4 for many cases, including the three cases suggested by Drisko.

Huang and Rota [12] showed that the Alon-Tarsi conjecture is equivalent to the following conjecture.

Conjecture 1.5. *When n is even, $R_n^{\text{RE}} \neq R_n^{\text{RO}}$.*

Actually, [12] considered the conjecture $L_n^{\mathrm{RE}} \neq L_n^{\mathrm{RO}}$ for even n, but this is equivalent to Conjecture 1.5, given (1.5). Some values of K_n^{RE} and K_n^{RO} were given in [9] for $n \leq 7$ (of which K_4^{RE} is incorrect and the sign of $K_7^{\mathrm{RE}} - K_7^{\mathrm{RO}}$ is missing; see also [29]). Table 3 lists R_n^{RE} and R_n^{RO} for $n \leq 9$. Since row permutations do not affect the row-sign of a Latin square, $R_n^{\mathrm{RE}} = (n-1)!K_n^{\mathrm{RE}}$ and $R_n^{\mathrm{RO}} = (n-1)!K_n^{\mathrm{RO}}$ (also see [14], [15], [16] for further results on the row-sign of Latin squares and Latin rectangles).

We also list the following related conjectures. The first conjecture was made by Zappa [27], and the second was not found in the literature.

CONJECTURE 1.6. *We have* $U_n^{\mathrm{E}} \neq U_n^{\mathrm{O}}$ *for* $n \geq 1$.

CONJECTURE 1.7. *We have* $R_n^{\mathrm{E}} \neq R_n^{\mathrm{O}}$ *for* $n \geq 1$.

For even n, (1.5) implies that

$$R_n^{\mathrm{E}} - R_n^{\mathrm{O}} = \frac{1}{n!(n-1)!}(L_n^{\mathrm{E}} - L_n^{\mathrm{O}}) = U_n^{\mathrm{E}} - U_n^{\mathrm{O}}. \tag{1.8}$$

However, for odd n, $U_n^{\mathrm{E}} - U_n^{\mathrm{O}}$ and $R_n^{\mathrm{E}} - R_n^{\mathrm{O}}$ might be different. For example, Tables 1 and 2 show that $R_7^{\mathrm{E}} - R_7^{\mathrm{O}} = 276480 \neq 368640 = U_7^{\mathrm{E}} - U_7^{\mathrm{O}}$ and $R_9^{\mathrm{E}} - R_9^{\mathrm{O}} = 31302667468800 \neq 2086844497920 = U_9^{\mathrm{E}} - U_9^{\mathrm{O}}$. Table 1 implies that $|R_n^{\mathrm{RE}} - R_n^{\mathrm{RO}}| = |U_n^{\mathrm{E}} - U_n^{\mathrm{O}}|$ for all n, so Conjecture 1.6 implies Conjecture 1.5.

In the following lemma, we prove the last row of Table 1 by exploiting the other identities in that table.

LEMMA 1.8. *For even* n, *we have* $R_n^{011} = R_n^{101} = R_n^{110}$ *and* $R_n^{100} = R_n^{010} = R_n^{001}$.

Proof. By (1.8), $R_n^{\mathrm{E}} - R_n^{\mathrm{O}} = U_n^{\mathrm{E}} - U_n^{\mathrm{O}}$. If $n \equiv 0 \pmod 4$, then $R_n^{000} + R_n^{110} - R_n^{011} - R_n^{101} = R_n^{000} + R_n^{101} - R_n^{011} - R_n^{110}$. Hence, $R_n^{101} = R_n^{110}$. The result follows since $R_n^{011} = R_n^{101}$ and $R_n^{111} = R_n^{100} = R_n^{010} = R_n^{001} = 0$. We can prove the claim for $n \equiv 2 \pmod 4$ similarly. ∎

Drisko [5] showed that $U_p^{\mathrm{E}} - U_p^{\mathrm{O}} \equiv (-1)^{(p-1)/2} \pmod p$ for odd primes p. Glynn [8] showed that $L_{p-1}^{\mathrm{E}} - L_{p-1}^{\mathrm{O}} \equiv (-1)^{(p-1)/2} \pmod p$ for odd primes p (see also [22]). Glynn also showed that the main results of Zappa [27] are unreliable, which has consequences for [5]. (Specifically, the claim in the title of [5] was, in fact, not proved, since it is reliant on an invalid result by Zappa. However, Drisko's proof of Conjecture 1.6 for prime n in [5] remains valid.) Marini and Pirillo (see [15], [27]) gave the values of $U_n^{\mathrm{E}} - U_n^{\mathrm{O}}$ for $n \leq 8$. Note that $U_9^{\mathrm{E}} - U_9^{\mathrm{O}} = R_9^{\mathrm{RE}} - R_9^{\mathrm{RO}}$, which is given in Table 3.

To review, we know that the Alon-Tarsi conjecture and Conjectures 1.5, 1.6, and 1.7 are true when $n = p \pm 1$ for some odd prime p and when $n \leq 9$ (see Table 2). Additionally, Conjecture 1.6 holds when n is a prime. In Section 4, we will give a conjecture that includes, as special cases, the Alon-Tarsi conjecture and Conjectures 1.5, 1.6, and 1.7.

We conclude this section by introducing some lemmas that we will use later in this paper. Let L be a Latin square. If M is a submatrix of L that is also a Latin square, then M is called a *subsquare* of L.

LEMMA 1.9. *Let L be a Latin square of order n. If M is a subsquare of L and $M \neq L$, then the order of M is at most $\lfloor n/2 \rfloor$.*

LEMMA 1.10. *Let L be a Latin square, and let $\theta = (\alpha, \beta, \gamma) \in \mathrm{Atp}(L)$. Let M denote the submatrix formed by the intersection of the rows whose indices are fixed by α and the columns whose indices are fixed by β. If M is not empty, then it is a subsquare of L.*

We will also make use of the following result from [25], which describes the effect of cycle switching on the parity of a Latin square. A *Latin rectangle* M is a matrix in which each symbol of M appears in every row of M and no symbol is repeated within a column. A *partial row switch* of length ℓ consists of swapping the two rows of a $2 \times \ell$ Latin rectangle within L. A *partial column switch* of length ℓ consists of swapping the two columns of an $\ell \times 2$ submatrix M within L, whose transpose M^T is a Latin rectangle.

