LATIN SQUARES

Definition 1. Given nonempty finite sets P, Q and N, a *Latin rectangle* L is a system of elements $L_{ij} \in N$ for $i \in P$ and $j \in Q$ such that

(a) For each $i \in P$, all the elements in the row L_{i*} are distinct. In more detail, if $i \in P$ and $j, j' \in Q$ with $j \neq j'$, then we must have $L_{ij} \neq L_{ij'}$.
(b) For each $j \in Q$, all the elements in the column L_{*j} are distinct. In more detail, if $j \in Q$ and $i, i' \in P$ with $i \neq i'$, then we must have $L_{ij} \neq L_{i'j}$.

We will usually write $p = |P|$ and $q = |Q|$ and $n = |N|$. Often (but not always) we will have $P = \{1, \dots, p\}$ or $P = \{0, \dots, p-1\}$ and similarly for P and Q.

Remark 2. In each column we have p entries from N which must all be different, and in each column we have q entries from N which must all be different. This can only work if $p, q \leq n$. Thus, if we fix N with $|N| = n$, then the maximum possible size of a Latin rectangle is $n \times n$.

Definition 3. A *Latin square* of size n is a Latin rectangle with $|P| = |Q| = |N| = n$.

Note that in a Latin square each row contains n different entries taken from N, but $|N| = n$, so each row must contain each element of N precisely once. Similarly, each column must contain each element of N precisely once.

Example 4. The matrix

$$\begin{bmatrix} 1 & 4 & 3 \\ 5 & 2 & 1 \end{bmatrix}$$

gives a Latin rectangle with $P = \{1, 2\}$ and $Q = \{1, 2, 3\}$ and $N = \{1, 2, 3, 4, 5\}$ so $p = 2$ and $q = 3$ and $n = 5$.

Example 5. The matrix

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

gives a Latin square with $P = Q = N = \{1, 2, 3, 4\}$ and $p = q = n = 4$.

Example 6. Let G be any finite group, with $|G| = n$. Take $P = Q = N = G$ and $L_{g,h} = g * h$. I claim that this is a Latin square. Indeed, if $L_{g,h} = L_{g,h'}$ then $g * h = g * h'$ and we can multiply on the left by g^{-1} to see that $h = h'$. By the contrapositive, if $h \neq h'$ then $L_{g,h} \neq L_{g,h'}$. By a similar argument, if $g \neq g'$ then $L_{g,h} \neq L_{g',h}$, as required.

Example 7. As a special case of the above, we can consider the group $\mathbb{Z}/n = \{0, \dots, n-1\}$, with addition mod n as the group operation. This gives a Latin square with $P = Q = N = \{0, \dots, n-1\}$ and $L_{ij} = i + j \pmod{n}$. For example, when $n = 5$ we get

$$L = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}.$$

This example shows that for any n, there is at least one $n \times n$ Latin square.

Theorem 8. *Let L be a Latin rectangle with $p < q = n$ (so L has the maximum possible width, but not the maximum possible height). Then L can be extended by adding extra rows to make an $n \times n$ Latin square.*

The proof of this theorem and the next theorem will depend on some extra definitions which we now explain.

Definition 9. Let L be a Latin rectangle with parameters p, q, n. For $k \in N$ we let $L(k)$ denote the number of occurrences of k in L, and we call this the *multiplicity* of k. We also put $E(k) = L(k) + n - p - q$ and call this the *excess* of k.

Example 10. For $L = \begin{bmatrix} 1 & 4 & 3 \\ 5 & 3 & 1 \end{bmatrix}$ we have $(p, q, n) = (2, 3, 5)$ so $n - p - q = -1$ and

$$L(1) = 2 \qquad L(2) = 0 \qquad L(3) = 2 \qquad L(4) = 1 L(5) = 1$$
$$E(1) = 1 \qquad E(2) = -1 \qquad E(3) = 1 \qquad E(4) = 0 E(5) = 0.$$

Remark 11. The occurrences of k in L must appear in different rows, so $L(k)$ can also be described as the number of rows that contain k. Similarly, the occurrences of k in L must appear in different columns, so $L(k)$ can also be described as the number of columns that contain k.

