Graeco-Latin Squares
and a Mistaken Conjecture of Euler*

Dominic Klyve
Lee Stemkoski

Introduction

Late in his long and productive career, Leonhard Euler published a hundred-page paper detailing the properties of a new mathematical structure: Graeco-Latin squares. In this paper, Euler claimed that a Graeco-Latin square of size n could never exist for any n of the form $4k+2$, although he was not able to prove it. In the end, his difficulty was validated. Over a period of 200 years, more than twenty researchers from five countries worked on the problem. Even then, they succeeded only after using techniques from many branches of mathematics including group theory, finite fields, projective geometry, and statistical and block designs; eventually, modern computers were employed to finish the job.

A *Latin square* (of order n) is an n-by-n array of n distinct symbols (usually the integers $1, 2, \ldots, n$) in which each symbol appears exactly once in each row and column. Some examples appear in Figure 1.

1	2	3
3	1	2
2	3	1

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

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

Figure 1: Latin squares of orders 3, 4, and 5

A *Graeco-Latin square* (of order n) is an n-by-n array of ordered pairs from a set of n symbols such that in each row and each column of the array, each symbol appears exactly once in each coordinate, and that each of the n^2 possible pairs appears exactly once in the entire square. Figure 2 shows one such example.

*to appear in *College Mathematics Journal*, January 2006

(1,1)	(2,5)	(3,4)	(4,3)	(5,2)
(2,2)	(3,1)	(4,5)	(5,4)	(1,3)
(3,3)	(4,2)	(5,1)	(1,5)	(2,4)
(4,4)	(5,3)	(1,2)	(2,1)	(3,5)
(5,5)	(1,4)	(2,3)	(3,2)	(4,1)

Figure 2: A Graeco-Latin square of order 5

Leonhard Euler published two papers concerning Graeco-Latin squares. The first, entitled *De Quadratis Magicis* [**9**], was written in 1776. In this short paper (seven pages in Euler's *Opera Omnia*), Euler considered magic squares, which are closely related to Graeco-Latin squares. He shows that a Graeco-Latin square of order n can be turned into a magic square by the following simple algorithm: replace the pair (a, b) with the number $(a-1)n+b$. For example, under this transformation, the Graeco-Latin square in Figure 2 becomes the magic square in Figure 3, all of whose rows and columns sum to 65. (Additional requirements are imposed if we require the diagonals to sum to 65.)

1	10	14	18	22
7	11	20	24	3
13	17	21	5	9
19	23	2	6	15
25	4	8	12	16

Figure 3: A magic square of order 5

Euler used Graeco-Latin squares of orders 3, 4, and 5 to construct magic squares. For an order-6 magic square, however, he used a different method. Perhaps because he was unable to construct an order-6 Graeco-Latin square, he was motivated to investigate their existence in a second paper [**10**], *Recherches sur une Nouvelle Espèce de Quarrés Magiques.* (Fans of Euler trivia should note that this was the only paper of Euler's originally published in a Dutch journal.) This was the first published mathematical analysis of Graeco-Latin squares. [1]

A lengthy paper (101 pages in the *Opera Omnia*), *Recherches* addressed many questions regarding Latin and Graeco-Latin squares. In this paper, we are primarily concerned with Euler's conclusions about the existence of Graeco-Latin squares of specific orders. In particular, he conjectured that there can be no such square of size $4k+2$ for any integer k. As we shall see, Euler was unable to prove this, although he did give plausibility arguments for squares of order 6, and he believed that his argument for squares of order 6 would generalize to the order $4k+2$ case.

[1] Graeco-Latin squares had appeared in print earlier. In his *Sources in Recreational Mathematics*, David Singmaster adds the following: "... there are pairs of orthogonal 4 by 4 squares in Ozanam [**18**] and Alberti [**1**].... a magic square of al-Buni, c1200, indicates knowledge of two orthogonal 4 by 4 Latin squares."

We begin our survey of the history of Euler's conjecture by carefully considering this paper and examining his results.

Euler

By 1782, when *Recherches* was published, Euler had returned to the St. Petersburg Academy, which was enjoying a modest renaissance under the patronage of Catherine the Great. Legend has it that Euler in fact first considered Graeco-Latin squares as a result of a question posed to him by the Empress: given 36 officers, six each of six different ranks and from six different regiments, can they be placed in a square such that exactly one officer of each rank and from each regiment appears in each row and column? Although this is the question with which Euler begins the paper, there is no mention of Catherine the Great and the attribution is probably apocryphal. He immediately claims that there is no solution, and then begins a hundred-page meandering path which eventually leads him to, if not a proof, then at least a plausibility argument for this claim.

