10.1 LATIN SQUARES

A *Latin square* is a type of combinatorial design most easily described as an $n \times n$ array.

DEF: A ***Latin square*** on a set X of n objects is an $n \times n$ array such that each object in X occurs once in each row and once in each column.

Example 10.1.1: A Latin square on four graphic patterns is shown in Figure 10.1.1.

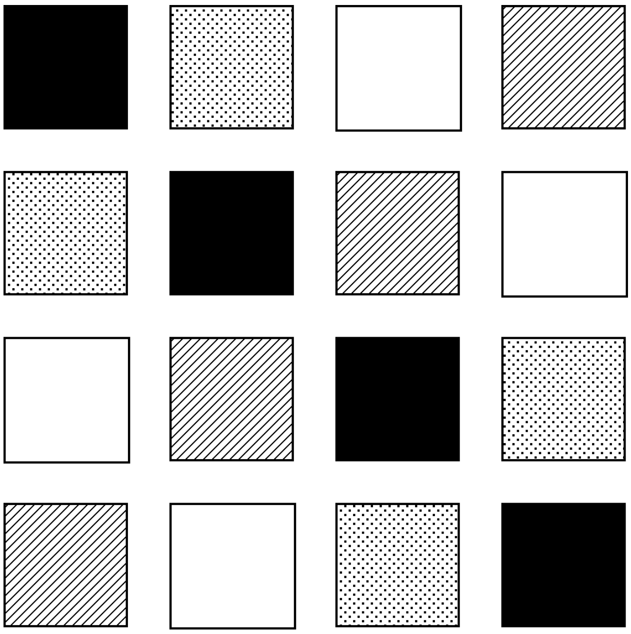

Fig 10.1.1 A 4×4 Latin square.

The standard symbols for an $n \times n$ Latin square are the integers modulo n. The rows and columns of a Latin square on $\mathbb{Z}_n$ are commonly indexed in $\mathbb{Z}_n$, so that there is a row

0 and a column 0. In particular, the following 4×4 Latin square on $\mathbb{Z}_4$ is obtainable from the Latin square of Figure 10.1.1 by a bijection of the symbol sets.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \tag{10.1.1}$$

Remark: A sudoku is a form of 9×9 Latin square on the numbers 1 to 9, with an additional requirement that each number occur exactly once in certain 3×3 sub-arrays.

It is easy enough to construct a Latin square of any given size.

Proposition 10.1.1. *For every positive integer n, there exists an $n \times n$ Latin square with $\mathbb{Z}_n$ as the set of objects.*

Proof: Let $L[i,j] = i + j$ modulo n. Thus,

$$L = \begin{pmatrix} 0 & 1 & 2 & \cdots & n-2 & n-1 \\ 1 & 2 & 3 & \cdots & n-1 & 0 \\ 2 & 3 & 4 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ n-2 & n-1 & 0 & \cdots & n-4 & n-3 \\ n-1 & 0 & 1 & \cdots & n-3 & n-2 \end{pmatrix}$$

Clearly the array L is a Latin square. $\diamondsuit$

Example 10.1.2: For $n = 4$, the construction of Proposition 10.1.1 yields the following Latin square.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \tag{10.1.2}$$

A *Latin square* can be recognized as a type of combinatorial design $\langle X, B \rangle$ with additional structure. The set B is ordered, corresponding to the order of the rows in the array. Each member $B_j \in B$ contains every object of X, is construed to be ordered, corresponding to the order of the elements of a row. Moreover, the number of subsets in B equals the number of objects in X, and for each object x and each possible position within a row, there is a unique row in which x occupies that position.

Product of Latin Squares

The next definition indicates a method of construction of a new Latin square, starting from two given Latin squares.

