Chapter 3

Latin squares

1. Definition and existence

Let us consider the following problem posed by Euler in 1779.

The thirty six officers problem. There are six regiments, each having six officers, one of each of six possible ranks. Is it possible to parade these thirty six officers in a six by six pattern, so that every row and every column contain exactly one officer of each rank and exactly one member of each regiment?

Euler conjectured that the answer was negative. This was finally proved by Tarry in 1900 by a systematic examination of all possibilities. Today this can be done relatively easily using computers.

Let us consider the first condition in the problem: every row and every column should contain exactly one officer of each rank. Denote the ranks by 1, 2, 3, 4, 5, 6, and replace the officers by their ranks. We obtain a 6×6 array of numbers $\{1, 2, 3, 4, 5, 6\}$, such that every row and every column of the array contain each number exactly once.

Definition 1.1. A *Latin square* of order n is an $n \times n$ array of numbers $\{1, 2, \ldots, n\}$ (or some other n symbols) in which every row and every column contains each number exactly once.

Do Latin squares exist? What are the possible orders of Latin squares? The following theorem answers these questions.

Theorem 1.2. *Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group of order n. The multiplication table for G is a Latin square. In particular, for each n there exists a Latin square of order n.*

Proof. We prove that an arbitrary row, corresponding to the element g_i, contains an arbitrary element g_k. The proof for columns is similar. Let $g_j = g_i^{-1} g_k$. Then the (g_i, g_j) entry in the table is $g_i g_j = g_i g_i^{-1} g_k = g_k$.

The second statement follows from the first and the fact that for every n there exists a group of order n (e.g. $\mathbb{Z}_n$). ■

2. Counting Latin squares

In this section we will prove that there are 'many' Latin squares of order n. To do this, we need to make a significant detour.

Let $A_1, \ldots, A_n$ be sets. A *system of distinct representatives* (SDR for short) for these sets is an n-tuple $(x_1, \ldots, x_n)$ of elements with the properties:

- $x_i \in A_i$ for $i = 1, \ldots, n$ (so that x_i is a representative of A_i);
- $x_i \neq x_j$ for $i \neq j$ (so that all representatives are distinct).

A system of distinct representatives therefore contains one element from each set A_i with $1 \leq i \leq n$, and these elements are all different.

Example 2.1. Let $A_1 := \{1, 2, 3, 4\}$, $A_2 := \{2, 4, 7\}$, and $A_3 := \{3, 4, 7\}$. There are many different SDRs for these three sets. Some are:

$$(1, 2, 3), (1, 2, 4), (1, 2, 7), (1, 4, 3), (1, 4, 7), (1, 7, 3), (1, 7, 4).$$

Theorem 2.2. *Let $(A_1, \ldots, A_n)$ be finite sets of size at least r satisfying*

$$|\bigcup_{j \in J} A_j| \geq |J| \text{ for all } J \subseteq \{1, \ldots, n\}. \qquad (*)$$

The number of SDRs for this family is at least

$$\begin{cases} r! & \text{if } r \leq n \\ r(r-1)\ldots(r-n+1) & \text{if } r > n. \end{cases}$$

Proof. Omitted. This is a version of Hall's Marriage Theorem, which is proved in MT4514 Graph Theory. ■

Theorem 2.3. *Let $(A_1, \ldots, A_n)$ be a family of subsets of $\{1, \ldots, n\}$, and let $r \leq n$. If each of the sets A_i has size r and if each element of $\{1, \ldots, n\}$ is contained in exactly r sets, then the family $(A_1, \ldots, A_n)$ has at least $r!$ SDRs.*

Proof. We prove that $(A_1, \ldots, A_n)$ satisfies $(*)$; the result then follows from Theorem 2.2.

For an arbitrary $J \subseteq \{1, \ldots, n\}$ we count in two different ways the number of pairs (j, x) where $j \in J$ and $x \in A_j$. There are $|J|$ choices for j, and, having chosen j, there are $|A_j| = r$ choices for x. So there are precisely $r|J|$ such pairs. On the other hand, there are $| \cup_{j \in J} A_j|$ choices for x, and, having chosen x, there are at most r possible choices for j, since x lies in precisely r sets. We conclude that $r|J| \leq r| \cup_{j \in J} A_j|$, implying $(*)$, as required. ■

Let us now return to our problem of counting Latin squares. The idea is to build a Latin square row by row, and to count how many choices for adding each new row we have. To this end we introduce a notion of a *Latin rectangle*: it is a $k \times n$ array (with $k \leq n$) with entries from $\{1, \ldots, n\}$ such that each entry occurs precisely once in each row and at most once in each column.