As we begin our survey of this paper, we mention Euler's notation for Graeco-Latin squares. In his second paragraph, Euler introduced the Latin and Greek notation (hence the name). Each cell of the square contains one Latin and one Greek letter, forming two Latin squares, such that the orthogonality condition is satisfied (that is, each Latin-Greek letter pair appears just once). He gives the example depicted in Figure 4, meant to demonstrate something very close to a solution of the 36-officer problem. Although the Latin letters and the Greek letters independently form Latin squares, this example is not a solution because the pairs bζ and dε occur twice, while bε and dζ do not occur at all.

aα	bζ	cδ	dε	eγ	fβ
bβ	cα	fε	eδ	aζ	dγ
cγ	dε	aβ	bζ	fδ	eα
dδ	fγ	eζ	cβ	bα	aε
eε	aδ	bγ	fα	dβ	aζ
fζ	eβ	dα	aγ	cε	bδ

Figure 4: Almost a Graeco-Latin square

By paragraph 5, however, Euler abandons this unwieldy notation, and instead opts to use integers for both sets of entries, writing one set as bases, and the other as exponents. An example of this notation appears in Figure 5. Euler uses this notation in defining *formules directrices*, or guiding formulas. A guiding formula for a given n is a list of the columns in which n appears as an exponent, starting from the first row and reading down. For example, to find a guiding formula for the exponent 1 in Figure 5: in the first row, the exponent 1 appears in column 1; in the second row, it appears in column 2; and so forth. Thus, the guiding formula for 1 is $(1, 2, 3, 4, 5)$. Similarly, the guiding formula for the exponent 2 is $(5, 1, 2, 3, 4)$.

1^1	2^5	3^4	4^3	5^2
2^2	3^1	4^5	5^4	1^3
3^3	4^2	5^1	1^5	2^4
4^4	5^5	1^2	2^1	3^5
5^5	1^4	2^3	3^2	4^1

Figure 5: An order-5 Graeco-Latin square, using Euler's preferred notation

In considering the 36-officer problem, Euler organizes Latin squares into categories. He then tries to find a general method for "completing" the squares in each category, that is, by adding exponents to create a Graeco-Latin square.

Single-Step Latin Squares

In a single-step Latin square, the first row is simply $1, 2, \ldots, n$. The remaining rows are formed by cyclically shifting the elements in the previous row one place to the left, as shown in Figure 6.

1	2	3	$\cdots$	$n-1$	n
2	3	$\cdots$	$n-1$	n	1
3	$\cdots$	$n-1$	n	1	2
$\vdots$					$\vdots$
n	1	2	3	$\cdots$	$n-1$

Figure 6: A Single-Step Latin Square

In this simple case, Euler was able to complete Latin squares of orders 3, 5, 7, and 9. More importantly, he proved that a single-step Latin square of even order can never be completed. As the proof of this is both easily understood and indicative of the style of reasoning Euler employs throughout his paper, it is worth considering here. His reasoning makes use of the previously defined guiding formulas. If one can show that a guiding formula cannot exist for some exponent of a given square, then one deduces that the square cannot be completed. In particular, Euler often simply proves that no guiding formula can exist for the exponent 1, which is sufficient to show that the given square cannot be completed.

Theorem. *No single-step Latin square of even order can be completed.*

Proof: Suppose there is a such a square of even order n. Without loss of generality, the entry 1^1 is in the first cell. Suppose that there is a guiding formula for the number 1: $(1, a, b, c, d, e, \ldots)$. Denote the consecutive bases of which 1 is an exponent (from top to bottom) by $(1, \alpha, \beta, \gamma, \delta, \varepsilon, \ldots)$.

Thus we have a situation similar to that depicted in Figure 7, where blank spaces denote unknown entries.

		Columns							
		1	$\cdots$	b	$\cdots$	a	$\cdots$	c	$\cdots$
Rows	1	1^1							
	2					α^1			
	3			β^1					
	4							γ^1	
	$\vdots$								

Figure 7: An example of labeling in Euler's proof

Since 1 occurs exactly once in each row and column, the lists contain the same entries, merely in a different order. Thus we have

$$a + b + c + \cdots \equiv \alpha + \beta + \gamma + \cdots \pmod{n}.$$

According to the labeling of the entries in the square, the base located in row 2, column a is α. Moreover, in the second row of a single-step Latin square, the bases have been (cyclically) shifted one position to the left, as compared with the first row. Thus the base in row 2, column a is also congruent to $a + 1 \pmod{n}$ ("modulo n" due to the shift being cyclic). Thus we have that

$$\alpha \equiv a + 1 \pmod{n}.$$

Similarly, since the entries in row r have been shifted $r - 1$ spaces to the left (relative to the first row), we obtain the equations

$$\beta \equiv b + 2 \pmod{n}, \quad \gamma \equiv c + 3 \pmod{n}, \quad \ldots.$$

Adding these $n - 1$ congruences, we see that

$$1 + 2 + \cdots + (n - 1) \equiv 0 \pmod{n}.$$

That is, $\frac{n(n-1)}{2}$ must be an integer multiple of n, so n must be odd. Since n was assumed to be even, there can be no guiding formula for the exponent 1, so no single-step Latin square of even order can be completed. $\square$

Multiple-Step Latin squares

For m a divisor of n, an m-step Latin square of order n is defined as follows: partition the n-by-n square into m-by-m blocks. In the first row of blocks, let each block contain an m-by-m single-step

Latin square, where the first block uses the numbers 1 through m, the second block uses $m + 1$ through $2m$, and so forth. The remaining rows of blocks are formed by cyclically shifting the blocks in the previous row one place to the left. Figure 8 shows a 2-step (or double-step) Latin square and a 3-step (or triple-step) Latin square.

