# Part 23
# Latin Squares

Printed version of the lecture *Discrete Mathematics* on 4. December 2012

Tommy R. Jensen, Department of Mathematics, KNU

23.1

## Contents




23.2

## 1 Latin Squares

### Latin Squares

Example:

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

Every number 0,1,2,3 appears once in every row and column.

**Definition**
Let $n$ be a positive integer.

A *Latin square of order $n$* is an array $A$ with $n$ rows and $n$ columns such that

- all entries are elements of $\{0, 1, 2, \ldots, n-1\} = Z_n$, and
- each element of $Z_n$ appears in every row of $A$, and
- each element of $Z_n$ appears in every column of $A$.

23.3

Using the pigeonhole principle, every element of $Z_n$ appears precisely once in every row and column of a Latin square $A$.

**Presentation of a Latin square**
If $A$ is an $n \times n$ array, then we write $A = (a_{ij})$ $(0 \leq i, j \leq n-1)$.

Then the rows of $A$ are numbered $0, 1, 2, \ldots, n-1$ from top to bottom.

And the columns of $A$ are numbered $0, 1, 2, \ldots, n-1$ from left to right.

The entry in row number $i$ and column number $j$ of a Latin square is the number $a_{ij} \in Z_n$.

The array $(a_{ij})$ $(0 \leq i, j < n)$ is a Latin square if for every $k \in Z_n$ :

- for every $i \in Z_n$ there is a $j \in Z_n$ such that $a_{ij} = k$, and
- for every $j \in Z_n$ there is an $i \in Z_n$ such that $a_{ij} = k$.

23.4

## Latin squares from modular addition

**Theorem 10.4.1**
Let

$$a_{ij} = i \oplus j \ \ (i, j \in Z_n).$$

Then $A = (a_{ij})$ is a Latin square of order $n$.

**Proof of Theorem 10.4.1**
Let $k \in Z_n$.

Then for every $i \in Z_n$ we can choose $j = -i \oplus k$, so that $a_{ij} = i \oplus (-i \oplus k) = k$.

And for every $j \in Z_n$ we can choose $i = k \oplus (-j)$, so that $a_{ij} = (k \oplus (-j)) \oplus j = k$.

This proves that $A = (a_{ij})$ is a Latin square. □

23.5

## Latin squares from modular multiplication

**Theorem 10.4.2**
Let $r$ be an element of $Z_n$ with a multiplicative inverse $r^{-1}$.

Define $A = (a_{ij})$ $(i, j \in Z_n)$ by the rule:

$$a_{ij} = (r \otimes i) \oplus j \ \ (i, j \in Z_n).$$

Then $A$ is a Latin square of order $n$.

**Proof of Theorem 10.4.2**
Let $k \in Z_n$.

Then for every $i \in Z_n$ we can choose $j = -(r \otimes i) \oplus k$, so that $a_{ij} = (r \otimes i) \oplus (-(r \otimes i) \oplus k) = ((r \otimes i) \oplus -(r \otimes i)) \oplus k = k$.

And for every $j \in Z_n$ we can choose $i = r^{-1} \otimes (k \oplus -j)$, so that $a_{ij} = r \otimes (r^{-1} \otimes (k \oplus -j)) \oplus j = (k \oplus -j) \oplus j = k$.

This proves that $A = (a_{ij})$ is a Latin square. □

This special Latin square has the name $L_n^r$.

23.6

### Example of a latin square $L_n^r$

Let $n=8$ and $r=3$.

Then $\gcd(n,r)=\gcd(8,3)=1$, this implies that $r=3$ has a multiplicative inverse in $Z_8$.

To calculate the entry $a_{ij}$ of $L_8^3$ for $i,j\in Z_8$ we have to calculate the remainder after division by 8 of

$$3\cdot i+j.$$

So we get the rules, using addition in $Z_8$ :

- the entry in the first row and the first column is $a_{00}=0$,
- we get the next entry to the right by adding 1, and
- we get the next lower entry of the column by adding 3.

23.7

### $L_8^3$

Following these rules it is easy to construct $L_8^3$ :

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

23.8

## 2 Orthogonal Latin Squares

### Orthogonal Latin squares

**Definition**

Let $A=(a_{ij})$ and $B=(b_{ij})$ be Latin squares.

They are called *orthogonal* Latin squares if they satisfy the following condition:

For any two elements $k$ and $\ell$ of $Z_n$, there exist $i$ and $j$ in $Z_n$ so that $a_{ij}=k$ and $b_{ij}=\ell$.

We can write another array (called the *juxtaposed* array) in which the position of row $i$ and column $j$ contains the pair $(a_{ij},b_{ij})$.

Then $A$ and $B$ satisfy the condition for being ortogonal, precisely if each possible pair $(k,\ell)$ of elements from $Z_n$ appear in this array.

23.9

### Example of orthogonal Latin squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix}$$

produce a juxtaposed array:

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

We can check that all pairs of elements from $Z_4$ appear in the array.