Lemma 12. *Suppose that $q = n$, so that L has the maximum possible width. Then we have $L(k) = p$ and $E(k) = 0$ for all k. Similarly, if $p = n$ (so that L has the maximum possible height) then $L(k) = q$ and $E(k) = 0$ for all k.*

Proof. Suppose that $q = n$. Then each row has n different elements but $|N| = n$ so each element $k \in N$ must occur precisely once in each of the p rows. From this we see that $L(k) = p$ and so $E(k) = p + n - p - q$. As $q = n$ this simplifies to $E(k) = 0$. The case where $p = n$ is essentially the same. □

Proof of Theorem 8. Let L be a $p \times n$ Latin rectangle. It will be enough to show that we can add one more row to get a $(p + 1) \times n$ Latin rectangle, because we can then repeat the process if necessary. It will also be harmless to assume that $P = \{1, \dots, p\}$ and $Q = N = \{1, \dots, n\}$.

For $j \in Q$, let $C[j] \subseteq N$ be the set of possible entries for position $(p + 1, j)$ in the new row. The numbers $L_{1j}, \dots, L_{pj}$ have already appeared in column j, so these are the ones that we are not allowed to use (and they are all different, because L is a Latin rectangle). We therefore have

$$C[j] = N \setminus \{L_{1j}, \dots, L_{pj}\}$$

and so $|C[j]| = n - p$. To make the new row, we need to choose an element $m_j \in C[j]$ for each $j \in Q$, in such a way that $m_1, \dots, m_n$ are all different. This is mathematically equivalent to a job allocation problem with Q as the set of jobs, and $C[j]$ as the set of candidates for job j. For each $k \in N$ put

$$D[k] = \{j \mid k \in C[j]\},$$

which is analogous to the set of jobs for which person k is qualified. We will use Corollary 55: if there is a constant d such that $|C[j]| = d$ for all j and $|D[k]| \leq d$ for all k, then the allocation problem is solvable. We will take $d = n - p$; we have already seen that $|C[j]| = d$ for all j. On the other hand, $D[k]$ is just the set of columns where we are allowed to put k in the new row, or in other words, the set of columns that do not already contain k. The number of columns that contain k is $L(k)$, which is p as we explained in Lemma 12. Thus, the number of columns that do not contain k is $|D[k]| = n - p = d$ as required. Thus, Corollary 55 is applicable, so we can solve the allocation problem, and the solution gives us an extra row. □

Example 13. Consider the following Latin rectangle, with $p = 2$ and $q = n = 5$:

$$L = \begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Recall that $C[j]$ is the set of possibilities for position j in the next row. For example, in column 2 we already have a 2 and a 1, so these are not allowed, so $C[2] = N \setminus \{2, 1\} = \{3, 4, 5\}$. We can display all the sets $C[j]$ as follows:

$$\begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 234 & 345 & 135 & 124 & 125 \end{bmatrix}$$

(We have used abbreviated notation, e.g. 234 for $\{2, 3, 4\}$.) To make the new row, we must choose one element from the possibilities in each column, making sure that we never choose the same element twice.

Corollary 55 tells us that this is possible, but does not tell us exactly how to do it. However, in this case it is not difficult: in each column we can just take the first choice that has not already been used. This gives $2, 3, 1, 4, 5$ as the new row. We can write in this new row and display the possibilities for row 4 as follows:

$$\begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 & 5 \\ 34 & 45 & 35 & 12 & 12 \end{bmatrix}$$

Again, in each column we can take the first choice that has not already been used. This gives row 4 and leaves only one possibility for row 5. We end up with the following Latin square:

$$\begin{bmatrix} 1 & 2 & 4 & 5 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 3 & 2 & 1 \end{bmatrix}$$

Corollary 14. *Let L be a Latin rectangle with $q < p = n$ (so L has the maximum possible height, but not the maximum possible width). Then L can be extended by adding extra columns to make an $n \times n$ Latin square.*

Proof. Note that the transpose L^T is a Latin square of maximum possible width, so we can use Theorem 8 to extend it to a Latin square, then take the transpose again at the end. This just amounts to doing the same steps as before, but with the roles of rows and columns exchanged. □

Now consider a Latin rectangle where both p and q are strictly less than n, so neither Theorem 8 nor Corollary 14 is applicable. Can we still extend it to give an $n \times n$ Latin square? It is not hard to find examples where this is not possible.

