Greco-Latin Squares and a Mistaken Conjecture of Euler

Dominic Klyve* Lee Stemkoski*

February 19, 2004

Abstract

Euler once conjectured that Graeco-Latin squares of order $4n + 2$ do not exist. We discuss the history of this problem and repeated attempts at proof and disproof. In addition, we survey a variety of mathematical techniques that were developed as a result during the following 200 years, culminating in a complete refutation of Euler’s conjecture.

1 Introduction

Toward the end of his long and productive career, Leonhard Euler published a 100-page paper detailing the properties of a new mathematical structure: Greco-Latin squares. Toward the end of the paper, Euler claimed that a Greco-Latin square of size $n$ could never exist for any $n = 4k + 2$, but was not able to prove this rigorously. Although Euler was eventually proven to be wrong, developing a complete set of counterexamples required the efforts of two dozen mathematicians working over 200 years, publishing in three languages, and using results from areas of mathematics such as manifold theory, finite fields, projective planes, group theory, statistical and block designs, and a heavy dose of computing power.

A Latin square (of order $n$) is an $n$ by $n$ array of $n$ distinct symbols (usually the set of integers $\{1, \ldots , n\}$ is often used for convenience) such that each symbol appears exactly once in each row and column. Some examples appear in figure 1.

\begin{center}
\begin{array}{ccc}
1 & 2 & 3 \\
3 & 1 & 2 \\
2 & 3 & 1 \\
\end{array}
\quad
\begin{array}{ccc}
4 & 3 & 1 & 2 \\
3 & 4 & 2 & 1 \\
1 & 2 & 4 & 3 \\
2 & 1 & 3 & 4 \\
\end{array}
\end{center}

A Greco-Latin square (of order $n$) is an $n$ by $n$ array of ordered pairs $\{(a, b) \mid a, b \in \{1, \ldots , n\}\}$ such that in each row and each column of the array, each integer $1, \ldots , n$ appears exactly once in each coordinate, and that each of the $n^2$ possible pairs appears exactly once in the entire square. Figure 2 contains such an example.

\begin{center}
\begin{array}{cccc}
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 \\
\end{array}
\end{center}

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

Figure 2: A Greco-Latin square of order 5

A Greco-Latin square is sometimes referred to as a pair of orthogonal Latin squares, since the square formed by taking either all first or all second coordinates will also be a Latin square. From this idea there is a natural and useful generalization to a set of $k$ mutually orthogonal Latin squares. A set of $k$ Latin squares is said to be mutually orthogonal if each pair of squares forms a Greco-Latin square: each Latin square can be thought of as one set of coordinates from a Greco-Latin square, and when put together in this way, each possible pair of numbers occurs exactly once. Two natural questions to ask, then, are: do

*Department of Mathematics, Dartmouth College, Hanover, NH
there exist Greco-Latin squares of all orders, and how many mutually orthogonal Latin squares there are of a given order \( n \)?

Leonhard Euler published two papers concerning Greco-Latin squares. The first, written in 1776, is entitled *De Quadratis Magicis* (E795) [Eu1]. In this fairly short paper (seven pages in the *Opera Omnia*), Euler considered magic squares, which share many properties with Greco-Latin squares. (In particular, a Greco-Latin square can be turned into a magic square by a simple algorithm.) This was one of the first papers published about magic squares, and probably the first to consider the generalized concept of magic square. However, the results contained in this paper are few, and none of them pertain to Greco-Latin squares, so we will not delve into *De Quadratis Magicis* in this paper.

Far more important to our inquiry is Euler’s second and final paper dealing with Greco-Latin squares, *Recherches sur une Nouvelle Espèce de Quarrés Magiques* (E530) [Eu2], published in 1782 in *Verhandelingen uitgegeven door het zeeruwsh Genootshap der Wetenschappen te Vlissingen*. (Fans of Euler trivia should note that this was the only paper of Euler’s first published in a Dutch journal.) As a testament to Euler’s prescience, this is the first appearance of Greco-Latin squares in the (mathematical) literature.\(^1\)

A lengthy paper (101 pages in the *Opera Omnia*), *Recherches* addressed many questions regarding Latin and Greco-Latin squares. In this paper, we are primarily concerned with Euler’s conclusions about the existence of Greco-Latin squares of various orders. In particular, he conjectured that there can be no Greco-Latin square of size \( 4k + 2 \), for any integer \( k \). As we shall see, Euler was unable to prove this conclusively, though he did give strong 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.

