

初等数论在正交拉丁方构造中的应用

李栋梁

南京特殊教育师范学院数学科学学院, 江苏 南京

收稿日期: 2026年8月1日; 录用日期: 2026年8月31日; 发布日期: 2026年9月8日

摘 要

初等数论是数学专业的一门基础课程, 学生在学习同余、可逆元和同余方程后, 往往难以认识这些知识的应用。本文以拉丁方和正交拉丁方为例, 介绍利用模运算构造循环拉丁方和一般线性拉丁方, 并利用一次同余方程的唯一可解性判定两个线性拉丁方的正交性。通过这些经典构造, 说明初等数论知识在组合设计中的具体应用, 引导学生理解同余理论的结构意义和应用价值。

关键词

初等数论, 同余, 拉丁方, 正交拉丁方

Application of Elementary Number Theory to Constructions of Orthogonal Latin Squares

Dongliang Li

School of Mathematical Sciences, Nanjing Normal University of Special Education, Nanjing Jiangsu

Received: August 1, 2026; accepted: August 31, 2026; published: September 8, 2026

Abstract

Elementary number theory is a fundamental course for mathematics majors, but students often find it difficult to recognize the applications of congruences, invertible elements, and congruence equations after learning these concepts. Taking Latin squares and orthogonal Latin squares as examples, this paper introduces the construction of cyclic Latin squares and general linear Latin squares using modular arithmetic, and presents a criterion for the orthogonality of two linear Latin squares based on the unique solvability of linear congruence equations. These classical constructions illustrate concrete applications of elementary number theory in combinatorial design and help students

understand the structural significance and application value of congruence theory.

Keywords

Elementary Number Theory, Congruence, Latin Square, Orthogonal Latin Square

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

高校专业基础课程既要保持理论体系的严谨性,也应通过适当的学科应用揭示概念之间的内在联系。教育部关于一流本科课程建设的相关要求强调,课程内容应体现高阶性、创新性和挑战度,并推动科研成果及时转化为教学内容[1]。对于数学类课程而言,这种转化不宜简单增加超出学生认知基础的前沿结论,而应选择能够由课程核心知识完整解释的对象,使学生看到抽象定义如何转化为可验证、可推广的数学结构。

初等数论主要研究整数的整除性、同余、同余方程等基本问题。相关知识具有较强的计算特征,例如利用欧几里得算法求最大公因数、求解一次同余方程等[2]。但若课程学习长期停留在求余数、解方程的层面,学生容易把各章内容理解为相互分散的技巧,而较难体会所学知识的实际应用。因而,选择一个定义直观、结论明确且能够使用初等数论知识完成构造和证明的对象,有助于呈现课程知识的结构价值。

拉丁方是组合设计理论中的基本结构,在试验设计、编码、密码及组合构造等领域具有重要作用[3]-[5]。其核心要求是每个符号在每一行、每一列中恰好出现一次;两个拉丁方正交时,叠置后形成的有序符号对也恰好各出现一次。欧拉三十六军官问题是经典组合问题之一[6],其归结于一对6阶正交拉丁方的存在性问题。拉丁方的构造及其正交性判定均属于组合设计理论中的经典内容。

本文以正交拉丁方为例,讨论初等数论知识在组合设计构造中的应用。第2节介绍同余、可逆元、拉丁方和正交拉丁方等预备知识;第3节依据经典文献,建立拉丁方及其正交性的判定方法,重点说明初等数论知识如何保证拉丁方中的无重复性和正交性;第4节给出总结与展望。

2. 预备知识

2.1. 同余与可逆元

设 n 为正整数。若 n 整除 $a-b$, 则称 a 与 b 对模 n 同余, 记作 $a \equiv b \pmod{n}$ 。同余关系把全体整数划分为 n 个剩余类。本文用 $Z_n = \{0, 1, \dots, n-1\}$ 表示一个完全剩余系, 并在其中按模 n 定义加法和乘法。对 $a \in Z_n$, 若存在 $x \in Z_n$, 使 $ax \equiv 1 \pmod{n}$, 则称 a 是模 n 的可逆元。初等数论中的基本结论指出, a 在模 n 意义下可逆当且仅当 a 与 n 互质[2]。因此, 乘法映射 $x \mapsto ax \pmod{n}$ 是 Z_n 上的一个置换, 当且仅当 a 与 n 互质。更一般地, 线性同余方程 $ax \equiv b \pmod{n}$ 对任意 $b \in Z_n$ 有解当且仅当 $\gcd(a, n) = 1$ [2]。