Example 15. Take $P = Q = \{1, 2\}$ and $N = \{1, 2, 3\}$ and $L = \begin{bmatrix} 2 & 3 \\ 3 & 2 \end{bmatrix}$. We could try to extend this to a 3×3 Latin square as follows:

$$\left[\begin{array}{cc|c} 2 & 3 & a \\ 3 & 2 & b \\ \hline c & d & e \end{array}\right].$$

To avoid a clash in row 1, we must take $a = 1$. To avoid a clash in row 2, we must also take $b = 1$. However, this creates an unavoidable clash in column 3. Thus, it is impossible to extend L.

Example 16. Take $P = Q = \{1, 2, 3, 4\}$ and $N = \{1, \ldots, 6\}$ and

$$L = \begin{bmatrix} 6 & 1 & 2 & 3 \\ 5 & 6 & 3 & 1 \\ 1 & 3 & 6 & 2 \\ 3 & 2 & 6 & 4 \end{bmatrix}.$$

It turns out that it is not possible to extend this to a 6×6 Latin square. It is a good exercise to prove this directly. However, we will deduce it from a general theorem instead. We can list the multiplicity and excess of the elements of N as follows:

k	1	2	3	4	5	6
$L(k)$	3	3	4	1	1	4
$E(k)$	1	1	2	-1	-1	2

It turns out that the key point is that some multiplicities are negative.

Definition 17. Let L be a Latin rectangle. We say that an element $k \in N$ is *plausible* if $E(k) \geq 0$. More precisely, we say that k is *barely plausible* if $E(k) = 0$, and *very plausible* if $E(k) > 0$.

Proposition 18. *If L can be extended to an $n \times n$ Latin square, then every element $k \in N$ is plausible for L.*

Proof. Choose a Latin square extending L. This will have the form

$$\left[\begin{array}{c|c} L & L' \\ \hline L'' & L''' \end{array}\right],$$

where L', L'' and L''' have shape $p \times (n-q)$, $(n-p) \times q$ and $(n-p) \times (n-q)$. Let L^* be the top part, consisting of L and L'. This is a $p \times n$ Latin rectangle, so Lemma 12 tells us that

$$L(k) + L'(k) = L^*(k) = p,$$

so $L(k) = p - L'(k)$. On the other hand, $L'(k)$ has $n-q$ columns, and there is at most one occurrence of k per column, so $L'(k) \leq n-q$, so $p - L'(k) \geq p+q-n$. Putting this together, we get $L(k) \geq p+q-n$ and so $E(k) = L(k) + n - p - q \geq 0$. □

In Example 16, we see that 4 and 5 have negative excess so they are not plausible, so there cannot be any extension to a 6×6 Latin square. We now discuss another example.

Example 19. Consider the following Latin rectangle with $p = 4$ and $q = 5$ and $n = 7$:

$$L = \begin{bmatrix} 5 & 6 & 1 & 3 & 2 \\ 6 & 5 & 2 & 4 & 7 \\ 1 & 4 & 3 & 5 & 6 \\ 4 & 7 & 5 & 6 & 1 \end{bmatrix}.$$

The multiplicities and excesses are as follows:

k	1	2	3	4	5	6	7
$L(k)$	3	2	2	3	3	4	2
$E(k)$	1	0	0	1	1	2	0

We have $E(k) \geq 0$ so all elements are plausible, so we might guess that L can be extended to a 7×7 Latin square. However, Proposition 18 does not give us any guarantees about this. If we had found that $E(k) < 0$ for some k, then Proposition 18 would tell us that is definitely no extension. However, when $E(k) \geq 0$ for all k we can only say (for the moment) that the question remains open. To go beyond this we need another lemma and another theorem.