DEF: Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares on $\mathbb{Z}_r$ and $\mathbb{Z}_s$, respectively. Then the ***product square*** $A \otimes B$ is the Latin square on $\mathbb{Z}_r \times \mathbb{Z}_s$

$$A \otimes B = \begin{pmatrix} a_{00} \times B & a_{01} \times B & \cdots & a_{0(r-1)} \times B \\ a_{10} \times B & a_{11} \times B & \cdots & a_{1(r-1)} \times B \\ \vdots & \vdots & \cdots & \vdots \\ a_{(r-1)0} \times B & a_{01} \times B & \cdots & a_{(r-1)(r-1)} \times B \end{pmatrix}$$

where the $s \times s$ submatrix $a_{ij} \times B$ is given by

$$a_{ij} \times B = \begin{pmatrix} (a_{ij}, b_{00}) & (a_{ij}, b_{01}) & \cdots & (a_{ij}, b_{0(s-1)}) \\ (a_{ij}, b_{10}) & (a_{ij}, b_{11}) & \cdots & (a_{ij}, b_{1(s-1)}) \\ \vdots & \vdots & \cdots & \vdots \\ (a_{ij}, b_{(s-1)0}) & (a_{ij}, b_{(s-1)1}) & \cdots & (a_{ij}, b_{(s-1)(s-1)}) \end{pmatrix}$$

Proposition 10.1.2. *Let $A = (a_{ij})$ and $B = (b_{ij})$ be Latin squares on $\mathbb{Z}_r$ and $\mathbb{Z}_s$, respectively. Their product $A \otimes B$ is a Latin square.*

Proof: Since each row of A contains each number in $\mathbb{Z}_r$ and each row of B contains each number in $\mathbb{Z}_s$, it follows that each row of $A \otimes B$ contains each pair in $\mathbb{Z}_r \times \mathbb{Z}_s$. The same fact holds for the columns. ♢

Example 10.1.3: If

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

then

$$A \otimes B = \begin{pmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) \\ (0,1) & (0,2) & (0,0) & (1,1) & (1,2) & (1,0) \\ (0,2) & (0,0) & (0,1) & (1,2) & (1,0) & (1,1) \\ (1,0) & (1,1) & (1,2) & (0,0) & (0,1) & (0,2) \\ (1,1) & (1,2) & (1,0) & (0,1) & (0,2) & (0,0) \\ (1,2) & (1,0) & (1,1) & (0,2) & (0,0) & (0,1) \end{pmatrix}$$

which we observe is equivalent to the Latin square

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 0 & 4 & 5 & 3 \\ 2 & 0 & 1 & 5 & 3 & 4 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 4 & 5 & 3 & 1 & 2 & 0 \\ 5 & 3 & 4 & 2 & 0 & 1 \end{pmatrix}$$

under the bijection $\mathbb{Z}_2 \times \mathbb{Z}_3 \to \mathbb{Z}_6$ given by

$$\begin{array}{lll} (0,0) \mapsto 0 & (0,1) \mapsto 1 & (0,2) \mapsto 2 \\ (1,0) \mapsto 3 & (1,1) \mapsto 4 & (1,2) \mapsto 5 \end{array}$$

Orthogonal Latin Squares

DEF: Two $n \times n$ Latin squares $A = (a_{i,j})$ and $B = (b_{i,j})$ are ***orthogonal Latin squares*** if the n^2 ordered pairs $(a_{i,j},\, b_{i,j})$ are mutually distinct.

Remark: By the pigeonhole principle, two $n \times n$ Latin squares are orthogonal if each possible ordered pair of domain elements occurs.

Example 10.1.4: It is easy enough to construct the pair of orthogonal 4×4 Latin squares in Figure 10.1.2 by ad hoc methods. One Latin square is represented pictorially by the outer pattern in an array location, and the other Latin square by the inner pattern.

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$
outer

$$\begin{pmatrix} 3 & 0 & 1 & 2 \\ 2 & 1 & 0 & 3 \\ 0 & 3 & 2 & 1 \\ 1 & 2 & 3 & 0 \end{pmatrix}$$
inner

