Latin Squares

Bhaskar Bagchi

In this article we discuss MacNeish's extension of Euler's conjecture on orthogonal Latin squares, and how these conjectures were disposed off.

Bhaskar Bagchi has been associated with Indian Statistical Institute for over forty years. Currently he is a Professor of Mathematics in its Bangalore centre. His interests include finite feometries, strongly regular graphs and combinatorial topology.

It is extremely rare for a piece of mathematics to make it to the front page headline of a major newspaper. So, one fine morning in 1959, the readers of *The New York Times* must have have been startled to open their favourite newspaper and find an article on Euler's Spoilers. It told the story of a 177 year old conundrum posed by the legendary mathematician Leonhard Euler (1707–1783) and how three mathematicians had "spoilt" Euler by proving that the solution guessed by the master was as wrong as it could be.

Euler had introduced [1] the notion of 'Graeco–Latin squares' and observed that there are no such squares of 'order' 2 or 6. He therefore had jumped to the surmise that there are no such squares whose orders belong to the sequence $2, 6, 10, 14, \cdots$ of the so-called 'oddly even' numbers. But R C Bose, S S Shrikhande and E T Parker had shown [2] that Graeco–Latin squares of order n actually exist for all numbers n except 2 and 6.

Euler had introduced the notion of 'Graeco–Latin squares'.

So what are Graeco–Latin squares? To define them, we must first talk of permutations and Latin squares. A permutation of a finite set of objects is a linear arrangement of these objects (in which each object occurs once and only once). For instance, the three objects $1, 2, 3$ have $1\times2\times3 = 6$ permutations. These are: $123, 132, 213, 231, 312, 321$. More generally, the number of permutations of a set of n objects is $n! = 1 \times 2 \times \cdot \cdot \times n$.

Keywords
Permutations, Graeco–Latin squares, orthogonality.

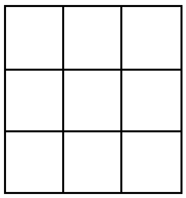

Figure 1. A 3 × 3 array waiting to be filled up.

Take a square array of size $n \times n$. It has n^2 positions arranged in $2n$ lines, of which n are rows (horizontal lines) and n are columns (vertical lines). We usually number the columns (left to right) and also the rows (top to bottom) as $1, 2, \ldots, n$. For any two numbers $1 \leq i, j \leq n$, the ith row and the jth column of the array has exactly one position (empty slot) in common; it is called the (i, j)th position of the array. For instance, *Figure* 1 shows a 3×3 array.

Now a Latin square of order n is an $n \times n$ array whose positions have been filled up by n distinct objects in such a way that each line (row or column) of the array is a permutation of these n objects. That is, each object occurs exactly once in each line and hence each object occurs n times in the entire array. The identity of the objects used is of no importance here, though traditionally they used to be Latin letters. Hence the name: Latin squares. For instance, two Latin squares of order 3 are shown in *Figure* 2. (Note that we have filled the first square with Greek letters, and the second with Latin letters.)

Some more examples of Latin squares of small orders (this time, filled up with the numerals $1, 2, 3, \cdots$) are shown in *Figure* 3.

The reader should have no difficulty in deciphering the construction of the nth Latin square (of order n) in this sequence. Indeed, the multiplication table of any finite group[1] of order n (abelian or not) is an example of a Latin square of order n. Thus, existence of Latin squares of any order is no problem.

[1] Recall that a finite group of order n is a finite set G of size n with a special element $1 \in G$ and a binary relation $\times$ on G (thus, for x,y in G, $x \times y$ is again an element of G) such that
(i) $x \times 1 = 1 \times x = x$,
(ii) $x \times (y \times z) = (x \times y) \times z$, and
(iii) $x \times y = x \times z$ implies $y = z$.
G is called an abelian group if, further, $x \times y = y \times x$ for all x,y in G. The multiplication table of G is the $n \times n$ array, with rows as well as columns indexed by G, whose (x,y) entry is $x \times y$. The cancellation property (iii) implies that the multiplication table of any finite group is a Latin square.

α	β	γ
β	γ	α
γ	α	β

a	c	b
b	a	c
c	b	a

Figure 2 (left). Two orthogonal Latin squares.

1

,

1	2
2	1

,

1	2	3
2	3	1
3	1	2

,

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

, …

Figure 3(right). A sequence of Latin squares.