LEMMA 1.11 ([25, Proposition 1]). *Let L be a Latin square of parity $\pi = \pi_{\mathrm{row}}\pi_{\mathrm{col}}\pi_{\mathrm{sym}}$.*

- *A partial row switch of length ℓ toggles both π_{col} and π_{sym} if and only if ℓ is odd, but leaves π_{row} unchanged.*
- *A partial column switch of length ℓ toggles both π_{row} and π_{sym} if and only if ℓ is odd, but leaves π_{col} unchanged.*

§2. Computational results and asymptotics

In this section, we describe how we found the values of R_n^π exactly for $n \leq 9$. Various combinations of these numbers were given for $n \leq 8$ (e.g., by Janssen [14] and Zappa [26]), which we verify and extend. Table 2 lists the results of our computations. These data motivate us to consider by how much the nonzero values of R_n^π can differ for a given n.

The set of all Latin squares isotopic to a given Latin square L is called the *isotopy class* of L. We can partition the set of Latin squares into isotopy

classes. The number of reduced Latin squares in the isotopy class containing L is $n!n/|\operatorname{Atp}(L)|$ (see, e.g., [19]).

We begin with a set Ω consisting of one representative from each isotopy class of Latin squares of order n. For $L \in \Omega$, let $I(L,\pi)$ be the number of reduced Latin squares isotopic to L that have parity $\pi = \pi_{\text{row}}\pi_{\text{col}}\pi_{\text{sym}}$. Hence,

$$R_n^{\pi} = \sum_{L\in\Omega} I(L,\pi).$$

For any given $L \in \Omega$, we have $\sum_{\pi} I(L,\pi) = n!n/|\operatorname{Atp}(L)|$. Using (1.2), we know that $I(L,\pi) \neq 0$ only if

$$\pi \in \begin{cases} \{000,011,101,110\} & \text{if } n \equiv 0 \text{ or } 1 \pmod 4, \\ \{111,100,010,001\} & \text{if } n \equiv 2 \text{ or } 3 \pmod 4. \end{cases} \tag{2.1}$$

In the case when n is even, isotopisms preserve the parity of a Latin square. Therefore, $I(L,\pi) = n!n/|\operatorname{Atp}(L)|$ when π is the parity of L, and $I(L,\pi) = 0$ otherwise. We consider the case of odd n in the following theorem. For $L \in \Omega$, let $r = r(L)$ be the number of odd rows, that is, the number of i such that $\epsilon(\sigma_i^{\text{row}}) = -1$, and let $c = c(L)$ be the number of odd columns, that is, the number of j such that $\epsilon(\sigma_j^{\text{col}}) = -1$. The row-parity of L is congruent to $r \pmod 2$, and the column-parity of L is congruent to $c \pmod 2$.

THEOREM 2.1. *Suppose that n is odd. Then suppose also that $L \in \Omega$. Let $\mu = (n-1)!/|\operatorname{Atp}(L)|$. If π satisfies (2.1), then*

$$I(L,\pi) = \begin{cases} (n-r)(n-c)\mu & \text{if } \pi_{\text{row}} \equiv r \text{ and } \pi_{\text{col}} \equiv c \pmod 2, \\ (n-r)c\mu & \text{if } \pi_{\text{row}} \equiv r \text{ and } \pi_{\text{col}} \not\equiv c \pmod 2, \\ r(n-c)\mu & \text{if } \pi_{\text{row}} \not\equiv r \text{ and } \pi_{\text{col}} \equiv c \pmod 2, \\ rc\mu & \text{if } \pi_{\text{row}} \not\equiv r \text{ and } \pi_{\text{col}} \not\equiv c \pmod 2. \end{cases}$$

Proof. From $L = (l_{ij})$ we can construct $n!n$, not necessarily distinct, reduced Latin squares by the following steps.

(I) Pick $i, j \in \mathbb{Z}_n$.
(II) Pick $\gamma \in S_n$ such that $\gamma(l_{ij}) = 0$.
(III) Pick $\alpha, \beta \in S_n$, such that $\alpha(i) = 0$ and $\beta(j) = 0$, and also such that $(\alpha,\beta,\gamma)(L)$ is reduced.

The permutations α and β in step (III) are determined by L and the choices made in steps (I) and (II). Furthermore, each of the $n!n/|\operatorname{Atp}(L)|$ reduced Latin squares isotopic to L can be constructed by steps (I)–(III).

If θ and φ are isotopisms such that $\theta(L) = \varphi(L)$, then $\theta\varphi^{-1}$ is an autotopism of L. Hence, each reduced Latin square isotopic to L is generated by steps (I)–(III) at most $|\operatorname{Atp}(L)|$ times. Since steps (I)–(III) generate $n!n$ reduced Latin squares, of which $n!n/|\operatorname{Atp}(L)|$ are distinct, we deduce that each reduced Latin square isotopic to L is generated by steps (I)–(III) exactly $|\operatorname{Atp}(L)|$ times.

Let $\theta = (\alpha, \beta, \gamma)$ as defined by steps (I)–(III). Observe that $\theta = (\gamma\sigma_j^{\mathrm{col}}, \gamma\sigma_i^{\mathrm{row}}, \gamma)$. The row-parity of $\theta(L)$ is incongruent to $r \pmod 2$ if and only if $-1 = \epsilon(\gamma)^n\epsilon(\sigma_i^{\mathrm{row}})^n\epsilon(\gamma)^n = \epsilon(\sigma_i^{\mathrm{row}})$. Similarly, the column-parity of $\theta(L)$ is incongruent to $c \pmod 2$ if and only if $-1 = \epsilon(\gamma)^n\epsilon(\sigma_j^{\mathrm{col}})^n\epsilon(\gamma)^n = \epsilon(\sigma_j^{\mathrm{col}})$. In particular, the row and column parities of $\theta(L)$ depend only on L and the choice of i and j.

We conclude that steps (I)–(III) generate, for example, exactly $(n-r)(n-c)\mu$ distinct reduced Latin squares with row-parity congruent to $r \pmod 2$ and column-parity congruent to $c \pmod 2$. The other cases are similar. □

The second author has used the algorithm described above to find the values of R_n^{π} given in Table 2, that is, for $n \le 9$. The first author independently tested the algorithm for $n \le 7$. From Table 2 we can deduce the data in Table 3 for R_n^{RO} and R_n^{RE}. We can also deduce from Table 2 that

$$R_n^{\pi} > 0 \tag{2.2}$$

Table 3: R_n^{RE} and R_n^{RO} for $1 \le n \le 9$

n	R_n^{RE}	R_n^{RO}	$R_n^{\mathrm{RE}} - R_n^{\mathrm{RO}}$
1	1	0	1
2	0	1	−1
3	1	0	1
4	4	0	4
5	16	40	−24
6	3552	5856	−2304
7	8286720	8655360	−368640
8	270746124288	264535277568	6210846720
9	188799828904378368	188797742059880448	2086844497920

whenever $n \geq 5$ and π satisfies (2.1). For any $n \geq 10$, we can build a reduced Latin square of order n containing a reduced Latin subsquare of order 5. By changing the subsquare, we can achieve four different parities, which must give us the four options in (2.1).

