THE 36 OFFICERS PROBLEM: EXISTENCE RESULTS FOR ORTHOGONAL PAIRS OF LATIN SQUARES

In 1782, Leonhard Euler introduced his famous Thirty-six officers problem. It is typically said that this problem marks the beginning of the systematic investigation of latin squares. Euler's problem is as follows: Given 6 distinct regiments each consisting of 6 distinct ranks, is it possible to arrange a 6 x 6 grid such that each row and each column of the grid contains exactly one representative from each regiment and exactly one representative of each rank? To get a feel for the type of answer Euler sought, let us consider a sixteen officer problem. Letting our ranks be $\{1, 2, 3, 4\}$ and our regiments be $\{A, B, C, D\}$, can we construct a 4x4 grid such that each rank and regiment appears exactly once in each row and column? Some effort by the reader will likely produce one of the following solutions:

4D	1A	2B	3C
2A	3D	4C	1B
3B	2C	1D	4A
1C	4B	3A	2D

4D	1A	2B	3C
3A	2D	1C	4B
1B	4C	3D	2A
2C	3B	4A	1D

4D	1A	2B	3C
2C	3B	4A	1D
3A	2D	1C	4B
1B	4C	3D	2A

We see above that each row and column contains exactly one of each rank and regiment. Despite the ease by which we were able to solve the 4 x 4 case, Euler could not find a satisfactory solution to his 6 x 6 case and, in fact, conjectured that there was no such arrangement. This paper will explore this conjecture by Euler via the demonstration and reporting of various existence results for what are called "orthogonal" latin squares. Before we talk about orthogonal latin squares, we must of course define what we mean by a latin square and discuss some of their basic properties.

Definition : A latin square of order n is an n x n array consisting of n distinct symbols such that each symbol appears exactly once in each row and exactly once in each column.

1	2
2	1

a	b	c	d
b	c	d	a
c	d	a	b
d	a	b	c

α	β	χ
β	χ	α
χ	α	β

Above, we have examples of order 2, 4, and 3, respectively. We see then that Euler's problem does not call for a latin square as his squares are comprised of n^2 distinct ordered pairs, each appearing once per square rather than n distinct elements each appearing n times. The square Euler was concerned with is called a graeco-latin square or an Euler square.

Theorem 1: For any natural number n, there exists a latin square of order n.

Proof. To show this, we will demonstrate the construction of an order n latin square. We begin by placing the first row in natural order. By construction, the first row contains exactly n distinct symbols. Next, we put the second row in natural order but shift it one space to the left. Again, we see that the second row contains exactly n distinct symbols and further, we see that no column contain the same symbol twice. We then place the third row in natural order shifting it two spaces to the left. Again, the third row contains exactly n distinct symbols and the columns do not have repeated elements. We continue on like this, shifting the ith row $i-1$ spaces to the left. Then, the nth row is shifted $n-1$ spaces and we see that the first column has exactly n distinct symbols. It follows that the other $n-1$ columns also contain exactly n distinct symbols. Then if L (pictured below) has n rows and n columns, is comprised of n distinct symbols, and each symbol appears exactly once in each row and column, L is a latin square of order n.

$L =$

1	2	3	...	n
2	3	4	...	1
3	4	5	...	2
⋮	⋮	⋮	⋱	⋮
n	1	2	...	n-1

□

Having established that there exists a latin square of order n for all natural numbers n, we next consider the the question of how many latin squares of order n there are. Consider the following example for $n = 3$. Beginning with the 3 x 3 latin square below, denoted by $*$, we can systematically permute the columns in 3! ways:

1	2	3
2	3	1
3	1	2

$^{(*)}$

2	1	3
3	2	1
1	3	2

2	3	1
3	1	2
1	2	3

1	3	2
2	1	3
3	2	1

3	1	2
1	2	3
2	3	1

3	2	1
1	3	2
2	1	3

We can follow this with permutation of the lower two rows to derive 6 additional latin squares:

1	2	3
3	1	2
2	3	1

2	1	3
1	3	2
3	2	1

2	3	1
1	2	3
3	1	2

1	3	2
3	2	1
2	1	3

3	1	2
2	3	1
1	2	3

3	2	1
2	1	3
1	3	2

We see then that we are able to generate 12 distinct latin squares of order 3 from our original. This original latin square we refer to as a reduced latin square of order 3.

Definition: A reduced latin square of order n is a latin square of order n such that the first row and first column are in natural order.

We see that our initial three examples are all reduced latin squares. The following theorem demonstrates how the total number of latin squares of order n is dependent upon the number of reduced latin squares of order n.

Theorem 2: For all natural numbers n, where $n \geqslant 2$, the total number of latin squares of order n, $L(n)$, is given by $L(n) = n!\ (n-1)!\ l(n)$ where $l(n)$ denotes the number of reduced latin squares of order n.

