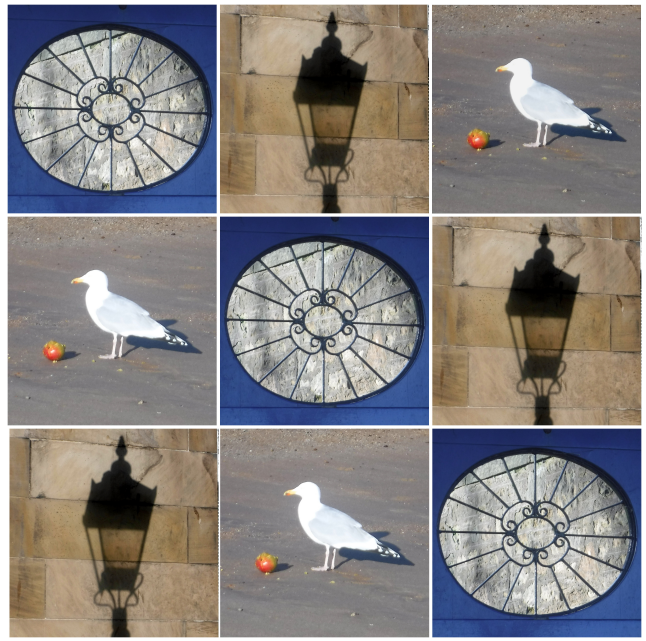
# Latin squares



Peter J. Cameron
University of St Andrews

Sutton Trust Talk
3 July 2019

# Who invented Sudoku?

In an appendix to a Sunday newspaper, entitled "Ten things you didn't know about Switzerland", some years ago, I read:

7. Leonhard Euler invented Sudoku.

In fact he didn't (I will tell you later who did), but the story is rather interesting, as is the reason why the things I am talking about are called Latin squares.
Euler was the most prolific mathematician of all time; his collected works run to over 80 volumes.

# Magic squares

A magic square is an $n \times n$ array, whose entries are the numbers from 1 to $n^2$, in such a way that the numbers in any row, column or diagonal of the square have the same sum. Since all the numbers from 1 to $n^2$ add up to $n^2(n^2+1)/2$, if each of the $n$ rows has the same sum, this sum must be $n(n^2+1)/2$. For $n = 3$, this magic sum is 15; for $n = 4$, it is 34. In former times, such squares were regarded as having very special properties. Some thought that, if worn in battle, a magic square would protect its wearer from injury! So finding magic squares was an important technology of the day.

# The *Lo Shu*

The Chinese had an example of a magic square of order 3, called the *Lo Shu*. It was supposedly written (in Chinese numerals) on the back of a turtle in the River Lo.

The picture is a Tibetan version of the Lo Shu. Here it is in modern Western form.

| | | |
|---|---|---|
| 4 | 9 | 2 |
| 3 | 5 | 7 |
| 8 | 1 | 6 |

# Dürer

The artist Albrecht Dürer produced a famous engraving called *Melancholy*, in which a moody-looking angel contemplates varies mathematical figures and tools. On the wall is a magic square, which Dürer has arranged so that the bottom row gives the date of the picture: 1514.


Do you think Dürer thought mathematicians were sad people?

# Graeco-Latin squares

Euler invented a new method for constructing magic squares. This was his idea.
Suppose that we can find two $n \times n$ squares, one with $n$ Latin letters and the other with $n$ Greek letters, so that

- each letter occurs once in each row and column of the relevant square;
- if the squares are superimposed, each combination of Latin and Greek letters occurs exactly once.

| | | |
|---|---|---|
| $C$ | $A$ | $B$ |
| $A$ | $B$ | $C$ |
| $B$ | $C$ | $A$ |

| | | |
|---|---|---|
| $\beta$ | $\alpha$ | $\gamma$ |
| $\gamma$ | $\beta$ | $\alpha$ |
| $\alpha$ | $\gamma$ | $\beta$ |

| | | |
|---|---|---|
| $C\beta$ | $A\alpha$ | $B\gamma$ |
| $A\gamma$ | $B\beta$ | $C\alpha$ |
| $B\alpha$ | $C\gamma$ | $A\beta$ |

Next we interpret that Latin letters as "tens digits" and Greek letters as "units digits" in whole numbers written to base $n$. For example, if $n = 3$, then $C\beta$ is interpreted as the number 21 in base 3, which is $2 \times 3 + 1 = 7$. The condition on the Graeco-Latin square shows that all pairs from $00 = 0$ up to $(n-1)(n-1) = n^2 - 1$ occurs once. Then add 1 to each entry so that the numbers run from 1 up to $n^2$.

| | | |
|---|---|---|
| $21 = 7$ | $00 = 0$ | $12 = 5$ |
| $02 = 2$ | $11 = 4$ | $20 = 6$ |
| $10 = 3$ | $22 = 8$ | $01 = 1$ |

| | | |
|---|---|---|
| 8 | 1 | 6 |
| 3 | 5 | 7 |
| 4 | 9 | 2 |

Finally you might have to rearrange the rows and columns to get the diagonal sums right. (In this case I have done it for you.)

