Divisors of the number of Latin rectangles[☆]

Douglas Stones[*], Ian M. Wanless

[a]*School of Mathematical Sciences, Monash University, VIC 3800 Australia*

Abstract

A $k \times n$ Latin rectangle on the symbols $\{1, 2, \ldots, n\}$ is called reduced if the first row is $(1, 2, \ldots, n)$ and the first column is $(1, 2, \ldots, k)^T$. Let $R_{k,n}$ be the number of reduced $k \times n$ Latin rectangles and $m = \lfloor n/2 \rfloor$. We prove several results giving divisors of $R_{k,n}$. For example, $(k-1)!$ divides $R_{k,n}$ when $k \leq m$ and $m!$ divides $R_{k,n}$ when $m < k \leq n$. We establish a recurrence which determines the congruence class of $R_{k,n} \pmod t$ for a range of different t. We use this to show that $R_{k,n} \equiv \left((-1)^{k-1}(k-1)!\right)^{n-1} \pmod n$. In particular, this means that if n is prime, then $R_{k,n} \equiv 1 \pmod n$ for $1 \leq k \leq n$ and if n is composite then $R_{k,n} \equiv 0 \pmod n$ if and only if k is larger than the greatest prime divisor of n.

Key words: Latin rectangles, Latin squares
2000 MSC: 05B15, 11B75

1. Introduction

For $1 \leq k \leq n$, a $k \times n$ *Latin rectangle* is a $k \times n$ array $L = (l_{ij})$ of n symbols such that each symbol occurs exactly once in each row and at most once in each column. We will usually take the symbol set to be $[n] = \{1, 2, \ldots, n\}$ to match the column indices, while the rows will be indexed by $[k]$. If $k = n$ then L is called a *Latin square*. A Latin rectangle on the symbols $[n]$ is called *normalised* if the first row is $(1, 2, \ldots, n)$, and *reduced* if the first row is $(1, 2, \ldots, n)$ and the first column is $(1, 2, \ldots, k)^T$. If the symbol set is not $[n]$, but does have a total order on it, then "reduced" and "normalised" can be defined analogously.

Let $\mathbb{N}$ denote the set of positive integers. In this paper, Latin rectangles will usually have dimensions $k \times n$ where $k, n \in \mathbb{N}$ and $k \leq n$. When n is known to be prime, p will be used instead. We will frequently use $m = \lfloor n/2 \rfloor$.

Let $L_{k,n}$ denote the number of $k \times n$ Latin rectangles, $K_{k,n}$ denote the number of normalised $k \times n$ Latin rectangles and $R_{k,n}$ denote the number of reduced $k \times n$ Latin rectangles, with the symbol set in each case understood to

[☆]Supported by ARC grant DP0662946.
[*]Corresponding author
Email addresses: douglas.stones@sci.monash.edu.au (Douglas Stones), ian.wanless@sci.monash.edu.au (Ian M. Wanless)

be $[n]$. In the case of Latin squares, the numbers $L_{n,n}$, $K_{n,n}$ and $R_{n,n}$ will be denoted L_n, K_n and R_n respectively. The three numbers $L_{k,n}$, $K_{k,n}$ and $R_{k,n}$ are related by

$$L_{k,n} = n!K_{k,n} = \frac{n!(n-1)!}{(n-k)!}R_{k,n}. \tag{1}$$

The enumeration of R_n has a history stretching back to Euler [11] and a good summary is provided by McKay, Meynert and Myrvold [26]. In some instances enumerations were performed incompletely or incorrectly. The congruences proved in this paper should provide a useful tool for identifying such mistakes in the future.

General formulae for L_n have been found by MacMahon [25] (a modern proof can be found in [37]), Jucys [20], Light Jr. [24], Nechvatal [30, 31], Gessel [15], Shao and Wei [36], Fu [13], Denés and Mullen [6] and in [28], however they are all impractical for enumeration purposes. McKay and Rogoyski [27] provided estimates for L_n for $11 \leq n \leq 15$, which for $n = 11$ was accurate to three significant figures.

Godsil and McKay [16] found the asymptotic value of $L_{k,n}$ as $n \to \infty$ with $k = o(n^{6/7})$. For a history of earlier asymptotic enumerations also see [16].

The number, D_n, of derangements (permutations without fixed points) of $[n]$ is related to the number of $2 \times n$ Latin rectangles by

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = K_{2,n} = (n-1)R_{2,n}. \tag{2}$$

The enumeration of $L_{3,n}$, the number of three-line Latin rectangles, has a long history. Recurrence formulae for $L_{3,n}$ were shown by Jacob [19] (which is invalid for $n \geq 8$), Kerewala [21] and Riordan [35]. Riordan [33, 34] established the link between three-line Latin rectangles and the famous *problème de ménages*. Dulmage [9] provided an explicit formula for $L_{3,n}$, which was later refined by Dulmage and McMaster [10]. Bogart and Longyear [4] provided a practical formula for $K_{3,n}$, which they used for $n \leq 11$ exactly (with typographical errors: $K_{3,7} = 1073760$, $K_{3,8} = 70299264$) and approximately for $n \leq 20$, accurate to 12 significant figures. Riordan [35] gave the credit to Yamamoto [38] for the equation

$$R_{3,n} = \sum_{i+j+k=n} n(n-3)!(-1)^j \frac{2^k i!}{k!} \binom{3i+j+2}{j}, \tag{3}$$

where i, j, k are non-negative integers. Gessel [14] provided a formula for $K_{3,n}$ based on the cycle decomposition of the permutations defined by the second and third rows of a normalised three-line Latin rectangle. Kerawala [22] and Yamamoto [39, 40] studied the asymptotic value of $L_{3,n}$. Goulden and Jackson [17] gave a generating function for $L_{3,n}$.

Riordan [35] gave the congruence $R_{3,n+p} \equiv 2R_{3,n} \pmod{p}$ for all odd primes p, which was generalised by Carlitz [5] to $R_{3,n+t} \equiv 2^t R_{3,n} \pmod{t}$ for all $t \in \mathbb{N}$.

In Corollary 6 we generalise these congruences to rectangles with arbitrarily many rows.

Light Jr. [23] and Athreya, Pranesachar and Singhi [2, 32] gave formulae for $L_{4,n}$, the number of four-line Latin rectangles. Gessel's [15] equation for general $L_{k,n}$ also provides a formula for $L_{4,n}$.

Drisko [7, 8] established congruences concerning the number of so-called even and odd Latin squares of order $n = p+1$ and $n = 2^r p$, where p is an odd prime, hence proving the Alon-Tarsi Conjecture for these cases.

Attention in this paper will be primarily upon $R_{k,n}$ since any divisibility property of $R_{k,n}$ transfers to $L_{k,n}$ and $K_{k,n}$ by (1). Relatively few results have been published regarding divisibility properties of $R_{k,n}$. After viewing a table of R_n up to $n = 9$, Alter [1] (see also [18, 29]) asked three interesting questions concerning the divisibility of R_n. These questions remained unanswered for thirty years until [28] proved a special case of Theorem 2 below. This answered the first of Alter's questions by showing that an increasing power of 2 does divide R_n, and the third question by showing that 3 divides R_n for all $n \geq 6$. In fact, they showed that for all $t \in \mathbb{N}$ the maximum power of t that divides R_n increases at least linearly with n. Alter's second question, which asks for the largest power of 2 dividing R_n, still remains open.