It was suggested in [25] that there should be roughly the same number of Latin squares of each possible parity. We now state a more specific formal conjecture. In this conjecture, $x \sim y$ denotes that x and y are asymptotically equal, in other words, $x/y \to 1$ as $n \to \infty$.

CONJECTURE 2.2. *We have the following:*

$$R_n^{000} \sim R_n^{011} \sim R_n^{101} \sim R_n^{110} \sim \frac{1}{4} R_n \quad \textit{for } n \equiv 0,1 \pmod 4,$$

$$R_n^{111} \sim R_n^{100} \sim R_n^{010} \sim R_n^{001} \sim \frac{1}{4} R_n \quad \textit{for } n \equiv 2,3 \pmod 4.$$

This conjecture implies that the number of even Latin squares is asymptotically equal to the number of odd Latin squares. As partial evidence for this conjecture we can consider the row-parity of Latin rectangles. *Row-parity* is defined for Latin rectangles analogously to how it was defined for Latin squares. A $k \times n$ Latin rectangle is *reduced* if its first row is $(0, 1, \ldots, n-1)$ and the first column is $(0, 1, \ldots, k-1)^T$. Let $L_{k,n}^{\mathrm{RE}}$, $L_{k,n}^{\mathrm{RO}}$, $R_{k,n}^{\mathrm{RE}}$, and $R_{k,n}^{\mathrm{RO}}$ be, respectively, the number of row-even, row-odd, reduced row-even, and reduced row-odd $k \times n$ Latin rectangles.

LEMMA 2.3. *If $2 \leq k \leq o(n)$ as $n \to \infty$, then $L_{k,n}^{\mathrm{RE}} \sim L_{k,n}^{\mathrm{RO}}$ and $R_{k,n}^{\mathrm{RE}} \sim R_{k,n}^{\mathrm{RO}}$.*

Proof. Starting from any reduced $k \times n$ Latin rectangle, we can obtain a reduced Latin rectangle of the opposite row-parity by interchanging the symbol x in the second position of the last row with some other symbol y to its right in the last row. This works provided that y does not already appear in the second column and x does not already appear in the column we are moving it to. There are between $n-2k$ and $n-k$ (inclusive) valid such interchanges. Since the starting rectangle was arbitrary and interchanges are reversible (i.e., whenever an interchange transforms rectangle L to L', then an interchange on the same positions transforms L' to L), we have

$$\frac{n-2k}{n-k} \leq \frac{R_{k,n}^{\mathrm{RE}}}{R_{k,n}^{\mathrm{RO}}} \leq \frac{n-k}{n-2k},$$

from which it follows that $R_{k,n}^{\mathrm{RE}} \sim R_{k,n}^{\mathrm{RO}}$. The same argument works to show that $L_{k,n}^{\mathrm{RE}} \sim L_{k,n}^{\mathrm{RO}}$. ∎

A similar result was given by Chow [3, Theorem 4] in the case when $k \le (\log n)^{3/2-\epsilon}$. Chow also claimed that McKay improved the bound to $k = o(n)$, although a proof of this result was not given in [3]. Habsieger and Janssen [9] conjectured that $R^{\mathrm{RE}}_{k,n} \ne R^{\mathrm{RO}}_{k,n}$ whenever $1 \le k \le n$ except when $(k,n) = (3,4)$. Actually, their conjecture was for *normalized* Latin rectangles (where the first row is in order) but it can be shown to be equivalent to the version just given. It is easy to show that $L^{\mathrm{RE}}_{k,n} = L^{\mathrm{RO}}_{k,n}$ for odd k, while for even k, the conjecture in [9] implies that $L^{\mathrm{RE}}_{k,n} \ne L^{\mathrm{RO}}_{k,n}$ whenever $2 \le k \le n$.

Although it is easy to find heuristic arguments in favor of Conjecture 2.2 (e.g., in [25], and Lemma 2.3 above), a formal proof does not seem easy. However, we can prove a weaker hypothesis on the supposition that n is odd. For odd $n \ge 3$, (1.6) implies that $L^{\pi}_n = L^{\pi'}_n$, provided that π and π' satisfy (2.1). Our next aim is to show that the ratio $R^{\pi}_n / R^{\pi'}_n$, which we believe tends to 1, is at least bounded. We need the following lemma, in which we again use the notation that $r = r(L)$ is the number of odd rows and $c = c(L)$ is the number of odd columns in a Latin square L of order $n = n(L)$. We say that *almost all* Latin squares satisfy a property P if $L^P_n \sim L_n$ as $n \to \infty$.

LEMMA 2.4. *Almost all Latin squares satisfy* $n/63 \le r \le 62n/63$ *and* $n/63 \le c \le 62n/63$.

Proof. Let η be the smallest even integer greater than $31n/63$. Let H_i be the set of Latin squares of order n in which there are i odd rows and $\eta - i$ even rows among the first η rows. By [11, Lemma 3.1],

$$\frac{|H_i|}{|H_{\eta/2}|} \le 3^{\eta/2} \binom{\eta}{i} \Big/ \binom{\eta}{\eta/2} = 3^{\eta/2} \frac{(\eta/2)!^2}{i!(\eta-i)!}$$

for $0 \le i \le \eta$, provided that n is sufficiently large. Thus, using Stirling's approximation, $|H_i|/|H_{\eta/2}| = o(0.999^n)$ whenever $i < \eta/31$ or $i > 30\eta/31$. Hence, almost all Latin squares L satisfy $n/63 \le r \le 62n/63$, and similarly, $n/63 \le c \le 62n/63$, by considering the transpose of L. □

THEOREM 2.5. *If* n *is odd and sufficiently large, then* $R^{\pi}_n / R^{\pi'}_n < 4000$ *for any two parities* π *and* π' *satisfying (2.1).*

Proof. As shown in [17], almost all Latin squares L have $|\operatorname{Atp}(L)| = 1$. Combined with Lemma 2.4 and Theorem 2.1, we find that almost all Latin squares L satisfy $n!n/63^2 \le I(L,\pi) \le n!n(62/63)^2$, provided that π satisfies (2.1) and that n is odd. The result follows since $62^2 = 3844 < 4000$. □