$$
\begin{array}{|cccccccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 & \cdots & \cdots & n-1 & n \\
2 & 1 & 4 & 3 & 6 & 5 & \cdots & \cdots & n & n-1 \\
3 & 4 & 5 & 6 & \cdots & \cdots & n-1 & n & 1 & 2 \\
4 & 3 & 6 & 5 & \cdots & \cdots & n & n-1 & 2 & 1 \\
5 & 6 & \cdots & \cdots & n-1 & n & 1 & 2 & 3 & 4 \\
6 & 5 & \cdots & \cdots & n & n-1 & 2 & 1 & 4 & 3 \\
\vdots & \vdots & & & & & & & \vdots & \vdots \\
\vdots & \vdots & & & & & & & \vdots & \vdots \\
n-1 & n & 1 & 2 & 3 & 4 & \cdots & \cdots & n-3 & n-2 \\
n & n-1 & 2 & 1 & 4 & 3 & \cdots & \cdots & n-2 & n-3 \\
\hline
\end{array}
$$

$$
\begin{array}{|cccccccccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 & \cdots & \cdots & \cdots & n-2 & n-1 & n \\
2 & 3 & 1 & 5 & 6 & 4 & \cdots & \cdots & \cdots & n-1 & n & n-2 \\
3 & 1 & 2 & 6 & 4 & 5 & \cdots & \cdots & \cdots & n & n-2 & n-1 \\
4 & 5 & 6 & \cdots & \cdots & \cdots & n-2 & n-1 & n & 1 & 2 & 3 \\
5 & 6 & 4 & \cdots & \cdots & \cdots & n-1 & n & n-2 & 2 & 3 & 1 \\
6 & 4 & 5 & \cdots & \cdots & \cdots & n & n-2 & n-1 & 2 & 3 & 1 \\
\vdots & \vdots & \vdots & & & & & & & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & & & & & & & \vdots & \vdots & \vdots \\
\vdots & \vdots & \vdots & & & & & & & \vdots & \vdots & \vdots \\
n-2 & n-1 & n & 1 & 2 & 3 & \cdots & \cdots & \cdots & n-5 & n-4 & n-3 \\
n-1 & n & n-2 & 2 & 3 & 1 & \cdots & \cdots & \cdots & n-4 & n-3 & n-5 \\
n & n-2 & n-1 & 2 & 3 & 1 & \cdots & \cdots & \cdots & n-3 & n-5 & n-4 \\
\hline
\end{array}
$$

Figure 8: A Double-Step Latin Square and a Triple-Step Latin Square

Recall that Euler was interested in solving the 36-officer problem, which in equivalent to finding an order-6 Graeco-Latin square, or completing an order-6 Latin square. An order-6 Latin square can be an m-step square only for $m = 1, 2, 3$. We have seen Euler's proof that a single-step Latin square of order 6 cannot be completed. Later in his paper, Euler proves that a double-step Latin square of order n can be completed only when n is a multiple of 4. He also gives a proof that a triple-step Latin square of order 6 cannot be completed. Therefore, Euler concludes that an order-6 Graeco-Latin square cannot be constructed by completing an m-step Latin square.

At the beginning of paragraph 140 of *Recherches*, Euler wrote

Ayant vu que toutes [les] méthodes que nous avons exposées jusqu'ici ne sauroient fournir aucun quarré magique pour le cas de $n = 6$ et que la même conclusion semble s'étendre à tous les nombres impairement pairs de n, on pourroit croire que, si de tels quarrés sont possibles, les quarreés latins qui leur servent de base, ne suivant aucun des ordres que nous venons de considérer, seroient tout à fait irréguliers. Il faudroit donc examiner tous les cas possibles de tels quarrés latins pour le cas de $n = 6$, dont le nombre est sans doute extrèmement grand.[2]

Because the number of cases was too large to check directly, Euler developed a set of transformations between Latin squares that preserved their ability to be completed. Obvious transformations include the swapping of two rows or two columns. Less obvious "completeness-preserving" transformations include finding a subrectangle of numbers with opposite corners matching, and then swapping the two corner numbers, as in Figure 9. Euler proved that if one of these squares can be completed, then both can.

$$
\begin{array}{|cccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
2 & \boxed{\mathbf{3}} & 4 & 5 & \boxed{\mathbf{6}} & 1 \\
3 & 4 & 5 & 6 & 1 & 2 \\
4 & 5 & 6 & 1 & 2 & 3 \\
5 & \boxed{\mathbf{6}} & 1 & 2 & \boxed{\mathbf{3}} & 4 \\
6 & 1 & 2 & 3 & 4 & 5 \\
\hline
\end{array}
\quad \text{becomes} \quad
\begin{array}{|cccccc|}
\hline
1 & 2 & 3 & 4 & 5 & 6 \\
2 & \boxed{\mathbf{6}} & 4 & 5 & \boxed{\mathbf{3}} & 1 \\
3 & 4 & 5 & 6 & 1 & 2 \\
4 & 5 & 6 & 1 & 2 & 3 \\
5 & \boxed{\mathbf{3}} & 1 & 2 & \boxed{\mathbf{6}} & 4 \\
6 & 1 & 2 & 3 & 4 & 5 \\
\hline
\end{array}
$$

Figure 9: Example of a "completeness-preserving" transformation

By using these and other clever transformations, Euler was able to represent by a single Latin square as many as 720 equivalent squares, thus dramatically reducing the amount of searching necessary to determine whether an order 6 square was possible. Here, however, Euler seems to have abandoned rigor in the face of the enormous number of cases he still needed to check. In paragraph 148, he writes

De là il est clair que, s'il existoit un seul quarré magique complet de 36 cases, on en pourroit déduire plusiers autres moyennant ces transformations, qui satisferient égalment aux conditions du problème. Or, ayant examiné un grand nombre de tels quarrés sans avoir recontré un seul, il est plus que probable qu'il n'y en ait aucun ... l'on voit que le nombre des variations pour le cas de $n = 6$ ne sauroit être si prodigiuex, que le nombre de 50 ou 60 que je pourrois avoir examinés n'en fût qu'une petite partie, J'observe encore

[2] Having seen that all methods that we have shown so far do not give any magic squares for the case of $n = 6$ and that the same conclusion seems to apply to any number of the form $4k + 2$, we could believe that if such squares are possible, the Latin squares that serve as their base, not following any order that we have just considered, would be completely irregular. Thus, it would be necessary to examine all the possible cases of such Latin squares for the case of $n = 6$, the number of which is undoubtedly extremely large.