Now, copy the two Latin squares of *Figure* 2 on two sheets of transparency and place the second transparency on top of the first. Keep the top one a little to the right of the bottom transparency, so that the Greek letters are not covered by their Latin counterparts. Then we see an array as shown in *Figure* 4 (obtained by 'superposing' the two Latin squares).

αa	βc	γb
βb	γa	αc
γc	αb	βa

Figure 4. A Graeco–Latin square.

Notice that, in this 3×3 square, the nine possible combinations (obtained by juxtaposing the three Latin letters a, b, c with the Greek letters α, β, γ) occur once each. We say that the two order-3 Latin squares of *Figure* 2 are orthogonal, and on superposition, they yield the order-3 Graeco–Latin square of *Figure* 4. Of course, this has nothing to do with Greek or Latin. Here is a formal definition. Let A and B be any two sets of size n. Let L and M be two Latin squares of order n with entries from A and B respectively. For $1 \leq i, j \leq n$, let l_{ij} (respectively m_{ij}) be the (i, j)th entry of L (respectively M). One writes $L = [l_{ij}]$ and $M = [m_{ij}]$. Consider the square $[l_{ij}m_{ij}]$ obtained by superimposing L and M. If, in this last square, all possible combinations ab, $a \in A$, $b \in B$, occur (once and only once), then we say that L and M are orthogonal Latin squares of order n, and the square $[l_{ij}m_{ij}]$ is a Graeco–Latin square of order n. Thus, a Graeco–Latin square is just a convenient way of recording a pair of orthogonal Latin squares. We repeat that, in this definition, ab for instance is just the object obtained by placing b to the right of a. It is not intended to denote any kind of multiplication.

The multiplication table of any finite group of order *n* (abelian or not) is an example of a Latin square of order *n*.

Now, it is trivial to verify that there is no Graeco–Latin square of order 2. Euler found by exhaustive search that there is no Graeco–Latin square of order 6 either (for a concise proof, see [3]). He then conjectured [1] that there are no Graeco–Latin squares (equivalently, pairs of orthogonal Latin squares) of order $2, 6, 10, 14, 18, \cdots$. This is the conjecture that Euler's spoilers disproved. (A warning to the reader: don't imagine that, in the

A Graeco–Latin square is just a convenient way of recording a pair of orthogonal Latin squares.

modern computer age, these are trivial problems. If you doubt me, try to construct Graeco–Latin squares of order 10 by mere computer power!).

There is no Graeco–Latin square of order 6.

Euler's problem may be generalized as follows [4]. For $n \geq 1$, let $N(n)$ denote the largest number such that there are $N(n)$ Mutually Orthogonal Latin squares (MOLs) of order n, i.e., $N(n)$ Latin squares of order n, any two of which are orthogonal[2] [5]. The reader may enjoy proving that $N(n) \leq n - 1$ for all n. In this notation, Euler's conjecture was that $N(n) = 1$ for all "oddly even" numbers n (i.e., numbers which leave a remainder 2 when divided by 4). The more general question is: what is the value of $N(n), n = 1, 2, 3, \cdots$? A set of MOLs is said to be *complete* if it consists of $n-1$ Latin squares of order n. An example is given in *Figure* 5.

[2] Latin squares and MOLs are useful in statistical experiments. For instance, they are very important in the design of agricultural and medical research. Of late, they have also been used in the architecture of data storage and data retrieval. Ignorance prevents the author from elaborating on these applications.

In fact, this complete set of MOLs of order 5 is constructed by a simple recipe. For $0 \leq i, j \leq 4$ and $1 \leq k \leq 4$, the (i, j)th entry of L_k is obtained by dividing $i+jk$ by 5, and then taking the remainder as the entry. The reader may easily verify that this recipe gives a complete set of MOLs of order n for every prime number n (and only then). Thus, there are complete sets of MOLs of every prime order. More generally, the theory of Galois fields may be used to generalize this construction to all prime power orders. One of the most famous open problems in combinatorics is to prove (or disprove !):

$$L_1 = \begin{array}{|c|c|c|c|c|}\hline 0&1&2&3&4\\\hline 1&2&3&4&0\\\hline 2&3&4&0&1\\\hline 3&4&0&1&2\\\hline 4&0&1&2&3\\\hline\end{array}, L_2 = \begin{array}{|c|c|c|c|c|}\hline 0&2&4&1&3\\\hline 1&3&0&2&4\\\hline 2&4&1&3&0\\\hline 3&0&2&4&1\\\hline 4&1&3&0&2\\\hline\end{array},$$