We will now show that [2, Conjecture 6.1] implies Conjecture 2.2 for odd n. A *derangement* is a permutation without fixed points. Let $X = (x_{ij})$ denote a Latin square chosen uniformly at random from the L_n Latin squares of order n. We can define a derangement ξ of $\mathbb{Z}_n$ by $x_{0j} \mapsto x_{1j}$. It was conjectured in [2] that ξ is distributed asymptotically uniformly among derangements of $\mathbb{Z}_n$. In particular (see, e.g., [9]), ξ would be even (or odd) with probability approaching $1/2$. Now $\epsilon(\sigma_1^{\mathrm{row}}(X)) = \epsilon(\sigma_0^{\mathrm{row}}(X))\epsilon(\xi)$, so it would follow that $\epsilon(\sigma_0^{\mathrm{row}}(X)) = \epsilon(\sigma_1^{\mathrm{row}}(X))$ with probability approaching $1/2$. The same would hold for any other pair of rows and also for any pair of columns. That can only be true if almost all Latin squares have $|r - n/2| \leq o(n)$ and $|c - n/2| \leq o(n)$. Together with the argument used to prove Theorem 2.5, it would follow that $R_n^\pi \sim R_n^{\pi'}$ and $L_n^\pi \sim L_n^{\pi'}$ for odd n. That is, the conjecture in [2] implies Conjecture 2.2 for odd n.

For even n, (1.5) implies that $L_n^\pi = n!(n-1)!R_n^\pi$ for all parities π. Hence, with n restricted to being even, if π and π' are two parities that satisfy (2.1), then $R_n^\pi \sim R_n^{\pi'}$ if and only if $L_n^\pi \sim L_n^{\pi'}$.

§3. Congruences

The aim of this section is to find congruences satisfied by R_n^{E} and R_n^{O} in order to respond to Drisko's comments in [4] as quoted in Section 1. We begin by specializing the proof template in [23] to be applicable to Latin squares of a given sign. Let $\mathcal{C}$ be the set of all reduced Latin squares of order n. Consider a group G of isotopisms that acts on $\mathcal{C}$. Suppose that G acts on a set $\mathcal{A}$ where $\{L \in \mathcal{C} : |\operatorname{Atp}(L) \cap G| > 1\} \subseteq \mathcal{A} \subseteq \mathcal{C}$. Unless otherwise specified, we will assume that $\mathcal{A} = \{L \in \mathcal{C} : |\operatorname{Atp}(L) \cap G| > 1\}$.

We will require the extra condition that G is *sign-preserving* on $\mathcal{C}$; that is, $\epsilon(\theta(L)) = \epsilon(L)$ for all $\theta \in G$ and $L \in \mathcal{C}$. For $x \in \{+1, -1\}$, we define $\mathcal{C}_x = \{L \in \mathcal{C} : \epsilon(L) = x\}$ and $\mathcal{A}_x = \{L \in \mathcal{A} : \epsilon(L) = x\}$. If G is sign-preserving on $\mathcal{C}$, then G acts separately on $\mathcal{C}_{+1}$ and $\mathcal{C}_{-1}$. Similarly, since $\mathcal{A}$ is closed under the action of G, if G is sign-preserving on $\mathcal{C}$, then G acts separately on $\mathcal{A}_{+1}$ and $\mathcal{A}_{-1}$. It follows that $|\mathcal{C}_x| \equiv |\mathcal{A}_x| \pmod{|G|}$ for $x \in \{+1, -1\}$. This proves the following lemma.

LEMMA 3.1. *We have* $R_n^{\mathrm{E}} \equiv |\mathcal{A}_{+1}| \pmod{|G|}$ *and* $R_n^{\mathrm{O}} \equiv |\mathcal{A}_{-1}| \pmod{|G|}$.

To ensure that G is sign-preserving and acts on $\mathcal{C}$, we choose G to consist only of isomorphisms and insist that each $(\alpha, \alpha, \alpha) \in G$ has $\alpha(0) = 0$. In fact, with this restriction, G preserves parity and sign, by (1.4).

We illustrate the use of our proof template with the following result.

THEOREM 3.2. *Both R_n^{E} and R_n^{O} are divisible by $(\lceil n/2\rceil - 1)!$ for all n. Moreover, R_n^{π} is divisible by $(\lceil n/2\rceil - 1)!$ for all parities π.*

Proof. This proof uses the setup for Lemma 3.1. Let G be the group of isomorphisms (α, α, α) such that α fixes each of the points $0, 1, \ldots, \lfloor n/2\rfloor$. If $\theta = (\alpha, \alpha, \alpha) \in G$ is a nontrivial automorphism of some $L \in \mathcal{C}$, then the rows and columns of L whose indices are fixed by α form a subsquare M of order at least $\lfloor n/2\rfloor + 1$, by Lemma 1.10. Lemma 1.9 therefore implies that $M = L$, but this contradicts that θ is nontrivial. Hence, $\mathcal{A} = \{L \in \mathcal{C} : |\operatorname{Atp}(L) \cap G| > 1\} = \emptyset$, so $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}| = 0$. The result now follows from Lemma 3.1.

Since isomorphisms preserve parity, the same argument implies the second claim of the theorem. □

Theorem 3.2 identifies that R_n^{E} and R_n^{O}, despite being conjectured to be different for all n, share a superexponential divisor as $n \to \infty$. Theorem 3.2 also implies that $(\lceil n/2\rceil - 1)!$ divides R_n, but this is no better than the following theorem in [17].

THEOREM 3.3 ([17, Theorem 4.1]). *Let $m = \lfloor n/2\rfloor$. Then $m!$ divides R_n. Moreover, if n is odd, then $\gcd(m!(m-1)!R_m, (m+1)!)$ divides R_n.*

In fact, the proof of Theorem 3.2 is a modified version of the proof of Theorem 3.3. The following theorem also incidentally gives a divisor for R_n, which sometimes improves on Theorem 3.3 (see [21] for more about R_n).

THEOREM 3.4. *Let n and c be positive integers, and let p be a prime such that $n/2 > (c-1)p$ and $n \geq cp + 3$. Then*

(i) $\gcd(p^c, (n-cp-1)!^2 R_{n-cp})$ *divides* R_n^{E} *and* R_n^{O} *if cp is odd;*
(ii) $\gcd(p^c, (n-cp-1)!^2 R_{n-cp}^{\mathrm{E}}, (n-cp-1)!^2 R_{n-cp}^{\mathrm{O}})$ *divides* R_n^{E} *and* R_n^{O}*;*
(iii) $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod{p^c}$ *if cp is odd.*

Proof. This proof uses the setup for Lemma 3.1. Define α_t to be the p-cycle $(1+pt, 2+pt, \ldots, p+pt)$. Let G be the group of isomorphisms generated by $\{(\alpha_t, \alpha_t, \alpha_t) : 0 \leq t \leq c-1\}$, so $|G| = p^c$.