Proof. We begin with a reduced latin square of order n, call it l_1. Then, as in the above example, there are $n!$ possible column permutations of l_1 which can be followed by $(n-1)!$ row permutations. So, in total, there are $n!\ (n-1)!$ distinct latin squares which can be generated from l_1. We know that of these $n!\ (n-1)!$ distinct latin squares, only l_1 is reduced because each permutation effects either the first row or first column. Then, it follows that if there exists a second reduced latin square, call it l_2, it too will have $n!\ (n-1)!$ distinct latin squares. Again, it follows that this second collection of distinct latin squares will have exactly one reduced latin square. Thus the result follows as $L(n) = n!\ (n-1)! + n!\ (n-1)! + \ldots + n!\ (n-1)!_{l(n)-times} = n!\ (n-1)!\ l(n)$. □

We see from this that in order to determine the number of latin squares of order n, we must first determine the number of reduced latin squares of order n. Unfortunately, this is not a simple quantity to calculate. In fact, combinatorial explosion makes this number notoriously difficult to calculate. Here are a few of the known values of $l(n)$:

$$l(1) = 1$$
$$l(2) = 1$$
$$l(3) = 1$$
$$l(4) = 4$$
$$l(5) = 56$$
$$l(6) = 9408$$
$$l(7) = 16,942,080$$
$$l(8) = 532,281,401,856$$
$$l(9) = 377,597,570,964,258,816$$
$$l(10) = 7,580,721,483,160,132,811,489,280$$
$$l(11) = 5,363,937,773,277,371,298,119,673,540,771,840$$

Returning to Euler's problem for a moment, what exactly does an affirmative solution to the problem of 36 officers entail? We have seen that his problem seeks a graeco-latin square of order 6, but what exactly does this graeco-latin square have to do with latin squares?

Definition: A pair of latin squares of order n are said to be orthogonal if, when juxtaposed, the juxtaposition produces n^2 distinct ordered pairs.

In light of this definition, let us reconsider one of our solutions to the sixteen officer problem:

4D	1A	2B	3C
2A	3D	4C	1B
3B	2C	1D	4A
1C	4B	3A	2D

Then, the juxtaposition referred to in the definition above can be understood as:

4D	1A	2B	3C
2A	3D	4C	1B
3B	2C	1D	4A
1C	4B	3A	2D

is

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

and

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

Thus we see that Euler's problem involves finding a pair of orthogonal latin squares of order 6. We found three solution for the sixteen officer problem, so what is it about the order 6 case that is unique? We proceed now with existence results for orthogonal pairs of latin squares.

Definition: An orthogonal family of size r is a collection of latin squares $\{L^{(1)}, L^{(2)}, \ldots, L^{(r)}\}$ such that $L^{(i)}$ is orthogonal to $L^{(j)}$ whenever $i \neq j$.

From this definition, we move immediately to the following result, which places an upper bound on the size of any orthogonal family.

Theorem 3: For any natural number n, where $n \geqslant 2$, the size of an orthogonal family of order n is less than or equal to $n - 1$.

To prove this, we will first consider the following lemma:

Lemma: For any orthogonal family of latin squares, it is possible to relabel the members of the family such that the first row of each member is in natural order. This can be done without effecting the size of the family.

demonstration : We shall demonstrate the lemma in the form of an example. Consider the $n = 3$ case and the following orthogonal pair:

$$L^{(1)} = \begin{array}{|c|c|c|}\hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline 1 & 2 & 3 \\ \hline \end{array} \quad , \quad L^{(2)} = \begin{array}{|c|c|c|}\hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline 1 & 2 & 3 \\ \hline \end{array}$$

We wish to place row 1 in natural order for both $L^{(1)}$ and $L^{(2)}$, while not effecting the orthogonality of $L^{(1)}$ and $L^{(2)}$. We proceed as follows: Since, $a_{11}^{(1)} = 2$, and $a_{11}^{(2)} = 3$, where the notation $a_{ij}^{(e)}$ indicates the element in the ith row and jth column of $L^{(e)}$, then we interchange 2 with 1 throughout $L^{(1)}$ and 3 with 1 throughout $L^{(2)}$, which yields the following:

$$L^{(1)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 3 & 2 & 1 \\ \hline 2 & 1 & 3 \\ \hline \end{array} \quad , \quad L^{(2)} = \begin{array}{|c|c|c|}\hline 1 & 3 & 2 \\ \hline 2 & 1 & 3 \\ \hline 3 & 2 & 1 \\ \hline \end{array}$$

We see that $L^{(1)}$ and $L^{(2)}$ remain orthogonal and we continue on. Because $a_{12}^{(1)} = 3$ and $a_{12}^{(2)} = 3$ we interchange 3 with 2 throughout both $L^{(1)}$ and $L^{(2)}$, giving us:

$$L^{(1)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array} \quad , \quad L^{(2)} = \begin{array}{|c|c|c|}\hline 1 & 2 & 3 \\ \hline 3 & 1 & 2 \\ \hline 2 & 3 & 1 \\ \hline \end{array}$$

Then it is readily seen that: $L^{(1)}, L^{(2)}$ is $\begin{array}{|c|c|c|}\hline 1,1 & 2,2 & 3,3 \\ \hline 2,3 & 3,1 & 1,2 \\ \hline 3,2 & 1,3 & 2,1 \\ \hline \end{array}$ and the squares are orthogonal.