$$L_3 = \begin{array}{|c|c|c|c|c|}\hline 0&3&1&4&2\\\hline 1&4&2&0&3\\\hline 2&0&3&1&4\\\hline 3&1&4&2&0\\\hline 4&2&0&3&1\\\hline\end{array}, L_4 = \begin{array}{|c|c|c|c|c|}\hline 0&4&3&2&1\\\hline 1&0&4&3&2\\\hline 2&1&0&4&3\\\hline 3&2&1&0&4\\\hline 4&3&2&1&0\\\hline\end{array}.$$

Figure 5. A complete set of MOLs.

Conjecture. A set of $n-1$ MOLs of order n exists (if and) only if n is a prime power (i.e., $n = p^e$, where p is a prime, and $e \geq 1$).

There is no complete set of MOLs of order 10.

In 1989, Lam *et al* [6]. combined deep results from coding theory with the might of a supercomputer to prove that there is no complete set of MOLs of order 10. The exact value of $N(n)$ is known for $n \leq 9$. Regarding the value of $N(10)$, the limit of current knowledge is $2 \leq N(10) \leq 6$.

Thus we have:

Open Problem. Construct a set of three MOLs of order 10, or show that no such set exists.

Let A and B be two Latin squares, say of order m and n. Then one can construct a Latin square $C = A \times B$ of order mn, called the Kronecker product of A and B, as follows. Let $A = [a_{ij}]$ and $B = [b_{ij}]$. For any symbol a, let aB denote the Latin square of order n whose (i, j)th entry is ab_{ij}. For $1 \leq i, j \leq m$, let $C_{ij} = a_{ij}B$. Then set

$$C = \begin{array}{|c|c|c|c|c|} \hline C_{11} & C_{12} & \cdots & \cdots & C_{1m} \\ \hline . & . & & & . \\ \hline . & & . & & . \\ \hline . & & & . & . \\ \hline C_{m1} & C_{m2} & \cdots & \cdots & C_{mm} \\ \hline \end{array}$$

It is easy to verify that, whenever A and B are Latin squares, so is $A \times B$. Also, if $A_1, \ldots, A_k$ (respectively $B_1, \ldots, B_k$) are k MOLs of order m (respectively n), then $A_1 \times B_1, \ldots, A_k \times B_k$ are k MOLs of order mn. This result shows that for any two numbers m and n, $N(mn) \geq \min(N(m), N(n))$. Iterating this construction, one sees that, for any t numbers $q_1, \cdots, q_t$, we have

$$N(q_1 q_2 \cdots q_t) \geq \min(N(q_1), \cdots, N(q_t)). \qquad (1)$$

Now, given any $n \geq 2, n$ can be uniquely factorized as $n = q_1 q_2 \cdots q_t$, where $2 \leq q_1 < q_2 < \cdots < q_t$ are powers of distinct primes. Since $N(q_i) = q_i - 1$ for each i, in conjunction with (1), we get that

$$N(n) \geq q_1 - 1, \tag{2}$$

where q_1 is the smallest prime power factor in the canonical factorization of n. This bound is due to MacNeish [7]. In 1922, he hazarded the following guess:

MacNeish's conjecture. For every $n \geq 2, N(n) = q_1 - 1$, where q_1 is the smallest prime power in the canonical factorization of n. (That is, equality always holds in (2).)

Notice that, when n is oddly even, we have $q_1 = 2$. Thus, MacNeish's conjecture is a bold generalization of Euler's. Also note that when $n \geq 2$ is not oddly even, (2) actually gives $N(n) \geq 2$. Perhaps Euler was aware of this last inequality and it led him to his conjecture.

The reader may be surprised to hear that, while Euler's conjecture was still open, MacNeish went ahead and made an even stronger and bolder conjecture. Mathematicians do this sort of thing all the time, in the strange hope (often realized!) that the more general (and, on the face of it, more difficult) problem may be easier to settle. Indeed, this is what happened with MacNeish's conjecture, though not in the way he had expected.

Bose and Shrikhande further developed and extended Parker's construction method to disprove Euler's conjecture for infinitely many orders. Finally, they collaborated with Parker to disprove Euler's conjecture for all orders $n > 6$.