For any $k \times n$ Latin rectangle, L, an ordered triplet of permutations $\theta = (\alpha, \beta, \gamma)$ will denote a mapping of L such that the rows of L are permuted according to α, the columns of L are permuted according to β and the symbols of L are permuted according to γ. For convenience, we will assume α is a permutation of $[n]$ that fixes $[k]$ setwise. The mapping θ is called an *isotopism*. If $\alpha = \beta = \gamma$, then θ is said to be an *isomorphism*. Isomorphisms $\theta = (\alpha, \alpha, \alpha)$ such that $\alpha(1) = 1$ map reduced Latin squares to reduced Latin squares. By assuming that α fixes $[k]$ setwise and $\alpha(1) = 1$, we also ensure that θ maps reduced $k \times n$ Latin rectangles to reduced $k \times n$ Latin rectangles. The identity permutation will be denoted ε.

Let L_1 and L_2 be Latin rectangles. If there exists an isotopism, θ, such that $\theta(L_1) = L_2$ then L_1 and L_2 are said to be *isotopic*. The set of all Latin rectangles isotopic to L is called the *isotopy class* of L. If $\theta(L) = L$, then θ is said to be an *autotopism* of L. Any autotopism other than $(\varepsilon, \varepsilon, \varepsilon)$ is *non-trivial*. If θ is an isomorphism and an autotopism of L then θ is said to be an *automorphism* of L.

If a submatrix, M, of L is also a Latin rectangle then M is called a *sub-rectangle* of L, and if M is a Latin square then M is called a *subsquare* of L.

Lemma 1. *Let $L = (l_{ij})$ be a Latin rectangle and let θ be an autotopism of L. If any two of row i, column j or symbol l_{ij} are fixed by θ, then so is the other.*

Lemma 1 is simple to prove and is used, for example, by McKay, Meynert and Myrvold [26].

2. Proof Template

Many of the proofs in this paper follow the same basic strategy. We have some set of Latin rectangles $\mathcal{C}$ and wish to calculate $|\mathcal{C}| \pmod{\mu}$ for some integer μ. Typically, $\mathcal{C}$ will be the set of reduced $k \times n$ Latin rectangles and we will often use L to denote an arbitrary Latin rectangle in $\mathcal{C}$. We choose a group of isotopisms G that acts on $\mathcal{C}$ such that μ divides $|G|$. For each $L \in \mathcal{C}$, let $G(L)$ denote the orbit of L under G, namely $G(L) = \{\theta(L) : \theta \in G\}$.

If there exist distinct $\theta_1, \theta_2 \in G$ such that $\theta_1(L) = \theta_2(L)$ then $\theta_2^{-1} \circ \theta_1 \in G$ is a non-trivial autotopism of L. Therefore if L does not admit a non-trivial autotopism in G then $|G(L)| = |G| \equiv 0 \pmod{\mu}$. Hence any $L \in \mathcal{C}$ such that $|G(L)| \not\equiv 0 \pmod{\mu}$ must admit a non-trivial autotopism in G.

We identify a subset $\mathcal{A} \subseteq \mathcal{C}$ such that:

- $\mathcal{A}$ contains every $L \in \mathcal{C}$ that admits a non-trivial autotopism in G.
- $\mathcal{A}$ is closed under the action of G.
- Members of $\mathcal{A}$ are characterised by some special structure, usually a subrectangle in a particular position.

With $\mathcal{A}$ satisfying these conditions, μ divides $|\mathcal{C} \setminus \mathcal{A}|$ and hence $|\mathcal{C}| \equiv |\mathcal{A}| \pmod{\mu}$ and $\gcd\big(\mu, |\mathcal{A}|\big)$ divides $|\mathcal{C}|$. We then either calculate $|\mathcal{A}|$ explicitly, evaluate $|\mathcal{A}| \pmod{\mu}$ or find some divisor of $|\mathcal{A}|$. We typically do this by defining an equivalence relation on $\mathcal{A}$ which utilises the special structure possessed by the elements of $\mathcal{A}$.

3. Factorial Divisors

In this section we prove that certain factorials divide $R_{k,n}$. Recall that $m = \lfloor n/2 \rfloor$.

Theorem 1. $\gcd\big(k!, (k-1)!R_{k,n-k}R_k\big)$ *divides* $R_{k,n}$ *when* $k \leq m$.

Proof. This proof follows the template in Section 2. Let G be the group of isotopisms of the form $\theta = (\varepsilon, \beta, \beta)$ such that β fixes $[n-k]$ pointwise. Let $\mathcal{C}$ be the set of reduced $k \times n$ Latin rectangles and $\mu = |G| = k!$. For arbitrary $L \in \mathcal{C}$ let $A = A(L)$ denote the square submatrix formed by the last k columns of L.

Suppose that L admits a non-trivial autotopism $\theta = (\varepsilon, \beta, \beta) \in G$. Let F denote the fixed points of β and $F^* = [n] \setminus F$ denote its complement. Since θ is non-trivial there exists $j \in F^*$. By Lemma 1, $l_{ij} \in F^*$ for all $1 \leq i \leq k$. Hence $|F^*| = k$ and so $F^* = [n] \setminus [n-k]$. By Lemma 1, A consists only of symbols in F^*, which implies that A is a subsquare of L.

Let $\mathcal{A} = \{L \in \mathcal{C} : A \text{ is a subsquare of } L\}$. Note that $\mathcal{A}$ is closed under the action of G and so $\gcd(k!, |\mathcal{A}|)$ divides $|\mathcal{C}| = R_{k,n}$. By construction, $|\mathcal{A}| = R_{k,n-k}K_k = (k-1)!R_{k,n-k}R_k$, by (1). □

Corollary 7 gives the values of $k \in \mathbb{N}$ such that k divides R_k and it will follow that $k!$ divides $R_{k,n}$ for all composite $k \leq m$. For prime k, the largest divisor proved by Theorem 1 will be $(k-1)!$ unless k divides $R_{k,n-k}$, as it does, for example, when $n = 12$, $k = 5$. Theorem 1 is extended in Theorem 3 for the special case $n \geq 3k$.

Theorem 1 provides a divisor for the number of "thin" Latin rectangles, when $k \leq m$, while the next theorem provides a divisor for the number of "fat" Latin rectangles, when $m < k \leq n$. Theorem 2 extends, to Latin rectangles, the techniques used in [28] to provide a factorial divisor for the number of Latin squares.

Theorem 2. *When $m < k \leq n$, $R_{k,n}$ is divisible by $m!$. If n is odd, $m+1 < k \leq n$, and $m+1$ is composite, then $(m+1)!$ divides $R_{k,n}$.*

Proof. This proof follows the template in Section 2. Let G be the group of isomorphisms $\theta = (\alpha, \alpha, \alpha)$ such that α fixes $\{1, 2, \ldots, k-r\} \cup \{k+1, k+2, \ldots, n\}$ pointwise, for some $1 \leq r < k$ to be specified later. Let $\mathcal{C}$ be the set of reduced $k \times n$ Latin rectangles and $\mu = |G| = r!$.

Suppose that $L = (l_{ij}) \in \mathcal{C}$ admits a non-trivial automorphism $\theta = (\alpha, \alpha, \alpha) \in G$. Let F denote the fixed points of α and let $F^* = [n] \setminus F$ denote its complement. Since θ is non-trivial there exists $i \in F^*$ such that $i \leq k$. If $j \in F$ then $l_{ij} \in F^*$, by Lemma 1. Hence

$$n - r \leq |F| \leq |F^*| \leq r. \tag{4}$$

We now consider two choices for r.