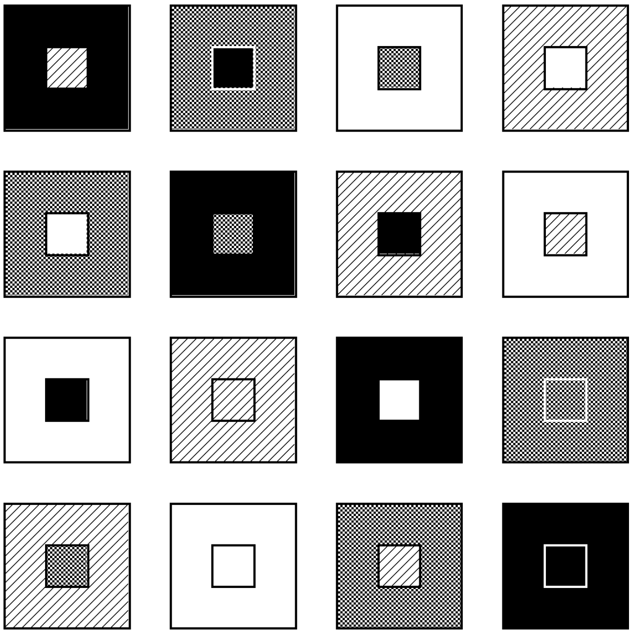

Fig 10.1.2 Two orthogonal Latin squares.

The next proposition indicates how to construct a family of mutually orthogonal Latin squares.

Proposition 10.1.3. *For $k = 1, \ldots, p-1$, where p is a prime number, let L_p^k be the $p \times p$ array such that*

$$L_p^k[i,j] \;=\; ki + j \bmod p \qquad 0 \le i, j \le p-1$$

Then the $p-1$ arrays

$$L_p^1, \quad L_p^2, \quad \ldots, \quad L_p^{p-1}$$

are mutually orthogonal Latin squares.

Proof: The entries in row i of the array L_p^k are

$$ki,\ ki+1,\ ki+2,\ \ldots,\ ki+(p-1)$$

which are clearly distinct. The entries in column j are

$$j,\ j+k,\ j+2k,\ \ldots,\ j+(p-1)k$$

Two of these entries differ by some number ck with $0 < c, k < p$. Since p is prime, $ck \not\equiv 0$ modulo p. Therefore, each of the arrays L_p^k is a Latin square.

Now suppose that the pairs of entries

$$\left(L_p^k[i,j],\ L_p^{k'}[i,j]\right) \quad \text{and} \quad \left(L_p^k[\hat{\imath},\hat{\jmath}],\ L_p^{k'}[\hat{\imath},\hat{\jmath}]\right)$$

are identical. Then

$$ki + j \;=\; k\hat{\imath} + \hat{\jmath} \tag{10.1.3}$$

and

$$k'i + j \;=\; k'\hat{\imath} + \hat{\jmath} \tag{10.1.4}$$

If $i \neq \hat{\imath}$, then $i - \hat{\imath}$ has a multiplicative inverse in $\mathbb{Z}_p$ (see Corollary 6.4.2). Hence,

$$k \;=\; \frac{\hat{\jmath} - j}{i - \hat{\imath}} \qquad \text{from (10.1.3)}$$

and

$$k' \;=\; \frac{\hat{\jmath} - j}{i - \hat{\imath}} \qquad \text{from (10.1.4)}$$

Therefore, $k = k'$. ♢

Example 10.1.5: The arrays L_5^2 and L_5^3 of Proposition 10.1.3 are orthogonal.

$$L_5^2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix} \quad L_5^3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$$

Remark: If p is not a prime, then L_p^k might not be a Latin square. For instance, row 2 of the array L_6^3 is identical to row 0.

Theorem 10.1.4 [MacNeish, 1922]. *Let*

$$A^{(1)},\ A^{(2)},\ \ldots,\ A^{(r)}$$

be r mutually orthogonal $m \times m$ Latin squares, and let

$$B^{(1)},\ B^{(2)},\ \ldots,\ B^{(r)}$$

be r mutually orthogonal $n \times n$ Latin squares. Then the Latin squares

$$A^{(1)} \otimes B^{(1)},\ A^{(2)} \otimes B^{(2)},\ \cdots,\ A^{(r)} \otimes B^{(r)}$$

are mutually orthogonal.

