

Problem There are six persons to test six different drugs.

How can we arrange the test if each person is going to take exactly one drug per day and all six drugs.

Name $\rightarrow$	Day $\downarrow$					
	M	Tue	W	Thr	F	S
A	α	β	γ	δ	ϵ	τ
B	β	γ	δ	ϵ	τ	α
C	γ	δ	ϵ	τ	α	β
D	δ	ϵ	τ	α	β	γ
E	ϵ	τ	α	β	γ	δ
F	τ	α	β	γ	δ	ϵ

Drugs are:

$\alpha, \beta, \gamma, \delta, \epsilon, \tau$

One arrangement

① 当然也可以每天大家都吃相同的药。

② What's the difference?

③ 上述的设计最早用于农作物的种植: Agriculture experiments

$\alpha \beta$
 $\alpha \beta$
 $\alpha \beta \dots$
 $\alpha \beta$
 $\alpha \beta$
 $\alpha \beta$

Definition (Latin square)

A Latin square L of order n based on an n -set S is an $n \times n$ array such that each element of S occurs exactly once in each row and each column respectively.

For convenience, we use $\mathbb{Z}_n$ for the n -set S . So, the following array is a Latin square of order 3.

0	1	2
1	2	0
2	0	1

(*) If we add side line and head line together with an operation " $\cdot$ ", then we have a multiplication table of an algebraic structure : $\langle \mathbb{Z}_3, \cdot \rangle$.

$\cdot$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

(*) Clearly, $\cdot$ is a binary operation. Since each row and each row are filled with different entries, $\langle \mathbb{Z}_3, \cdot \rangle$ also satisfies the followings

$$(1) \left\{ \begin{array}{l} a \cdot x = b \\ y \cdot a = b \end{array} \right. \text{ have unique solution resp. } \forall a, b \in \mathbb{Z}_3.$$

Definition (Quasigroup)

An algebraic structure $\langle S, \cdot \rangle$ is a quasigroup if for any $a, b \in S$, both $a \cdot x = b$ and $y \cdot a = b$ have unique solution.

(..) Clearly, the conditions hold for a group. Hence, a group is also a quasigroup.

(...) So, what's the difference between a quasigroup and a group?

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

Quasigroup, Not group.

$$(1 * 1) * 2 = 0 * 2 = 2$$

$$1 * (1 * 2) = 1 * 1 = 0$$

類似群的運算不一定有結合律 (Associative Law)

Important fact

The Cayley table of a quasigroup $\langle S, * \rangle$ is a Latin square of order $|S|$. For Latin square, we only consider $|S| < +\infty$, but not a quasigroup.

Problem What's the number of different Latin squares of order n ? L_n

Partial solutions

Standard form

0	1	2	...	$n-1$
1				
2				
$\vdots$				
$n-1$				

$$L_1 = 1$$

$$L_2 = 2$$

$$L_3 = 12 = 3! \cdot 2! \cdot 1$$

$$L_4 = 576 = 4! \cdot 3! \cdot l_4, \quad l_4 = 4$$

$\vdots$

$$L_6 = 9,408$$

$$L_{10} = 7,580,721,483,140,132,811,489,280.$$

$$L_{15} \approx 1.5 \cdot 10^{86}$$

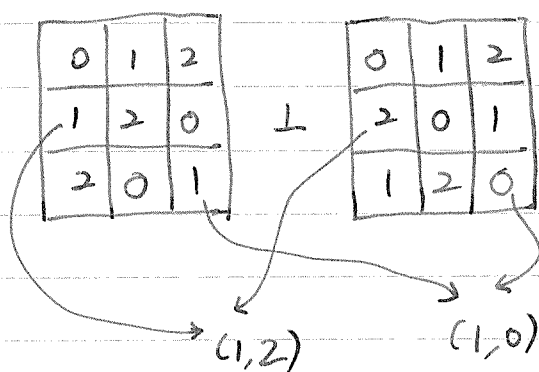
(*) Sudoku is a special Latin square!

First published paper about Latin squares

Definition (Orthogonal Latin squares)

Two Latin squares of order n , $L = [l_{ij}]$ and $M = [m_{ij}]$, are orthogonal (垂直) if $\{(l_{ij}, m_{ij}) \mid i, j \in \mathbb{Z}_n\} = \mathbb{Z}_n^2$.

e.g.



Lemma Let L and M be two orthogonal Latin squares of order n . Then, $\forall i, j; i', j'$, if $l_{ij} = l_{i'j'}$, then $m_{ij} \neq m_{i'j'}$. (Two finger's rule!)

Proof. By definition.

Problem Can we place 16 court cards of Bridge inside a 4×4 grid such that each row, column and diagonal contain exactly one card of each suit and one card of each rank?

