Latin Squares and Graeco-Latin Squares

Bob Schmalzried

Spring 2021

A Latin square is defined as an n x n array that contains n distinct elements arranged such that each element appears exactly once in each row and once in each column. Each element will appear n times in the array. Some examples of Latin Squares are the following.

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

Theorem 1: Let n be a positive integer. Let A be the n x n array whose entry

$a_{ij} = i + j$ (addition mod n), where i, j = 0, 1, 2, …, n-1), then A is a Latin square of order n based on Z_n.

Proof: Suppose that in some row i of the array, the elements in positions a_{ij} and a_{ik} are identical. That would mean that i + j = i + k.

So, -i + i + j = -i + i + k.

Hence, j = k.

So, there is no repeated element in row i.

Suppose that in some column j of the array, the elements in positions a_{ij} and a_{kj} are identical. That would mean that i + j = k + j.

So, i + j – j = k + j – j.

Hence, i = k.

So, there is no repeated element in column j.

Since there is no repeated element in any row or column, A is a Latin square.

Additional Latin squares can be created by switching any row with another row or any column with another column. For example, if we have the Latin square

$\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$ and switch rows 1 and 2, we get $\begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{bmatrix}$ which is also a Latin square.

We also have other techniques for creating Latin squares.

Theorem 2: Let n be a positive integer and let r be a nonzero integer in Z_n such that the GCD of r and n is 1. Let L_n^r be the n x n array whose entry a_{ij} in row i and column j is a_{ij} = r x i + j (arithmetic mod n) where i, j = 0, 1, 2, … , n-1), then A is a Latin square based on Z_n.

Proof: Suppose that the elements in positions a_{ij} and a_{ik} are identical. That would mean that r x i + j = r x i + k.

An additive inverse for r x i exists mod n.

So, -(r x i) + (r x i) + j = -(r x i) + (r x i) + k.

Hence, j = k.

So, there is no repeated element in row i.

Suppose the elements in positions a_{ij} and a_{kj} are identical. That would mean that

r x i + j = r x k + j.

So, r x i + j - j = r x k + j – j

Then, r x i = r x k.

Since, GCD(r, n) = 1, a multiplicative inverse exist for r.

So, r^{-1} x r x i = r^{-1} x r x k.

Hence, i = k.

So, there is no repeated element in column j.

Since there is no repeated element in any row or column, A is a Latin square.

An example of the previous theorem is shown using a 4 x 4 array and r = 3.

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

A Graeco-Latin square is created if we take the elements from the same positions of two Latin squares as an ordered pair, and each ordered pair exist exactly once.

Consider the Latin squares $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{bmatrix}$

Combining those together as ordered pairs gives us

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

Each of the 9 possible ordered pairs exist exactly once. Each first element appears exactly once in each row and column, and each second element exists in each row and column. Therefore, the array is a Graeco-Latin square.

There is not a 2 x 2 Graeco-Latin square. This can be proven by listing all of the possible 2 x 2 Latin squares and showing that none of the combinations create a Graeco-Latin squares.

$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ are the only 2 x 2 Latin squares. If we combine those attempting to create a Graeco-Latin square, we get $\begin{bmatrix} (0,1) & (1,0) \\ (1,0) & (0,1) \end{bmatrix}$, and that is not a Graeco-Latin square, so no such square exists for 2 x 2 array.

It can be shown that Graeco-Latin squares exist for 1 x1 $[(0,0)]$

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

4 x 4 $\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{bmatrix}$

and 5 x 5 $\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) & (4,4) \\ (1,2) & (2,3) & (3,5) & (4,1) & (0,1) \\ (2,4) & (3,0) & (4,1) & (0,2) & (1,3) \\ (3,1) & (4,2) & (0,4) & (1,4) & (2,0) \\ (4,3) & (0,4) & (1,0) & (2,1) & (3,2) \end{bmatrix}$

Euler was unable to find a 6 x 6 Graeco-Latin square and made a conjecture in 1782 that Graeco-Latin squares do not exist for n x n squares where n ≡ 2 (mod 4).

The 2 x 2 case was shown earlier.

The 6 x 6 case was resolved in 1901 by Gaston Tarry. He examined all possible cases and showed that none of them produce a Graeco-Latin square.