Proof: Suppose that the pair of entries at location $ij \times k\ell$ of the Latin square $A^{(x)} \times B^{(x)}$ and of the Latin square $A^{(y)} \times B^{(y)}$, i.e.,

$$(a_{ij}^{(x)}, b_{k\ell}^{(x)}) \quad \text{and} \quad (a_{ij}^{(y)}, b_{k\ell}^{(y)})$$

is the same as the pair in location $pq \times uv$ of those two Latin squares, i.e., as the pair

$$(a_{pq}^{(x)}, b_{uv}^{(x)}) \quad \text{and} \quad (a_{pq}^{(y)}, b_{uv}^{(y)})$$

Then the pairs

$$(a_{ij}^{(x)}, a_{ij}^{(y)}) \quad \text{and} \quad (a_{pq}^{(x)}, a_{pq}^{(y)})$$

are identical, which implies, since $A^{(x)}$ and $A^{(y)}$ are orthogonal, that

$$i = p \quad \text{and} \quad j = q$$

Similarly,

$$k = u \quad \text{and} \quad \ell = v$$

Therefore, $A^{(x)} \times B^{(x)}$ and $A^{(y)} \times B^{(y)}$ are orthogonal. ♢

Proposition 10.1.5. *For every odd number $n > 1$, there is a pair of orthogonal $n \times n$ Latin squares.*

Proof: This follows from Proposition 10.1.3 and Theorem 10.1.4, since every odd number factors into a product of odd primes. ♢

Proposition 10.1.6. *Let $n = 2^k$ with $k \geq 2$. Then there is a pair of orthogonal $n \times n$ Latin squares.*

Proof: Example 10.1.4 gives a pair of orthogonal 4×4 Latin squares. The following is a pair of orthogonal 8×8

Latin squares.

$$\begin{pmatrix} 0&1&2&3&4&5&6&7\\ 1&0&3&2&5&4&7&6\\ 2&3&0&1&6&7&4&5\\ 3&2&1&0&7&6&5&4\\ 4&5&6&7&0&1&2&3\\ 5&4&7&6&1&0&3&2\\ 6&7&4&5&2&3&0&1\\ 7&6&5&4&3&2&1&0 \end{pmatrix} \qquad \begin{pmatrix} 0&1&2&3&4&5&6&7\\ 7&6&5&4&3&2&1&0\\ 3&2&1&0&7&6&5&4\\ 4&5&6&7&0&1&2&3\\ 6&7&4&5&2&3&0&1\\ 1&0&3&2&5&4&7&6\\ 5&4&7&6&1&0&3&2\\ 2&3&0&1&6&7&4&5 \end{pmatrix}$$

If k is even, then n is a power of 4, and if k is odd, then n is a product of 8 with a power of 4. It follows from the base cases 4×4 and 8×8 and Theorem 10.1.4 that there is a pair of orthogonal $n \times n$ Latin squares. $\diamondsuit$

There are only two possible 2×2 Latin squares in $\mathbb{Z}_2$, and they are not orthogonal. Euler conjectured in 1782 that for n odd, there is no orthogonal pair of $2n \times 2n$ Latin squares. In 1901, Gaston Tarry [Tarr1901] proved by exhaustion that there is no 6×6 pair. However, Ernest Parker [Park1959] produced a 10×10 pair in 1960, and then Bose, Shrikhande, and Parker [BSP1960] proved that there is a $2n \times 2n$ orthogonal pair except for $n = 1$ or 3.

Summary. *For every positive integer n except 1, 2, and 6, there is a pair of orthogonal $n \times n$ Latin squares.*

Isotopic Latin Squares

DEF: The Latin squares $L[i, j]$ and $L'[i, j]$ on $\mathbb{Z}_n$ are ***isotopic Latin squares*** if L' can be obtained from L by a sequence of transformations, each chosen from any of the following three types.

- A permutation of the rows.
- A permutation of the columns.
- Applying a permutation $\sigma : \mathbb{Z}_n \to \mathbb{Z}_n$ to the symbols of the array.

Example 10.1.6: Swapping rows 0 and 1 of the Latin square

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \tag{10.1.2}$$

yields the Latin square

$$\begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

Example 10.1.7: Swapping the symbols 0 and 1 in the Latin square (10.1.2) yields this Latin square.

$$\begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 2 & 3 & 1 & 0 \\ 3 & 1 & 0 & 2 \end{pmatrix}$$

Remark: Clearly, isotopy on Latin squares is an equivalence relation.

DEF: A Latin square on $\mathbb{Z}_n$ is said to be ***normalized*** if its initial row is

$$0 \quad 1 \quad \cdots \quad n-1$$

and its initial column is

$$\begin{array}{c} 0 \\ 1 \\ \vdots \\ n-1 \end{array}$$

Clearly, every Latin square is isotopic to a normalized Latin square.