Lemma 20. *Let L be a $p \times q$ Latin rectangle, where $0 < p < n$ and $0 < q \leq n$, and suppose that every $k \in N$ is plausible for L. Then we can add an extra row to obtain a $(p+1) \times q$ Latin rectangle L' such that every $k \in N$ is still plausible for L'.*

Proof. We set up a job allocation problem similar to the one in the proof of Theorem 8. We again put $d = n - p > 0$. We again have a job for each $j \in Q$, with candidates $C[j] = N \setminus \{L_{1j}, \ldots, L_{pj}\}$, so $|C[j]| = n - p = d$. We again put $D[k] = \{j \mid k \in C[j]\}$, which corresponds to the set of columns not containing k. Remark 11 tells us that the number of columns that do contain k is $L(k)$, so the number of columns that do not contain k is $|D[k]| = q - L(k)$. The plausibility condition says that $L(k) + n - p - q \geq 0$, which translates to $q - L(k) \leq n - p = d$, so we see that $|D[k]| \leq d$. In fact, we have $|D[k]| = d$ iff $E(k) = 0$ iff k is barely plausible. Now recall Corollary 56. That result referred to an allocation problem in which each job has exactly d candidates, and each person can do at most d jobs, and the people who can do d jobs are called "talented". The conclusion is that the jobs can be allocated in such a way that every talented person gets a job. This is mathematically equivalent to our current problem, with the talented people corresponding to the barely plausible elements of N. It is therefore possible to add a new row to give a $(p+1) \times q$ Latin rectangle L', in such a way that every barely plausible element appears in the new row. Now note that

$$L'(k) = \begin{cases} L(k) + 1 & \text{if } k \text{ is in the new row} \\ L(k) & \text{otherwise} \end{cases}$$

so

$$E'(k) = L'(k) + n - p - q - 1 = \begin{cases} E(k) & \text{if } k \text{ is in the new row} \\ E(k) - 1 & \text{otherwise} , \end{cases}$$

so in particular $E'(k) \geq E(k) - 1$ in all cases. Thus, if $E(k) > 0$ then $E'(k) \geq 0$. On the other hand, if $E(k) = 0$ then k is barely plausible for L, so k appears in the new row by construction, so $E'(k) = E(k) = 0$. Thus, in all cases we have $E'(k) \geq 0$. □

Theorem 21. *Let L be a $p \times q$ Latin rectangle, and suppose that every $k \in N$ is plausible for L. Then L can be extended to an $n \times n$ Latin square.*

Proof. We can apply the lemma repeatedly until we get a $n \times q$ Latin rectangle, then we can apply Corollary 14 to get an $n \times n$ Latin rectangle. □

Example 22. We now show how to extend the the rectangle from Example 19. The process is controlled by the following two tables.

$$\left[\begin{array}{ccccc|cc}
5 & 6 & 1 & 3 & 2 & 47^1 & \mathbf{4} \\
6 & 5 & 2 & 4 & 7 & 13^4 & \mathbf{3} \\
1 & 4 & 3 & 5 & 6 & 27^2 & \mathbf{7} \\
4 & 7 & 5 & 6 & 1 & 23^3 & \mathbf{2} \\
\hline
\mathbf{2}37 & 12\mathbf{3} & 46\mathbf{7} & \mathbf{1}27 & 34\mathbf{5} & 56^6 & \mathbf{6} \\
\mathbf{3}7 & \mathbf{1}2 & \mathbf{4}6 & 2\mathbf{7} & 3\mathbf{5} & 16^5 & \mathbf{1} \\
\mathbf{7} & \mathbf{1} & \mathbf{6} & \mathbf{2} & \mathbf{3} & 45^7 & \mathbf{5}
\end{array}\right]$$

k	1	2	3	4	5	6	7
$E(k)$	1	0	0	1	1	2	0
$E'(k)$	1	0	0	1	0	1	0
$E''(k)$	0	0	0	1	0	0	0