If two Latin squares combined create a Graeco-Latin square, we say that the Latin squares are *mutually orthogonal*. For every n, except n = 2 and n = 6, there exist at least two mutually orthogonal Latin squares.

Recall that L_n^r is a Latin square that was constructed in Theorem 2.

Theorem 3: Let n be a prime number. Then $L_n^1, L_n^2, \dots, L_n^{n-1}$ are n – 1 mutually orthogonal Latin squares of order n.

Proof: Since n is prime, each nonzero integer in Z_n has a multiplicative inverse. Using the previous theorem, the arrays $L_n^1, L_n^2, \dots, L_n^{n-1}$ are Latin squares because GCD of n and any element equals 1. Let r and s be distinct nonzero integers in Z_n. Then, L_n^r and L_n^s are orthogonal. Suppose that combining the arrays together, $L_n^r \times L_n^s$ has an ordered pair that occurs twice. Say that is occurs in a_{ij} and a_{kl}, then

$r \times i + j = r \times k + l$ and $s \times i + j = s \times k + l$.

So, $r \times (i - k) = (l - j)$ and $s \times (i - k) = (l - j)$ by rearranging the previous step algebraically.

Then, $r \times (i - k) = s \times (i - k)$ by substitution.

Suppose that $i \neq k$, the $(i - k) \neq 0$ and has a multiplicative inverse in Z_n.

If we multiply each side of the equation by that inverse, we get r = s, which is a contradiction. Hence, i = k and j = l. So, the only way that the two positions in $L_n^r \times L_n^s$ can contain the same ordered pair is for them to be in the same position. Therefore, L_n^r and L_n^s are orthogonal for all $r \neq s$ and $L_n^1, L_n^2, \dots, L_n^{n-1}$ are mutually orthogonal Latin squares.

Theorem 4: Let $n = p^k$ be an integer that is a power of a prime number p. Then there exist n – 1 mutually orthogonal Latin squares of order n.

This can be shown for order 4 by using the arithmetic of the field $a_0 = 0$, $a_1 = 1$, $a_2 = i$, $a_3 = 1 + i$

$$L_4^1 = \begin{bmatrix} 0 & 1 & i & 1+i \\ 1 & 0 & 1+i & i \\ i & 1+i & 0 & 1 \\ 1+i & i & 1 & 0 \end{bmatrix}$$

$$L_4^i = \begin{bmatrix} 0 & 1 & i & 1+i \\ i & 1+i & 0 & 1 \\ 1+i & i & 1 & 0 \\ 1 & 0 & 1+i & i \end{bmatrix}$$

$$L_4^{1+i} = \begin{bmatrix} 0 & 1 & i & 1+i \\ 1+i & i & 1 & 0 \\ 1 & 0 & 1+i & i \\ i & 1+i & 0 & 1 \end{bmatrix}$$

L_4^1, L_4^i, and L_4^{1+i} are mutually orthogonal Latin squares.

Theorem 5: Let n be an odd integer. Then there exist at least two mutually orthogonal Latin squares of size n.

Proof: Let n be an odd integer. Consider the addition table A and the subtraction table B of Z_n. A and B are Latin squares. Then, $a_{ij} = i + j$ and $b_{ij} = i - j$. Suppose that $(a_{ij}, b_{ij}) = (a_{kl}, b_{kl})$.

Then, $i + j = k + l$ and $i - j = k - l$.

Adding these equations together gives us $2i = 2k$.

Subtracting these equations together gives us $2j = 2l$.

Since n is odd, GCD(2, n) = 1, so multiplicative inverse of 2 exists, so $i = k$ and $j = l$. So, the only way for A x B to have the same ordered pair in two positions is for the positions to be the same. Therefore, A and B are orthogonal.

Mutually orthogonal Latin squares can be combined together to create a larger order mutually orthogonal Latin square.

Theorem 6: If there is a pair of mutually orthogonal Latin squares of order m and a pair of mutually orthogonal Latin squares of order k, then there is a pair of mutually orthogonal Latin squares of order mk.

An example of this is shown below.