Euler’s conjecture would be repeatedly examined over the next two centuries. In the end, Euler’s difficulty in proving the result was validated; it took more than 20 researchers from five countries publishing in three languages to solve the problem, and then only after utilizing techniques from many diverse branches of mathematics. These included Manifold Theory, Algebraic Topology, Abstract Algebra, Projective Geometry and Combinatorial Designs, Statistical Analysis, and, in addition, a fair amount of modern computing power.

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

\(^1\) Although their existence had been noted previously. In his *Sources in Recreational Mathematics*, David Singmaster adds the following: “... there are pairs of orthogonal 4 by 4 squares in Ozanam [Oz] and Alberti [Al]. (The pair in Bachet is due to the 1874 editor.) ... a magic square of al-Buni, c1200, indicates knowledge of two orthogonal 4 by 4 Latin squares.”
was originally stated as follows: There are 36 officers, 6 each of 6 different ranks and from 6 different regiments. How 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? There seems to be no historical basis for this story, and it is probably apocryphal. This is the question with which Euler opens the paper, albeit without any mention of Catherine the Great. He immediately claims that there is no solution, and then begins a 100-page meandering path which eventually leads him to, if not a proof, then at least a plausibility argument of this claim. We first examine this path of Euler’s.

The first thing we call attention to is the notation that Euler used for his Greco-Latin squares. In paragraph 2, Euler introduced the now-immortalized Latin and Greek notation. In particular, each cell of the square contained one Latin and one Greek letter, forming two Latin squares, such that the orthogonality condition is satisfied (that is, each letter-letter combination appears in exactly one cell). He gives the example depicted in figure 3, meant to demonstrate something very close to a solution of the 36-officer problem. Although either the Latin or Greek letters taken independently form a Latin square, this example is not a solution because the terms \( b\zeta \) and \( d\varepsilon \) occur twice, while \( b\varepsilon \) and \( d\zeta \) do not occur at all.

![Figure 3: Almost a Greco-Latin square](image)

By paragraph 5, however, Euler discards this notion as being unwieldy, and instead opts to use integers for both sets of entries, writing one set as bases, and one as exponents. An example of this notation appears in figure 4. Using this method, both the bases and the exponents in each row and column can be enumerated. Euler uses this notation in defining les formules directrices: guiding formulas, explained below.

![Figure 4: An order 5 Greco-Latin square, using Euler’s preferred notation](image)

For a Greco-Latin square written with this notation, Euler describes guiding formulas for each of the exponents. To find a guiding formula for a given \( n \), we read from the top row down, and record the columns in which \( n \) appears as an exponent. For example, to find a guiding formula for the exponent 1 in figure 4: in the first row, the exponent 1 appears in column 1; in the second row, it appears in column 2, etc. Thus, the guiding formula for 1 is \( (1, 2, 3, 4, 5) \). Similarly, the guiding formula for the exponent 2 is \( (5, 1, 2, 3, 4) \).

After paragraph 5, the Latin and Greek letters do not surface again as entries of a Greco-Latin square in Recherches. Euler himself refers to the squares as “complete squares” in his paper. An anecdotally interesting aside here is the history of the terminology for these squares; as we move through the 200 years of work on this problem, we will see the name of the Greco-Latin squares change from complete squares
(1782) to Euler squares (1900) to Greco-Latin squares (1930s) to pairs of orthogonal Latin squares (1940s) and back to Greco-Latin squares (1950s).

Philology aside, we turn to Euler’s mathematics. In order to consider the 36-officer problem, Euler organized all Latin squares into broad categories. The simplest of these were the single-step, double-step, and triple-step Latin squares. Then he considered, for each category of squares, whether a given Latin square from the category could be completed (i.e., could be one of the two squares of a Greco-Latin square). The “step” defining each category is best conveyed visually by considering figures 5, 6, and 7.