Consider the structure of any $L \in \mathcal{C}$ that admits a nontrivial automorphism $\theta \in G$. By Lemma 1.10, the rows and columns whose indices are fixed by θ form a subsquare M of order at least $n - cp$. Furthermore, the structure of G implies that the order of M is congruent to $n \pmod p$. Lemma 1.9 implies that the order of M is no more than $n/2 = n - n/2 < n - (c-1)p$, by assumption. Hence, the order of M must be exactly $n - cp$,

and therefore, M must be formed by the rows and columns whose indices are $0, cp+1, cp+2, \ldots, n-1$. For any $L \in \mathcal{C}$, let X be the submatrix formed by the rows and columns whose indices are $0, cp+1, cp+2, \ldots, n-1$. Let $\mathcal{A} = \{L \in \mathcal{C} : X \text{ is a subsquare of } L\}$.

We partition $\mathcal{A}$ into equivalence classes in the following way. Two Latin squares L and L' in $\mathcal{A}$ are equivalent if $\epsilon(L) = \epsilon(L')$ and L' can be constructed from L by the following steps.

(a) Replace the subsquare X by any of the R_{n-cp} reduced Latin squares on the same symbol set.
(b) Apply some permutation to the set of partial rows $\{(l_{i1}, l_{i2}, \ldots, l_{i(cp)}) : cp+1 \leq i \leq n-1\}$.
(c) Apply some permutation to the set of partial columns $\{(l_{1j}, l_{2j}, \ldots, l_{(cp)j}) : cp+1 \leq j \leq n-1\}$.

Different choices for steps (a)–(c) generate distinct Latin squares in $\mathcal{A}$. Since $n \geq cp+3$, the sets in (b) and (c) have cardinality at least 2.

To prove statement (i), suppose that cp is odd. We can choose arbitrarily from R_{n-cp} reduced Latin squares in step (a) and from $(n-cp-1)!$ permutations in step (b). After steps (a) and (b), to ensure that $\epsilon(L) = \epsilon(L')$, we see from Lemma 1.11 that we can only choose from $(1/2)(n-cp-1)!$ permutations in step (c). Hence, each equivalence class has cardinality $(1/2)(n-cp-1)!^2 R_{n-cp}$. The stated result follows, since p is odd.

The odd cp case of statement (ii) is true by statement (i). Now assume that cp is even. In step (a) we must replace X by a subsquare of sign $\epsilon(X)$, but the permutations in steps (b) and (c) may be chosen arbitrarily. Hence, each equivalence class has cardinality $(n-cp-1)!^2 R^{\mathrm{E}}_{n-cp}$ or $(n-cp-1)!^2 R^{\mathrm{O}}_{n-cp}$.

To prove statement (iii), equivalence on $\mathcal{A}$ is instead defined by switching the pair of partial rows

$$(l_{(cp+1)1}, l_{(cp+1)2}, \ldots, l_{(cp+1)(cp)}) \leftrightarrow (l_{(cp+2)1}, l_{(cp+2)2}, \ldots, l_{(cp+2)(cp)}),$$

which both exist since $n \geq cp+3$. Since cp is odd, this equivalence partitions $\mathcal{A}$ into pairs $\{L, L'\}$, in which $\epsilon(L) = -\epsilon(L')$. Hence, $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. □

Any divisor of both R^{E}_n and R^{O}_n is also a divisor of R_n. In some instances, Theorem 3.4 can imply a divisor for R_n that is not implied by Theorem 3.3. Specifically, for some primes p there are finitely many values of n for which we can now prove that p^c divides R_n using Theorem 3.4, whereas Theorem 3.3 proves only that p^{c-1} divides R_n. The first such examples are for

$p = 3$, where Theorem 3.4 implies that 3^2 divides R_{10} and 3^3 divides R_{15} and R_{16}, whereas Theorem 3.3 shows only that 3 divides R_{10} and 3^2 divides R_{15} and R_{16}. In any case, to possibly improve on earlier results, we require c in Theorem 3.4 to be as large as possible while satisfying $n/2 > (c-1)p$, and we need $\lfloor n/2 \rfloor < p^2$.

In Table 4 we tabulate the divisors for R_n, R_n^{E}, and R_n^{O} given by Theorems 3.2, 3.3, and 3.4, for $7 \le n \le 18$, making use of the data in Table 2. The shaded cells in Table 4 are when the divisor for R_n from Theorem 3.3 is improved upon. We will use Theorem 3.4(ii) to prove three instances of Theorem 3.6, which cannot be proved by the other theorems in this section; the required data are marked with an asterisk in Table 4.

THEOREM 3.5. *Let p be a prime, and let $n \ge p+2$. Then $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod p$.*

Proof. Table 2 and Theorem 3.2 imply that Theorem 3.5 is true when $p = 2$, so assume that p is an odd prime. Theorem 3.4(iii) handles $n \ge p+3$, so assume that $n = p+2$. The remainder of the proof is similar in spirit to that of Theorem 3.4 with $c = 1$. One difference is that we define $\mathcal{A} = \{L \in \mathcal{C} : (\alpha, \alpha, \alpha) \in \mathrm{Atp}(L)\}$, where $\alpha = (0)(1, 2, \ldots, p)(p+1)$. From $L \in \mathcal{A}$, we construct L' in the following way.

(a) Switch the partial columns $(l_{10}, l_{20}, \ldots, l_{p0}) \leftrightarrow (l_{1(p+1)}, l_{2(p+1)}, \ldots, l_{p(p+1)})$ to obtain the Latin square L^*.
(b) Apply the unique isotopism of the form $\theta = (\tau, \varepsilon, \varepsilon)$ so that $L' = \theta(L^*)$ is reduced.

We observe that $\tau = \alpha^a$ for some a since $(\alpha, \alpha, \alpha) \in \mathrm{Atp}(L)$ and α fixes 0 and $p+1$. Hence, $\epsilon(L^*) = \epsilon(\theta(L^*))$ since α is an even permutation. By Lemma 1.11, step (a) causes $\epsilon(L) = -\epsilon(L^*)$, and hence $\epsilon(L) = -\epsilon(L')$. Finally, observe that $L' \in \mathcal{A}$. Hence, we have partitioned $\mathcal{A}$ into pairs $\{L, L'\}$, where $\epsilon(L) = -\epsilon(L')$. It follows that $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. ∎

It is possible to prove versions of Theorem 3.4(iii) and Theorem 3.5 for R_n^{π} using Table 1 and Lemma 1.11, since isomorphisms preserve the parity of a Latin square. Specifically, $R_n^{000} \equiv R_n^{011} = R_n^{101} \equiv R_n^{110} \pmod{p^c}$ and $R_n^{111} \equiv R_n^{100} = R_n^{010} \equiv R_n^{001} \pmod{p^c}$ if p, c, and n satisfy the conditions of Theorem 3.4(iii) or if $c = 1$ and p and n satisfy the conditions of Theorem 3.5. We omit the full details.