In the left hand table, the top left block is the original matrix L. In the right hand table, the second row shows the excesses of $1, \ldots, 7$ in L; in particular, the numbers 2, 3 and 7 have $E(k) = 0$ so they are barely plausible. We want to add a new row, making sure that we include the barely plausible numbers 2, 3 and 7. The possibilities for columns $1, \ldots, 6$ are 237, 123, 467, 127 and 345, as shown in row 5 on the left. From these sets we choose 2, 3, 7, 1 and 4, as indicated by the bold entries in row 5. This gives a 5×5 Latin rectangle which we call L'. For the next step, we need to know the excesses for L', which we denote by $E'(k)$. As we saw in the proof of Lemma 20, we have $E'(k) = E(k)$ if k appears in the new row, and $E'(k) = E(k) - 1$ if k does not appear in the new row. The resulting values are shown in row 3 of the right hand table. In particular, $2, 3, 5$ and 7 are barely plausible for L'. To get the potential entries for row 6, we simply take the sets of potential entries from row 5 and remove the bold ones, leaving 37, 12, 46, 27 and 35. We must choose five distinct numbers, one from each of these sets, in such a way that the barely plausible numbers $2, 3, 5$ and 7 are included. We choose $3, 2, 4, 7, 5$, as indicated by the bold entries in row 6. This gives a 6×5 Latin rectangle which we call L''. The excesses for E'' are again shown in the right hand table. However, we do not really need them, because there is now only one possible way to fill in row 7, namely $(7, 1, 6, 2, 3)$. This gives a 7×5 Latin rectangle. As this has the maximum possible height, we are back in the context of Corollary 14, and we do not need to keep track of excesses any more. To the right of the vertical bar, we have written the possible entries for column 7. As our first step (indicated by the superscript 1) we decide to try choosing 7 for the entry in row 1. For the second step (indicated by the superscript 2) we consider row 3. The possible choices there are 2 and 7, but we already used 7 for row 1, so we must use 2 for row 3. For the third step, we consider row 4. The possible choices there are 2 and 3, but we already used 2 for row 3, so we must use 3 for row 4. Continuing in the same way, we must use 1 in row 2, then 6 in row 6, then 5 in row 5, then 4 in row 7. This gives $(7, 1, 2, 3, 5, 6, 4)$ as column 6, and leaves $(4, 3, 7, 2, 6, 1, 5)$ as the only possibility for column 7. We end up with the following Latin square:

$$\begin{bmatrix}
5 & 6 & 1 & 3 & 2 & 7 & 4 \\
6 & 5 & 2 & 4 & 7 & 1 & 3 \\
1 & 4 & 3 & 5 & 6 & 2 & 7 \\
4 & 7 & 5 & 6 & 1 & 3 & 2 \\
2 & 3 & 7 & 1 & 4 & 5 & 6 \\
3 & 2 & 4 & 7 & 5 & 6 & 1 \\
7 & 1 & 6 & 2 & 3 & 4 & 5
\end{bmatrix}$$

We now start to discuss the theory of orthogonal Latin squares. We will give an example before the definition.

Example 23. Consider the following matrices:

$$L = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \qquad M = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix} \qquad L * M = \begin{bmatrix} 00 & 12 & 21 \\ 11 & 20 & 02 \\ 22 & 01 & 10 \end{bmatrix}$$

Both L and M are Latin squares. The matrix $L * M$ is formed by merging L and M in an obvious way: in symbols, the entry $(L*M)_{ij}$ is the ordered pair (L_{ij}, M_{ij}). There are 9 possible pairs uv with $u, v \in \{0, 1, 2\}$, as follows:

$$00,\ 01,\ 02, \quad 10,\ 11,\ 12, \quad 20,\ 21,\ 22.$$

It is not hard to check that each of these pair occurs precisely once in $L * M$.

Definition 24. Let L and M be two $n \times n$ Latin squares, with the same sets P, Q and N. Let $L * M$ be the matrix with entries $(L * M)_{ij} = (L_{ij}, M_{ij}) \in N^2$ for each $i \in P$ and $j \in Q$. We say that L and M are *orthogonal* if each of the n^2 elements of N^2 occurs precisely once in $L * M$. Equivalently, L and M are orthogonal if the entries in $L * M$ are all different.