In general then, if $a_{11}^{(e)} = k$, we switch k with 1 and 1 with k throughout $L^{(e)}$. Then $L(e)$ will still be orthogonal to $L(i)$ because if $(a_{11}^{(e)}, a_{11}^{(i)}) = (k, t)$ originally, we now have $(a_{11}^{(e)}, a_{11}^{(i)}) = (1, t)$ and the ordered pair which was formerly $(1, s)$ is now (k, s). It is clear that these new ordered pairs are unique in the juxtaposed square since the original ordered pairs were unique. We see also that this process can be continued until the first row of each member of our orthogonal family is in natural order. *end.*

Proof of Theorem 3. Let $L^{(1)}, L^{(2)}, \ldots, L^{(r)}$ be an orthogonal family of latin squares. By our above lemma, we can relabel the members of the family such that the first row of each member is in natural order. Assume we do this and consider members $L^{(i)}$ and $L^{(j)}$.

$$L^{(i)} = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & \ldots\ b\ \ldots & \mathrm{n} \\ \hline \mathrm{s} & & & \ldots & \\ \hline & & & \ldots & \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline & & & \ldots & \\ \hline \end{array} \quad , \quad L^{(j)} = \begin{array}{|c|c|c|c|c|}\hline 1 & 2 & 3 & \ldots\ b\ \ldots & \mathrm{n} \\ \hline \mathrm{t} & & & \ldots & \\ \hline & & & \ldots & \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline & & & \ldots & \\ \hline \end{array}$$

Given $L^{(i)}$ and $L^{(j)}$ above, we have $a_{21}^{(i)} = s$ and $a_{21}^{(j)} = t$. First, we see that $s \neq 1$ and $t \neq 1$ because if $s = 1$ or $t = 1$, then $L^{(i)}$ and $L^{(j)}$ are not latin. We next observe that $s \neq t$ because if $s = t$, then letting $s = t = b$ we have $(a_{21}^{(i)}, a_{21}^{(j)}) = (b, b)$. But, we know that $(a_{1b}^{(i)}, a_{1b}^{(j)}) = (b, b)$ in the first row, so if $s = t = b$ then $L^{(i)}$ and $L^{(j)}$ are not orthogonal. Then, if $s \neq t$ and neither of the two can equal 1, there are at most $n - 1$ choices for s or t. Thus it follows that there are at most $n - 1$ orthogonal latin squares in any family. $\square$

We note that the above result says nothing about whether or not there exists an orthogonal family, only that there is necessarily a limit to the size of any family that may exist. If there does exist an orthogonal family for order n and the size of this family is $n - 1$, then we refer to the family as "complete."

As an example, we again consider order 4. We see that there exists a complete family of order 4 since we are able to find 3 mutually orthogonal latin squares.

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

,

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

,

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

Theorem 4: If p is prime and $k \geqslant 1$, then there exists a complete orthogonal family of latin squares order $n = p^k$.

To demonstrate this theorem, we will utilize an algorithm for producing complete families. This algorithm is referred to as the Moore algorithm[1] in honor of it's discoverer E. H. Moore. The algorithm relies on finite fields, which are also referred to as Galois fields and typically denoted $GF(p^k)$. The order of any finite field is always a prime power and for any prime power, p^k, there exists exactly one finite field, up to isomorphism, of order p^k. It is easy to see that for $k = 1$, the field, $GF(p)$, is the integers modulo p, whereas this is not the case for $k > 1$. For $k > 1$, $GF(p^k)$ may be constructed using a monic polynomial of degree k with coefficients from the field Z_p. We offer an example of this procedure below for $n = 2^2$.

To construct $GF(2^2)$, we need a quadratic monic polynomial with coefficients from $Z_2 = \{0, 1\}$, which is irreducible over $Z_2[x]$. We see that $x^2 + x + 1$ is such a polynomial. Then, if we let a be a root of this polynomial (i.e. $a^2 + a + 1 = 0$) we can generate the powers of a: a, $a^2 = a + 1$, $a^3 = a^2 + a = 1$, which form the multiplicative group $GF(2^2)^*$ (i.e. $GF(2^2)$ without the additive identity). With the inclusion of the additive identity, we have $GF(2^2) = \{0, 1, a, a + 1\}$, which has the following multiplication and addition tables:

X		0	1	a	a+1
0		0	0	0	0
1		0	1	a	a+1
a		0	a	a+1	1
a+1		0	a+1	1	a

+		0	1	a	a+1
0		0	1	a	a+1
1		1	0	a+1	a
a		a	a+1	0	1
a+1		a+1	a	1	0

These may be relabeled for convenience sake using: $1 = 1$, $a = 2$, $a + 1 = 3$, and $0 = 4$ and thus produce:

$*$		4	1	2	3
4		4	4	4	4
1		4	1	2	3
2		4	2	3	1
3		4	3	1	2

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

Moore Algorithm: For $n = p^k$, and $GF(n) = \{g_1, g_2, \ldots, g_n\}$ where g_1 denotes the multiplicative identity and g_n denotes the additive identity, $L^{(e)} = \{a_{ij}^{(e)}\}$ is defined by: $a_{ij}^{(e)} = (g_e * g_i) + g_j$ for $e = 1, 2, \ldots, n-1$.