Figure 5: A Single-Step Latin Square

Figure 6: A Double-Step Latin Square

Figure 7: A Triple-Step Latin Square
Single-Step Latin Squares

In this simple case, Euler was able to construct many Greco-Latin squares of orders 3, 5, 7, and 9. More importantly, he proved that a single-step Latin square can never be completed (i.e., made into a Greco-Latin square by adding exponents) if its order is even. As the proof of this is both easily understood and indicative of the style of reasoning Euler employs throughout his paper, it is worthwhile to consider the proof of this statement here. His reasoning makes use of the previously defined guiding formulas. If Euler can show that a guiding formula cannot exist for all the exponents of a given square, then certainly the square can not be completed. In particular, Euler often simply proves that a guiding formula cannot 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 \( n \) can be completed.

**Proof:** Without loss of generality, assume row 1, column 1 contains the entry \( 1^1 \). Assume that there is a guiding formula for the number 1: \((1, a, b, c, d, e, \ldots)\). Denote the bases of which 1 is an exponent (as we read down the rows from top to bottom) by \((1, \alpha, \beta, \gamma, \delta, \epsilon, \ldots)\). Thus we have a situation similar to the one depicted in figure 8, where blank spaces denote unknown entries.

<table>
<thead>
<tr>
<th>Columns</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>( \cdots )</td>
</tr>
<tr>
<td>( b )</td>
</tr>
<tr>
<td>( \cdots )</td>
</tr>
<tr>
<td>( a )</td>
</tr>
<tr>
<td>( \cdots )</td>
</tr>
<tr>
<td>( c )</td>
</tr>
<tr>
<td>( \cdots )</td>
</tr>
<tr>
<td>( \vdots )</td>
</tr>
</tbody>
</table>

Figure 8: 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. Then 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 \( \alpha \). Moreover, in the second row of a single-step Latin square, all the bases have been (cyclically) shifted one position to the left, as compared with the first row. Thus the entry in row 2, column \( a \) is also congruent to \( a + 1 \) modulo \( n \) (the “modulo \( n \)” required due to the shift being cyclic). Thus we have that

\[
a \equiv \alpha + 1 \pmod{n}
\]

And similarly, since the entries in row \( r \) have been shifted \( r - 1 \) spaces to the left (as compared with the first row), we obtain the equations

\[
b \equiv \beta + 2 \pmod{n}; \quad c \equiv \gamma + 3 \pmod{n}; \quad \ldots
\]

Now let \( S = \alpha + \beta + \gamma + \delta + \cdots \). Then we have

\[
a + b + c + \cdots \equiv S + 1 + 2 + \cdots (n - 1) \pmod{n}
\]

\[
a + b + c + \cdots - S \equiv 1 + 2 + \cdots (n - 1) \pmod{n}
\]

Since \( a + b + c + \cdots \equiv \alpha + \beta + \gamma + \cdots \equiv S \pmod{n} \), we have

\[
0 \equiv 1 + 2 + \cdots (n - 1) \pmod{n}
\]
\[
\frac{1}{2}n(n - 1) \equiv 0 \pmod{n}
\]

\[
\frac{1}{2}n(n - 1) = m \cdot n \quad \text{(some integer } m)\]

and thus \(\frac{1}{2}(n - 1) = m\). This contradicts that \(n\) is even. \(\square\)

Therefore there can be no guiding formula for the exponent 1, hence an even order single-step Latin square cannot be completed. This obviously eliminates the possibility of a Greco-Latin square of order 6 in this simple case.

### Multiple-step Latin squares

Euler went on to consider double, triple, and quadruple-step Latin squares, proving that no order 6 Latin square of any of these types can be completed. Note that since a double-step Latin square must have an order which is a multiple of 2, a triple-step Latin square must have an order which is a multiple of 3, etc, Euler had to consider just the double- and triple-step Latin squares as a basis for his attack on the order 6 case (since the step size must always divide the order of the square, and a sextuple-step Latin square of order 6 is identical to a single-step square of order 6).

For the double-step case, Euler proved that the only possible squares were of order \(4k\), and went on to provide a method of constructing complete squares for all orders \(4k\). Proceeding on to the triple-step case, Euler was again able to prove that an order 6 square cannot be completed by dividing the square into four quarters, and proving that the needed orthogonality relations can never hold.