Case I: $r = m$.

This case requires $k > m$. If n is odd we contradict (4), so it is sufficient to choose $\mathcal{A} = \emptyset$ in order to deduce that $m!$ divides $|\mathcal{C}|$.

Now consider even $n = 2m$. To satisfy (4), we must have $F = \{1, 2, \ldots, k - r\} \cup \{k+1, k+2, \ldots, n\}$ and $F^* = \{k - r + 1, k - r + 2, \ldots, k\}$. Furthermore the $m \times m$ submatrix A, formed by the rows and columns indexed by F^*, is a subsquare of L. We let $\mathcal{A} = \{L \in \mathcal{C} : A \text{ is a subsquare of } L\}$, which is closed under the action of G.

We define the Latin rectangles equivalent to $L \in \mathcal{A}$ to be those formed by replacing A by one of the L_m Latin squares on the same symbols. Since $m!$ divides L_m by (1), $m!$ also divides $|\mathcal{A}|$ and hence $m!$ divides $|\mathcal{C}| = R_{k,n}$.

Case II: Odd $n = 2m + 1$ and $r = m + 1$.

This case requires $k > m + 1$. By (4) and since $|F| + |F^*| = n$, we must have $|F^*| = m+1$ and $|F| = m$. Let A denote the $(m+1) \times (m+1)$ submatrix of L formed by the rows and columns indexed by F^*, and let B denote the $(m+1) \times m$ submatrix formed by the remainder of the cells in those rows.

The submatrix B contains only symbols in F^* and therefore A contains one symbol from F^* in each row. Furthermore A contains one symbol from F^* in each column, otherwise there exists a column of A without a symbol from F^* and therefore it contains $m+1$ symbols in F, contradicting $|F| = m$. Let $\mathcal{A} \subseteq \mathcal{C}$

be the set of Latin rectangles with submatrices A and B of this description. Note that $\mathcal{A}$ is closed under the action of G.

We define two Latin rectangles, $L_1, L_2 \in \mathcal{A}$, to be equivalent if:

- The first $k-r$ rows are identical in L_1 and L_2 and
- For each column c the set of symbols which occur in c is the same for L_1 and L_2.

We will now enumerate the rectangles equivalent to any given $L \in \mathcal{A}$. Let D denote the set of entries of A with symbols in F^*. We can replace A by one of K_{m+1} different Latin square of order $m+1$ on the symbols $\{0\} \cup F$ such that the 0 entries occur in the positions in D. We then replace the 0 entries with D.

Irrespective of the previous replacements, we now can replace B by the transpose of one of the $K_{m,m+1} = K_{m+1}$ normalised $m \times (m+1)$ Latin rectangles on the same symbols. Then we replace the symbols in D appropriately so that the set of symbols in each row is $[n]$, which is a unique replacement. Then we permute the columns of A so that the set of symbols in each column is the same as in L, for which there is a unique permutation.

Therefore L is equivalent to K_{m+1}^2 Latin rectangles. Hence K_{m+1}^2 divides $|\mathcal{A}|$ and so $\gcd(\mu, K_{m+1}^2)$ divides $|\mathcal{C}| = R_{k,n}$. Therefore by (1), $\gcd\left((m+1)!, m!^2\right)$ divides $R_{k,n}$. Note that $m!$ is divisible by $m+1$ unless $m+1$ is prime or $m+1=4$. In the latter case $n = 2m+1 = 7$ and Figure 1 says that $R_{5,7}$ and $R_{6,7} = R_{7,7}$ are divisible by 4!. □

In Figure 1 we compare the results of Theorems 1 and 2 with the greatest factorial divisors of $R_{k,n}$ from the known data [28]. Let $\psi = \psi(k,n)$ denote the largest integer such that $\psi!$ divides $R_{k,n}$. Theorems 1 (dark) and 2 (light) provide a lower bound on ψ. This bound is the actual value of ψ, except for the entries marked with an asterisk, where Theorem 2 only proves that $(\psi-1)!$ divides $R_{k,n}$. We omit $R_{1,n} = 1$ and $R_{n,n} = R_{n,n-1}$.

In [28] it is also shown that 7! divides R_{13}, which is the first case when $n = 2m+1$ such that $m+1$ is prime and $(m+1)!$ divides R_n. Judging from the results in Figure 1, it would not be surprising if 9! divides R_{13}, in which case Theorem 2 is well short of best possible. For $1 \le n \le 11$, Theorem 1 gives the best possible factorial divisor for "thin" Latin rectangles while, for "fat" Latin rectangles, Theorem 2 is slightly deficient in some cases.

Corollary 1. *If n is composite and $k > m$ then n divides $R_{k,n}$.*

Proof. Since n is composite, $n = \lambda q$ for some prime $q \le m$ and $2 \le \lambda \le m$. By Theorem 2, $m!$ divides $R_{k,n}$ and therefore $R_{k,n} \equiv 0 \pmod{n}$ except possibly when $\lambda = q$ and $m < 2q$. But $m = \lfloor q^2/2 \rfloor < 2q$ only if $q = 2$ or 3, that is when $n = 4$ or 9, and these cases are resolved by Figure 1. □

A complete determination of when n divides $R_{k,n}$ is given in Corollary 8, and $R_{k,n} \pmod{n}$ is given for all k and n in Theorem 8.

Corollary 2. *If k is composite then k divides $R_{k,n}$.*

n,k	$R_{k,n}$	ψ
$3,2$	1	1
$4,2$	3	1
3	2^2	2
$5,2$	11	1
3	$2{\cdot}23$	2
4	$2^3{\cdot}7$	2
$6,2$	53	1
3	$2^3{\cdot}7{\cdot}19$	2
4	$2^3{\cdot}3^2{\cdot}7{\cdot}13$	4^*
5	$2^6{\cdot}3{\cdot}7^2$	4^*
$7,2$	$3{\cdot}103$	1
3	$2^4{\cdot}2237$	2
4	$2^5{\cdot}3{\cdot}19{\cdot}709$	4^*
5	$2^8{\cdot}3{\cdot}5^2{\cdot}587$	5^*
6	$2^{10}{\cdot}3{\cdot}5{\cdot}1103$	5^*
$8,2$	$13{\cdot}163$	1
3	$2^6{\cdot}26153$	2
4	$2^6{\cdot}3{\cdot}159{\cdot}14713$	4
5	$2^{11}{\cdot}3{\cdot}23{\cdot}192529$	4
6	$2^{11}{\cdot}3{\cdot}7{\cdot}173{\cdot}45077$	4
7	$2^{17}{\cdot}3{\cdot}1361291$	4