Let us apply the algorithm to the case of $n = 3$. Letting $GF(3) = \{1, 2, 3\}$ we have:

$$\begin{array}{lll} a_{11}^{(1)} = (1*1)+1 = 2 & a_{21}^{(1)} = (1*2)+1 = 3 & a_{31}^{(1)} = (1*3)+1 = 1 \\ a_{12}^{(1)} = (1*1)+2 = 3 & a_{22}^{(1)} = (1*2)+2 = 1 & a_{32}^{(1)} = (1*3)+2 = 2 \\ a_{13}^{(1)} = (1*1)+3 = 1 & a_{23}^{(1)} = (1*2)+3 = 2 & a_{33}^{(1)} = (1*3)+3 = 3 \end{array}$$

$$\begin{array}{lll} a_{11}^{(2)} = (2*1)+1 = 3 & a_{21}^{(2)} = (2*2)+1 = 2 & a_{31}^{(2)} = (2*3)+1 = 1 \\ a_{12}^{(2)} = (2*1)+2 = 1 & a_{22}^{(2)} = (2*2)+2 = 3 & a_{32}^{(2)} = (2*3)+2 = 2 \\ a_{13}^{(2)} = (2*1)+3 = 2 & a_{23}^{(2)} = (2*2)+3 = 1 & a_{33}^{(2)} = (2*3)+3 = 3 \end{array}$$

Which produces: $L^{(1)} = \begin{array}{|c|c|c|}\hline 2&3&1\\\hline 3&1&2\\\hline 1&2&3\\\hline\end{array}$, $L^{(2)} = \begin{array}{|c|c|c|}\hline 3&1&2\\\hline 2&3&1\\\hline 1&2&3\\\hline\end{array}$ which are indeed orthogonal.

Using the addition and multiplication tables for $GF(2^2)$ above, we can apply the algorithm and generate the following order 4 latin squares:

$$L^{(1)} = \begin{array}{|c|c|c|c|}\hline 4&3&2&1\\\hline 3&4&1&2\\\hline 2&1&4&3\\\hline 1&2&3&4\\\hline\end{array}, \; L^{(2)} = \begin{array}{|c|c|c|c|}\hline 3&4&1&2\\\hline 2&1&4&3\\\hline 4&3&2&1\\\hline 1&2&3&4\\\hline\end{array}, \; L^{(3)} = \begin{array}{|c|c|c|c|}\hline 2&1&4&3\\\hline 4&3&2&1\\\hline 3&4&1&2\\\hline 1&2&3&4\\\hline\end{array}$$

The three above comprise a complete orthogonal family of order 4. To prove theorem 4, we will show that the Moore algorithm produces $n-1$ distinct and pairwise orthogonal latin squares.

Proof of Theorem 4. Assume that $n = p^k$, and let $GF(n) = \{g_1, g_2, \ldots, g_n\}$ be the Galois field of order n where g_1 denotes the multiplicative identity and g_n denotes the additive identity.

We begin by showing that the Moore algorithm produces latin squares. Consider $L^{(e)}$ for $1 \leqslant e \leqslant n-1$ and assume that $a_{ij}^{(e)} = a_{ik}^{(e)}$, which is to say that two elements in the same row are identical. Then by the construction of $L^{(e)}$, we have $a_{ij}^{(e)} = (g_e * g_i) + g_j$ and $a_{ik}^{(e)} = (g_e * g_i) + g_k$, so $(g_e * g_i) + g_j = (g_e * g_i) + g_k$ by assumption. Because $GF(n)$ is a field, there exists an additive inverse for $(g_e * g_i)$, then $(-(g_e * g_i)) + (g_e * g_i) + g_j = (-(g_e * g_i)) + (g_e * g_i) + g_k$ is $g_j = g_k$, which implies that $j = k$. Then if two elements of $L^{(e)}$ in the same row are

equal, they are in the same column. Next assume that $a_{ji}^{(e)} = a_{ki}^{(e)}$, which is to say that two elements in the same column are identical. As before, by construction of $L^{(e)}$, we have $a_{ji}^{(e)} = (g_e * g_j) + g_i$ and $a_{ki}^{(e)} = (g_e * g_k) + g_i$, so we have $(g_e * g_j) + g_i = (g_e * g_k) + g_i$. By adding $(-g_i)$ to both sides, we have $(g_e * g_j) = (g_e * g_k)$. Then, $g_e^{-1} * (g_e * g_j) + g_i = g_e^{-1} * (g_e * g_k)$ is $g_j = g_k$ which implies that $j = k$. Thus if two elements in the same column are equal, they are in the same row. It follows from this that $L^{(e)}$ is latin.

Next, we will show that the Moore algorithm produces orthogonal latin squares. Assume that $e \neq f$ and that $(a_{ij}^{(e)}, a_{ij}^{(f)}) = (a_{kl}^{(e)}, a_{kl}^{(f)})$, which is to say that the juxtaposition of $L^{(e)}$ and $L^{(f)}$ produces two identical ordered pairs in the ith row jth column and the kth row lth column. Then $a_{ij}^{(e)} = a_{kl}^{(e)}$ and $a_{ij}^{(f)} = a_{kl}^{(f)}$ implies $(g_e * g_i) + g_j = (g_e * g_k) + g_l$ and $(g_f * g_i) + g_j = (g_f * g_k) + g_l$. Subtracting one from the other, we have $(g_e * g_i) - (g_f * g_i) = (g_e * g_k) - (g_f * g_k)$ which is $g_i * (g_e - g_f) = g_k * (g_e - g_f)$. Because $e \neq f$, we see that $(g_e - g_f) \neq 0$ thus there exists a multiplicative inverse of $(g_e - g_f)$. Then $g_i * (g_e - g_f) * (g_e - g_f)^{-1} = g_k * (g_e - g_f) * (g_e - g_f)^{-1}$ is $g_i = g_k$ which implies that $i = k$.