We combine previous results to give the following theorem.

Table 4: Divisors of R_n, R_n^{E}, and R_n^{O}

n	*Theorem 3.3 ([17])* *divisor of* R_n	*Theorem 3.2* *divisor of* R_n, R_n^{E}, R_n^{O}	*Theorem 3.4(i)* *divisor of* R_n, R_n^{E}, R_n^{O}	*Theorem 3.4(ii)* *divisor of* R_n, R_n^{E}, R_n^{O}
7	$2^2 \cdot 3$	$2 \cdot 3$	3	$2^2 \cdot 3$
8	$2^3 \cdot 3$	$2 \cdot 3$	3	$2^2 \cdot 3$
9	$2^3 \cdot 3$	$2^3 \cdot 3$	3	$2^2 \cdot 3$
10	$2^3 \cdot 3 \cdot 5$	$2^3 \cdot 3$	3	$*2^3 \cdot 3^2$
11	$2^4 \cdot 3^2 \cdot 5$	$2^3 \cdot 3 \cdot 5$	$3 \cdot 5$	$*2^3 \cdot 3^2 \cdot 5$
12	$2^4 \cdot 3^2 \cdot 5$	$2^3 \cdot 3 \cdot 5$	$3 \cdot 5 \cdot 7$	$*2^3 \cdot 3^2 \cdot 5$
13	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5$	$3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5$
14	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5$	$3^2 \cdot 5$	$2^4 \cdot 3^2 \cdot 5$
15	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$3^3 \cdot 5 \cdot 7$	$2^4 \cdot 3^3 \cdot 5 \cdot 7$
16	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$3^3 \cdot 5 \cdot 7$	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7$
17	$2^7 \cdot 3^4 \cdot 5 \cdot 7$	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$3^3 \cdot 5 \cdot 7$	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7$
18	$2^7 \cdot 3^4 \cdot 5 \cdot 7$	$2^7 \cdot 3^2 \cdot 5 \cdot 7$	$3^3 \cdot 5 \cdot 7$	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7$

THEOREM 3.6. *If $2 \le t \le n-1$, then $R_n^{\mathrm{E}} \not\equiv R_n^{\mathrm{O}} \pmod t$ if and only if $t = n-1$ is prime.*

Proof. Our proof is based on the following three cases.

Case I: $t = n-1$ is prime. Table 2 lists $R_3^{\mathrm{E}} \not\equiv R_3^{\mathrm{O}} \pmod 2$. If t is an odd prime, then Theorem 1.4 and (1.5) imply that $R_n^{\mathrm{E}} \not\equiv R_n^{\mathrm{O}} \pmod t$.

Case II: t is a prime such that $t \le n-2$. This case is precisely Theorem 3.5.

Case III: t is composite. Theorem 3.2 implies that $R_n^{\mathrm{E}} \equiv 0 \equiv R_n^{\mathrm{O}} \pmod t$ except possibly if

$$(t,n) \in \big\{(4,5),(4,6),(4,7),(4,8),(9,10),(9,11),(9,12)\big\}.$$

The $t=4$ cases are resolved in Table 2. The $t=9$ cases are resolved in Table 4 (marked by an asterisk). ∎

Drisko [4] worked with L_{p+1}^{E} and L_{p+1}^{O} modulo p^3 for prime p. For comparison, we give the following result which is implied by Theorem 3.6, (1.5), and (1.7).

COROLLARY 3.7. *Let $t \le n$. Then $L_{n+1}^{\mathrm{E}} \not\equiv L_{n+1}^{\mathrm{O}} \pmod{t^3}$ if and only if $t = n$ is an odd prime.*

As for R_n^{E} and R_n^{O} modulo n, we give the following theorem.

THEOREM 3.8. *If n is composite, then $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod n$.*

Proof. Theorem 3.2 implies that $R_n^{\mathrm{E}} \equiv 0 \equiv R_n^{\mathrm{O}} \pmod n$ except possibly if $n \in \{8,9\} \cup \{2p : p \text{ is a prime}\}$. Table 2 shows that $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod n$ when $n \in \{4,8,9\}$. Now assume that $n = 2p$ for some odd prime p. Theorem 3.2 implies that 2 divides R_n^{E} and R_n^{O}, so it is sufficient to show that $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod p$. The rest of this proof uses the setup for Lemma 3.1. Let G be the group of isomorphisms generated by $\theta := (\alpha,\alpha,\alpha)$, where α is the p-cycle $(1,2,\dots,p)$.

Let $P = \{1,2,\dots,p\}$, and let $P^* = \mathbb{Z}_n \setminus P$. If $L = (l_{ij}) \in \mathcal{A}$, then Lemma 1.10 implies that the submatrix formed by the rows and columns whose indices are in P^* is a subsquare of L. We can therefore apply the partial column switch

$$(l_{1(p+1)}, l_{2(p+1)}, \dots, l_{p(p+1)}) \leftrightarrow (l_{1(p+2)}, l_{2(p+2)}, \dots, l_{p(p+2)})$$

to generate a distinct Latin square $L' \in \mathcal{A}$ for which $\epsilon(L) = -\epsilon(L')$, by Lemma 1.11. These partial columns exist since $n = 2p \ge p+3$. Hence $|\mathcal{A}_{+1}| = |\mathcal{A}_{-1}|$. ∎

Judging from the data in Table 2, it appears that the converse of Theorem 3.8 might also be true. Specifically, Table 2 here clearly implies that

$$\left(R_n^{\mathrm{E}} - R_n^{\mathrm{O}} \pmod n\right)_{1\le n\le 9} = (0,1,1,0,4,0,1,0,0).$$

Drisko [5] showed that $U_n^{\mathrm{E}} - U_n^{\mathrm{O}} \equiv (-1)^{(n-1)/2} \pmod n$ when n is an odd prime. However, it seems difficult to modify Drisko's proof to find $R_n^{\mathrm{E}} - R_n^{\mathrm{O}} \pmod n$ instead. The values of $U_n^{\mathrm{E}} - U_n^{\mathrm{O}}$ for $n \le 8$ were listed in [27], which we can verify and extend using the data in Table 3, since Table 1 implies that

$$(U_n^{\mathrm{E}}, U_n^{\mathrm{O}}) = \begin{cases} (R_n^{\mathrm{RE}}, R_n^{\mathrm{RO}}) & \text{if } n \equiv 0 \text{ or } 1 \pmod 4, \\ (R_n^{\mathrm{RO}}, R_n^{\mathrm{RE}}) & \text{if } n \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

A result of Glynn [8] implies that $R_n^{\mathrm{E}} \not\equiv R_n^{\mathrm{O}} \pmod{n+1}$ if $n+1$ is an odd prime.