n,k	$R_{k,n}$	ψ
$9,2$	$11{\cdot}37{\cdot}41$	1
3	$2^5{\cdot}13{\cdot}167{\cdot}1489$	2
4	$2^7{\cdot}3^4{\cdot}20025517$	4
5	$2^{11}{\cdot}3^4{\cdot}13{\cdot}52251029$	4
6	$2^{14}{\cdot}3^5{\cdot}3253351007$	4
7	$2^{15}{\cdot}3^2{\cdot}61{\cdot}12923{\cdot}965171$	4
8	$2^{21}{\cdot}3^2{\cdot}5231{\cdot}3824477$	4
$10,2$	$3^2{\cdot}16481$	1
3	$2^6{\cdot}23{\cdot}61{\cdot}90821$	2
4	$2^8{\cdot}3^3{\cdot}71{\cdot}271{\cdot}1106627$	4
5	$2^{16}{\cdot}3^6{\cdot}19{\cdot}97{\cdot}8483617$	4
6	$2^{14}{\cdot}3^3{\cdot}5{\cdot}26053{\cdot}15110358097$	6^*
7	$2^{20}{\cdot}3^3{\cdot}5{\cdot}509{\cdot}2458531126109$	6^*
8	$2^{21}{\cdot}3^3{\cdot}5{\cdot}11{\cdot}13^2{\cdot}37{\cdot}1381{\cdot}159597187$	6^*
9	$2^{28}{\cdot}3^2{\cdot}5{\cdot}31{\cdot}37{\cdot}1468457{\cdot}547135293937$	6^*
$11,2$	1468457	1
3	$2^7{\cdot}13{\cdot}23{\cdot}20851549$	2
4	$2^{10}{\cdot}3^2{\cdot}1823{\cdot}8569184461$	4
5	$2^{13}{\cdot}3^2{\cdot}29{\cdot}168293{\cdot}20936295857$	4
6	$2^{17}{\cdot}3^2{\cdot}5{\cdot}31{\cdot}2334139{\cdot}225638611943$	6^*
7	$2^{21}{\cdot}3^2{\cdot}5{\cdot}9437{\cdot}269623520098467133$	6
8	$2^{28}{\cdot}3^2{\cdot}5{\cdot}97{\cdot}73488673152815765447$	6
9	$2^{32}{\cdot}3^3{\cdot}5{\cdot}61{\cdot}7487{\cdot}260951{\cdot}42053669617$	6
10	$2^{35}{\cdot}3^4{\cdot}5{\cdot}2801{\cdot}2206499{\cdot}62368028479$	6

Figure 1: Prime factorisation of $R_{k,n}$ for $2 \le k < n \le 11$ and the largest integer ψ such that $\psi!$ divides $R_{k,n}$.

Proof. When $k \leq m$, Theorem 1 implies that $\gcd(k!, (k-1)!R_k)$ divides $R_{k,n}$. When $k = 4$, $R_4 = 4$ divides $R_{4,n}$ and when $k > 4$, k divides $(k-1)!$, since k is composite.

When $m < k \leq n$, Theorem 2 implies that k divides $R_{k,n}$, except possibly when $k = p^2$ for some prime p such that $m < 2p$. But then $2p > m = \lfloor n/2 \rfloor \geq \lfloor p^2/2 \rfloor$, which can only be satisfied in the following cases, that are resolved by Figure 1: when $k = p^2 = 4$ and $n \in \{4, 5, 6, 7\}$ and when $k = p^2 = 9$ and $n \in \{9, 10, 11\}$. □

The converse of Corollary 2 is false. For example, $R_{5,7} = 11270400 \equiv 0 \pmod 5$. The following theorem extends Theorem 1 in the special case $n \geq 3k$.

Theorem 3. *Suppose $k, n \in \mathbb{N}$ where $n \geq 2k + r$ for some $k \leq r < 2k$. Then $(k-1)!\,P$ divides $R_{k,n}$ where P denotes the product of all composite numbers c such that $k \leq c \leq r$.*

Proof. This proof follows the template in Section 2. Let G be the group of isotopisms of the form $\theta = (\varepsilon, \beta, \beta)$ such that β fixes $[n-r]$ pointwise. Let $\mathcal{C}$ be the set of reduced $k \times n$ Latin rectangles and $\mu = (k-1)!\,P$.

Suppose that $L \in \mathcal{C}$ admits a non-trivial autotopism $\theta = (\varepsilon, \beta, \beta) \in G$. Let A denote the submatrix formed by the last r columns of L. By Lemma 1, the columns of L that are not fixed by θ form a $k \times i$ subrectangle of L in A for some $k \leq i \leq r$.

For all $k \leq i \leq r$, let $\mathcal{A}_i = \{L \in \mathcal{C} : A \text{ contains a } k \times i \text{ subrectangle of } L\}$ and let $\mathcal{A} = \cup_i \mathcal{A}_i$. Note that each $\mathcal{A}_i$ is closed under the action of G and so $|\mathcal{C}| \equiv |\mathcal{A}| \pmod \mu$. Since $r < 2k$ the $\mathcal{A}_i$ are disjoint and so $|\mathcal{A}| = \sum_{k \leq i \leq r} |\mathcal{A}_i|$.

By construction

$$|\mathcal{A}_i| = \binom{r}{i} K_{k,i} R_{k,n-i} = \frac{r!}{i(r-i)!(i-k)!} R_{k,i} R_{k,n-i},$$

by (1).

Since $n \geq 2k + r \geq 2k + i$ for all $k \leq i \leq r$, we get that $k \leq \lfloor (n-i)/2 \rfloor$. Therefore by Theorem 1, $(k-1)!$ divides $R_{k,n-i}$ and we know that $(r-i)!(i-k)!$ divides $(r-k)!$ which divides $(k-1)!$ since $r < 2k$.

If i is a prime then μ divides $r!/i$, since $k \leq i \leq r$, and so μ divides $|\mathcal{A}_i|$. If i is composite, i divides $R_{k,i}$ by Corollary 1 since $i \leq r < 2k$ and therefore $r!$ divides $|\mathcal{A}_i|$.

Hence μ divides $|\mathcal{A}_i|$ for all $k \leq i \leq r$ and so $R_{k,n} = |\mathcal{C}| \equiv |\mathcal{A}| = \sum_{k \leq i \leq r} |\mathcal{A}_i| \equiv 0 \pmod \mu$. □

4. Recurrence congruences

In this section we establish congruences for $R_{k,n}$ and $K_{k,n}$ modulo t for a range of $t \in \mathbb{N}$. With the results presented in this section, we use the convention that $R_{k,n} = K_{k,n} = 0$ whenever $n < k$. We will also use the following notation throughout this section. Let $n = b_0 + b_1 + \cdots + b_s$ be a partition of the integer

n where $s \geq 1$. Let $t = \prod_{1 \leq i \leq s} b_i$ and $t' = b_0 t$. For any $I \subseteq \{0, 1, \ldots, s\}$, let $\|I\|$ denote $\sum_{i \in I} b_i$. Let Q be the set of partitions of the set $\{0, 1, \ldots s\}$ into at least two parts. For $U \in Q$, define $u_0 = u_0(U)$ to be the part of U containing 0. For any integer $r \geq 2$, let $\mathrm{gpd}(r)$ denote the greatest prime divisor of r.

Theorem 4. *If $b_0 \geq k$ then*

$$R_{k,n} \equiv \sum_{U \in Q} (-1)^{|U|} (|U| - 1)! R_{k,\|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k,\|u\|} \pmod{t}. \tag{5}$$

Proof. This proof follows the template in Section 2. Let $\mathcal{C}$ be the set of reduced $k \times n$ Latin rectangles.

Let $b_0^* = 0$ and for $1 \leq i \leq s$, let $b_i^* = b_{i-1}^* + b_{i-1}$. Let M_i be the submatrix consisting of the b_i columns $b_i^* + 1, b_i^* + 2, \ldots, b_i^* + b_i$.