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 carré 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 carrés sont possibles, les carrés latins qui leur servent de base, ne suivant aucun des ordres que nous venons de considérer, seraient tout à fait irréguliers. Il faudrait donc examiner tous les cas possibles de tels carrés latins pour le cas de \(n = 6\), dont le nombre est sans doute extrêmement grand.\(^2\)

Because the number of cases was too large to check directly, Euler came up with a set of transformations between Latin squares that preserved their ability to be completed (made into Greco-Latin squares). 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 two squares can be completed, then both can.

By using these and other clever transformations, Euler was able to change any Latin square of order 6 into as many as 720 other squares, thus dramatically reducing the amount of searching he had to do to determine whether an order 6 square was possible. Here, however, Euler seems to have abandoned rigor in the face of what remained an enormous number of cases to check. In paragraph 148, he writes

De là il est clair que, s’il existoit un seul carré magique complet de 36 cases, on en pourrait déduire plusieurs autres moyennant ces transformations, qui satisferaient également aux conditions du problème. Or, ayant examiné un grand nombre de tels carrés sans avoir rencontré un seul, il est plus que probable qu’il n’y en ait aucun … l’on voit que le nombre des variations pour

\(^2\)Having seen that all the methods that we have looked at so far have failed to generate a complete Latin square of order 6, and that the same conclusion seems to apply to all numbers of the form \(4k + 2\), one might think that, if such squares were possible, the Latin squares which serve as their base would be of an irregular form which we have not considered. It remains, therefore, to examine all possible cases of such Latin squares for the case of \(n = 6\), the number of which is undoubtedly extremely large.
Figure 9: Example of a “completeness-preserving” transformation

le cas de \( n = 6 \) ne saurait être si prodigieux, que le nombre de 50 ou 60 que je pourrois avoir examinés n’en fût qu’une petite partie, J’observe encore à cette occasion que le parfait 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:

\[\ldots\text{ à voir s’il y a des moyens pour achever l’énumerations de tous les cas possibles, ce quit paroit fournir un vaste champ pour des recherches nouvelles et intéressantes}\] \[\text{[emphasis added]}\].

Je mets fin ici aux miennes sur une question qui, quoique en elle-même de peu d’utilité, nous a conduit à des observations assés importantes tant pour la doctrine des combinaisons que pour la théories générale des quarrés magique.\(^4\)

### 3 Early “Proofs” of the 36-Officer Problem

The first actual proof of the 36-officer problem was probably given by Thomas Clausen [Sh], an assistant to Heinrich Schumacher, a nineteenth-century astronomer in Altona. Schumacher and Carl Gauss, then astronomer in Göttingen, enjoyed a brief correspondence, and in a letter dated August 10, 1842, Schumacher wrote that Clausen had proved the nonexistence of 2 orthogonal Latin squares of order 6. Apparently Clausen proved this by dividing all Latin squares of order 6 into 17 families, and 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:

\[\text{Der Beweis der vermutheten Unmöglichkeit für 10, so geführt wie er ihn für 6 geführt hat, würde wie er sagt, vielleicht für menschliche Kräfte unausführbar seyn.}\] \[\text{[emphasis added]}\]

Sadly, although Clausen published over 150 papers during his scientific career, few of them remain, 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 evaluate his claim.

The definitive published study on Thomas Clausen is a paper by Biermann [Bi]. The paper describes Clausen as “a remarkable man”. By the age of 23, Clausen had mastered Latin, Greek, French, English,

\[^{3}\text{From this it is clear that, if there is a single complete Latin square of order 6, we know that there must be many others which are also complete. But, having examined a large number of such squares without having found even one, it is more than probable that there are none at all . . . one sees that the number of variations for the case of } n = 6 \text{ is known to be so extraordinary that the 50 or 60 that I have examined are only a small part. Further, I observe here that the complete enumeration of all possible cases is something worthy of the attention of mathematicians.}\]

\[^{4}\text{Seeing whether there is a method for achieving the enumeration of all the possible cases will begin to provide a vast field for new and interesting research} \] \[\text{[emphasis added]}\]. I add a final thought that, although this work in itself has little applicability, through the observations we have a conduit as much for the doctrine of combinations as for the general theory of magic squares.