Lemma 2.4. *Given a $k \times n$ Latin rectangle with $k < n$, there are at least $(n-k)!$ ways to add a row to form a $(k+1) \times n$ Latin rectangle.*

Proof. Let A_i be the set of all entries *not* appearing in the ith column. We see that $(x_1, \ldots, x_n)$ is a possible $(k+1)$st row if and only if $x_i \in A_i$ and $x_i \neq x_j$ for $i \neq j$, i.e. if and only if $(x_1, \ldots, x_n)$ is an SDR for $(A_1, \ldots, A_n)$.

Now, clearly each set A_i has size $n - k$. Also, a fixed entry x appears precisely k times (once in each row), and so it belongs to precisely $n - k$ sets. The conditions of Theorem 2.3 are fulfilled for $r = n - k$, and the lemma follows. ■

Theorem 2.5. *The number of Latin squares of order n is at least $n!(n-1)! \ldots 2!1!$.*

Proof. There are $n!$ choices for the first row; having chosen it, there are at least $(n-1)!$ choices for the second row, etc. ■

3. Orthogonality

Let us analyse the thirty six officers problem in more detail. We have already considered the ranks of the officers. The second requirement is that every row and every column contain one officer from each regiment. So if we denote each regiment by 1, 2, 3, 4, 5, 6, and replace each officer by the number of its regiment we obtain another Latin square. Thus we have two Latin squares: L_1 representing the ranks and L_2 representing the regiments. These two Latin squares are related by the condition that every regiment has one officer of each rank.

Let us put the square L_2 over L_1, so that in each cell we can see a pair of numbers. Now, it cannot happen that a pair (i, j) occurs twice, as it would mean that the regiment j has two officers of rank i. Since there are 36 cells and 36 pairs of numbers $\{1, 2, 3, 4, 5, 6\}$, we conclude that each pair must occur exactly once.

Definition 3.1. Two Latin squares $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times n}$ are *orthogonal* if the set $\{(a_{ij}, b_{ij}) : 1 \le i, j \le n\}$ contains all possible pairs.

Example 3.2. The following two Latin squares are orthogonal:

$$\boxed{\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}}\;\boxed{\begin{array}{cccc} 1 & 4 & 3 & 2 \\ 3 & 2 & 1 & 4 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \end{array}}$$

One may ask for which values of n there exist orthogonal squares of order n? It is clear that they do not exist for $n = 2$. Also, Tarry's solution to the thirty six officers problem means that there are no orthogonal Latin squares of order 6. On the other hand we shall prove in Section 5 that if $n \not\equiv 2 \pmod 4$ then there exist orthogonal Latin squares of order n. Euler conjectured that the converse was also true: if $n \equiv 2 \pmod 4$ then orthogonal squares of order n do not exist. However, he was wrong: Bose, Shrikhande and Parker proved in 1960 that for every n, except for $n = 2$ and $n = 6$, orthogonal squares exist.

Another interesting question that one may ask is the following.

Question 3.3. What is the maximal number of mutually orthogonal Latin squares of order n? (Latin squares $A_1, A_2, \ldots, A_k$ are *mutually orthogonal* if each pair A_i and A_j are orthogonal.)

The following notion will be useful in considering the above question.

Definition 3.4. A Latin square $A = (a_{ij})_{n\times n}$ is in *standard form* if its first row is $123\ldots n$.

It is clear that every Latin square A can be *standardised* by reordering the symbols in it; we denote the resulting square by A^*.

Example 3.5. The first square A in Example 3.2 is in standard form. The second square B in the same example has standardisation

$$B^* = \boxed{\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{array}}$$

Note that A and B^* are orthogonal.