Example 25. Consider the following matrices:

$$L = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \qquad M = \begin{bmatrix} 1 & a & b \\ c & d & e \\ f & g & 2 \end{bmatrix} \qquad L * M = \begin{bmatrix} 11 & 2a & 3b \\ 3c & 1d & 2e \\ 2f & 3g & 12 \end{bmatrix}$$

We will try to find $a, \ldots, g$ such that M is a Latin square and is orthogonal to L.

- $L * M$ must contain 13 somewhere, and this can only happen if $d = 3$ so that 13 appears as the middle entry.
- In M, entry b lies in the same row as 1 and in the same column as 2, so it must be different from 1 and 2, so it must be equal to 3. By the same logic we also have $f = 3$.
- Now M is as shown on the left below. To make this a Latin square, each row must contain $1, 2$ and 3, and each column must contain $1, 2$ and 3. The only way to achieve this is to take $a = c = 2$ and $e = g = 1$, giving the matrix shown on the right below.

$$M = \begin{bmatrix} 1 & a & 3 \\ c & 3 & e \\ 3 & g & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

- We now have

$$L * M = \begin{bmatrix} 11 & 22 & 33 \\ 32 & 13 & 21 \\ 23 & 31 & 12 \end{bmatrix}.$$

  Inspection shows that each of the 9 possible pairs $11,\ 12,\ 13, 21,\ 22,\ 23, 31,\ 32,\ 33$ appears precisely once in $L * M$, so we have succeeded in finding a Latin square that is orthogonal to L.

We now discuss some facts about the number of possible $n \times n$ Latin squares. (**Note:** I prepared this material but did not cover it in lectures so it is not examinable. I am including it for interest and in case I need it next year.)

Definition 26. We let $\mathcal{L}_n$ denote the set of all Latin squares L with $P = Q = N = \{1, \ldots, n\}$. We will find $|\mathcal{L}_n|$ for $n \leq 4$. We say that a Latin square $L \in \mathcal{L}_n$ is *reduced* if the first row is $(1, 2, \ldots, n)$ and the first column is also $(1, 2, \ldots, n)$. We write $\mathcal{R}_n$ for the set of reduced Latin squares.

Example 27. For the degenerate case $n = 1$ the only possible Latin square is $L = \begin{bmatrix} 1 \end{bmatrix}$, so $\mathcal{L}_1 = \mathcal{R}_1$ and $|\mathcal{L}_1| = |\mathcal{R}_1| = 1$.

Example 28. For $n = 2$ we have $\mathcal{L}_2 = \left\{ \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \right\}$. The first of these lies in $\mathcal{R}_2$ but the second does not. We therefore have $|\mathcal{R}_2| = 1$ and $|\mathcal{L}_2| = 2$.

Example 29. For $n = 3$ there are 12 Latin squares, as follows:

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

Of these only the first lies in $\mathcal{R}_3$. Thus, we have $|\mathcal{R}_3| = 1$ and $|\mathcal{L}_3| = 24$.

Proposition 30. *For any n we have $|\mathcal{L}_n| = n!(n-1)!|\mathcal{R}_n|$.*

Proof. (a) We can permute the columns of a Latin square and it will still be a Latin square.
(b) We can also permute the rows of a Latin square and it will still be a Latin square.
(c) There is a unique way to permute the columns so that the first row becomes $(1, \dots, n)$.
(d) After we have done this, the top left entry will be 1, and the first entries in columns $2, \dots, n$ will therefore be $2, \dots, n$ in some order. Thus, there is a unique way to permute rows $2, \dots, n$ so that the first column becomes $1, \dots, n$. We now have a Latin square in $\mathcal{R}_n$.