Suppose $U \in Q$. If, for each $u \in U$, the submatrix $\cup_{j \in u} M_j$ is a subrectangle of L, then we say L is *U-decomposable* and that U is a *decomposition* of L. For all $U, V \in Q$ we write $V \lhd U$ and $U \rhd V$ whenever V is a refinement of U and $V \neq U$. Call U an *irreducible* decomposition of L if there does not exist $V \lhd U$ such that L is V-decomposable. For all $U \in Q$, let $\mathcal{A}_U = \{L \in \mathcal{C} : U \text{ is an irreducible decomposition of } L\}$. Let $\mathcal{A} = \cup_{U \in Q} \mathcal{A}_U$.

Define the b_i-cycle $\beta_i = \left(b_i^* + 1 \;\; b_i^* + 2 \;\; \cdots \;\; b_i^* + b_i\right)$. Let G be the group of order t generated by the isotopisms $(\varepsilon, \beta_i, \beta_i)$ for $1 \leq i \leq s$. Since $k \leq b_0$, G acts on $\mathcal{C}$. Suppose $L \in \mathcal{C}$ admits a non-trivial autotopism $\theta \in G$. Lemma 1 implies that the columns fixed by θ form a subrectangle of L and hence $L \in \mathcal{A}$. Note that $\mathcal{A}_U$ is closed under the action of G for all $U \in Q$ and hence $R_{k,n} = |\mathcal{C}| \equiv |\mathcal{A}| \pmod{t}$.

The key observation is that every $L \in \mathcal{A}$ admits exactly one irreducible decomposition. Therefore $\{\mathcal{A}_U\}_{U \in Q}$ partitions $\mathcal{A}$ and so $|\mathcal{A}| = \sum_{U \in Q} |\mathcal{A}_U|$, giving

$$R_{k,n} \equiv \sum_{U \in Q} |\mathcal{A}_U| \pmod{t}. \tag{6}$$

In order to count $|\mathcal{A}_U|$, we first count the total number of U-decomposable $L \in \mathcal{A}_U$, which is $R_{k,\|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k,\|u\|}$ and then subtract the number of $L \in \mathcal{A}$ that have some irreducible decomposition $V \lhd U$ of L, giving

$$|\mathcal{A}_U| = R_{k,\|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k,\|u\|} - \sum_{V \lhd U} |\mathcal{A}_V|. \tag{7}$$

Therefore,

$$\sum_{U \in Q} |\mathcal{A}_U| = \sum_{U \in Q} c_{|U|} R_{k,\|u_0\|} \prod_{u \in U \setminus \{u_0\}} K_{k,\|u\|} \tag{8}$$

for some integer coefficients, $c_{|U|}$. It is not immediately obvious that the required coefficients depend only on the size of the partition, but the decision to write $c_{|U|}$ rather than c_U will be justified by the next calculation.

We will now show, by induction on $|U|$, that $c_{|U|} = (-1)^{|U|}(|U| - 1)!$. If $|U| = 2$ then $c_{|U|} = 1 = (-1)^{|U|}(|U| - 1)!$, by (7) and (8). Now assume $c_{|V|} =$

$(-1)^{|V|}(|V|-1)!$ for all $V \triangleright U$. By (7),

$$c_{|U|} = 1 - \sum_{V \triangleright U} c_{|V|} = 1 - \sum_{i=2}^{|U|-1} S(|U|,i)c_i = 1 - \sum_{i=2}^{|U|-1} S(|U|,i)(-1)^i(i-1)!$$

where $S(\cdot,\cdot)$ denotes the Stirling number of the second kind. We use the well-known identity $\sum_{i=1}^{|U|} S(|U|,i)(-1)^i(i-1)! = 0$ to obtain $c_{|U|} = (-1)^{|U|}(|U|-1)!$. □

It is possible to provide a similar proof for normalised $k \times n$ Latin rectangles. Since the proof is analogous, it is omitted.

Theorem 5.

$$K_{k,n} \equiv \sum_{U \in Q} (-1)^{|U|}(|U|-1)! \prod_{u \in U} K_{k,\|u\|} \pmod{t'}. \tag{9}$$

Theorems 4 and 5 provide numerous interesting corollaries, which we will now present.

Corollary 3. *Suppose p is prime and $n \in \mathbb{N}$. If $d \geq k > p$ then $p^{\lfloor n/p \rfloor}$ divides $R_{k,n+d}$ and $K_{k,n}$.*

Proof. When $n < p$, $R_{k,n+d}$ and $K_{k,n}$ are both divisible by $p^{\lfloor n/p \rfloor} = 1$, so assume $n \geq p$ and hence $a := \lfloor n/p \rfloor \geq 1$. Choose $b_0 = n - sp$ and $b_1 = b_2 = \cdots = b_s = p$ where $s = a - 1$ if p divides n and $s = a$ otherwise. By Theorem 5 and induction on n, $K_{k,n} \equiv 0 \pmod{p^a}$. Similarly, $R_{k,n+d} \equiv 0 \pmod{p^a}$ follows from Theorem 4, if we instead use $b_0 = n + d - ap \geq k$. □

Corollary 3 implies that for any prime $p < k$ the largest $x \in \mathbb{N}$ such that p^x divides $R_{k,n}$ increases at least linearly with n.

Corollary 4. *Let $d, k, n \in \mathbb{N}$ be such that $d \geq k > \mathrm{gpd}(n)$. Then n divides $K_{k,n}$ and $R_{k,n+d}$.*

Proof. Note that $R_{k,n+d} \equiv R_{k,d}K_{k,n} \pmod{n}$ by Theorem 4. Since $k > \mathrm{gpd}(n)$, if n is prime then $K_{k,n} = 0$ and hence $R_{k,n+d} \equiv 0 \pmod{n}$. So assume n is composite. If p^x divides n, for some $x \in \mathbb{N}$ and prime p, then $p^{n/p}$ divides $K_{k,n}$ and $R_{k,n+d}$, by Corollary 3. However, $n/p \geq p^{x-1} \geq x$ if $x \geq 2$ and $n/p \geq x$ if $x = 1$, hence p^x divides $p^{n/p}$ which in turn divides $K_{k,n}$ and $R_{k,n+d}$. The result follows since p^x was an arbitrary prime power divisor of n. □

A complete determination of when n divides $R_{k,n}$ is given later, in Corollary 8.

Corollary 5. *If $k > \mathrm{gpd}(t')$ then $K_{k,n} \equiv 0 \pmod{t'}$ and if $b_0 \geq k > \mathrm{gpd}(t)$ then $R_{k,n} \equiv 0 \pmod{t}$.*

Proof. The result follows from Theorems 4 and 5 by induction on s. Note that if $s = 1$ then $R_{k,n} \equiv R_{k,b_0}K_{k,b_1} \equiv 0 \pmod{t}$ and $K_{k,n} \equiv K_{k,b_0}K_{k,b_1} \equiv 0 \pmod{t'}$, using Corollary 4. □

We can use Theorem 4 and Corollary 5 repeatedly with the same choice of k and n but with various values of b_0 and t. For example, suppose we seek congruences involving $R_{6,20}$. There are various choices for $(b_i)_{i=0}^s$ that satisfy $b_0 \geq 6$ and $n = 20$ but produce different values of t. The order of the subsequence $(b_i)_{i=1}^s$ does not affect the results. Also, there is little advantage in choosing a composite b_i when $i \geq 1$, since a composite term can be replaced by its prime factors and b_0 and s increased accordingly to preserve $n = \sum_{0 \leq i \leq s} b_i$. In Figure 2, we choose the subsequence $(b_i)_{i=1}^s$ to be a single prime repeated s times. See Figure 1 for the values of $R_{k,n}$ for $1 \leq n \leq 11$. Recall that $K_{k,n} = (n-1)!R_{k,n}/(n-k)!$ by (1).