\[^{5}\text{The proof that } |\text{order}| 10 \text{ is impossible, based on the proof of the } |\text{order}| 6 \text{ [square], is perhaps impractical for human forces.}\]
and Italian, and had gained sufficient notoriety in mathematics and astronomy to earn him an appointment at Altona Observatory in 1824. He was well known to the leading scientists of his day, including Carl Gauss. Not known for being overly gracious with praise of others, Gauss nevertheless described him as “a man of outstanding talents”. Clausen won the prize of the Copenhagen Academy for his work on determining the orbit of the comet of 1770. Perhaps more impressive was his factorization of the 6th 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 factorization (the smallest factor is 274177). 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 respectability 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 G. Tarry in 1900 (discussed later). All of this leads the authors to believe that the priority claims for the first correct proof of the 36-officer problem can be rightly given to Thomas Clausen.

The first surviving published proof of the 36-officer problem is that of Gaston Tarry [Ta], a French schoolteacher who published his paper in the centennial year of 1900. Tarry’s paper was necessarily quite lengthy; he proved the impossibility of an order 6 Greco-Latin square by individually considering not only 17 families, but also 9408 separate cases. Thus did Tarry fulfill Euler’s 118-year-old request for a “complete enumeration” of all possible cases.

Given that Tarry’s proof is both extant and correct, one may wonder at this point why any more work was done on the existence of Greco-Latin squares. The reasons are twofold, and are worth reiterating here. The first is that, to a mathematician, a proof using case-by-case analysis is not particularly satisfying. One may now believe that Euler’s conjecture is true, but the more interesting question of why it is true remains unanswered, and only a general proof can make that clear. Even more important is that at this point, Euler’s conjecture had been shown only to be partially true. Recall that Euler believed not only that no Greco-Latin square could exist for order 6, but in general could not exist of order \(4k + 2\), for any integer \(k\). With the exception of the trivial case of order 2, and the now-demonstrated case of order 6, it was still unknown whether Greco-Latin squares of order 10, 14, or beyond could exist.

After the appearance of Tarry’s paper, mathematicians began to search for a more clever proof of the 36-officer problem. In 1902, J. Peterson published *Les 36 Officiers* [Pe], 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) one of Euler’s formulas\(^6\) to construct impossibility relations between the number of 0- 1- and 2-cells in his complexes to prove that the order 6 Latin squares could not be completed.

Then, in 1910, P. Wernicke published *Das Problem der 36 Offiziere* [We], 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 can exist no more than one orthogonal Latin square of order 6, implying that constructing a Greco-Latin square of order 6 is impossible.

4 A Resolution of Euler’s Conjecture

As time went on and the vocabulary of mathematics grew richer, an algebraic foundation for Latin Squares was developed. In particular, using modern terminology a Latin square can be encoded in terms of a specific relation between the number of faces \(f\), edges \(e\), and vertices \(v\) of a polyhedron, namely \(f - e + v = 2\).
A *quasigroup* is a set *Q* with a binary relation • such that for all elements *a* and *b* of *Q*, the equations
\[ a \bullet x = b \quad \text{and} \quad y \bullet a = b \]
have unique solutions for *x* and *y*. For example, let *Q* = \{0, 1, 2\} and *a \bullet b = (2a + b + 2) \mod 3*. Then the multiplication table of the operation • is given in figure 10. Notice that the interior of the multiplication table is in fact a Latin square. It turns out that this is true in general: the multiplication tables of quasigroups are Latin squares (and vice versa). As a special case, the multiplication table of a group is a Latin square, since a group is an associative quasigroup with an identity element.

\[
\begin{array}{c|ccc}
\cdot & 0 & 1 & 2 \\
0 & 2 & 0 & 1 \\
1 & 1 & 2 & 0 \\
2 & 0 & 1 & 2 \\
\end{array}
\]

Figure 10: Multiplication table for the quasigroup \((Q, \bullet)\)