> à cette occasion que le parfair dénombrement de tous les cas possibles de variations semblables seroit un objet digne de l'attention de Géomètres.[3]

Although he had not provided rigorous demonstration of all his claims, Euler still ends his paper with a fascinating and prescient conclusion:

> ... à voir s'il y a des moyens pour achever l'énumerations de tous les cas possibles, ce qui paroît fournir *un vaste champ pour des recherches nouvelles et intéressantes* [emphasis added]. Je mets fin ici aux miennes sur une question qui, quoique en elle-même de peu d'utilité, nous a conduit à des observations assées importantes tant pour la doctrine des combinaisions que pour la théories générale des quarrés magique.[4]

Early "Proofs" of the 36-Officer Problem

The first proof of the 36-officer problem was apparently by Thomas Clausen [**23**], an assistant to Heinrich Schumacher, a nineteenth-century astronomer in Altona, Germany. Schumacher and Carl Gauss, then Astronomer in Göttingen, enjoyed a brief correspondence; in a letter dated August 10, 1842, Schumacher wrote that Clausen had proved the nonexistence of orthogonal Latin squares of order 6. Apparently Clausen proved this by dividing all Latin squares of order 6 into 17 families and then proving that each in turn could not be completed. Clausen also believed, as Euler did, that a similar result was possible for order-10 squares, but he reported that:

> Der Beweis der vermutheten Unmöglichkeit für 10, so geführt wie er ihn für 6 geführt hat, würde wie er sagt, vielleicht für menschliche Kräfte unausführbar seyn.[5]

Sadly, although Clausen published over 150 papers during his scientific career, few of them survive, and no record of his alleged proof can be found. Thus, in order to establish precedence in the proof of the 36-officer problem, which is tantamount to determining whether Clausen gave a correct proof, we can only consider his record as a scientist and a mathematician in order to assess his claim.

[3] From here it is clear that if there existed a single complete magic square with 36 entries, we could derive several others using these transformations that would also satisfy the conditions of the problem. But, having examined a large number of such squares without having encountered a single one, it is most likely that there are none at all.... we see that the number of variations for the case of $n = 6$ cannot be so prodigious that the 50 or 60 that I have examined were but a small part. I observe further here that the exact count of all the possible cases of similar variations would be an object worthy of the attention of Geometers [mathematicians].

[4] ...seeing if there are methods of achieving the enumeration of all the possible cases would seem to provide a vast field for new and interesting research. Here, I bring to an end my [work] on a question that, although is of little use itself, has led us to some observations just as important for the doctrine of combinations as for the general theory of magic squares.

[5] The proof that [order] 10 is impossible, based on the proof of the [order] 6 [square], is perhaps impractical for human forces.

The definitive published study on Clausen is by Biermann [**2**], who describes him as "a remarkable man". By the age of 23, Clausen had mastered Latin, Greek, French, English, and Italian, and had gained sufficient notoriety in mathematics and astronomy to earn him an appointment at the Altona Observatory in 1824. He was well known to the leading scientists of his day, including Gauss. Not known for generously praising others, Gauss nonetheless described Clausen as a man of "outstanding talents". Clausen won the prize of the Copenhagen Academy for his paper on the comet of 1770 [**7**]. Perhaps more impressive was his factorization of the 6^{th} Fermat number, $2^{64}+1$, showing that it was not prime. It is still not known how, without the aid of modern computational devices, Clausen was able to do this (the smallest factor is 274,177). In his article, Biermann writes that "He possessed an enormous facility for calculation, a critical eye, and perseverance and inventiveness in his methodology".

Certainly these facts give Clausen a strong degree of authenticity in his claims. Further evidence for his claim is the fact that his method of breaking Latin squares into 17 families directly foreshadows the earliest surviving proof, by Tarry in 1900. All of this leads the authors to believe that the claims of priority for the first correct proof of the 36-officer problem rightly belong to Thomas Clausen.

The first surviving proof of this problem is that of Gaston Tarry, a French schoolteacher, who published his work [**25**] in 1900. Tarry's paper was necessarily quite lengthy; he proved the non-existence of an order-6 Graeco-Latin square by individually considering not only 17 families, but 9408 separate cases. Thus did Tarry fulfill Euler's 118-year-old request for a "complete enumeration" of all possible cases.

After the appearance of Tarry's paper, mathematicians began to search for a more clever proof. In 1902, Peterson published *Les 36 Officiers* [**21**], in which he attempted to provide a proof using a geometrical argument. He constructed simplicial complexes from Latin squares, and used a generalization of (fittingly enough) Euler's polyhedron formula[6] to construct impossibility relations between the numbers of 0-, 1-, and 2-cells in his complexes to prove that the order-6 Latin squares could not be completed.