2.2. 拉丁方与正交拉丁方

定义1[4] 设 S 为 n 元集, L 为 S 上的 $n \times n$ 方阵。若 L 的每行每列都是 S 中元素的一个全排列, 则称 L 为 S 上的一个 n 阶拉丁方, 记为 $LS(n)$ 。

定义 2 [4] 设 S_1 和 S_2 为 n 元集, $L = (l_{ij})$ 与 $M = (m_{ij})$ 分别为 S_1 和 S_2 上的 n 阶拉丁方。若将二者叠置后得到的 n^2 个有序对 (l_{ij}, m_{ij}) 两两不同, 则称 L 与 M 正交, 记为 $\text{MOLS}(n)$ 。

由于可能的有序对总数恰好为 n^2 , 因此定义 2 中的 n^2 个有序对两两不同等价于每个有序对恰好出现一次。

拉丁方强调行、列方向上的无重复性, 正交性则进一步要求两个方阵叠置后的有序对在整个方阵中完全均匀。对于一般方阵, 这些性质可以逐行、逐列或逐格检验。对于由同余公式定义的方阵, 则可以把无重复和唯一出现转化为同余方程是否具有唯一解, 从而得到统一的数论判定。

2.3. 正交阵列

定义 3 [4] 设 N, k, s, t 为正整数, $t \leq k$ 。设 A 是 v 元集 V 上的 $k \times N$ 阵列, 若对 A 的任意 $t \times N$ 子阵, V 上每个 $t \times 1$ 列向量作为该子阵的列各出现 λ 次, 则称 A 约束数 k 、水平数 v 、强度 t 和指标 λ 的正交阵列, 记为 $\text{OA}(N, k, v, t)$ 。

由此定义易知, $N = \lambda v^t$ 。当 $\lambda = 1$ 时, 简记 $\text{OA}(N, k, v, t)$ 为 $\text{OA}(t, k, v)$ 。

3. 初等数论在正交拉丁方构造中的应用

本节涉及的循环拉丁方、一般线性拉丁方及线性拉丁方的正交性判定, 均为组合设计中的经典内容 [3]-[5]。本文按照初等数论课程中同余、可逆元和一次同余方程的知识顺序对其重新组织, 并给出相应的初等证明, 以说明这些数论知识如何参与拉丁方的构造及正交性的判定。

3.1. 循环拉丁方

定理 1 对任意整数 $n \geq 2$, 存在 n 阶拉丁方。

证明: 对任意 $i, j \in Z_n$, 定义方阵 L 第 i 行第 j 列的元素 $L(i, j) = i + j \pmod{n}$ 。下证 L 是 n 阶拉丁方。

根据定义, 需证明 L 中每行每列元素均为 Z_n 中元素的全排列。采用反证法。固定第 i 行, 对任意 $j_1, j_2 \in Z_n$, $j_1 \neq j_2$, 若第 j_1 列和 j_2 列的元素相同, 则

$$i + j_1 \equiv i + j_2 \pmod{n}.$$

由同余消去律可得,

$$j_1 \equiv j_2 \pmod{n}.$$

由于 $j_1, j_2 \in Z_n$, 故 $j_1 = j_2$, 这与 j_1 和 j_2 的取法矛盾, 因此 L 中第 i 行没有重复的元素。又因为该行恰有 n 个位置, 所以恰好包含 Z_n 中的所有元素。