The first application of the group-theoretic techniques described above was implemented by H. MacNeish in 1922 [Mac1]. The next serious attempt at dealing with the mathematics of Latin squares, MacNeish disproved Wernicke’s earlier results [Mac2] (just as Wernicke had disproven Peterson’s results). MacNeish’s greatest contribution was the introduction of the direct product of Latin squares. The direct product is a method for taking two Latin squares and combining them to make a Latin square whose order is the product of the orders of the original squares, and whose symbols are composites of the symbols of the original squares. To get an idea of how this construction works, and since an example provides the insight of a thousand words, consider the two following Latin squares, denoted \(L, M\), in Figure 11.

\[
\begin{array}{cccc}
A & C & D & B \\
D & B & A & C \\
B & D & A & C \\
C & A & B & D \\
\end{array}
\quad
\begin{array}{c|ccc}
2 & 3 & 1 \\
3 & 1 & 2 \\
1 & 2 & 3 \\
\end{array}
\]

Figure 11: Latin squares \(L\) and \(M\)

An advantage to 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 up large Greco-Latin squares from smaller ones. Unfortunately, this will not help to construct a Greco-Latin square or order 6 or 10 (if they exist), because 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 \(\{L_1, L_2, L_3\}\) be mutually orthogonal Latin squares of order \(a\); let \(\{M_1, M_2, M_3, M_4, M_5\}\) be mutually orthogonal Latin squares of order \(b\). Then, \(\{L_1 \times M_1, L_2 \times M_2, L_3 \times M_3\}\) are all mutually orthogonal Latin squares of order \(ab\) (and there may be others). MacNeish then proves the stronger result: If \(n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}\) is the prime factorization of \(n\),
then \( N(n) = \min\{p_i^{e_i} - 1\} \) (To prove this, he used group-theoretic techniques to construct large numbers of mutually orthogonal Latin squares of prime power order.) Finally, 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 that Euler’s conjecture is true, since 2 is the smallest prime power in the factorization of \( 4^k + 2 \).

The next surge of research on Latin squares was motivated by practical applications. In the late 1930s, R. Fisher and F. Yates began to advocate the use of Latin squares and sets of mutually orthogonal Latin squares in the statistical design of experiments [Fi]. For example, imagine that we wish to test five different fertilizers but only have a single plot of land in 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 these or other position-dependent factors, we divide the plot of land into a five-by-five grid and number each subplot as we would an order five Latin Square, and place each type of fertilizer in the subplots assigned 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 every other group 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 mouse in the opposite group, and no mouse runs in the same maze twice. A schedule for the tests can be developed by a Greco-Latin square (two mutually orthogonal Latin squares, corresponding to the two groups) 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 maximal set of orthogonal Latin squares (i.e. a set of \( n - 1 \) mutually orthogonal Latin squares of order \( n \)) exists for each prime power order. This was proven soon after by R. Bose in 1938 [Bo], using finite fields (sometimes referred to as Galois fields) and finite projective planes. So far, we have seen that one can use groups – algebraic structures with a single binary operation – to construct Latin squares. One of Bose’s great contributions was that he developed a method to use fields – algebraic structures with two binary operations – to construct sets of mutually orthogonal Latin squares. In essence, one operation allows the construction of a Latin square, and the second enables us to permute the entries to create other squares orthogonal to it. More precisely, given a (finite) field \( \mathbb{F} \) of \( n \) elements, \( \mathbb{F} = \{g_1, g_2, \ldots, g_n\} \), choose some nonzero element \( g \) in \( \mathbb{F} \), and we
Create the order \( n \) Latin square associated to \( g \), denoted \( L_g \), as follows. Let the entry in the \( i \)th row and the \( j \)th column be given by

\[
((g \cdot g_i) + g_j)
\]

Not only is it true that \( L_g \) is a Latin square, it is also true that if \( g \) and \( h \) are distinct nonzero elements in \( \mathbb{F} \), then \( L_g \) and \( L_h \) are orthogonal Latin squares! For example, consider the field \( \mathbb{F} = \{0, 1, 2, 3, 4\} \) with the two operations of addition and multiplication modulo 5. Then we can construct the Latin squares \( L_2 \) and \( L_3 \) as in figure 13, and one can check that they are orthogonal.