23.10

## 3 MOLS

### Mutually orthogonal Latin squares

**Definition**
Let $A_1, A_2, \ldots, A_k$ be Latin squares of order $n$.

They are called *mutually orthogonal* if $A_r$ and $A_s$ are orthogonal for all $r$ and $s$ with $1 \leq r < s \leq k$.

A set of Mutually Orthogonal Latin Squares is called a *MOLS*.

**Theorem 10.4.3**
If $n$ is a prime number, then

$$L_n^1, L_n^2, \ldots, L_n^{n-1}$$

form a set of MOLS with $n-1$ squares each of order $n$.

**Proof of Theorem 10.4.3**
We know from Theorem 10.4.2 that $L_n^r$ is always a Latin square of order $n$. It remains to prove that $L_n^r$ and $L_n^s$ are orthogonal for all $r \neq s$ with $r, s \in \{1, 2, \ldots, n-1\}$.

23.11

### Proof that $L_n^r$ and $L_n^s$ are orthogonal for all $r \neq s$.

By definition of orthogonal Latin squares, we have to show, for each $k$ and each $\ell$ in $Z_n$ that $(k, \ell)$ is in some entry of the juxtaposed array of $L_n^r$ and $L_n^s$

We know that $L_n^r$ contains the number $r \otimes i \oplus j$ in its $ij$-entry.

And $L_n^s$ contains the number $s \otimes i \oplus j$ in its $ij$-entry.

If we can find $i$ and $j$ so that

$$\begin{aligned} r \otimes i \oplus j &= k \\ s \otimes i \oplus j &= \ell \end{aligned}$$

are satisfied, then we know that $(k, \ell)$ is in the $ij$-entry of the juxtaposed square.

23.12

### Proof that $L_n^r$ and $L_n^s$ are orthogonal for all $r \neq s$, continued

We want to find $i$ and $j$ to solve the equations

$$\begin{aligned} r \otimes i \oplus j &= k \\ s \otimes i \oplus j &= \ell \end{aligned}$$

Finding additive inverses of the second equation we get:

$$\begin{aligned} r \otimes i \oplus j &= k \\ -s \otimes i \oplus -j &= -\ell \end{aligned}$$

We can add these two equations, and we get:

$$r \otimes i \oplus -s \otimes i = (r \oplus -s) \otimes i = k \oplus -\ell.$$

Since $r \neq s$, it follows that $r \oplus -s \neq 0$, and therefore the multiplicative inverse $(r \oplus -s)^{-1}$ exists in $Z_n$, since $n$ is a prime.

Now $i = (r \oplus -s)^{-1} \otimes (r \oplus -s) \otimes i = (r \oplus -s)^{-1} \otimes (k \oplus -\ell)$.

From $r \otimes i \oplus j = k$ we get $j = k \oplus -r \otimes i$.

We have now calculated the entry in which the pair $(k, \ell)$ appears in the juxtaposed square from $L_n^r$ and $L_n^s$. □

23.13

### Constructing a MOLS of prime power order

**Theorem 10.4.4**
If $p$ is a prime and $n = p^k$ for some positive number $k$, then there exists a MOLS of $n-1$ squares of order $n$.

**Proof of Theorem 10.4.4**
The proof is the same as for Theorem 10.4.3, using addition and multiplication of the finite field of order $n = p^k$. □

23.14

### The maximal number of squares in a MOLS

**Theorem 10.4.5**
If a MOLS consists of squares of order $n$, then it has at most $n-1$ squares.

**Theorem (Tarry 1900)**
There are no two orthogonal Latin squares of order 6.

**Theorem 10.4.6**
For every odd number $n$, there exist orthogonal Latin squares of order $n$.

**Theorem (Parker, Bose and Shrikhande 1959)**
For every number $n > 6$ there exist orthogonal Latin squares of order $n$.

23.15

# 4 Conclusion

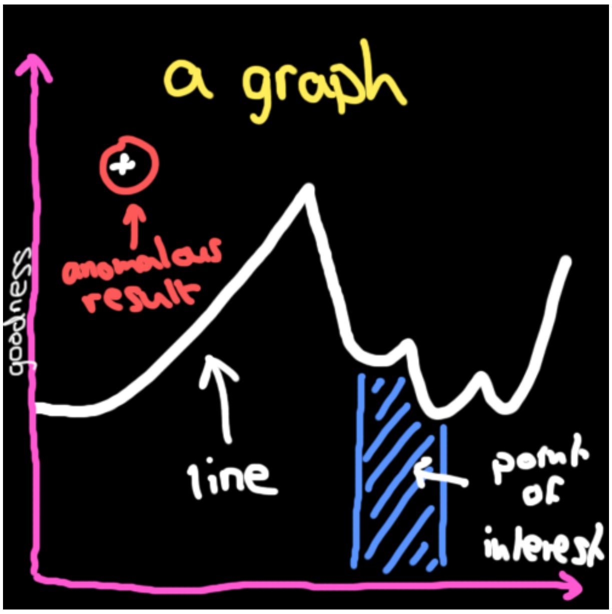
## Conclusion

*This ends the lecture!*


23.16

## Next time:

Graph Theory




23.17