In 1958, E T Parker used finite projective planes to disprove MacNeish's conjecture in many cases. For instance, he constructed three mutually orthogonal Latin squares of order 21, showing that $N(21) \geq 3$. When Raj Chandra Bose [8, 9]saw Parker's paper, he brought it to the attention of Sharadchandra Shankar Shrikhande, then a PhD student of Bose. Together, Bose and Shrikhande further developed and extended Parker's construction method to disprove Euler's conjecture for infinitely many orders. Finally, they collaborated with Parker to disprove Euler's conjecture for all orders $n > 6$. Their method of proof [10] makes clever uses of certain finite geometries called linear spaces (or Partially Balanced Designs). This method is way beyond the scope of the present article.

We have seen that the theory of Latin squares is still full of unsolved problems, some of which may well be within the reach of enterprising and clever students. I can't resist the temptation to end this article with a problem which has haunted me for some time now.

Let $a_1, a_2, \ldots, a_n$ be a permutation of $1, 2, \ldots, n$. An inversion in this permutation is a pair $1 \leq i < j \leq n$ such that $a_i > a_j$. The permutation is called even (resp. odd) if it has an even (resp. odd) number of inversions. This is standard terminology. Now recall that with any Latin square of order n (with $1, 2, \cdots, n$ as entries) there are associated $2n$ permutations of $1, 2, \ldots, n$ corresponding to the $2n$ lines (rows and columns) of the Latin square. Let us say that the Latin square is 'even' if the number of odd permutations among these $2n$ permutations is even. Call the Latin square 'odd' if it is not even. If L is a Latin square of odd order $n > 1$, and L' is the Latin square obtained from L by interchanging the first two rows, then one can easily see that L is even if and only if L' is odd. Thus, for every odd $n > 1$, there are equally many even and odd Latin squares of order n. It is not difficult to see that, further, the multiplication table of any finite group is an even Latin square. I have observed that there is no odd Latin square of order 2 or 4. Euler's posthumous experience notwithstanding, I've jumped ahead to propose:

My conjecture. There is no odd Latin square of even order[3].

The reader may enjoy proving me wrong by constructing an odd Latin square of order six!

[3] The referee kindly pointed out that this conjecture has the same sort of flavour as an old conjecture (still unsolved) of Ryser. A transversal in a Latin square of order n is a set of n positions, one in each line of the square, on which all n symbols occur. Ryser conjectured that any even (resp. odd) order Latin square has an even (resp. odd) number of transversals.

Suggested Reading

[1] L Euler, *A New Type of Magic Squares*, 1782, collected works.

[2] R C Bose, S S Shrikhande and E T Parker, Further results in the construction of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Canadian Journal of Mathematics*, Vol.12, pp.189–203, 1960.

[3] D R Stinson, Nonexistence of a pair of orthogonal Latin squares of order six, *Journal of Combinatorial Theory*, (A) Vol.36, pp.373–376, 1984.

[4] S Chowla, P Erdös and E G Strauss, On the maximal number of pairwise orthogonal Latin squares of a given order, *Canadian Journal of Mathematics*, Vol.12, pp.204–208, 1960.

[5] P J Schellenberg, G M J Van Reas and S A Vanstone, Four pairwise orthogonal Latin squares of order 15, *Ars Combinatoria*, Vol.6, pp.141–150, 1978.

[6] C W Lam, S Swierez and L Thiel, The non-existence of finite projective planes of order 10, *Canadian Journal of Mathematics*, Vol.41, pp.1117–1123, 1989.

[7] H F MacNeish, 'Euler squares', *Annals of Mathematics*, Vol.23, 1922.

[8] R C Bose, On the application of the properties of Galois Fields to the problem of construction of hyper Graeco–Latin squares, *Sankhya*, Vol.3, pp.323–338, 1938.

[9] C S Yogananda, 'Raj Chandra Bose', *Resonance*, Vol.8, No.9, p.51, 2003.

[10] J H Van Lint and R M Wilson, *A Course in Combinatorics*, (Chapter 22), Cambridge University Press, 2001.

Address for Correspondence
Bhaskar Bagchi
Indian Statistical Institute
8th Mile, Mysore Road
RVCE Post
Bangalore 560 059, India.
Email: bbagchi@isibang.ac.in