By thinking about these steps in the reverse order, we obtain the following fact. We can obtain any Latin square in $\mathcal{L}_n$ by starting with a square in $\mathcal{R}_n$, permuting rows $2, \dots, n$ in any of $(n-1)!$ possible ways, then permuting the columns in any of $n!$ possible ways. The claim is clear from this. □

Proposition 31. *We have $|\mathcal{R}_4| = 4$ and so $|\mathcal{L}_4| = 4! \times 3! \times 4 = 576$.*

Proof. We claim that $\mathcal{R}_4$ consists of the following 4 squares. The superscripts are just there to help us follow the proof.

$$L^1 = \begin{bmatrix}1&2&3&4\\2&3^{0*}&4^{2}&1^{1}\\3&4^{4}&1^{6}&2^{5}\\4&1^{3}&2^{7}&3^{8}\end{bmatrix}\quad L^2 = \begin{bmatrix}1&2&3&4\\2&4^{0*}&1^{1}&3^{2}\\3&1^{3}&4^{6}&2^{5}\\4&3^{4}&2^{7}&1^{8}\end{bmatrix}\quad L^3 = \begin{bmatrix}1&2&3&4\\2&1^{0*}&4^{1}&3^{2}\\3&4^{3}&1^{5*}&2^{6}\\4&3^{4}&2^{7}&1^{8}\end{bmatrix}\quad L^4 = \begin{bmatrix}1&2&3&4\\2&1^{0*}&4^{1}&3^{2}\\3&4^{3}&2^{5*}&1^{6}\\4&3^{4}&1^{7}&2^{8}\end{bmatrix}$$

The numbers in the superscripts indicate the order in which we should think about the entries; the stars indicate places where we have a choice about what to do.

The first row and column have to be $(1, 2, 3, 4)$. Thus, the first place where we have any choice is the $(2, 2)$ position, which we have marked with the superscript $0*$. We already have a 2 in the corresponding row (and also in the corresponding column), so we cannot put a 2 in this position; we must have a 3, a 4 or a 1. For square L^1 we choose to put a 3 in the $(2, 2)$ position. It turns out that we then have no more choices. To see this, consider the superscript 1, which appears in position $(2, 4)$ in L^1. There we have already placed a 2 and a 3 in the same row and a 4 in the same column, so we have to put a 1 in that slot. Now consider the superscript 2, which appears in position $(2, 3)$ in L^1. We have already placed 1, 2 and 3 in the same row, so we are forced to put 4 in this slot. Now continue with the positions with superscripts $3, 4, \dots, 8$; we again see that there is never any choice, and we have to fill in the entries as in L^1. Thus, L^1 is the only possible Latin square in $\mathcal{R}_4$ that has a 3 in position $(2, 2)$. Similarly, L^2 is the only Latin square in $\mathcal{R}_4$ that has a 4 in position $(2, 2)$. The only other possibility is to put a 1 in position $(2, 2)$, as in L^3. Just as in the case of L^1 and L^2, we find that there is no choice about what to put in the positions with superscripts $1, \dots, 4$. However, when we get to the superscript $5*$ in position $(3, 3)$, we find that we do have a choice: we can either put in a 1 or a 2. If we put in a 1 then we are forced to fill in the remaining 3 slots as in L^3, but if we put in a 2 then we are forced to fill in the remaining 3 slots as in L^4. We thus have $\mathcal{R}_4 = \{L^1, L^2, L^3, L^4\}$ as claimed. □

Remark 32. The numbers $|\mathcal{R}_n|$ grow very quickly as n increases:

n	$\lvert\mathcal{R}_n\rvert$
1	1
2	1
3	1
4	4
5	56
6	9,408
7	16,942,080
8	535,281,401,856

We will not prove any of this.

We now consider a different problem. Given $n > 0$, can we find a long list of $n \times n$ Latin squares $L^1, \dots, L^r$ such that L^u and L^v are orthogonal when $u \neq v$? Our first result gives an upper bound on the possible length of such a list.