固定第 j 列, 同理可得每一列也无重复元素。证毕。

上述构造本质是循环群 Z_n 的加法表, 也是拉丁方理论中最基本的经典构造之一 [3]-[5], 其每一行均由上一行循环平移一个位置, 因而称为循环拉丁方。其经典性并不在于构造复杂, 而在于它清楚展示了同余消去律保证方阵中每行每列元素不重复这一对应关系。张蓉蓉、刘兴祥也从矩阵及初等变换角度讨论了拉丁方的构造问题 [7]。从初等数论课程的角度看, 循环拉丁方可以作为学生由具体模运算进入一般证明的一个例子。

3.2. 一般线性拉丁方

循环拉丁方只使用模加法, 为体现模乘法与可逆元的作用, 可进一步考虑一般线性拉丁方。对

$a, b \in Z_n$, 定义

$$L(i, j) = ai + bj \pmod{n}, \quad i, j \in Z_n.$$

循环拉丁方对应于 $a = b = 1$ 的特殊情形。

定理 2 L 是 n 阶拉丁方当且仅当 $\gcd(a, n) = \gcd(b, n) = 1$ 。

证明: 先证充分性。若 $\gcd(b, n) = 1$, 则 b 在模 n 意义下可逆。固定 i , 对任意 $j_1, j_2 \in Z_n$, $j_1 \neq j_2$, 若第 j_1 列和 j_2 列的元素相同, 即

$$ai + bj_1 \equiv ai + bj_2 \pmod{n}.$$

整理得,

$$b(j_1 - j_2) \equiv 0 \pmod{n}.$$

两边同乘 b^{-1} , 得

$$j_1 \equiv j_2 \pmod{n}.$$

由于 $j_1, j_2 \in Z_n$, 故 $j_1 = j_2$, 矛盾。因此 L 中第 i 行没有重复的元素。固定第 j 列, 同理可得每一列也无重复元素。

再证必要性。若 $d = \gcd(b, n) > 1$, 令 $h = \frac{n}{d}$, 则 $0 < h < n$, 且

$$bh \equiv 0 \pmod{n}.$$

于是对任意固定的 i 和任意 j , 有

$$ai + b(j + h) \equiv ai + bj \pmod{n}.$$

即 L 的第 i 行中出现相同的元素, 这与 L 为拉丁方矛盾。因此必有 $\gcd(b, n) = 1$ 。同理, 若 $\gcd(a, n) > 1$, 则某一列中必有重复元素, 所以必有 $\gcd(a, n) = 1$ 。证毕。

该定理揭示了线性拉丁方中两个系数的不同作用。系数 b 控制同一行中列指标 j 的变化, 系数 a 控制同一列中行指标 i 的变化。只有当二者都是模 n 的可逆元时, 乘法才保持 Z_n 中各剩余类的互异性。例如在模 6 意义下, 方阵 $L(i, j) = 2i + j \pmod{6}$ 的每一行仍包含全部符号, 但固定任意一列后, 第 0 行和第 3 行会出现相同元素, 因此该方阵不是拉丁方。可逆元由最大公因数判定, 因而拉丁方的行列均衡性被归结为两个初等数论计算。

3.3. 线性拉丁方的正交性判定

设 $L(i, j) = ai + bj \pmod{n}$, $M(i, j) = ci + dj \pmod{n}$, 且 L 与 M 均为 n 阶拉丁方。由定理 2 可知, a, b, c, d 均为模 n 的可逆元。要判断二者是否正交, 需要考察任意有序对 $(x, y) \in Z_n \times Z_n$ 是否恰好在同一位置 (i, j) 出现, 即同余方程组

$$\begin{cases} ai + bj \equiv x \pmod{n} & (1) \\ ci + dj \equiv y \pmod{n} & (2) \end{cases}$$

是否对每个 $x, y \in Z_n$ 都有唯一解。

定理 3 设 $L(i, j) = ai + bj \pmod{n}$ 与 $M(i, j) = ci + dj \pmod{n}$ 均为 n 阶拉丁方, 则 L 与 M 正交当且仅当 $\gcd(ad - bc, n) = 1$ 。