In the case of powers of 5 dividing $R_{6,20}$, we can actually prove a larger divisor by using Theorem 5 rather than Theorem 4. When $(b_i)_{i=0}^s = (5,5,5,5)$, Theorem 5 gives $K_{6,20} \equiv 0 \pmod{5^4}$ and so $360R_{6,20} \equiv 0 \pmod{5^4}$ by (1). Therefore $R_{6,20} \equiv 0 \pmod{5^3}$. Together with Figure 2, this establishes that $R_{6,20} \equiv 308448000 \pmod{1297296000}$ and also that $R_{6,20} \equiv 47R_{6,13} \pmod{7^2}$, where $R_{6,13} \pmod{7^2}$ is currently unknown.

$(b_i)_{i=0}^s$	Congruence for $R_{6,20}$
$(6,2,2,2,2,2,2,2)$	$0 \pmod{2^7}$
$(8,3,3,3,3)$	$0 \pmod{3^4}$
$(10,5,5)$	$0 \pmod{5^2}$
$(13,7)$	$R_{6,13}K_{6,7} \equiv R_{6,6}K_{6,7}^2 \equiv 0 \pmod{7}$
$(6,7,7)$	$R_{6,6}K_{6,14} + 2R_{6,13}K_{6,7} - 2R_{6,6}K_{6,7}^2 \equiv 47R_{6,13} \pmod{7^2}$
$(9,11)$	$R_{6,9}K_{6,11} \equiv 3 \pmod{11}$
$(7,13)$	$R_{6,7}K_{6,13} \equiv 3R_{6,13} \equiv 3 \pmod{13}$

Figure 2: Congruences for $R_{6,20}$ implied by Theorem 4.

An interesting property of Corollary 5 is that, for a given n, it provides an increasing prime power divisor of $R_{k,n}$ with decreasing k. For example, it implies that $R_{7,11} \equiv R_{6,11} \equiv 0 \pmod{2^2}$, $R_{5,11} \equiv R_{4,11} \equiv 0 \pmod{2^3}$ and $R_{3,11} \equiv 0 \pmod{2^4}$. From Figure 1, it appears that the largest power of 2 dividing $R_{k,n}$ generally increases with k, although $R_{6,10}$ is an exception. The powers of 2 in Figure 1 are surprisingly large and their great size remains mostly unexplained.

The following is a special case of Theorem 4, using (1).

Corollary 6. *If $k \leq n$ then $R_{k,n+d} \equiv (-1)^{k-1}(k-1)!R_{k,n}R_{k,d} \pmod{d}$ for all $d \in \mathbb{N}$.*

Upon inspection of Figure 1 we see that $R_{3,n}$ is indivisible by 3 for $3 \leq n < 6$ and indivisible by 5 for $3 \leq n < 8$. Therefore Corollary 6 implies that 3 and 5 do not divide $R_{3,n}$ for any $n \geq 3$. In this way, Corollary 6 can be used to discover indivisibility properties of $R_{k,n}$. In the next section we will see that Corollary 6 generalises earlier results by Riordan and Carlitz.

5. Modulo n

We turn our attention to the value of $R_{k,n} \pmod n$, which is listed in Figure 3 for small values of k and n. For $n \le 11$ the values of $R_{k,n}$ have been explicitly calculated [28], while $R_{k,n}$ for $k \le 3$ can be enumerated by (2) and (3). The remaining values are established later, in Theorem 8.

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$k=1$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	3	1	5	1	7	1	9	1	11	1	13	1	15	1	17
3		1	0	1	2	1	0	4	2	1	8	1	2	4	0	1	14
4			0	1	0	1	0	0	4	1	0	1	8	6	0	1	0
5				1	0	1	0	0	4	1	0	1	10	6	0	1	0
6					0	1	0	0	0	1	0	1	6	0	0	1	0
7						1	0	0	0	1	0	1	6	0	0	1	0
8							0	0	0	1	0	1	0	0	0	1	0
9								0	0	1	0	1	0	0	0	1	0
10									0	1	0	1	0	0	0	1	0
11										1	0	1	0	0	0	1	0

Figure 3: Values of $R_{k,n} \pmod n$ for some small values of k and n.

Our first theorem for this section shows that the $k = 3$ case of Corollary 6 includes the congruences due to Riordan [35] and Carlitz [5] mentioned in the introduction.

Theorem 6.

- *For $n \ge 2$, $R_{2,n} \equiv (-1)^{n+1} \pmod n$ and $R_{2,n}$ is odd.*
- *For $n \ge 3$, $R_{3,n} \equiv 2^{n-1} \pmod n$ and $R_{3,n} \equiv 2^{n-1}(1-n-n^2) \pmod 3$.*

Proof. By (2), $R_{2,n} \equiv -D_n = -n!\sum_{k=0}^{n}(-1)^k/k! \equiv (-1)^{n+1} \pmod n$. Euler [12] proved the recurrence $D_n = (n-1)(D_{n-1}+D_{n-2})$ with $D_1 = 0$ and $D_2 = 1$. Therefore $D_n \equiv 0 \pmod 2$ for odd n and, by induction, $D_n \equiv 1 \pmod 2$ for even n. Hence $R_{2,n} = D_n/(n-1) = D_{n-1} + D_{n-2} \equiv 1 \pmod 2$.

The summands in (3) are integer multiples of n except possibly when $n-2 \le k \le n$, which is when $(i,j,k) \in \big\{(0,0,n),(1,0,n-1),(0,1,n-1),(2,0,n-2),(1,1,n-2),(0,2,n-2)\big\}$. Hence

$$R_{3,n} \equiv \frac{2^{n-1}}{(n-1)(n-2)}(2+n-3n) + \frac{2^{n-2}n}{n-2}(2-6+6) = 2^{n-1} \pmod n.$$

The summands in (3) are integer multiples of 3 except possibly when $n-2 \le k \le n$ or $(i,j,k) \in \{(0,3,n-3),(1,3,n-4)\}$. Similarly to the modulo n case, this yields $R_{3,n} \equiv 2^{n-1} - 2^{n-3}10n - 2^{n-4}56n(n-3) \equiv 2^{n-1}(1-n-n^2) \pmod 3$. □

We now make an interesting observation, that will lead to the evaluation of $R_{k,p} \pmod p$ for all primes p, in Theorem 7.

Lemma 2. *Let p be a prime, and let $Z_{k,p}$ denote the number of reduced $k \times p$ Latin rectangles that are isotopic to a subrectangle of $\mathbb{Z}_p$, the addition table for integers modulo p. Then $Z_{k,p} = (p-2)!$ when $1 < k \leq p$.*

Proof. Each reduced $2 \times p$ Latin rectangle, L, can be interpreted as a permutation σ_L in 2-row format. It is easy to show that L is isotopic to a subrectangle of $\mathbb{Z}_p$ if and only if σ_L is a p-cycle. There are $(p-2)!$ different p-cycles that map 1 to 2, therefore $Z_{2,p} = (p-2)!$.