Theorem 33. *Suppose we have a list $L^1, \dots, L^r$ of mutually orthogonal Latin squares of size n. Then $r \leq n - 1$.*

Proof. Look at the first two rows of L^u:

	1		m_u		n
1			x		
2	x				

In position $(2, 1)$ (at the beginning of the second row), we have some number $x \in \{1, \dots, n\}$. Because L^u is a Latin square, every number must appear in every row. In particular, x must also appear in row 1. It cannot appear in position $(1, 1)$, because we would then have two x's in the first column. So x must also appear at position $(1, m_u)$ for some $m_u \in \{2, \dots, n\}$. We have now defined numbers $m_1, \dots, m_r$; we claim that they are all different. Indeed, suppose that $v \neq u$, so the first two rows of L^v have the form

	1		m_v		n
1			y		
2	y				

If m_u and m_v were the same, then in $L^u * L^v$ we would have a pattern like this:

	1		$m_u = m_v$		n
1			xy		
2	xy				

so xy would appear twice in $L^u * L^v$. However, L^u and L^v are assumed to be orthogonal, so each pair occurs precisely once in $L^u * L^v$, so xy cannot appear twice, so m_v must be different from m_u.

We now know that the numbers $m_1, \dots, m_r$ are all different and all lie in $\{2, \dots, n\}$. This is clearly only possible if $r \leq n - 1$. □

We now see that the maximum possible length of a list of mutually orthogonal $n \times n$ Latin squares is at most $n - 1$. Can we achieve this upper bound? A key example is as follows.

Proposition 34. *Let p be a prime. For $0 < u < p$ define $L^u_{ij} = i + uj \pmod p$. Then L^u is a Latin square (with $P = Q = N = \mathbb{Z}/p$). Moreover, L^u and L^v are orthogonal if $u \neq v$ (so we have a list of $p - 1$ mutually orthogonal Latin squares of size p).*

Proof. First recall that $\mathbb{Z}/p$ is a field. Thus, if $a, b \in \mathbb{Z}/p$ with $b \neq 0$ then a/b makes sense as an element of $\mathbb{Z}/p$, and fractions like this have all the usual properties.

Now fix u with $0 < u < p$, and put $L^u_{ij} = i + uj$. If $L^u_{ij} = L^u_{i'j}$ we have $i + uj = i' + uj$ so $i = i'$. Similarly, if $L^u_{ij} = L^u_{ij'}$ then $i + uj = i + uj'$ in $\mathbb{Z}/p$. We can rearrange to get $u.(j - j') = 0$ but u is invertible in $\mathbb{Z}/p$ so we can multiply by u^{-1} to get $j - j' = 0$ and so $j = j'$ (in $\mathbb{Z}/p$). This shows that L^u is a Latin square.

Now consider $L^u * L^v$, where $0 < u, v < p$ with $u \neq v$, so $(L^u * L^v)_{ij} = (i + uj, i + vj)$. We want to show that every pair $(x, y) \in (\mathbb{Z}/p)^2$ appears precisely once in this table, or in other words that there is a unique pair (i, j) with$(i + uj, i + vj) = (x, y)$, or that the simultaneous equations $i + uj = x$ and $i + vj = y$ have a unique solution. These equations can be solved in the standard way to give $i = (vx - uy)/(v - u)$ and $j = (x - y)/(u - v)$ as required. □

Remark 35. Now consider a number n that is a prime power, say $n = p^v$ for some prime number p and some $v > 1$. In this case the ring $\mathbb{Z}/n$ is not a field, but there is a more complicated way to define a field F with $|F| = n$. We will not discuss the construction here, but it can be found in most books on field theory. Now suppose that $u \in F$ with $u \neq 0$ (so there are $n - 1$ possible choices for u). We can again define a Latin square L^u with $P = Q = N = F$ by $L^u_{ij} = i + uj$, and we again find that L^u and L^v are orthogonal when $u \neq v$. Thus, we have a list of $n - 1$ mutually orthogonal Latin squares of size n.

The first number that is not a prime or prime power is 6. This case is already hard.

Theorem 36. *There are not even two mutually orthogonal Latin squares of size* 6*.*

Proof. This was conjectured by Euler in the 18th century, and proved by Tarry in 1900. A more digestible proof was given by Stinson in 1982. We will not give any details here. □