Then if $g_i = g_k$, we return to our expression from above: $(g_e * g_i) + g_j = (g_e * g_k) + g_l$, this implies $(g_e * g_i) - (g_e * g_k) + g_j = g_l$ and letting $g_i = g_k = d$ we have $d * (g_e - g_e) + g_j = g_l$ and $g_j = g_l$, which shows that $j = l$. Thus if the juxtaposition of $L^{(e)}$ and $L^{(f)}$ produces two identical ordered pairs in the ith row jth column and the kth row lth column we have that the ordered pairs are in the same row ($i = k$) and the same column ($j = l$) and $L^{(e)}$ and $L^{(f)}$ are orthogonal.

Finally, we see that because $L^{(e)}$ and $L^{(f)}$ are orthogonal, it is implicit that they are distinct. Thus, we have shown that the Moore algorithm produces $n - 1$ distinct and pairwise orthogonal latin squares and therefore when p is prime and $k \geqslant 1$, there exists a complete orthogonal family of latin squares order $n = p^k$. □

So we have now that there exists a complete family of orthogonal latin squares when $n = p^k$ and $k \geqslant 1$. We note however that for $n = 2$, there does not exist an orthogonal pair as the only two squares of order 2 are clearly not orthogonal. What if $n \neq p^k$ for example $n = 10$? We see that Euler's 36 officers problem considers the case of $n = 6$. Euler conjectured that there did not exist an orthogonal pair of latin squares order n if n was an odd multiple of 2. That is, when $n = 2p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ where p_i is an odd prime. Euler's conjecture stood until the mid 1900's when it was shown to be false for all odd multiples of 2 that are greater than 6. Although we will not demonstrate the refutation of Euler's conjecture, due primarily to the length and complexity of the proofs involved, we will state the result, which along with the following several demonstrations will entirely settle the question of whether or not there exists an orthogonal pair for a given order.

We next consider existence results for orthogonal pairs of order n, where $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ is the ordered prime power factorization of n (i.e. $p_1^{e_1} < p_2^{e_2} < \dots < p_s^{e_s}$) and $p_1^{e_1} > 2$. For this, we will need to utilize some important machinery for dealing with latin squares and we therefore proceed with a description of the Kronecker product and an important theorem by MacNeish.

Definition: Let A and B be latin squares of order n and m, respectively, then the Kronecker product, also called the matrix direct product, of A and B is:

$$A \otimes B = \begin{array}{|c|c|c|c|} \hline (a_{11}, B) & (a_{12}, B) & \dots & (a_{1n}, B) \\ \hline (a_{21}, B) & (a_{22}, B) & \dots & (a_{2n}, B) \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline (a_{n1}, B) & (a_{n2}, B) & \dots & (a_{nn}, B) \\ \hline \end{array}$$

with each (a_{ij}, B) entry in the above square is given by the m x m matrix:

$$(a_{ij}, B) = \begin{pmatrix} a_{ij}, b_{11} & a_{ij}, b_{12} & \dots & a_{ij}, b_{1m} \\ a_{ij}, b_{21} & a_{ij}, b_{22} & \dots & a_{ij}, b_{2m} \\ \vdots & \vdots & & \vdots \\ a_{ij}, b_{m1} & a_{ij}, b_{m2} & \dots & a_{ij}, b_{mm} \end{pmatrix}$$

So, we see that the Kronecker product $A \otimes B$ produces an mn x mn array of ordered pairs. Consider the following example:

$$A = \begin{array}{|c|c|} \hline 2 & 1 \\ \hline 1 & 2 \\ \hline \end{array} \quad B = \begin{array}{|c|c|c|} \hline 3 & 1 & 2 \\ \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline \end{array}$$

Then the Kronecker product of A and B is:

$$A \otimes B = \begin{array}{|c|c|} \hline \text{(2,B)} & \text{(1,B)} \\ \hline \text{(1,B)} & \text{(2,B)} \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|} \hline 23 & 21 & 22 & 13 & 11 & 12 \\ \hline 21 & 22 & 23 & 11 & 12 & 13 \\ \hline 22 & 23 & 21 & 12 & 13 & 11 \\ \hline 13 & 11 & 12 & 23 & 21 & 22 \\ \hline 11 & 12 & 13 & 21 & 22 & 23 \\ \hline 12 & 13 & 11 & 22 & 23 & 21 \\ \hline \end{array}$$

We see that $A \otimes B$ is a 6 x 6 latin square comprised of the alphabet: $\{23, 21, 22, 13, 11, 12\}$. We can easily relabel the square for convenience, using: $23 = 1, 21 = 2, 22 = 3, 13 = 4, 11 = 5, 12 = 6$, which produces:

$$A \otimes B = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 2 & 3 & 1 & 5 & 6 & 4 \\ \hline 3 & 1 & 2 & 5 & 4 & 5 \\ \hline 4 & 5 & 6 & 1 & 2 & 3 \\ \hline 5 & 6 & 4 & 2 & 3 & 1 \\ \hline 6 & 4 & 5 & 3 & 1 & 2 \\ \hline \end{array}$$

a latin square of order 6.

This leads us to an important result by MacNeish[2], which, as we'll see, when later coupled with theorem 4 will guarantee the existence of an orthogonal pair for $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, where p_i is prime, $p_1^{e_1} < p_2^{e_2} < \dots < p_s^{e_s}$, and $p_1^{e_1} > 2$.