\[
\begin{array}{ccccc}
0 & 1 & 2 & 3 & 4 \\
2 & 3 & 4 & 0 & 1 \\
4 & 0 & 1 & 2 & 3 \\
1 & 2 & 3 & 4 & 0 \\
3 & 4 & 0 & 1 & 2 \\
\end{array}
\quad \quad
\begin{array}{ccccc}
0 & 1 & 2 & 3 & 4 \\
3 & 4 & 0 & 1 & 2 \\
1 & 2 & 3 & 4 & 0 \\
4 & 0 & 1 & 2 & 3 \\
2 & 3 & 4 & 0 & 1 \\
\end{array}
\]

Figure 13: Orthogonal Latin squares constructed from a field

Bose also developed a way to turn finite projective planes into sets of mutually orthogonal Latin squares, and conversely. A projective plane of order \( n \) is a set of \((n^2 + n + 1)\) elements called points and a collection of subsets called lines that satisfy four conditions: two points determine a line, two lines determine a point, each point is on \((n^2 + 1)\) lines, and each line contains \( n + 1 \) points.

Projective planes are only known to exist when \( n \) is the power of a prime, so they cannot be used to yield any Greco-Latin squares of orders we did not know existed before. For example, although we could use a projective plane of order 125 to build a Greco-Latin square of order 125, we could have just as easily used a pair of orthogonal Latin squares of order 5 (e.g. those constructed in figure 13) and the direct product construction 3 times (since \( 5^3 = 125 \)). Nevertheless, the equivalence of the two problems is in itself interesting.

The construction of orthogonal Latin squares from a projective plane is outlined as follows: choose one of the lines in the projective plane, and label the points on that line \( P_0, P_1, \ldots, P_n \). Remove the chosen line. Each of the remaining lines goes through exactly one of the remaining points; these lines are labelled in a particular way. The lines are then used to coordinatize the remaining points, and the coordinates of each point yield the entries for a set of orthogonal Latin squares. For a fully worked-out example (the simplest of which is still rather lengthy) we refer the reader to [Man2].

At this point, using the methods we have discussed so far, we can now construct Greco-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 Greco-Latin squares which Euler stated were constructable. The next step in settling Euler’s conjecture was to look at the methods of construction, as done by H. Mann in 1942 [Man1]. Mann introduced a general framework in which to view all the work that preceded him. Let \( S_n \) denote the group of permutations of the set \( \{1, 2, \ldots, n\} \). Given a Latin square of order \( n \), associate an element \( g \) of \( S_n \) to each row, where \( g \) sends \((1, 2, \ldots, n)\) to that row. For an example, see the Latin square in figure 14.

If these permutations form a group \( G \), the Latin square is said to be based on the group \( G \). For example, the Latin square in figure 14 is based on the subgroup of \( S_5 \) consisting of the permutations \( \{(1)(2)(3)(4)(5), (12345), (13524), (14253), (15432)\} \). If each square in a set of orthogonal Latin squares is based on the same group \( G \), then the set is said to be based on \( G \). Mann notes that all constructions up to this point (those of Euler, Yates, Bose, etc.) have been based on groups. He went on to prove that for all Latin squares based on groups, MacNeish’s conjecture is true, and thus Euler’s conjecture is true. However, in one paper he 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. Therefore, any counterexample to
Euler’s conjecture must involve constructing Latin squares in a way entirely different from those which had been considered up to this point in time.

Not for another 17 years did somebody succeed in methodically constructing Latin squares using methods not based on groups. In 1959, E. T. Parker [Pa1] 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 \( \{1, 2, \ldots, n\} \) such that if you restrict the matrix to 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 record the information present in a set of mutually orthogonal Latin squares as follows: 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 15 shows a Greco-Latin square and its corresponding orthogonal array. As an example of how the correspondence works: the 7th column of the orthogonal array, \((3, 1, 3, 2)\), states that in row 3 column 1 of its corresponding Greco-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.