A_S	K_H	Q_D	J_C
Q_C	J_D	A_H	K_S
J_H	Q_S	K_C	A_D
K_D	A_C	J_S	Q_H

S: Spade

H: Heart

D: Diamond

C: Club

Jacques Ozanam (1725)Euler's Six-Officers problem
 $1_1 \quad 2_2 \quad 3_3 \quad 4_4 \quad 5_5 \quad 6_6$







(*) 每行每列都有來自六個不同兵種, 六個不同階級的
軍官。(一共有六個兵種, 六個階級)

橋牌問題能夠解決是因為我們可以找到兩個互相垂直的對角拉丁方陣 (Diagonal Latin square).

↓
Each element of $\mathbb{Z}_n$ occurs in the main diagonal.

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

A, K, Q, J.

0	1	2	3
3	2	1	0
1	0	3	2
2	3	0	1

花色 S, H, D, C.

(*) Euler's problem is equivalent to find two orthogonal Latin squares of order 6. (Not possible!)

(***) So, the search of orthogonal squares starts!

Example

Construct 4 mutually orthogonal Latin squares of order 5.

Use the idea of "Finite Fields".

Consider

$$\langle \mathbb{Z}_5, + \rangle \text{ and } \langle \mathbb{Z}_5^*, \cdot \rangle$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

L_1

$l_{i,j} = i + j$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

L_2

0 1 2 3 4

0	0	2	4	1	3
1	1	3	0	2	4
2	2	4	1	3	0
3	3	0	2	4	1
4	4	1	3	0	2

L_3

$l_{i,j} = i + 3j$

	0	1	2	3	4
0	0	3	1	4	2
1	1	4	2	0	3
2	2	0	3	1	4
3	3	1	4	2	0
4	4	2	0	3	1

L_4

$l_{i,j} = i + 4j$

	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

Theorem For each prime power q , there exists $q-1$ MOLS(q)'s.

Proof. Use $GF(q)$ where $q = p^n$, p is a prime and $n \in \mathbb{N}$.

$$L_k(i, j) = i + k \cdot j, \quad \forall k \in \{1, 2, \dots, q-1\}.$$

(*) So far, this is the best result on constructing MOLS(n).

(**) Row-complete Latin squares

0	5	1	4	2	3
1	0	2	5	3	4
2	1	3	0	4	5
3	2	4	1	5	0
4	3	5	2	0	1
5	4	0	1	2	3

6x6

Any pair of distinct elements in $\mathbb{Z}_6$ occurs next to each other in a row.

(***) We can construct such squares of order n provided n is even. The first row can be

$$0, 2m-1, 1, 2m-2, 2, 2m-3, \dots, m-1, m.$$

The other rows are obtained by adding the same elements respectively (mod n).

Definition (Partial Latin square of order n), $PLS(n)$.

An $n \times n$ array defined on $\mathbb{Z}_n$ with (possibly) some empty cells is called a partial Latin square if each element of $\mathbb{Z}_n$ occurs in each row and resp. each column "at most" once.

0	1		
1			
			2

← Completed uniquely?

A partial Latin square of order 4.

(.) An example of Sudoku is a partial Latin square of order 9. (数独)
 ↳ Unique completion!!?

(oo) In fact, this partial Latin square can be completed under extra condition.

Definition (Critical Set)

A $PLS(n)$ is a critical set of a Latin square of order n if it is a minimal $PLS(n)$ which can be completed uniquely.

0	1		
1			
			2

→

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

0	2	1	3
1	3	2	0
2	0	3	1
3	1	0	2

↗

→

0	2	1	3
1	3	2	0
2	0	3	1
3	1	0	2

少了一个位置就有两种不同的 Completions!

(*) Conjecture We need at least $\lceil \frac{n^2}{4} \rceil$ entries for a critical set of a Latin square of order n .

(**) There are critical sets of size larger than $\lceil \frac{n^2}{4} \rceil$.

0	1	2	
1	2		
2			

← A critical set?

Transversals in a Latin square

Problem In a Latin square of order n , how many distinct elements can we find such that no two of them are in the same row or in the same column.

e.g.

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

4

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

3?

Ryser's Conjecture (1)

For each Latin square of order n , if n is odd, then we can find n distinct elements satisfying the transversal requirement. These n entries form a Latin transversal.

(*) If L is a Latin square of order n , then L has a Latin transversal if L has an orthogonal mate M , i.e. $\exists M$, s.t. $L \perp M$.

Ryser's Conjecture (2)

If n is even, then there exists a transversal which contains at least $n-1$ elements.

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

Another example with no orthogonal mate!

(***) Both conjectures remain open.

(****) You are encouraged to try: either verify or disprove the above two conjectures.