Latin Squares 12.3

Def A latin square of order n is an $n \times n$ matrix with entries in $\{1, \ldots, n\}$ s.t. $\forall$ i appears in exactly one row and one column.

Example $n=3$

$$\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix} \qquad \begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$$

Instead of $\{1, \ldots, n\}$ can fill with any "alphabet"

$A \leftarrow$ finite set

$|A| = n$.

In other words a latin square is a mapping

$$L : \{1, \dots, n\} \times \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$$

s.t. $L(i,j) = L(i',j) \implies i = i'$

and $L(i,j') = L(i,j') \implies j = j'$.

"Latin" because Euler used latin alphabet $\{A, B, C, \dots\}$ instead of $\{1, \dots, n\}$.

Example $\quad n=4$

$$\begin{array}{c|ccc} 1 & 2 & 3 & 4 \\ \hline 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 2 & 1 \\ 4 & 3 & 1 & 2 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array} \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{array}$$

Up to reordering rows + columns there are only 4 distinct latin squares of order 4.

For any n a latin square is given by

$$\begin{matrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 4 & \cdots n & 1 \\ 3 & 4 & 5 & \cdots n-1 & 2 \\ \vdots & & & & \\ n & 1 & 2 & \cdots & n-1 \end{matrix} \Rightarrow \exists \text{ a latin square of any order}$$

Def Latin squares L, L' of order n are **orthogonal** if $\forall$ pair $(a_1, a_2) \in \{1, .., n\} \times \{1, .., n\}$ there is exactly one position (i,j) s.t.

$$L(i,j) = a_1 \qquad L'(i,j) = a_2.$$

Example: L, L' are orthogonal!

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \qquad L' = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}$$

11	22	33
23	31	12
32	13	21

There are no orthogonal latin squares of order 2.

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \qquad \begin{matrix} 2 & 1 \\ 1 & 2 \end{matrix}$$

only two distinct latin squares.

$$\begin{matrix} 12 & 21 \\ 21 & 12 \end{matrix}$$

NOT ORTHOGONAL!!

Conjecture (Euler 1782) Two orthogonal latin squares do not exist for order $n=4k+2$.

FALSE!

The case $n=6$ is famously known as the 36 officer problem. Solution does not exist!

Def A collection of latin squares $L_1, \ldots, L_k$ are mutually orthogonal if L_i, L_j are orthogonal for all $i \neq j$.

Question What is the maximal # of mutually orthogonal latin squares of order n?

Call this $N(n)$.

$N(2) = 1$
$N(6) = 1$

Here Euler's conjecture is true.

Thm 12.3 For $n \geq 2$ we have

$N(n) \leq n-1$ and $N(n) = n-1$

for $n = p^m$ p prime.

Proof Upper bound.

Let $L_1, \dots, L_t$ be mutually orth. latin squares of order n. Reorder the columns so that $\forall\ i \in \{1, \dots, t\}$.

$$L_i(1,1) = 1, \ L_i(1,2) = 2, \dots\dots, L_i(1,n) = n.$$

This preserves orthogonality!

Now consider $L_i(2,1) \neq 1$.

By orthogonality $L_i(2,1) \neq L_j(2,1)$ $\forall$ $i \neq j$. Therefore we can have at most $n-1$ mutually orthogonal latin squares.

Construction when $n = p^m$ prime power.

$\exists$ $GF(n) = \{\overset{0}{\overset{\shortparallel}{a_0}}, \ldots, a_{n-1}\}$ a finite field.

For $h = 1, \ldots, p^m - 1$ define:

$$L_h(a_i, a_j) = a_h a_i + a_j$$ ← latin square.

since $L_h(a_i, a_j) = L_h(a_{i'}, a_j)$

$\Longrightarrow$ $a_h a_i + \cancel{a_j} = a_h a_{i'} + \cancel{a_j}$

$\Longrightarrow$ $a_i = a_{i'}$ since a_h has mult. inverse.

Also if $L_h(a_i, a_j) = L_h(a_i, a_j')$

$$\Rightarrow \quad \cancel{a_h a_i} + a_j = \cancel{a_h a_i} + a_j'$$

$$a_j = a_j'.$$

This shows each elt of $GF(n)$ appears exactly once in each row and column of L_h. $\Rightarrow L_h$ is a latin square.

Consider L_h, L_k two such latin squares and let $(a_r, a_s) \in GF(n) \times GF(n)$

$$\left.\begin{aligned} a_r &= a_h x + y \\ a_s &= a_k x + y \end{aligned}\right]$$ — This has a unique solution, since $GF(n)$ is a field.

ie. $\exists$ a unique i,j s.t.

$$L_h(a_i, a_j) = a_r$$
$$L_k(a_i, a_j) = a_s.$$

Hence L_h, L_k are orthogonal.

$N(n) = n-1$ when $n = p^m$. $\square$

Thm 12.4 Let $n = n_1 n_2$ then

$$N(n_1, n_2) \geq \min(N(n_1), N(n_2))$$

Proof Let $K = \min(N(n_1), N(n_2))$.

Then $\exists$:

$L_1, \ldots, L_K$ mutually orth. on A_1 with $|A_1| = n_1$

$L_1', \ldots, L_K'$ mutually orth on A_2 with $|A_2| = n_2$.

$A = \underbrace{A_1 \times A_2}$ then $|A| = n_1 n_2 = \underline{\underline{n}}$.

$L_h^* : A \times A \longrightarrow A$.

$L_h^*((i,i'),(j,j')) := (L_h(i,j), L_h'(i',j'))$

Check that L_h^* is a latin square and L_h^*, L_ℓ^* are orthogonal for $h \neq \ell$. $\square$.

Corollary 12.5

Let $n = p_1^{k_1} \cdots p_t^{k_t}$ be prime decomposition. Then

$$N(n) \geq \min_{1 \leq i \leq t} (p_i^{k_i} - 1).$$

In particular, $N(n) \geq 2$ $\forall\, n \not\equiv 2 \mod 4$. (ie $n \neq 4k+2$).

Cases left open for existence of orthogonal latin squares are the conjecture of Euler.

Bose, Shrikhande, Parker showed

$N(n) \geq 2$ for all $n \neq 2, 6$ (1960)

Euler's conjecture is false except for $n = 2, 6$.

"Euler Spoilers"

Not a single value of $N(n)$ is

known beyond $n = 2, 6, p^m$!