Then, in 1910, Wernicke published *Das Problem der 36 Offiziere* [**26**], in which he shows that Peterson's proof is incomplete. He goes on to use a group-theoretic technique to put limits on the maximum possible number of mutually orthogonal Latin squares of order n. He purports to show that there do not exist two orthogonal Latin squares of order 6; in other words, there is no Graeco-Latin square of order 6.

A Resolution of Euler's Conjecture

Recall that Euler believed not only that Graeco-Latin squares of order 6 could not exist, but in general could not exist with any order of the form $4k+2$. Euler was unable to resolve this conjecture

[6] on the relation between the number of faces f, edges e, and vertices v of a polyhedron, namely $f - e + v = 2$

with techniques then available. However, as time passed, a variety of new tools became available that could be used to investigate Graeco-Latin squares.

The first modern reformulation involved endowing Latin squares with an algebraic structure, as follows: a *quasigroup* is a set Q with a binary relation $\circ$ such that for all elements a and b, the equations $a \circ x = b$ and $y \circ a = b$ have unique solutions. For example, let $Q = \{0, 1, 2\}$ and $a \circ b = (2a + b + 2) \bmod 3$. The multiplication table for this operation is given in Figure 10. Note that this is in fact a Latin square. It turns out that this is true in general: the multiplication tables of a quasigroup is a Latin square (and vice versa). In particular, the multiplication table of a group is a Latin square, since a group is an associative quasigroup with an identity element.

$\circ$	0	1	2
0	2	0	1
1	1	2	0
2	0	1	2

Figure 10: Multiplication table for a quasigroup

The first application of group-theoretic techniques to Latin squares was implemented by MacNeish [**15**] in 1922. He also disproved Wernicke's earlier results, just as Wernicke had disproven Peterson's. MacNeish's greatest contribution was the introduction of the concept of the direct product of Latin squares, a method for combining two Latin squares to make a third, whose order is the product of the orders of the original two. To get an idea of how this construction works, consider the two Latin squares and their direct product in Figure 11. In a sense, it is as though we have superimposed the pattern of the second Latin square on each entry of the first.

A useful property of this construction is that if we have a pair of orthogonal Latin squares A and B (necessarily of the same size), and another orthogonal pair C and D, then $A \times C$ and $B \times D$ are orthogonal! This allows us to build large Graeco-Latin squares from smaller ones. Unfortunately, this could not be used to construct a Graeco-Latin square or order 6 or 10, since there is no such square of order 2.

From this method, MacNeish proved the following result: Let $N(n)$ be the number of mutually orthogonal Latin squares of order n. Then,

$$N(ab) \geq \min\{N(a), N(b)\}.$$

As a feasibility argument, we present the following example: Let L_1, L_2, and L_3 be mutually orthogonal Latin squares of order a, and let M_1, M_2, M_3, and M_4 be mutually orthogonal Latin squares of order b. Then, $L_1 \times M_1, L_2 \times M_2$, and $L_3 \times M_3$ are all mutually orthogonal Latin squares of order ab. MacNeish then proved a stronger result: If the prime factorization of n is $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then $N(n) \geq \min\{p_i^{e_i} - 1\}$. (To prove this, he used group-theoretic techniques to construct large numbers of mutually orthogonal Latin squares of prime power order.) Finally,

A	B	C	D
B	C	D	A
C	D	A	B
D	A	B	C

1	2	3
2	3	1
3	1	2

A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3
A2	A3	A1	B2	B3	B1	C2	C3	C1	D2	D3	D1
A3	A1	A2	B3	B1	B2	C3	C1	C2	D3	D1	D2
B1	B2	B3	C1	C2	C3	D1	D2	D3	A1	A2	A3
B2	B3	B1	C2	C3	C1	D2	D3	D1	A2	A3	A1
B3	B1	B2	C3	C1	C2	D3	D1	D2	A3	A1	A2
C1	C2	C3	D1	D2	D3	A1	A2	A3	B1	B2	B3
C2	C3	C1	D2	D3	D1	A2	A3	A1	B2	B3	B1
C3	C1	C2	D3	D1	D2	A3	A1	A2	B3	B1	B2
D1	D2	D3	A1	A2	A3	B1	B2	B3	C1	C2	C3
D2	D3	D1	A2	A3	A1	B2	B3	B1	C2	C3	C1
D3	D1	D2	A3	A1	A2	B3	B1	B2	C3	C1	C2

Figure 11: Two Latin squares and their direct product

MacNeish conjectured that equality holds; that is, the number of mutually orthogonal Latin squares is actually equal to $\min\{p_i^{e_i}-1\}$. If true, this would imply Euler's conjecture, since 2^1 is the smallest prime power in the factorization of $4k+2$.

The next surge of research on Latin squares was motivated by practical applications. In the late 1930s, Fisher and Yates began to advocate the use of Latin squares and sets of mutually orthogonal Latin squares in the statistical design of experiments [**11**]. For example, suppose that we wish to test five different fertilizers but only have a single plot of land on which to do so. There may be unknown characteristics of the land, such as soil variation or a moisture gradient, that may bias the results of the experiment. To minimize the effects of such position-dependent factors, we divide the plot of land into a five-by-five grid, number the subplot as a Latin square, and place each type of fertilizer in those subplots with a particular number.