证明: 因为 b 为模 n 的可逆元, 故由(1)可得, $j \equiv b^{-1}(x - ai) \pmod{n}$ 。代入(2)式可得,

$$(ad-bc)i \equiv dx-by \pmod{n}.$$

若 $\gcd(ad-bc, n)=1$, 则上式对任意 x, y , 都有唯一的 i 。进而由 $j \equiv b^{-1}(x-ai) \pmod{n}$ 得到唯一的 j 。因此每个有序对 (x, y) 恰好出现一次, L 与 M 正交。反之, 若 $\gcd(ad-bc, n)>1$, 则 $ad-bc$ 不是模 n 的可逆元。当 $x=y=0$ 时, 同余方程 $(ad-bc)i \equiv 0 \pmod{n}$ 在模 n 意义下至少有两个不同解。对每个这样的 i , 由 $j \equiv b^{-1}(x-ai) \pmod{n}$ 得到相应的 j , 于是有序对 $(0, 0)$ 在叠置方阵中出现不止一次, 故二者不正交。证毕。

结合定理 2 和 3, 对两个线性方阵 $ai+bj$ 与 $ci+dj$, 若构成一对 n 阶正交拉丁方, 当且仅当 a, b, c, d 以及 $ad-bc$ 都是模 n 的可逆元, 即

$$\gcd(a, n) = \gcd(b, n) = \gcd(c, n) = \gcd(d, n) = \gcd(ad-bc, n) = 1.$$

以 $n=5$ 为例, 在 Z_{5^2} 上取 $L(i, j) = i + j \pmod{5}$, $M(i, j) = i + 2j \pmod{5}$ 。四个系数均与 5 互质, 且 $ad-bc=1$ 。因此由定理 3 可知两者正交, 见表 1。与逐格叠置并检查 25 个有序对相比, 数论方法只需检查若干最大公因数。由此, 正交性的组合要求被压缩为一次同余方程的唯一可解性, 体现了初等数论中可逆概念对有限组合结构的控制作用。

Table 1. A pair of orthogonal latin squares of order 5

表 1. 一对 5 阶正交拉丁方

$$L = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{pmatrix} \quad M = \begin{pmatrix} 0 & 2 & 4 & 1 & 3 \\ 1 & 3 & 0 & 2 & 4 \\ 2 & 4 & 1 & 3 & 0 \\ 3 & 0 & 2 & 4 & 1 \\ 4 & 1 & 3 & 0 & 2 \end{pmatrix}$$

需要指出的是, 定理 3 给出的是剩余类环 Z_n 上的一类经典线性构造, 其结论不能直接概括一般正交拉丁方的存在性。例如当 n 为偶数时, 模 n 的可逆元均为奇数, 若 a, b, c, d 均为模 n 的可逆元, 则 $ad-bc$ 为偶数, 因而不可能仍是模 n 的可逆元, 这也说明了定理 3 的方法无法构造出一对正交的 6 阶拉丁方。Bose、Shrikhande 和 Parker 借助平衡不完全区组设计、可分组设计以及递归复合等组合方法, 将局部结构拼接为整体设计, 最终否定了欧拉关于阶数 $n \equiv 2 \pmod{4}$ 不存在正交拉丁方的猜想, 并建立了除 2 阶和 6 阶外均存在一对正交拉丁方的结论[8]。

4. 总结与展望

本文在经典文献基础上, 围绕循环拉丁方、一般线性拉丁方和线性拉丁方的正交性判定, 讨论了初等数论知识在组合设计中的具体应用。模加法及同余消去律保证循环拉丁方中行、列元素无重复; 模 n 可逆元刻画了一般线性方阵成为拉丁方的充要条件; 两个线性拉丁方的正交性则可以转化为一次同余方程组的唯一可解性, 并最终归结为相关系数是否为模 n 的可逆元。由此, 同余、最大公因数、可逆元和一次同余方程不再是彼此孤立的计算工具, 而是在同一组合结构的构造与判定过程中发挥作用。

从初等数论课程教学的角度看, 拉丁方及正交拉丁方为抽象的同余理论提供了较为直观的应用载体。相关构造仅需利用同余、可逆元和一次同余方程等基础知识, 学生即可理解其基本思想和证明过程。将这些经典组合结构引入课程内容, 可以帮助学生认识到初等数论不仅能够解决整数计算和同余方程问题, 还能够用于刻画有限组合结构中的无重复性、均衡性和正交性, 从而深化对数论概念本质及其应用价值的理解。