![Figure 14: A Latin square and the permutations associated to its rows](image)

![Figure 15: A Greco-Latin square and its corresponding orthogonal array](image)

To determine which \( k \) by \( n^2 \) matrices yield valid orthogonal arrays (those which 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 for producing Latin squares earlier, but since block designs have greater flexibility, Parker was able to use them to produce Latin squares not based on groups and was thus able to circumvent the limitations proven earlier by Mann. In particular, Parker constructed four orthogonal Latin squares of order 21 using this method, thus disproving MacNeish’s conjecture, since

\[
N(21) = N(3 \cdot 7) \neq \min\{3 - 1, 7 - 1\} = 2 \quad \text{(since } N(21) \geq 4)\]

However, while this did cast some doubt on Euler’s conjecture by disproving the major conjecture that supported it, Euler’s conjecture was still at least plausible; no Greco-Latin square of order \( 4k + 2 \) had been found during the past 180 years.
After this paper was written by Parker, a flurry of correspondence ensued between Parker, Bose, and Shrikhande, which eventually resulted in the publication of a series of papers which contained a complete refutation of Euler’s conjecture. Bose and Shrikhande ([BoSh1], [BoSh2]) expanded on Parker’s results and used block designs to produce a Greco-Latin square of order 22, the first counterexample to Euler’s conjecture. Parker then constructed an order 10 Greco-Latin square (the minimal counterexample to Euler’s conjecture) using orthogonal arrays [Pa2]. The components of the columns were elements of a particular field, permuted via an algorithm similar to that in Bose’s paper of 1938, with the exception of 9 columns which corresponded to a 3 by 3 Greco-Latin subsquare (which does not contradict Mann’s results). Parker attributed the inspiration to Bose and Shrikhande. All these authors collaborated on a final paper in which counterexamples are found for all orders \( n = 4k + 2 \) except for \( n = 2 \) and \( n = 6 \) [BoShPa]. Their proof involves the use of block designs in a lengthy case-by-case analysis, and techniques from their earlier papers.

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

The singular direct product (SDP) of Latin squares requires the following ingredients: a Latin square of order \((m + n)\) containing a Latin subsquare of order \(m\), and two more of orders \(n\) and \(k\). The construction produces a Latin square of order \((m + nk)\). As with the direct product, if the process is performed on two pairs of squares which are respectively orthogonal, the resulting pair of squares will be orthogonal. The actual details of the construction are not complicated but numerous; the point of the matter, and the importance of this method, is that it takes Latin squares and combines them to make a Latin square whose order is not necessarily a multiple of the orders of any of the input squares. Using previous methods (such as MacNeish’s direct product), we could not build up a Greco-Latin square of order 22 (or any order \(4k + 2\)) from smaller squares because a Greco-Latin square of order 2 does not exist. Sade’s SDP, however, allowed him to construct this and many other Greco-Latin squares, and in fact an infinite number of counterexamples to Euler’s conjecture via purely algebraic methods, in contrast to the somewhat unsystematic method of block designs. With a set of squares as in figure 16, the SDP produces a Latin square as in figure 17.

![Figure 16: Latin squares of size \((m + n) = 5\) (with a Latin subsquare of order \(m = 2\), \(n = 3\), and \(k = 3\)](image)

A few subsequent contributions to the Greco-Latin square problem are worth noting. In 1975, Crampin and Hilton [CrHi] showed that Sade’s SDP can produce a complete set of counterexamples to Euler’s conjecture if one is given orthogonal Latin squares of size 10, 14, 18, 26, and 62 from which the other squares are built up. Also, using a computer, they showed that the SDP can be used to construct self-orthogonal Latin squares (Latin squares orthogonal to their transpose) of all but 217 sizes. Stinson [St], in 1984, gave a modern mathematical tour de force, proving the 36-officer problem in only three pages by using a transversal design, finite vector spaces, and graph theory. And finally, in 1982, Zhu Lie [Li] 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 the attempts to solve it generate. By this measure, Euler’s conjecture of 1782 surely must rank among the most fertile problems in the history of mathematics, and it is a testament to his mathematical insight that he understood so early the ramifications of so simple a question. Although this conjecture has certainly been resolved, the allure of a better, shorter solution will continue to entice future researchers to explore new areas of combinatorics, and indeed all of mathematics.

References