Sets of mutually orthogonal Latin squares have their uses as well. A set of k orthogonal Latin squares of size n gives a schedule for an experiment with k groups of n subjects each such that

1. Each subject meets every subject in each of the other groups exactly once;

2. Each subject is tested once at each location (to remove location-dependent bias).

For example, say that we want to test two groups of laboratory mice (an experimental group and a control group) in a series of n mazes so that each mouse races against each one in the other group, and no mouse runs in the same maze twice. A schedule for the tests can be developed by a Graeco-Latin square of order n.

After Yates constructed sets of mutually orthogonal Latin squares of orders 4, 8, and 9, Fisher conjectured during a seminar at the Indian Statistical Institute that a maximum set of orthogonal Latin squares of order n (i.e. a set of $n-1$) exists for each prime power order. This was proven soon after by Bose [**3**] in 1938, using finite fields (sometimes called Galois fields). Until this point, mathematicians had used groups – algebraic structures with a single binary operation – to construct Latin squares. One of Bose's great contributions was that he developed a method that used fields – algebraic structures with *two* binary operations. In essence, one operation allows the construction of a Latin square, and the second enables the permutation of the entries to create other squares orthogonal to it. More precisely, given a field $\mathbb{F}$ of n elements, $\mathbb{F} = \{g_1, g_2, \ldots, g_n\}$, choose some nonzero element g in $\mathbb{F}$. Define an order-n Latin square L_g by assigning to the position in the i^{th} row and the j^{th} column the element $(g \cdot g_i) + g_j$. Furthermore, it is also true that if g and h are different nonzero elements in $\mathbb{F}$, then L_g and L_h are orthogonal! For example, consider the field $\mathbb{F} = \{0, 1, 2, 3, 4\}$ with the operations of addition and multiplication modulo 5. Then the Latin squares L_2 and L_3, shown in Figure 12, are orthogonal.

$$L_2 = \begin{array}{|ccccc|} \hline 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \\ \hline \end{array} \qquad L_3 = \begin{array}{|ccccc|} \hline 0 & 1 & 2 & 3 & 4 \\ 3 & 4 & 0 & 1 & 2 \\ 1 & 2 & 3 & 4 & 0 \\ 4 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 0 & 1 \\ \hline \end{array}$$

Figure 12: Orthogonal Latin squares constructed from a field

Bose was also able to construct orthogonal Latin squares using projective geometry. A *projective plane of order* n is a set of $n^2 + n + 1$ elements (where $n \geq 2$) called *points* and a collection of subsets called *lines* that satisfy two conditions: each pair of points lies on exactly one line, and each pair of lines meet in exactly one point. (From these conditions it follows that there are $n+1$ points on each line, and each point is on $n+1$ lines.) Bose developed a method to turn a finite projective plane of order n into a set of $n-1$ mutually orthogonal Latin squares of order n, and conversely. For a fully worked-out example when $n = 3$ (which is rather lengthy) we refer the reader to [**17**].

Projective planes are known to exist only when n is the power of a prime, so they cannot be used to yield any Graeco-Latin squares of orders not constructible by the field method. For example, although we could use a projective plane of order 125 to build a Graeco-Latin square of order 125, we could have just as easily used a pair of orthogonal Latin squares of order 5 (such as those in Figure 12) and the direct product construction three times (since $5^3 = 125$). Nevertheless, the equivalence of the two problems is in itself interesting.

At this point, using the methods we have discussed so far, we can now construct Graeco-Latin squares of every order n except those values for which the prime factorization of n contains only a single factor of 2; equivalently, we can construct exactly those Graeco-Latin squares which Euler stated were constructible. The next step in settling Euler's conjecture was to look at the methods of construction, as done by Mann [**16**] in 1942. He introduced a general framework in which to view all the work that preceded him.

Assume that a given Latin square is in standard form, that is, the first row contains the numbers 1 through n in order from left to right. Let σ_i be the permutation of $1, 2, \ldots, n$ that sends j to the element of the Latin square in row i, column j. In this manner we associate a permutation with each row. Since we require that the entries be in standard form, the first row is associated with the identity permutation. For an example, see Figure 13.

$$\begin{array}{|ccccc|} \hline 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ \hline \end{array} \quad \begin{array}{l} \Rightarrow (1)(2)(3)(4)(5) \\ \Rightarrow (12345) \\ \Rightarrow (13524) \\ \Rightarrow (14253) \\ \Rightarrow (15432) \end{array}$$

Figure 13: A Latin square and the permutations associated with its rows

If these permutations form a group G, the Latin square is said to be based on G. For example, the Latin square in Figure 13 is based on the subgroup of S_5 consisting of the permutations

$$(1)(2)(3)(4)(5), (12345), (13524), (14253), (15432).$$

Mann noted that all constructions up to this point (those of Euler, Yates, Bose, etc.) had been based on groups. He went on to prove that for all group-based Latin squares, MacNeish's conjecture is true, and thus Euler's conjecture is true. However, Mann demonstrates that not all sets of orthogonal Latin squares are based on groups, and he gives an example of two such squares of order 12 in [**17**]. Therefore, any counterexample to Euler's conjecture must involve constructing Latin squares in a way entirely different from those that had been considered up to this point.