正交拉丁方与正交阵列等组合设计结构之间又具有密切联系。设 L_1 与 L_2 是一对 n 阶正交拉丁方，对所有 $(i, j) \in Z_n \times Z_n$ ，依次写出三元组 $(i, L_1(i, j), L_2(i, j))$ 。由于每个拉丁方在固定行中均为一个排列，故 $(i, L_1(i, j))$ 与 $(i, L_2(i, j))$ 包含 $Z_n \times Z_n$ 中的每个有序对恰好一次；又由于 L_1 与 L_2 正交，故 $(L_1(i, j), L_2(i, j))$ 也包含 $Z_n \times Z_n$ 中的每个有序对恰好一次。因此这些 n^2 个三元组构成 $OA(n^2, 3, n, 2)$ 。例如，在 Z_3 上取 $L_1(i, j) = i + j$ ， $L_2(i, j) = i + 2j$ ，所得到的 $OA(9, 3, 3, 2)$ 见表 2。

Table 2. The orthogonal array $OA(9, 3, 3, 2)$ constructed from a pair of orthogonal Latin squares of order 3

表 2. 由一对 3 阶正交拉丁方构造的正交阵列 $OA(9, 3, 3, 2)$

i	$L_1(i, j)$	$L_2(i, j)$
0	0	0
0	1	2
0	2	1
1	1	1
1	2	0
1	0	2
2	2	2
2	0	1
2	1	0

表 2 中任意两列均包含 0、1、2 组成的 9 个有序对且各出现一次。该例表明，在本文所介绍的经典构造基础上，还可以进一步结合初等数论中的同余理论研究相关正交阵列的构造问题，并与试验设计等应用建立联系[9]，从而拓展初等数论知识的应用范围。本文的主要目的并非给出新的组合设计结果，而是通过对经典构造的重新组织和初等化解释，展示初等数论知识在拉丁方、正交拉丁方及相关组合设计问题中的具体应用，为学生理解数学理论与实际组合结构之间的联系提供一个较为直观的案例。后续如何巧妙的将初等数论的理论知识与更多相关的应用问题联系起来，引导学生学以致用，需要进一步探索。

基金项目

江苏省高等学校基础科学(自然科学)研究面上项目(25KJB110009)。

参考文献

- [1] 教育部关于一流本科课程建设的实施意见 教高〔2019〕8 号[EB/OL]. http://www.moe.gov.cn/srcsite/A08/s7056/201910/t20191031_406269.html, 2019-10-31.
- [2] 潘承洞, 潘承彪. 初等数论[M]. 第 3 版. 北京: 北京大学出版社, 2013.
- [3] Dénes, J. and Keedwell, A.D. (2015) Latin Squares and Their Applications. 2nd Edition, North-Holland.
- [4] Stinson, D.R. (2004) Combinatorial Designs: Constructions and Analysis. Springer.
- [5] Colbourn, C.J. and Dinitz, J.H. (2007) Handbook of Combinatorial Designs. 2nd Edition, Chapman and Hall/CRC. <https://doi.org/10.1201/9781420010541>
- [6] Euler, L. (1782) Recherches sur une nouvelle espèce de quarrés magiques. *Verhandelingen uitgegeven door het Zeeuwsch Genootschap der Wetenschappen te Vlissingen*, 9, 85-239.
- [7] 张蓉蓉, 刘兴祥. 构造拉丁方的初等变换法[J]. 应用数学进展, 2022, 11(1): 78-83.
- [8] Bose, R.C., Shrikhande, S.S. and Parker, E.T. (1960) Further Results on the Construction of Mutually Orthogonal Latin

Squares and the Falsity of Euler's Conjecture. *Canadian Journal of Mathematics*, **12**, 189-203.
<https://doi.org/10.4153/CJM-1960-016-5>

- [9] Hedayat, A.S., Sloane, N.J.A. and Stufken, J. (1999) *Orthogonal Arrays: Theory and Applications*. Springer.
<https://doi.org/10.1007/978-1-4612-1478-6>