Theorem 5: If there exists an orthogonal family of r latin squares of order m and an orthogonal family of s latin squares of order n, with $r \leqslant s$, then there exists an orthogonal family of r latin squares of order mn.

Before proving theorem 5, we consider the following example: Let $A^{(1)}, A^{(2)}$ and $B^{(1)}, B^{(2)}$ be two orthogonal pairs of latin squares with order 3 and 4, respectively.

$$A^{(1)} = \begin{array}{|c|c|c|}\hline 2&3&1\\\hline 3&1&2\\\hline 1&2&3\\\hline\end{array} \quad A^{(2)} = \begin{array}{|c|c|c|}\hline 3&1&2\\\hline 2&3&1\\\hline 1&2&3\\\hline\end{array} \quad \textit{and} \quad B^{(1)} = \begin{array}{|c|c|c|c|}\hline 4&1&2&3\\\hline 1&4&3&2\\\hline 2&3&4&1\\\hline 3&2&1&4\\\hline\end{array} \quad B^{(2)} = \begin{array}{|c|c|c|c|}\hline 4&1&2&3\\\hline 2&3&4&1\\\hline 3&2&1&4\\\hline 1&4&3&2\\\hline\end{array}$$

The Kronecker product $A^{(1)} \otimes B^{(1)} = K^{(1)}$ and $A^{(2)} \otimes B^{(2)} = K^{(2)}$ produces:

$$K^{(1)} = \begin{array}{|c|c|c|}\hline (2,B^{(1)})&(3,B^{(1)})&(1,B^{(1)})\\\hline (3,B^{(1)})&(1,B^{(1)})&(2,B^{(1)})\\\hline (1,B^{(1)})&(2,B^{(1)})&(3,B^{(1)})\\\hline\end{array} = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|}\hline 24&21&22&23&34&31&32&33&14&11&12&13\\\hline 21&24&23&22&31&34&33&32&11&14&13&12\\\hline 22&23&24&21&32&33&34&31&12&13&14&11\\\hline 23&22&21&24&33&32&31&34&13&12&11&14\\\hline 34&31&32&33&14&11&12&13&24&21&22&23\\\hline 31&34&33&32&11&14&13&12&21&24&23&22\\\hline 32&33&34&31&12&13&14&11&22&23&24&21\\\hline 33&32&31&34&13&12&11&14&23&22&21&24\\\hline 14&11&12&13&24&21&22&23&34&31&32&33\\\hline 11&14&13&12&21&24&23&22&31&34&33&32\\\hline 12&13&14&11&22&23&24&21&32&33&34&31\\\hline 13&12&11&14&23&22&21&24&33&32&31&34\\\hline\end{array}$$

$$K^{(2)} = \begin{array}{|c|c|c|} \hline (3,B^{(2)}) & (1,B^{(2)}) & (2,B^{(2)}) \\ \hline (2,B^{(2)}) & (3,B^{(2)}) & (1,B^{(2)}) \\ \hline (1,B^{(2)}) & (2,B^{(2)}) & (3,B^{(2)}) \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|} \hline 34 & 31 & 32 & 33 & 14 & 11 & 12 & 13 & 24 & 21 & 22 & 23 \\ \hline 32 & 33 & 34 & 31 & 12 & 13 & 14 & 11 & 22 & 23 & 24 & 21 \\ \hline 33 & 32 & 31 & 34 & 13 & 12 & 11 & 14 & 23 & 22 & 21 & 24 \\ \hline 31 & 34 & 33 & 32 & 11 & 14 & 13 & 12 & 21 & 24 & 23 & 22 \\ \hline 24 & 21 & 22 & 23 & 34 & 31 & 32 & 33 & 14 & 11 & 12 & 13 \\ \hline 22 & 23 & 24 & 21 & 32 & 33 & 34 & 31 & 12 & 13 & 14 & 11 \\ \hline 23 & 22 & 21 & 24 & 33 & 32 & 31 & 34 & 13 & 12 & 11 & 14 \\ \hline 21 & 24 & 23 & 22 & 31 & 34 & 33 & 32 & 11 & 14 & 13 & 12 \\ \hline 14 & 11 & 12 & 13 & 24 & 21 & 22 & 23 & 34 & 31 & 32 & 33 \\ \hline 12 & 13 & 11 & 14 & 22 & 23 & 21 & 24 & 32 & 33 & 31 & 34 \\ \hline 13 & 12 & 11 & 14 & 23 & 22 & 21 & 24 & 33 & 32 & 31 & 34 \\ \hline 11 & 14 & 13 & 12 & 21 & 24 & 23 & 22 & 31 & 34 & 33 & 32 \\ \hline \end{array}$$

Which are both latin squares of order 12. We can observe further that $K^{(1)}$ and $K^{(2)}$ are orthogonal since their juxtaposition produces 144 distinct 4-tuples:

2344	2311	2322	2333	3144	3111	3122	3133	1244	1211	1222	1233
2312	2343	2334	2321	3112	3143	3134	3121	1212	1243	1234	1221
2323	2332	2341	2314	3123	3132	3141	3114	1223	1232	1242	1214
2331	2324	2313	2342	3113	3124	3113	3141	1231	1224	1213	1242
3244	3211	3222	3233	1344	1311	1322	1333	2144	2111	2122	2133
3212	3243	3234	3221	1312	1343	1334	1321	2112	2143	2134	2121
3223	3232	3241	3214	1323	1332	1341	1314	2123	2132	2141	2114
3231	3224	3213	3242	1331	1324	1313	1342	2131	2124	2113	2142
1144	1111	1122	1133	2244	2211	2222	2233	3344	3311	3322	3333
1112	1143	1134	1121	2212	2243	2234	2221	3312	3343	3334	3321
1123	1132	1141	1114	2223	2232	2241	2214	3323	3332	3341	3314
1131	1124	1113	1142	2231	2224	2213	2242	3331	3324	3313	3341

Notice in the above Euler square that the order of the components is rearranged to better illustrate the idea in the proof of theorem 5.