Not for another 17 years did someone succeed in methodically constructing Latin squares using methods not based on groups. In 1959, E. T. Parker [**19**] began to use orthogonal arrays to represent sets of mutually orthogonal Latin squares. An orthogonal array of order n is a k-by-n^2 matrix filled with the symbols $1, 2, \ldots, n$ so that in any 2-by-n^2 submatrix, each of the possible n^2 pairs of symbols from $\{1, 2, \ldots, n\}$ occurs exactly once. Orthogonal arrays can encode the information present in a set of mutually orthogonal Latin squares: the first row of the array represents row indices (of the Latin square), the second row represents column indices, and the remaining rows represent the entries in a given cell. Figure 14 shows a Graeco-Latin square and its corresponding orthogonal array. To see how this correspondence works, consider the seventh column of the orthogonal array, $(3, 1, 3, 2)$. This means that in row 3 column 1 of its corresponding Graeco-Latin square, we will find the symbol 3, then 2. One of the advantages to working with orthogonal arrays is that permuting the data is easier: we could in fact take any two rows to represent row and column indices and still obtain a valid set of orthogonal Latin squares.

(1,1)	(2,2)	(3,3)
(2,3)	(3,1)	(1,2)
(3,2)	(1,3)	(2,1)

$$\begin{pmatrix} 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 1 & 2 & 3 & 1 & 2 & 3 & 1 & 2 & 3 \\ 1 & 2 & 3 & 2 & 3 & 1 & 3 & 1 & 2 \\ 1 & 2 & 3 & 3 & 1 & 2 & 2 & 3 & 1 \end{pmatrix}$$

Figure 14: A Graeco-Latin square and its corresponding orthogonal array

To determine which k-by-n^2 matrices correspond to orthogonal Latin squares, Parker used the incidence properties of block designs – combinatorial designs similar to projective planes, but with fewer structural restrictions. Recall that Bose had used projective planes to produce Latin squares earlier, but since block designs have greater flexibility, Parker was able to use them to produce Latin squares that were not based on groups, and he was thus able to circumvent the limitations discovered earlier by Mann. In particular, Parker constructed four orthogonal Latin squares of order 21 using this method, thus disproving MacNeish's conjecture (since $N(21) \geq 4$ but $\min\{3 - 1, 7 - 1\} = 2$). While this cast some doubt on Euler's conjecture (by disproving the major conjecture that supported it), the conjecture was still at least plausible. No Graeco-Latin square of order $4k + 2$ had been found in 180 years of searching.

After the appearance of Parker's paper, a flurry of correspondence ensued between Parker, Bose, and Shrikhande; this eventually resulted in the publication of a series of papers that completely refuted Euler's conjecture. Bose and Shrikhande expanded on Parker's results and used block designs to produce a Graeco-Latin square of order 22, the first counterexample to Euler's conjecture ([**4**], [**5**]). Parker then constructed one of order 10 (the minimum possible order of a counterexample) using orthogonal arrays [**20**]. The components of the columns were elements of a field, permuted via an algorithm similar to that in Bose's 1938 paper, with the exception of nine columns that corresponded to a 3-by-3 Graeco-Latin subsquare (which does not contradict Mann's results). Parker attributed the inspiration to Bose and Shrikhande. All three authors collaborated on a final paper in which counterexamples are given for all orders $n = 4k + 2 \geq 10$ [**6**]. Their proof involves the use of block designs (in a lengthy case-by-case analysis), and techniques from their earlier papers. A modern description of these techniques can be found in [**14**].

Thus, by 1960, Euler's conjecture had been settled, and it was shown to be almost entirely incorrect. However, a good problem is never truly finished, and work continued on the conjecture for years afterwards. The most significant contribution to the refinement of the disproof of Euler's conjecture was by Sade [**22**]. He developed a singular direct product construction for quasigroups (recall that the multiplication tables of quasigroups are equivalent to Latin squares), and this provided counterexamples to Euler's conjecture via purely algebraic methods. However, this result was mostly overlooked at the time since Bose, Shrikhande, and Parker had just completed their seminal paper.

The singular direct product (SDP) of Latin squares requires three Latin squares, one each of orders k, n, and $n+m$, the last containing a Latin square of order m, and produces a Latin square of order $m+nk$. An example of this construction with squares of size $k=3$, $n=3$, and $n+m=5$ appears in Figure 15.

As with the direct product, if the process is performed on set of squares that are orthogonal, the resulting squares will also be orthogonal. Details aside, the important point is that the result is a Latin square whose order is not necessarily a multiple of any of the orders of the input squares. Using previous methods (such as MacNeish's direct product), one could not construct a Graeco-Latin square of order $4k+2$ from smaller squares because a Graeco-Latin square of order 2 does not exist. Sade's SDP, however, allowed him to construct many such squares, and in fact an infinite number of counterexamples to Euler's conjecture via purely algebraic methods.

3	4	5
4	5	3
5	3	4

A	C	B
C	B	A
B	A	C

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

1	2	3A	4A	5A	3B	4B	5B	3C	4C	5C
2	1	4A	5A	3A	4B	5B	3B	4C	5C	3C
3A	5A	1	2	4A	3C	4C	5C	3B	4B	5B
4A	3A	5A	1	2	4C	5C	3C	4B	5B	3B
5A	4A	2	3A	1	5C	3C	4C	5B	3B	4B
3B	5B	3C	4C	5C	1	2	4B	3A	4A	5A
4B	3B	4C	5C	3C	5B	1	2	4A	5A	3A
5B	4B	5C	3C	4C	2	3B	1	5A	3A	4A
3C	5C	3B	4B	5B	3A	4A	5A	1	2	4C
4C	3C	4B	5B	3B	4A	5A	3A	5C	1	2
5C	4C	5B	3B	4B	5A	3A	4A	2	3C	1