Let $\mathrm{Aut}(\mathbb{Z}_p)$ be the autotopism group of the Cayley table of $\mathbb{Z}_p$. The autotopism group of the Cayley table of a finite group is described by, for example, Bailey [3]. As a corollary $|\mathrm{Aut}(\mathbb{Z}_p)| = p^2(p-1)$ and so

$$Z_{p,p} = \frac{(p!)^3}{p!(p-1)!|\mathrm{Aut}(\mathbb{Z}_p)|} = (p-2)!.$$

Each reduced $k \times p$ Latin rectangle isotopic to a subrectangle of $\mathbb{Z}_p$ can easily be extended to a $(k+1) \times p$ such rectangle. Hence

$$(p-2)! = Z_{2,p} \leq Z_{3,p} \leq \cdots \leq Z_{p,p} = (p-2)!,$$

from which the result follows. □

Theorem 7. *Let p be a prime and $1 \leq k \leq p$. Then $R_{k,p} \equiv 1 \pmod{p}$.*

Proof. It will be assumed that $k > 1$ since $R_{1,p} = 1$. Let G be the group of isotopisms generated by $(\varepsilon, \beta, \beta)$ where $\beta = (12 \cdots p)$. Our proof follows the basic template in Section 2, except that G acts on the set of *normalised* $k \times p$ Latin rectangles, while we choose $\mathcal{C}$ to be the set of *reduced* $k \times p$ Latin rectangles.

For any isotopy class I, let $\mathrm{Norm}(I)$ be the number of normalised Latin rectangles in I and let $\mathrm{Red}(I)$ be the number of reduced Latin rectangles in I. Then $\mathrm{Norm}(I) = (p-1)! \cdot \mathrm{Red}(I)/(p-k)!$. If every normalised $L \in I$ does not admit a non-trivial autotopism in G then p divides $\mathrm{Norm}(I)$ and so p also divides $\mathrm{Red}(I)$. So choose $\mathcal{A}$ to be the set of reduced $k \times p$ Latin rectangles that are isotopic to a Latin rectangle that admits a non-trivial autotopism in G. Hence $R_{k,p} = |\mathcal{C}| \equiv |\mathcal{A}| \pmod{p}$.

If a Latin rectangle L admits a non-trivial autotopism in G, then $(\varepsilon, \beta, \beta)$ is an autotopism of L, since p is a prime. Therefore, in each row of L the symbols occur in cyclic order, so L is isotopic to a subrectangle of $\mathbb{Z}_p$. So $\mathcal{A}$ is precisely the set of reduced $k \times p$ Latin rectangles that are isotopic to a subrectangle of $\mathbb{Z}_p$. By Lemma 2 and Wilson's Theorem $|\mathcal{A}| = Z_{k,p} = (p-2)! \equiv 1 \pmod{p}$. □

Theorem 7 and Corollary 6 imply that $R_{k,n+p} \equiv (-1)^{k-1}(k-1)!R_{k,n} \pmod{p}$ for prime $p \geq k$. Together Theorem 7 and Corollary 1 show the surprising fact that $R_n \pmod{n}$ is an indicator variable for primality of n.

Corollary 7. *$R_n \equiv 0 \pmod{n}$ for composite n and $R_n \equiv 1 \pmod{n}$ for prime n.*

Corollaries 6 and 7 imply that $R_{k,n+k} \equiv -R_{k,n} \pmod{k}$, when $n \geq k$. Hence $R_{p,\lambda p} \equiv (-1)^{\lambda-1} \pmod{p}$ for any prime p, by Theorem 7.

Corollary 8. *$R_{k,n} \equiv 0 \pmod{n}$ if and only if $k > \operatorname{gpd}(n)$.*

Proof. Let $q = \operatorname{gpd}(n)$. If $n = q$ then Theorem 7 implies that $R_{k,q} \equiv 1 \not\equiv 0 \pmod{q}$ for all $1 \leq k \leq q = n$. So assume $n = \lambda q$ where $\lambda \geq 2$. By Theorem 7 and repeated application of Corollary 6, $R_{k,n} \equiv (-1)^{(\lambda-1)(k-1)}(k-1)!^{\lambda-1} \pmod{q}$. If $k \leq q$ this congruence is non-zero, so $R_{k,n} \not\equiv 0 \pmod{n}$.

Conversely we will show that $R_{k,n} \equiv 0 \pmod{n}$ when $k > q$. The $m < k \leq n$ case is precisely Corollary 1, so assume $q < k \leq m$.

Suppose p^x is a prime power divisor of n. If $x = 1$ then Corollary 6 implies that $R_{k,n} \equiv (-1)^{k-1}(k-1)!R_{k,n-p}R_{k,p} \equiv 0 \pmod{p}$, since $p < k$. So assume $x \geq 2$. If $n \geq 2px$ then $n \geq m + px \geq k + px$ and so Corollary 3 implies that $R_{k,n} \equiv 0 \pmod{p^x}$. But $n \geq p^x \geq 2px$ for all n except $n \in \{4, 8, 9\}$. These cases are resolved by Figure 3. □

We conclude with an exact formula for $R_{k,n} \pmod{n}$ for all $k, n \in \mathbb{N}$. In fact Theorem 8 is true even if $k > n$, where $R_{k,n} = 0$.

Theorem 8. $R_{k,n} \equiv \left((-1)^{k-1}(k-1)!\right)^{n-1} \pmod{n}$

Proof. Let $a = a(k) = (-1)^{k-1}(k-1)!$. We want to show that $R_{k,n} \equiv a^{n-1} \pmod{n}$ for all $n \in \mathbb{N}$, $1 \leq k \leq n$.

Let $x, y \in \mathbb{N}$ such that $\gcd(x, y) = 1$ and $R_{k,x} \equiv a^{x-1} \pmod{x}$ and $R_{k,y} \equiv a^{y-1} \pmod{y}$. By Theorem 4, $R_{k,xy} \equiv aR_{k,x(y-1)}R_{k,x} \equiv a^2R_{k,x(y-2)}R_{k,x}^2 \equiv \cdots \equiv a^{y-1}R_{k,x}^y \equiv a^{y-1}a^{y(x-1)} \equiv a^{xy-1} \pmod{x}$. By symmetry, $R_{k,xy} \equiv a^{xy-1} \pmod{y}$. Since x and y are coprime, $R_{k,xy} \equiv a^{xy-1} \pmod{xy}$. Observe that this argument is still valid even if k is greater than x or y. Therefore it is sufficient to show that $R_{k,p^s} \equiv a^{p^s-1} \pmod{p^s}$ for an arbitrary prime p and all $s \in \mathbb{N}$.

If $k > p$ then Corollary 8 implies that $R_{k,p^s} \equiv 0 \equiv a^{p^s-1} \pmod{p^s}$. Therefore assume $k \leq p$. As $K_{k,p^s} \equiv aR_{k,p^s} \pmod{p^s}$ by (1), it is therefore sufficient to show that $K_{k,p^s} \equiv a^{p^s} \pmod{p^s}$ since p does not divide a.

When $s = 1$, Theorem 7 and Fermat's Little Theorem imply that $R_{k,p} \equiv 1 \equiv a^{p-1} \pmod{p}$. For the sake of induction, assume $K_{k,p^{s-1}} \equiv a^{p^{s-1}} \pmod{p^{s-1}}$. By repeated application of Theorem 5, we get $K_{k,p^s} \equiv K_{k,p^{s-1}}^p \equiv \left(cp^{s-1} + a^{p^{s-1}}\right)^p \pmod{p^s}$ for some integer c. Using the Binomial Theorem, $K_{k,p^s} \equiv a^{p^s} \pmod{p^s}$. □

Theorem 8 implies that $R_{k,n} \equiv 1 \pmod{n}$ whenever n is a base $(k-1)!$ Fermat pseudoprime. For example, when $n = 11 \cdot 31$ and $k = 3$ we get $R_{3,341} \equiv 2^{341-1} \equiv 1 \pmod{341}$ and so the converse of Theorem 7 is false. Furthermore, if n is a Carmichael number and p is the smallest prime that divides n then $R_{k,n} \equiv 1 \pmod{n}$ for $1 \leq k \leq p$.