Proof of Theorem 5. Let $Family_A = \{A^{(1)}, A^{(2)}, \ldots, A^{(r)}\}$ and $Family_B = \{B^{(1)}, B^{(2)}, \ldots, B^{(s)}\}$ be orthogonal families of order n and m, respectively, with $r \leqslant s$. If $r < s$, we consider only r distinct members of $Family_B$ and if $r = s$, we consider all members of $Family_B$. Then, using the Kronecker product, we acquire $K^{(e)}$ and $K^{(f)}$ below, which are both latin squares of order mn.

$$A^{(e)} \otimes B^{(e)} = K^{(e)} = \begin{array}{|c|c|c|c|} \hline (a_{11}^{(e)}, B^{(e)}) & (a_{12}^{(e)}, B^{(e)}) & \ldots & (a_{1n}^{(e)}, B^{(e)}) \\ \hline (a_{21}^{(e)}, B^{(e)}) & (a_{22}^{(e)}, B^{(e)}) & \ldots & (a_{2n}^{(e)}, B^{(e)}) \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline (a_{n1}^{(e)}, B^{(e)}) & (a_{n2}^{(e)}, B^{(e)}) & \ldots & (a_{nn}^{(e)}, B^{(e)}) \\ \hline \end{array}$$

$$A^{(f)} \otimes B^{(f)} = K^{(f)} = \begin{array}{|c|c|c|c|} \hline (a_{11}^{(f)}, B^{(f)}) & (a_{12}^{(f)}, B^{(f)}) & \dots & (a_{1n}^{(f)}, B^{(f)}) \\ \hline (a_{21}^{(f)}, B^{(f)}) & (a_{22}^{(f)}, B^{(f)}) & \dots & (a_{2n}^{(f)}, B^{(f)}) \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline (a_{n1}^{(f)}, B^{(f)}) & (a_{n2}^{(f)}, B^{(f)}) & \dots & (a_{nn}^{(f)}, B^{(f)}) \\ \hline \end{array}$$

Then by juxtaposing $K^{(e)}$ and $K^{(f)}$ we have:

$(a_{11}^{(e)}, a_{11}^{(f)} B^{(e)} B^{(f)})$	$(a_{12}^{(e)}, a_{12}^{(f)} B^{(e)} B^{(f)})$	$\dots$	$(a_{1n}^{(e)}, a_{1n}^{(f)} B^{(e)} B^{(f)})$
$(a_{21}^{(e)}, a_{21}^{(f)} B^{(e)} B^{(f)})$	$(a_{12}^{(e)}, a_{22}^{(f)} B^{(e)} B^{(f)})$	$\dots$	$(a_{2n}^{(e)}, a_{2n}^{(f)} B^{(e)} B^{(f)})$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(a_{21}^{(e)}, a_{21}^{(f)} B^{(e)} B^{(f)})$	$(a_{12}^{(e)}, a_{22}^{(f)} B^{(e)} B^{(f)})$	$\dots$	$(a_{2n}^{(e)}, a_{2n}^{(f)} B^{(e)} B^{(f)})$

Because $A^{(e)}$ and $A^{(f)}$ are orthogonal, we know that each prefix pair $a_{ij}^{(e)}, a_{ij}^{(f)} \neq a_{kl}^{(e)}, a_{kl}^{(f)}$, for $i \neq k$ and $j \neq l$. Then, consider each sub-matrix:

$$(a_{ij}^{(e)}, a_{ij}^{(f)} B^{(e)} B^{(f)}) = \begin{pmatrix} a_{ij}^{(e)} a_{ij}^{(f)} b_{11}^{(e)} b_{11}^{(f)} & a_{ij}^{(e)} a_{ij}^{(f)} b_{12}^{(e)} b_{12}^{(f)} & \dots & a_{ij}^{(e)} a_{ij}^{(f)} b_{1m}^{(e)} b_{1m}^{(f)} \\ a_{ij}^{(e)} a_{ij}^{(f)} b_{21}^{(e)} b_{21}^{(f)} & a_{ij}^{(e)} a_{ij}^{(f)} b_{22}^{(e)} b_{22}^{(f)} & \dots & a_{ij}^{(e)} a_{ij}^{(f)} b_{2m}^{(e)} b_{2m}^{(f)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{ij}^{(e)} a_{ij}^{(f)} b_{m1}^{(e)} b_{m1}^{(f)} & a_{ij}^{(e)} a_{ij}^{(f)} b_{m2}^{(e)} b_{m2}^{(f)} & \dots & a_{ij}^{(e)} a_{ij}^{(f)} b_{mm}^{(e)} b_{mm}^{(f)} \end{pmatrix}$$

Within each m x m submatrix, we find that the suffix ordered pair $b_{ts}^{(e)} b_{ts}^{(f)} \neq b_{gh}^{(e)} b_{gh}^{(f)}$ for $t \neq g$ and $s \neq h$ precisely because $B^{(e)}$ and $B^{(f)}$ are orthogonal. Thus we see that if two ordered pair prefixes are the same, their ordered pair suffixes are different and if two ordered pair suffixes are the same, their ordered pair prefix is different. Then we have mn^2 distinct 4-tuples and $K^{(e)}$ is orthogonal to $K^{(f)}$.