Lemma 3.6. *If A and B are orthogonal Latin squares, then so are A^* and B^*.*

Proof. Let $A = (a_{ij})_{n\times n}$ and $B = (b_{ij})_{n\times n}$. Standardisation of A is achieved by means of a permutation σ of the set $\{1, 2, \dots, n\}$, so that $A^* = (\sigma(a_{ij}))_{n\times n}$. Similarly, we have $B^* = (\tau(b_{ij}))_{n\times n}$ for some other permutation τ. Assume that A^* and B^* are not orthogonal. This means that among the pairs $(\sigma(a_{ij}), \tau(b_{ij}))$ $(1 \le i, j \le n)$ at least one pair occurs twice. Thus we have

$$(\sigma(a_{ij}), \tau(b_{ij})) = (\sigma(a_{kl}), \tau(b_{kl})),$$

for some i, j, k, l. Since σ and τ are permutations, this implies $a_{ij} = a_{kl}$ and $b_{ij} = b_{kl}$, which contradicts the fact that A and B are orthogonal. ■

The following theorem gives an upper bound for the maximal number of mutually orthogonal Latin squares of order n.

Theorem 3.7. *If $A_1, A_2, \dots, A_m$ are mutually orthogonal Latin squares of order n then $m \le n - 1$.*

Proof. Let $A_k = (a_{ij}^{(k)})_{n\times n}$. By Lemma 3.6 we may assume that all $A_1, \dots, A_m$ are in standard form (otherwise we standardise them, without affecting orthogonality), i.e.

$$a_{1j}^{(k)} = j.$$

Consider the set

$$S = \{(i, j, k) \ : \ a_{ij}^{(k)} = 1\}.$$

Clearly, the number of elements of S is equal to the total number of 1's in $A_1, \dots, A_m$, so that

$$|S| = nm. \tag{3.1}$$

Consider a triple $(i, j, k) \in S$. Each of the squares has 1 in the position $(1, 1)$. Hence, if $i = j = 1$ then k can be arbitrary. Also, no other entry in the position $(1, j)$ or $(i, 1)$ can be 1, so that we cannot have one of i and j being equal to 1 and the other one not. Finally, if $i \ne 1$ and $j \ne 1$ then, because of orthogonality, there may exist at most one k such that $(i, j, k) \in S$. We conclude that

$$|S| \le m + (n - 1)^2. \tag{3.2}$$

Combining (3.1) and (3.2) we obtain $m \le n - 1$, as required. ■

4. Latin squares from finite fields

Theorem 3.7 gives no indication about the sharpness of the given bound. Here we show that for infinitely many n there are sets of $n - 1$ mutually orthogonal Latin squares, namely whenever n is a prime power. To do so we introduce a method of constructing orthogonal Latin squares from finite fields.

Theorem 4.1. *If $n = p^t$, where p is a prime and $t \ge 1$, then there exist $n - 1$ mutually orthogonal Latin squares of order n.*

Proof. By the Fundamental Theorem for Finite Fields (Theorem 2.5 in Chapter 1) there exists a finite field $F = \{f_1, f_2, \dots, f_n = 0\}$ of order n. Define $n - 1$ arrays $A_k = (a_{ij}^{(k)})_{n\times n}$, $1 \le k \le n - 1$, with elements from F by setting

$$a_{ij}^{(k)} = f_i f_k + f_j.$$

First we prove that each A_k is a Latin square. Assume that two elements $a^{(k)}_{ij_1}$ and $a^{(k)}_{ij_2}$ in the ith row are equal. This means that

$$f_i f_k + f_{j_1} = f_i f_k + f_{j_2},$$

so that $f_{j_1} = f_{j_2}$, and hence $j_1 = j_2$. Similarly, if $a^{(k)}_{i_1 j} = a^{(k)}_{i_2 j}$, we have

$$f_{i_1} f_k + f_j = f_{i_2} f_k + f_j \Rightarrow f_{i_1} f_k = f_{i_2} f_k \Rightarrow f_{i_1} = f_{i_2} \Rightarrow i_1 = i_2,$$

since F is a field and $f_k \neq 0$.