Figure 15: Three Latin squares and their singular direct product

A few subsequent contributions to the Graeco-Latin square problem are worth noting. In 1975, Crampin and Hilton [**8**] showed that if one starts with Latin squares of orders 10, 14, 18, 26, and 62, Sade's construction yields a complete set of counterexamples to Euler's conjecture. Using a computer, they also showed that the SDP can be used to construct self-orthogonal Latin squares (Latin squares orthogonal to their transpose) of all but 217 sizes. In 1984, Stinson [**24**] gave a modern mathematical *tour de force* by proving the 36-officer problem in only three pages by using a transversal design, finite vector spaces, and graph theory. Finally, in 1982, Zhu Lie [**13**] published what is considered by many to be the most elegant disproof of Euler's conjecture, using the SDP, a related construction of his own, and nothing else.

A good measure of the value of a mathematical problem is the number of interesting results generated by attempts to solve it. By this measure, Euler's conjecture of 1782 surely must rank among the most fertile problems in the history of mathematics. Although he was mistaken in his conjecture, it is a testimony to Euler's mathematical insight that he understood the importance of investigating such a simple problem.

References

[**1**] G.A. Alberti, *Giuochi Numerici Fatti Arcani Palesati*, Bologna, Bartolomea Borghi(1747).

[**2**] K.R. Biermann, Thomas Clausen, Mathematiker und Astronom, *J. für die reine und angewandte Mathematik*, 216 (1964) 159-198.

[**3**] R.C. Bose, On the Application of the Properties of Galois Fields to the Problem of Constructions of Hyper-Graeco-Latin Squares, *Sankhya: The Indian Journal of Statistics,* 3 (1938) 323–338.

[**4**] R.C. Bose and S.S. Shrikhande, On the falsity of Euler's conjecture about the non-existence of two orthogonal Latin squares of order $4t+2$, *Proc. Nat. Acad. Sci. U.S.A.,* 45 (1959) 734–737.

[**5**] R. C. Bose and S.S. Shrikhande, On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler, *Trans. Amer. Math. Soc.,* 95 (1960) 191–209.

[**6**] R.C. Bose, S.S. Shrikhande, and E.T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.,* 12 (1960) 189–203.

[**7**] T. Clausen, Determination of the Path of the 1770 Comet. *Astronomische Nachrichten*, 19 (1842), 121–168.

[**8**] D.J. Crampin and A.J. Hilton, Remarks on Sade's disproof of the Euler conjecture with an application to Latin squares orthogonal to their transpose, *J. Comb. Theory Ser. A,* 18 (1975) 47–59.

[**9**] L. Euler, De Quadratis Magicis. *Opera Omnia,* Ser. I, Vol 7: 441–457, *Commentationes arithmeticae* 2 (1849), 593–602. Also available online at http://www.eulerarchive.org.

[**10**] L. Euler, Recherches sur une nouvelle espèce de quarrés magiques. *Opera Omnia,* Ser. I, Vol 7, 291–392, *Verhandelingen uitgegeven door het zeeuwsch Genootschap der Wetenschappen te Vlissingen* 9 (1782), 85–239. Also available online at http://www.eulerarchive.org.

[**11**] Sir R. A. Fisher, *The Design of Experiments*, 9th Ed. Hafner Press (Macmillan), 1971.

[**12**] M. Gardner, *New Mathematical Diversions*, Simon and Schuster, 1966.

[**13**] Z. Lie, A short disproof of Euler's conjecture concerning orthogonal Latin squares, *Ars Combinatoria,* 14 (1982) 47–55.

[**14**] C.C. Lindner and C.A. Rodger, *Design theory,* CRC Press, 1997.

[**15**] H.F. MacNeish, Euler Squares, *Annals of Mathematics,* 23 (1922) 221–227.

[**16**] H.B. Mann, The construction of orthogonal Latin squares, *Ann. Math. Stat.,* 13 (1942) 418–423.

[**17**] H.B. Mann, On orthogonal Latin squares, *Bull. Amer. Math. Soc.,* 50 (1950) 249–257.

[**18**] Ozanam. *Récréations Mathématiques*, 1697.

[**19**] E.T. Parker, Construction of some sets of mutually orthogonal latin squares. *Proc. Amer. Math. Soc.,* 10 (1959) 946–994.

[**20**] E. T. Parker, Orthogonal Latin Squares. *Proc. Nat. Acad. Sci. U.S.A.,* 45 (1959) 859–862.

[**21**] J. Peterson, Les 36 officiers, *Annuaire des mathematicians,* (1902) 413–426.

[**22**] A. Sade, Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens, *Ann. Soc. Sci. Bruxelles Sér. I,* 74 (1960) 91–99.

[**23**] Letter from Shumacher to Gauss, regarding Thomas Clausen, August 10, 1842. Gauss, *Werke* Bd. 12, p.16. Göttingen, Dieterich, (1863).

[**24**] D.R. Stinson, A short proof of the nonexistence of a pair of orthogonal Latin squares of order six, *J. Combin. Theory Ser. A,* 36 (1984) 373–376.

[**25**] G. Tarry, Le problème des 36 officiers, *Comptes Rendus Assoc. France Av. Sci.* 29, part 2 (1900) 170–203.

[**26**] P. Wernicke, Das Problem der 36 Offiziere, *Jahresbericht der deutschen Mathematiker-Vereinigung,* 19 (1910) 264.