§4. Another generalized Alon-Tarsi conjecture

In this section, we offer the following conjecture, which includes, as special cases, the Alon-Tarsi conjecture and its generalizations. For $n \ge 1$, define

$$\vec{r}_n = \begin{cases} (R_n^{000}, R_n^{011}, R_n^{101}, R_n^{110}) & \text{for } n \equiv 0 \text{ or } 1 \pmod 4, \\ (R_n^{111}, R_n^{100}, R_n^{010}, R_n^{001}) & \text{for } n \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Note that all four components of $\vec{r}$ are nonzero for $n \ge 5$ (see (2.2)).

CONJECTURE 4.1. *Let $\vec{a}$ be any $(-1,+1)$-vector of length 4. Then $\vec{a}\cdot\vec{r}_n \ne 0$ when $n \ge 1$.*

In Table 5 we note how Conjecture 4.1 generalizes the previous conjectures. We can check that Conjecture 4.1 is true for $n \le 9$ using the data in Table 2. The values of $|\vec{a}\cdot\vec{r}_n|$ obtained are listed in Table 6. Clearly, multiplying $\vec{a}$ by -1 does not affect whether $\vec{a}\cdot\vec{r}_n \ne 0$, so we can assume that the first entry of $\vec{a}$ is $+1$.

Table 5: Showing how various conjectures are special cases of Conjecture 4.1

Alon-Tarsi conjecture	$\vec{a} = (+1,-1,-1,+1)$	for even $n \ge 2$; uses (1.8)
Conjecture 1.5	$\vec{a} = (+1,+1,-1,-1)$	for even $n \ge 2$
Conjecture 1.6	$\vec{a} = (+1,-1,+1,-1)$	for all $n \ge 1$
Conjecture 1.7	$\vec{a} = (+1,-1,-1,+1)$	for all $n \ge 1$

Table 6: The set of possible values of $|\vec{a} \cdot \vec{r}_n|$ for $1 \leq n \leq 9$

n	*Possible values of* $\lvert\vec{a} \cdot \vec{r}_n\rvert$	*gcd of values*	*Factorization of gcd*
1	{1}	1	1
2	{1}	1	1
3	{1}	1	1
4	{4}	4	2^2
5	{8, 24, 40, 56}	8	2^3
6	{1248, 2304, 5856, 9408}	96	$2^5 \cdot 3$
7	{276480, 368640, 7964160, 8609280, 8701440, 16942080}	7680	$2^9 \cdot 3 \cdot 5$
8	{6210846720, 258324430848, 270746124288, 535281401856}	393216	$2^{17} \cdot 3$
9	{2086844497920, 31302667468800, 188781047303897088, 188785220992892928, 188814436815863808, 377597570964258816}	18874368	$2^{21} \cdot 3^2$

We list below some cases in which Conjecture 4.1 is true.

- If $\vec{a} = (+1, +1, +1, +1)$, then Conjecture 4.1 is trivially true.
- If $\vec{a} \in \{(+1, +1, -1, +1), (+1, -1, +1, +1)\}$, then Conjecture 4.1 is true since the second and third components of $\vec{r}_n$ are identical.
- If $\vec{a} = (+1, +1, +1, -1)$ and n is even, then Conjecture 4.1 is true since the second and fourth components of $\vec{r}_n$ are identical.
- Let $N = \{\text{even } n : \text{ there exists an odd prime } p \leq n-2 \text{ for which } R_n \not\equiv 0 \pmod{p}\}$. Suppose that $\vec{a}$ has three negative or three positive components. We claim that Conjecture 4.1 is true for $\vec{a}$ for all $n \in N$. We will illustrate how we came to this conclusion when $n \equiv 2 \pmod 4$; for $n \equiv 0 \pmod 4$ we can use the same proof with parities toggled: $111 \mapsto 000$, $100 \mapsto 011$, $010 \mapsto 101$, and $001 \mapsto 110$.

  Since n is even, we have the identity $R_n^{100} = R_n^{010} = R_n^{001}$. Theorem 3.5 implies that $R_n^{\mathrm{E}} \equiv R_n^{\mathrm{O}} \pmod p$, so

$$R_n^{111} - R_n^{100} \equiv 0 \pmod p. \tag{4.1}$$

  If Conjecture 4.1 is false for $\vec{a}$ and some $n \in N$, then either

$$-R_n^{111} + 3R_n^{100} \equiv 0 \pmod p \tag{4.2}$$

  or

$$R_n^{111} + R_n^{100} \equiv 0 \pmod p. \tag{4.3}$$

  Summing (4.1) and whichever of (4.2) or (4.3) is appropriate gives $R_n^{100} \equiv 0 \equiv R_n^{111} \pmod p$, since p is odd. Hence, $R_n^{\pi} \equiv 0 \pmod p$ for all π, implying that $R_n \equiv 0 \pmod p$, giving a contradiction. Note that $\{8, 10\} \cup \{14, 16, \ldots, 30\} \subseteq N$, as shown in [24].

Therefore, to prove Conjecture 4.1, it is sufficient to prove it only in the following cases.

- $\vec{a} = (+1, -1, -1, -1)$ for all $n \geq 11$ except $n \in \{14, 16, \ldots, 30\}$. For even n, we could instead prove that $n \in N$.
- $\vec{a} = (+1, +1, +1, -1)$ for odd $n \geq 11$.
- $\vec{a} = (+1, -1, +1, -1)$ for all composite $n \geq 15$ for which $n \pm 1$ are both also composite, that is, Conjecture 1.6 (a generalization of the Alon-Tarsi conjecture), excluding the cases proved in [4], [5], [8], and Table 2.
- $\vec{a} = (+1, -1, -1, +1)$ for all $n \geq 11$ for which $n \pm 1$ are both also composite, that is, Conjecture 1.7, excluding the cases proved in [4], [8], and Table 2.

If Conjecture 2.2 is true, then the first two of these cases would be true for sufficiently large n.