We complete the proof by showing that A_k and A_l are orthogonal for arbitrary k, l, with $k \neq l$. Assume that they are not; this means that

$$(a^{(k)}_{i_1 j_1}, a^{(l)}_{i_1 j_1}) = (a^{(k)}_{i_2 j_2}, a^{(l)}_{i_2 j_2}),$$

for some i_1, i_2, j_1, j_2, yielding the system

$$f_{i_1} f_k + f_{j_1} = f_{i_2} f_k + f_{j_2} \tag{3.3}$$
$$f_{i_1} f_l + f_{j_1} = f_{i_2} f_l + f_{j_2}. \tag{3.4}$$

Subtracting (3.4) from (3.3) we obtain

$$f_{i_1}(f_k - f_l) = f_{i_2}(f_k - f_l).$$

Since $k \neq l$, we have $f_k - f_l \neq 0$, so that $f_{i_1} = f_{i_2}$ and hence $i_1 = i_2$. Substituting $f_{i_1} = f_{i_2}$ back into (3.3) we obtain $f_{j_1} = f_{j_2}$, and hence $j_1 = j_2$. Therefore, A_k and A_l are orthogonal. ■

Example 4.2. Let us use the finite field $\mathbb{Z}_5$ to construct 4 mutually orthogonal Latin squares of order 5. First, we let

$$f_1 = 1,\ f_2 = 2,\ f_3 = 3,\ f_4 = 4,\ f_5 = 0.$$

The first Latin square $A_1 = (a^{(1)}_{ij})_{5\times 5}$ is given by $a^{(1)}_{ij} = f_i + f_j$:

		j	1	2	3	4	5
i	f_i	f_j	1	2	3	4	0
1	1		2	3	4	0	1
2	2		3	4	0	1	2
3	3		4	0	1	2	3
4	4		0	1	2	3	4
5	0		1	2	3	4	0

Similarly, the second Latin square $A_2 = (a^{(2)}_{ij})_{5\times 5}$ is given by $a^{(2)}_{ij} = 2f_i + f_j$:

			j	1	2	3	4	5
i	f_i	$2f_i$	f_j	1	2	3	4	0
1	1	2		3	4	0	1	2
2	2	4		0	1	2	3	4
3	3	1		2	3	4	0	1
4	4	3		4	0	1	2	3
5	0	0		1	2	3	4	0

Repeating similar calculations for A_3 and A_4 we obtain the squares:

$$A_1 = \begin{array}{|ccccc|}\hline 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ \hline \end{array}, \quad A_2 = \begin{array}{|ccccc|}\hline 3 & 4 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ \hline \end{array}$$

$$A_3 = \begin{array}{|ccccc|}\hline 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ \hline \end{array}, \quad A_4 = \begin{array}{|ccccc|}\hline 0 & 1 & 2 & 3 & 4 \\ 4 & 0 & 1 & 2 & 3 \\ 3 & 4 & 0 & 1 & 2 \\ 2 & 3 & 4 & 0 & 1 \\ 1 & 2 & 3 & 4 & 0 \\ \hline \end{array}$$

At present it is not known whether the converse of Theorem 4.1 holds, i.e. whether from the existence of $n-1$ mutually orthogonal squares of order n it follows that n is a prime power.

5. Direct products

Direct products are a means of constructing new Latin squares from existing ones.

Definition 5.1. Let $A = (a_{ij})_{m\times m}$ and $B = (b_{ij})_{n\times n}$ be two Latin squares. Their *direct product* $C = A \times B$ is an $mn \times mn$ array, indexed by the elements of $\{1,\dots,m\} \times \{1,\dots,n\}$ and entries

$$c_{(i,j),(k,l)} = (a_{ik}, b_{jl}).$$

Theorem 5.2. *The direct product of two Latin squares is again a Latin square.*

Proof. Let $A = (a_{ij})_{m\times m}$ and $B = (b_{ij})_{n\times n}$ be two Latin squares, and let C be their direct product. Assume that in the row indexed by (i,j) we have two identical entries:

$$c_{(i,j),(k_1,l_1)} = c_{(i,j),(k_2,l_2)}.$$

This means that

$$a_{ik_1} = a_{ik_2},\ b_{jl_1} = b_{jl_2}.$$

Since A and B are Latin squares we have $k_1 = k_2$ and $l_1 = l_2$. The proof for the columns is analogous. ■