Clearly, this process can be extended:

$$\begin{gathered} A^{(1)} \otimes B^{(1)} = K^{(1)} \\ A^{(2)} \otimes B^{(2)} = K^{(2)} \\ \vdots \\ A^{(r)} \otimes B^{(r)} = K^{(r)} \end{gathered}$$

Thus we have $Family_K = \{K^{(1)}, K^{(2)}, \dots, K^{(r)}\}$ whose members are pairwise orthogonal and of order mn. □

Theorem 5 allows us then to construct an orthogonal pair from any two orthogonal pairs such that the order of the produced orthogonal pair is the product of the orders of the previous two. For example, if we have a family of order 7, and a family of order 11, theorem 4 says that each family is complete and of size 6 and 10, respectively. We can then apply theorem 5 and produce an orthogonal family of size 6 for order 77. It is important to recognize that the result by MacNeish says nothing about the actual number of pairwise orthogonal squares for a given order, but rather gives a lower bound on the number of latin squares in a family of a particular order. It is entirely possible that the total number of pairwise orthogonal latin squares of order 77 is greater than 6. The next theorem shows how we can guarantee the existence of an orthogonal pair for any n, when n is an even mupltiple of 2.

Theorem 6: If $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, for p_i a prime number and $p_1^{e_1} < p_2^{e_2} < \dots < p_s^{e_s}$, then there exists an order n orthogonal family of size $p_1^{e_1} - 1$.

Proof. Let $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, for p_i a prime number and $p_1^{e_1} < p_2^{e_2} < \dots < p_s^{e_s}$. Then, by theorem 4, for each $p_i^{e_i}$ in the prime factorization of n, we have the following families:

$$\begin{aligned} Family_1 &= \{A^{1(1)}, A^{1(2)}, \dots, A^{1(p_1^{e_1}-1)}\} \\ Family_2 &= \{A^{2(1)}, A^{2(2)}, \dots, A^{2(p_1^{e_1}-1)}, \dots, A^{2(p_2^{e_2}-1)}\} \\ &\vdots \\ Family_s &= \{A^{s(1)}, A^{s(2)}, \dots, A^{s(p_1^{e_1}-1)}, \dots, A^{s(p_s^{e_s}-1)}\} \end{aligned}$$

Then, by repeated use of the Kronecker product and according to theorem 5, we can create pairwise orthogonal latin squares of order $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ as follows:

$$\begin{aligned} A^{1(1)} \otimes A^{2(1)} \otimes \dots \otimes A^{s(1)} &= K^1 \\ A^{1(2)} \otimes A^{2(2)} \otimes \dots \otimes A^{s(2)} &= K^2 \\ &\vdots \\ A^{1(p_1^{e_1}-1)} \otimes A^{2(p_1^{e_1}-1)} \otimes \dots \otimes A^{s(p_1^{e_1}-1)} &= K^{\,p_1^{e_1}-1} \end{aligned}$$

Then, $Family_K = \{K^1, K^2, \dots, K^{\,p_1^{e_1}-1}\}$ is an orthogonal family of order $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ and size $p_1^{e_1} - 1$. □

With theorem 6, we have that an orthogonal pair of latin squares exists for order n when $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$, where $p_1^{e_1} > 2$. So for any odd natural number n, we now know that there exists an orthogonal pair of latin squares order n. For any even natural number n, there exists an orthogonal pair order n whenever the prime factorization of n contains 2^k, with $k > 1$. The only thing remaining to be dealt with is the Euler conjecture, which states that there does not exist an orthogonal pair of latin squares order n if n is an odd multiple of 2 (i.e. $n = 2p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ where p_i is an odd prime). In 1900 an exhaustive search by G. Tarry[3] through more than 10,000 order 6 latin squares showed that in fact

there does not exist an orthogonal pair of latin squares for order 6 and that the problem of the 36 officers has no affirmative solution. In 1960, after constructing orthogonal pairs for both $n = 10$ and $n = 22$, Bose, Shrikhande, and Parker, generalizing their construction, published a paper[4] containing a refutation of the Euler conjecture. As mentioned above, the demonstration is quite long and employs results which are complex and beyond the scope of this paper. However, the result shows that there exists an orthogonal pair of latin squares for every natural number except 1, 2, and 6.

1. Moore, E. H. "Tactical Memoranda I-III." Amer. J. Math. 18, 264, 1896.

2. MacNeish, H.F. "Euler Squares." Ann. Math. 23, 221, 1921.

3. Tarry, G. "Le problme de 36 officiers." Compte Rendu de l'Assoc. Franais Avanc. Sci. Naturel 1, 122, 1900.

4. Bose, R.C.; Shrikhande, S.S.; and Parker, E.T. "Further Results on the Construction of Mutually Orthogonal Latin Squares and the Falsity of Euler's Conjecture." Canad. J. Math. 12, 189, 1960.