6. Concluding remarks

We have established the exact value of $R_{k,n} \pmod n$ in Theorem 8. It would also be interesting to find a formula for $R_{k,n} \pmod k$. We know this value when k is composite, by Corollary 2, and for $k \leq 3$ by Theorem 6.

The comment following Corollary 7 implies that $R_{k,n} \equiv \big((-1)^{k-1}(k-1)!\big)^{n-1} p_k(n) \pmod k$ for some polynomial p_k, which has degree at most $k-1$. The polynomial $p_k(n)$ can be determined by Lagrange interpolation from the values of $R_{k,n} \pmod k$ for $k \leq n < 2k$. For example, Figure 1 tells us that $p_5(n) = 1 - n^2 - 2n^3 - n^4 \pmod 5$.

Acknowledgement

The authors would like to thank Rod Canfield and Brendan McKay for bringing the interesting pattern of $R_n \pmod n$ in Corollary 7 to their attention.

References

[1] R. Alter, *How many Latin squares are there?*, Amer. Math. Monthly, 82 (1975), pp. 632–634.

[2] K. B. Athreya, C. R. Pranesachar, and N. M. Singhi, *On the number of Latin rectangles and chromatic polynomial of $L(K_{r,s})$*, European J. Combin., 1 (1980), pp. 9–17.

[3] R. A. Bailey, *Latin squares with highly transitive automorphism groups*, J. Aust. Math. Soc., 33 (1982), pp. 18–22.

[4] K. P. Bogart and J. Q. Longyear, *Counting 3 by n Latin rectangles*, Proc. Amer. Math. Soc., 54 (1976), pp. 463–467.

[5] L. Carlitz, *Congruences connected with three-line Latin rectangles*, Proc. Amer. Math. Soc., 4 (1953), pp. 9–11.

[6] J. Denés and G. L. Mullen, *Enumeration formulas for Latin and frequency squares*, Discrete Math., 111 (1993), pp. 157–163.

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

[8] ——, *Proof of the Alon-Tarsi conjecture for $n = 2^r p$*, Electron. J. Combin., 5 (1998). R28, 5 pp.

[9] A. L. Dulmage, *E650*, Amer. Math. Monthly, 52 (1945), p. 458.

[10] A. L. Dulmage and G. E. McMaster, *A formula for counting three-line Latin rectangles*, Congr. Numer., 14 (1975), pp. 279–289.

[11] L. Euler, *Recherches sur une nouvelle espéce de quarrés magiques*, Verh. Zeeuwsch. Gennot. Weten. Vliss., 9 (1782), pp. 85–239. Eneström E530, Opera Omnia OI7, pp. 291-392.

[12] ——, *Solutio quaestionis curiosae ex doctrina combinationum*, Mémoires de l'Académie des Sciences de St. Pétersbourg, 3 (1811), pp. 57–64. E738, OI7, pp. 435-440.

[13] Z.-L. Fu, *The number of Latin rectangles*, Math. Practice Theory, (1992), pp. 40–41. In Chinese.

[14] I. M. Gessel, *Counting three-line Latin rectangles*, in Proceedings of the Colloque de Combinatoire Énumérative, G. Labelle and P. Leroux, eds., Springer, 1986.

[15] ——, *Counting Latin rectangles*, Bull. Amer. Math. Soc., 16 (1987), pp. 79–83.

[16] C. D. Godsil and B. D. McKay, *Asymptotic enumeration of Latin rectangles*, J. Combin. Theory Ser. B, 48 (1990), pp. 19–44.

[17] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, Wiley, 1983.

[18] J. R. Hamilton and G. L. Mullen, *How many $i - j$ reduced Latin rectangles are there?*, Amer. Math. Monthly, 87 (1980), pp. 392–394.

[19] S. M. Jacob, *The enumeration of the Latin rectangle of depth three by means of a formula of reduction, with other theorems relating to non-clashing substitutions and Latin squares*, Proc. London Math. Soc. (2), 31 (1930), pp. 329–354.

[20] A.-A. A. Jucys, *The number of distinct Latin squares as a group-theoretical constant*, J. Combin. Theory Ser. A, 20 (1976), pp. 265–272.

[21] S. M. Kerawala, *The enumeration of the Latin rectangle of depth three by means of a difference equation*, Bull. Calcutta Math. Soc., 33 (1941), pp. 119–127.

[22] ——, *The asymptotic number of three-deep Latin rectangles*, Bull. Calcutta Math. Soc., 39 (1947), pp. 71–72.

[23] F. W. Light, Jr, *A procedure for the enumeration of $4 \times n$ Latin rectangles*, Fibonacci Quart., 11 (1973), pp. 241–246.

[24] ——, *Enumeration of truncated Latin rectangles*, Fibonacci Quart., 17 (1979), pp. 34–36.

[25] P. A. MacMahon, *Combinatory Analysis*, Chelsea, 1960.

[26] B. D. McKay, A. Meynert, and W. Myrvold, *Small Latin squares, quasigroups, and loops*, J. Combin. Des., 15 (2007), pp. 98–119.

[27] B. D. McKay and E. Rogoyski, *Latin squares of order ten*, Electron. J. Combin., 2 (1995). N3, 4 pp.

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

[29] G. L. Mullen, *How many $i - j$ reduced Latin squares are there?*, Amer. Math. Monthly, 82 (1978), pp. 751–752.

[30] J. R. Nechvatal, *Counting Latin Rectangles*, PhD thesis, University of Southern California, 1979.

[31] ——, *Asymptotic enumeration of generalized Latin rectangles*, Util. Math., 20 (1981), pp. 273–292.

[32] C. R. Pranesachar, *Enumeration of Latin rectangles via SDR's*, in Combinatorics and Graph Theory, A. Dold, B. Eckmann, and S. B. Rao, eds., Springer, 1981, pp. 380–390.

[33] J. Riordan, *Three-line Latin rectangles*, Amer. Math. Monthly, 51 (1944), pp. 450–452.

[34] ——, *Three-line Latin rectangles-II*, Amer. Math. Monthly, 53 (1946), pp. 18–20.

[35] ——, *A recurrence relation for three-line Latin rectangles*, Amer. Math. Monthly, 59 (1952), pp. 159–162.

[36] J.-Y. Shao and W.-D. Wei, *A formula for the number of Latin squares*, Discrete Math., 110 (1992), pp. 293–296.

[37] D. C. van Leijenhorst, *Symmetric functions, Latin squares and Van der Corput's "scriptum 3"*, Expo. Math., 18 (2000), pp. 343–356.

[38] K. Yamamoto, *Asymptotic number of Latin rectangles and the symbolic method*, Sûgaku, 2 (1949).

[39] ——, *An asymptotic series for the number of three-line Latin rectangles*, J. Math. Soc. Japan, 1 (1950), pp. 226–241.

[40] ——, *Symbolic methods in the problem of three-line Latin rectangles*, J. Math. Soc. Japan, 5 (1953), pp. 13–23.