Abstract Latin Squares

Isotopy allows three natural kinds of transformation on Latin squares that may be regarded as natural equivalences. The following alternative conceptualization of a Latin square allows some additional equivalences.

DEF: An ***abstract Latin square*** on $\mathbb{Z}_n$ is a set L of triples

$$(r,\ c,\ s)$$

in $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ such that

- For any $(i, j) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $i = r$ and $j = c$.
- For any $(i, k) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $i = r$ and $k = s$.
- For any $(j, k) \in \mathbb{Z}_n \times \mathbb{Z}_n$ there is a unique triple $(r,\ c,\ s)$ in L such that $j = c$ and $k = s$.

Proposition 10.1.7. *Every abstract Latin square corresponds to a unique concrete Latin square (i.e., the array form). Conversely, for every concrete Latin square, there is a unique abstract Latin square.* $\diamondsuit$

We observe that the operation of transposition on the array form of a Latin square has as its abstract counterpart the operation of swapping the first and second entry in each triple. Yet from the abstract perspective, we could equally well swap the first and third entry of each triple. Indeed, we equally apply any of the six possible permutations uniformly to all the triples. This motivates the following definition.

DEF: Let π be a permutation on the set $\{1,\ 2,\ 3\}$. The operation of transforming a Latin square by applying π to the coordinates of the triples is called a ***conjugacy operation.*** The array resulting from applying π to a Latin square L is called the π-***conjugate*** of L. It may be denoted L^π.

Example 10.1.8: Consider the following Latin square in array and abstract form.

$$L = \begin{pmatrix} 0 & 3 & 1 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} \qquad \begin{matrix} (0,0,0) & (0,1,3) & (0,2,1) & (0,3,2) \\ (1,0,1) & (1,1,2) & (1,2,0) & (1,3,3) \\ (2,0,3) & (2,1,0) & (2,2,2) & (2,3,1) \\ (3,0,2) & (3,1,1) & (3,2,3) & (3,3,0) \end{matrix}$$

Applying the permutation $(1,2)(3)$ to the set of triples means swapping the first and second coordinates of each triple, thereby obtaining

$$\begin{matrix} (0,0,0) & (1,0,3) & (2,0,1) & (3,0,2) \\ (0,1,1) & (1,1,2) & (2,1,0) & (3,1,3) \\ (0,2,3) & (1,2,0) & (2,2,2) & (3,2,1) \\ (0,3,2) & (1,3,1) & (2,3,3) & (3,3,0) \end{matrix}$$

which is the abstract form of the Latin square

$$L^{(1,2)(3)} = \begin{pmatrix} 0 & 1 & 3 & 2 \\ 3 & 2 & 0 & 1 \\ 1 & 0 & 2 & 3 \\ 2 & 3 & 1 & 0 \end{pmatrix}$$

Observing that $L^{(1,2)(3)}$ is simply the transpose of L, we recognize that the transformation $L \mapsto L^{(1,2)(3)}$ simply swaps the roles of rows and columns.

Alternatively, applying the permutation $(1,3)(2)$ to the set of triples means swapping the first and third coordinates of each triple, thereby obtaining

$$\begin{matrix} (0,0,0) & (3,1,0) & (1,2,0) & (2,3,0) \\ (1,0,1) & (2,1,1) & (0,2,1) & (3,3,1) \\ (3,0,2) & (0,1,2) & (2,2,2) & (1,3,2) \\ (2,0,3) & (1,1,3) & (3,2,3) & (0,3,3) \end{matrix}$$

which is the abstract form of the Latin square

$$L^{(1,3)(2)} = \begin{pmatrix} 0 & 2 & 1 & 3 \\ 1 & 3 & 0 & 2 \\ 3 & 1 & 2 & 0 \\ 2 & 0 & 3 & 1 \end{pmatrix}$$

Remark 1: We observe that conjugacy is an equivalence relation on the Latin squares. The possible class sizes are 1, 2, 3, and 6.

Remark 2: For $n \leq 5$, the conjugacy operations on a Latin square produce only Latin squares that could be obtained by isotopy operations. However, for $n \geq 6$, they produce additional Latin squares.

DEF: Two Latin squares L and L' are ***main class isotopic*** if L is isotopic to any conjugate of L'.