Consider $A = \begin{bmatrix} (0,0) & (1,2) & (2,1) \\ (1,1) & (2,0) & (0,2) \\ (2,2) & (0,1) & (1,0) \end{bmatrix}$ and $B = \begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,2) & (0,3) & (3,0) & (2,1) \\ (2,3) & (3,2) & (0,1) & (1,0) \\ (3,1) & (2,0) & (1,3) & (0,2) \end{bmatrix}$

These can be combined to create

C =

$$\begin{bmatrix}
(0,0) & (1,1) & (2,2) & (3,3) & (4,8) & (5,9) & (6,10) & (7,11) & (8,4) & (9,5) & (10,6) & (11,7)) \\
(1,2) & (0,3) & (3,0) & (2,1) & (5,10) & (4,11) & (7,8) & (6,9) & (9,6) & (8,7) & (11,4) & (10,5) \\
(2,3) & (3,2) & (0,1) & (1,0) & (6,11) & (7,10) & (4,9) & (5,8) & (10,7) & (11,6) & (8,5) & (9,4) \\
(3,1) & (2,0) & (1,3) & (0,2) & (7,9) & (6,8) & (5,11) & (4,10) & (11,5) & (10,4) & (9,7) & (8,6) \\
(4,4) & (5,5) & (6,6) & (7,7) & (8,0) & (9,1) & (10,2) & (11,3) & (0,8) & (1,9) & (2,10) & (3,11) \\
(5,6) & (4,7) & (7,4) & (6,5) & (9,2) & (8,3) & (11,0) & (10,1) & (1,10) & (0,11) & (3,8) & (2,9) \\
(6,7) & (7,6) & (4,5 & (5,4) & (10,3) & (11,2) & (8,1) & (9,0) & (2,11) & (3,10 & (0,9) & (1,8) \\
(7,5) & (6,4) & (5,7 & (4,6) & (11,1) & (10,0) & (9,3) & (8,2) & (3,9) & (2,8) & (1,11) & (0,10) \\
(8,8) & (9,9) & (10,10 & (11,11) & (0,4) & (1,5) & (2,6) & (3,7) & (4,0) & (5,1) & (6,2) & (7,3) \\
(9,10) & (8,11) & (11,8 & (10,9) & (1,6) & (0,7) & (3,4) & (2,5) & (5,2) & (4,3) & (7,0) & (6,1) \\
(10,11) & (11,10) & (8,9 & (9,8) & (2,7) & (3,6) & (0,5) & (1,4) & (6,3) & (7,2) & (4,1) & (5,0) \\
(11,9) & (10,8) & (9,11) & (8,10) & (3,5) & (2,4) & (1,7) & (0,6) & (7,1) & (6,0) & (5,3) & (4,2)
\end{bmatrix}$$

Theorem 6: Let $n \geq 2$ be an integer and let $n = p_1^{e1} \times p_2^{e2} \times \ldots \times p_k^{ek}$ be the factorization of n into distinct prime numbers $p_1, p_2, \ldots, p_k$. Then, the number of mutually orthogonal Latin squares is greater than or equal to $\min\{p_i^{ei} - 1 : i = 1, 2, \ldots, k\}$

Proof: For each prime factor to a power, except 2^1, there exist at least 2 mutually orthogonal Latin squares. We have already shown that if there is a pair of mutually orthogonal Latin squares of order m and a pair of mutually orthogonal Latin squares of order k, then there is a pair of mutually orthogonal Latin squares of order mk. Therefore, the number of mutually orthogonal Latin squares is greater than or equal to $\min\{p_i^{ei} - 1 : i = 1, 2, \ldots, k\}$

Using all of the previous theorems and properties, we can show that Graeco-Latin squares exist for size n where n is either odd or a multiple of 4.

In other words, Graeco-Latin squares exist for size n except where $n \equiv 2 \pmod 4$.

In 1959, Parker, Bose, and Shrikhande disproved Euler's conjecture by showing the counterexample for a 10 x 10 array through the use of a computer. They went on to show that for every n, except for n = 2 and n = 6, there exists a Graeco-Latin square of size n.

Applications of Graeco-Latin squares include designs of experiments and tournament scheduling.

References:

Introductory Combinatorics, Fifth Edition (ISBN 978-0-13-602040-0) by Richard A. Brualdi, Copyright © 2010, 2004, 1999, 1992, 1977 by Pearson Education, Inc.

Klyve, Dominic, and Lee Stemkoski. "Graeco-Latin Squares and a Mistaken Conjecture of Euler." *The College Mathematics Journal*, vol. 37, no. 1, 2006, p. 2., doi:10.2307/27646265.