Example 5.3. Consider the following two Latin squares

$$\begin{array}{|cc|}\hline 1 & 2 \\ 2 & 1 \\ \hline \end{array} \quad \begin{array}{|ccc|}\hline 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \\ \hline \end{array}$$

Their direct product, according to the definition, is

	$(1,1)$	$(1,2)$	$(1,3)$	$(2,1)$	$(2,2)$	$(2,3)$
$(1,1)$	$(1,2)$	$(1,3)$	$(1,1)$	$(2,2)$	$(2,3)$	$(2,1)$
$(1,2)$	$(1,3)$	$(1,1)$	$(1,2)$	$(2,3)$	$(2,1)$	$(2,2)$
$(1,3)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,1)$	$(2,2)$	$(2,3)$
$(2,1)$	$(2,2)$	$(2,3)$	$(2,1)$	$(1,2)$	$(1,3)$	$(1,1)$
$(2,2)$	$(2,3)$	$(2,1)$	$(2,2)$	$(1,3)$	$(1,1)$	$(1,2)$
$(2,3)$	$(2,1)$	$(2,2)$	$(2,3)$	$(1,1)$	$(1,2)$	$(1,3)$

After renumbering this becomes

2	3	1	5	6	4
3	1	2	6	4	5
1	2	3	4	5	6
5	6	4	2	3	1
6	4	5	3	1	2
4	5	6	1	2	3

The above example suggests an alternative way of constructing the direct product of two Latin squares $A = (a_{ij})_{m\times m}$ and $B = (b_{ij})_{n\times n}$. We let $B_1, B_2, \ldots, B_m$ be copies of B, each with its own set of symbols. Then we replace the entries of A by the corresponding B_i's. In other words we form the array $(B_{a_{ij}})_{m\times m}$, and this array is the direct product of A and B.

Next we prove that direct products preserve orthogonality.

Theorem 5.4. *If A and B are orthogonal Latin squares of order m, and if C and D are orthogonal Latin squares of order n, then $A\times C$ and $B\times D$ are also orthogonal Latin squares.*

Proof. Let $A = (a_{ij})_{m\times m}$, $B = (b_{ij})_{m\times m}$, $C = (c_{ij})_{n\times n}$, $D = (d_{ij})_{n\times n}$, $X = A \times C$, $Y = B \times D$. Assume that X and Y are not orthogonal. This means that

$$\begin{aligned} x_{(i_1,j_1),(k_1,l_1)} &= x_{(i_2,j_2),(k_2,l_2)}, \\ y_{(i_1,j_1),(k_1,l_1)} &= y_{(i_2,j_2),(k_2,l_2)}, \end{aligned}$$

for some $i_1, i_2, j_1, j_2, k_1, k_2, l_1, l_2$. From the definition of the direct product we have

$$a_{i_1k_1} = a_{i_2k_2} \tag{3.5}$$

$$c_{j_1l_1} = c_{j_2l_2} \tag{3.6}$$

$$b_{i_1k_1} = b_{i_2k_2} \tag{3.7}$$

$$d_{j_1l_1} = d_{j_2l_2}. \tag{3.8}$$

From (3.5), (3.7) and the fact that A and B are orthogonal we deduce that $i_1 = i_2$ and $k_1 = k_2$. Similarly, from the other two equations and the orthogonality of C and D we deduce that $j_1 = j_2$ and $l_1 = l_2$. ■

Corollary 5.5. *If $n \not\equiv 2 \pmod 4$ then there exists a pair of orthogonal Latin squares of order n.*

Proof. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be the decomposition of n into a product of primes, with $p_1 < p_2 < \ldots < p_k$. Since $n \not\equiv 2 \pmod 4$ it follows that if n is odd then $p_1^{\alpha_1} \geq 3$ and if n is even then $p_1^{\alpha_1} \geq 4$. Thus in either case $p_1^{\alpha_1} > 2$, and so $p_i^{\alpha_i} > 2$ for every i. By Theorem 4.1, for each i $(1 \leq i \leq k)$ there exists a pair A_i, B_i of orthogonal Latin squares of order $p_i^{\alpha_i}$. But then the Latin squares $A = A_1 \times \ldots \times A_k$ and $B = B_1 \times \ldots \times B_k$ are orthogonal by Theorem 5.4 and have order n. ■