§5. Concluding remarks

This work is a significant blow to the hopes of proving more special cases of the Alon-Tarsi conjecture and its generalizations using a modified version of Drisko's methodology. For our subsequent discussion, note that a prime-power divisor p^a of x satisfies $R_n^{\mathrm{E}} \not\equiv R_n^{\mathrm{O}} \pmod{p^a}$ only if p divides $x/\gcd(R_n^{\mathrm{E}} - R_n^{\mathrm{O}}, x)$.

If we attempt to use a group of isomorphisms (whose order must divide $n!$), then we would require $a_n := n!/\gcd(R_n^{\mathrm{E}} - R_n^{\mathrm{O}}, n!)$ to have a prime divisor other than those already found. The values of a_n for $n \geq 1$ are $1, 2, 6, 6, 5, 5, 7, 7, 1, \ldots$. In particular, $a_9 = 1$, so this method would not work for $n = 9$, regardless of which group of isomorphisms we tried to use.

If we instead attempt to use a group of isotopisms (whose order must divide $n!^3$), then we will likely need to act on the set of all Latin squares (not just those that are reduced) and assume that n is even; otherwise, $L_n^{\mathrm{E}} = L_n^{\mathrm{O}}$. Now we would require $b_n := n!^3/\gcd(L_n^{\mathrm{E}} - L_n^{\mathrm{O}}, n!^3)$ to have a prime divisor other than those already found. Let $c_n = n!n/\gcd(R_n^{\mathrm{E}} - R_n^{\mathrm{O}}, n!n)$. For even n, (1.8) implies that $b_n = c_n$ (whereas $b_n = 1$ for odd $n \geq 3$). For $n \geq 1$, the sequence c_n is $1, 4, 18, 24, 25, 15, 49, 7, 1, \ldots$. Here also, $c_9 = 1$.

Finally, we remark that the Alon-Tarsi conjecture is quite peculiar—it asserts the inequality of two numbers L_n^{E} and L_n^{O} for even n, that are likely to be asymptotically equal, that are congruent modulo t for a variety of different t, and that are, in fact, equal for odd n.

References

[1] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica **12** (1992), 125–134.

[2] N. J. Cavenagh, C. Greenhill, and I. M. Wanless, *The cycle structure of two rows in a random Latin square*, Random Structures Algorithms **33** (2008), 286–309.

[3] T. Y. Chow, *On the Dinitz conjecture and related conjectures*, Discrete Math. **145** (1995), 73–82.

[4] A. A. Drisko, *On the number of even and odd Latin squares of order $p+1$*, Adv. Math. **128** (1997), 20–35.

[5] ———, *Proof of the Alon-Tarsi conjecture for $n = 2^r p$*, Electron. J. Combin. **5** (1998), no. R28.

[6] P. Erdős, A. L. Rubin, and H. Taylor, "Choosability in graphs" in *Proceedings of the West Coast Conference on Combinatorics, Graph Theory and Computing (Arcata, Calif., 1979)*, Congr. Numer. **26**, Utilitas Mathematica, Winnipeg, 1980, 125–157.

[7] F. Galvin, *The list chromatic index of a bipartite multigraph*, J. Combin. Theory Ser. B **63** (1995), 153–158.

[8] D. G. Glynn, *The conjectures of Alon-Tarsi and Rota in dimension prime minus one*, SIAM J. Discrete Math. **24** (2010), 394–399.

[9] L. Habsieger and J. C. M. Janssen, *The difference in even and odd Latin rectangles for small cases*, Ann. Sci. Math. Québec **19** (1995), 69–77.

[10] R. Häggkvist, "Towards a solution of the Dinitz problem?" in *Graph Theory and Combinatorics (Cambridge 1988)*, Discrete Math. **75**, Elsevier, Amsterdam, 1989, 247–251.

[11] R. Häggkvist and J. C. M. Janssen, *All-even Latin squares*, Discrete Math. **157** (1996), 199–206.

[12] R. Huang and G.-C. Rota, *On the relations of various conjectures on Latin squares and straightening coefficients*, Discrete Math. **128** (1994), 225–236.

[13] J. C. M. Janssen, *The Dinitz problem solved for rectangles*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), 243–249.

[14] ———, *On even and odd Latin squares*, J. Combin. Theory Ser. A **69** (1995), 173–181.

[15] A. Marini and G. Pirillo, *Signs on Latin squares*, Adv. in Appl. Math. **15** (1994), 490–505.

[16] ———, *Signs on group Latin squares*, Adv. in Appl. Math. **17** (1996), 117–121.

[17] B. D. McKay and I. M. Wanless, *On the number of Latin squares*, Ann. Comb. **9** (2005), 335–344.

[18] S. Onn, *A colorful determinantal identity, a conjecture of Rota, and Latin squares*, Amer. Math. Monthly **104** (1997), 156–159.

[19] A. Sade, *Autotopies des quasigroupes et des systèmes associatifs*, Arch. Math. (Brno) **4** (1968), 1–23.

[20] T. Slivnik, *Short proof of Galvin's theorem on the list-chromatic index of a bipartite multigraph*, Combin. Probab. Comput. **5** (1996), 91–94.

[21] D. S. Stones, *The many formulae for the number of Latin rectangles*, Electron. J. Combin. **17** (2010), no. A1.

[22] ———, *Formulae for the Alon-Tarsi conjecture*, preprint, to appear in SIAM J. Discrete Math.

[23] D. S. Stones and I. M. Wanless, *Divisors of the number of Latin rectangles*, J. Combin. Theory Ser. A **117** (2010), 204–215.

[24] ———, *A congruence connecting Latin rectangles and partial orthomorphisms*, preprint, to appear in Ann. Comb.

[25] I. M. Wanless, *Cycle switches in Latin squares*, Graphs Combin. **20** (2004), 545–570.

[26] P. Zappa, *Triplets of Latin squares*, Boll. Un. Mat. Ital. A (7) **10** (1996), 63–69.

[27] ———, *The Cayley determinant of the determinant tensor and the Alon-Tarsi conjecture*, Adv. in Appl. Math. **19** (1997), 31–44.

[28] D. Zeilberger, *The method of undetermined generalization and specialization*, Amer. Math. Monthly **103** (1996), 233–239.

[29] J. Zeng, *The generating function for the difference in even and odd three-line Latin rectangles*, Ann. Sci. Math. Québec **20** (1996), 105–108.

Douglas S. Stones
School of Mathematical Sciences and
Clayton School of Information Technology
Monash University
Victoria 3800
Australia
the_empty_element@yahoo.com

Ian M. Wanless
School of Mathematical Sciences
Monash University
Victoria 3800
Australia
ian.wanless@monash.edu