# Euler's construction

So Euler needed to be able to construct Graeco-Latin squares of order $n$ (this means $n \times n$) for as many $n$ as possible.
He found that he was able to produce a construction for any number $n$ not of the form $4k + 2$ (that is, not leaving a remainder of 2 when divided by 4.
Here is a construction you can try for yourself. It involves modular arithmetic, that is doing calculations and then taking the remainder on dividing by $n$ (much as you do with the hours on a clock, with $n = 12$.)
This construction works for all *odd* numbers $n$. We take the rows, columns, and letters all to be the numbers $0, 1, 2, \ldots, n-1$. In row $i$ and column $j$ of the first square, you put $i + j$; in the second square, you put $i + 2j$. (So, for example, if $n = 5$, then in row 3 and column 4 in the first square you put 2, and in the second square you put 1.)

# Euler's conjecture

It is easy to see that there is no Graeco-Latin square of order 2.
You can try that for yourself.
Euler was unable to find a Graeco-Latin square of order $n = 6$.
So he posed his "problem of the 36 officers":

> *Thirty-six officers, of six different ranks and from six different regiments (each combination of rank and regiment represented by one officer) are to be arranged on a parade ground in a* $6 \times 6$ *square in such a way that in each row and each column, each rank and each regiment occurs exactly once.*

Indeed, Euler came to think after exhaustive trials that this was impossible:

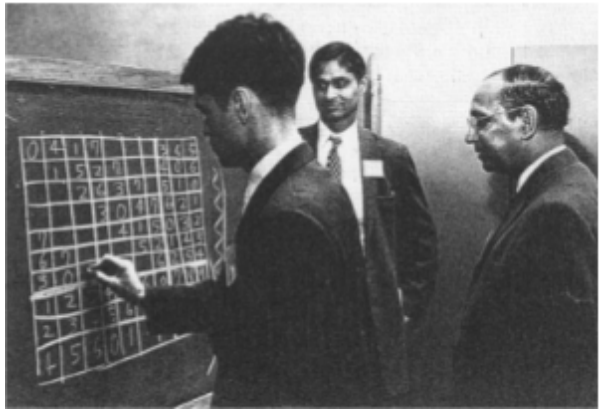
Euler conjectured that, furthermore, no solution could be found for any number $n$ of the form $4k + 2$.

# What happened to Euler's conjecture?

To run the story forward: In 1900, Tarry proved, by exhaustive case analysis, that Euler was right about 6, and there was indeed no Graeco-Latin square of order 6.
However, he may not have been the first. On 10 August 1842, Heinrich Schumacher, the astronomer in Altona, Germany, wrote a letter to Gauss, telling him that his assistant, Thomas Clausen, had proved that there is no Graeco-Latin square of order 6.
However, Clausen's calculations have never been found.

# The end of the conjecture

In 1959, R. C. Bose and S. S. Shrikhande constructed a Graeco-Latin square of order 22, and E. T. Parker found others of orders 10, 34, 46 and 70.
The three authors joined forces, and in 1960 showed that Euler was as wrong as he could be: they constructed Graeco-Latin squares of all orders except $n = 2$ or $n = 6$.
Their result made the front page of the *New York Times*, and they became known as the *Euler spoilers*.



# Latin squares

A Latin square is an $n \times n$ array whose cells contain entries from a set of $n$ letters so that each letter occurs once in each row and once in each column.
Thus, if we take a Graeco-Latin square and ignore the Greek letters, we get a Latin square: hence the name. (Of course, if we ignore the Latin letters and just use the Greek letters, we also get a Latin square ...)
There is no difficulty in constructing Latin squares. Just write $1, \ldots, n$ in the first row; then, in each successive row, move the first element to the end and everything else left one place (as in Scottish dancing):

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 2 | 3 | 4 | 1 |
| 3 | 4 | 1 | 2 |
| 4 | 1 | 2 | 3 |

# Algebra

Let's think about modular arithmetic again. We can represent modular addition and multiplication by tables: here they are for $n = 5$:

| $+$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

| $\times$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

The addition table is a Latin square; in fact it is the same one that we just constructed. The multiplication table is not, since all the entries in row 0 are 0 (as 0 times anything is 0). But if we just look at the other rows and columns, we see a Latin square. This works whenever $n$ is a prime number, and gives an algebraic structure called a field. Try it for yourself, both for primes, and for composite numbers.

# Algebra and Graeco-Latin squares

Algebra repays its debt. Whenever we have a field of order $n$ (and in particular, in modular arithmetic with $n$ prime), we can construct $n-1$ latin squares, such that every pair forms a Graeco-Latin square. Take squares $A_1, \ldots, A_{n-1}$, where the entry in row $i$ and column $j$ of $A_k$ is $i + kj$.

It can be shown that $n-1$ is the largest number of such squares possible with any two forming a Graeco-Latin square. There are important connections with geometry as well. But there is a big open problem. We only know examples when $n$ is a power of a prime number. *Do such sets of Latin squares exist for any other values of n?*

This problem still awaits its "Euler spoilers".

# Statistics

Rothamsted experimental station, near Harpenden in Hertfordshire, has been conducting agricultural experiments since 1843. Here is an experiment from the 20th century, on the effects of different insecticides on a crop of beans:

Agricultural land in England has been cultivated for centuries, and there maybe systematic effects on soil fertility in the direction of ploughing, so we don't want to confuse these with the effects of the insecticide. So we use each insecticide once in each row and once in each column: that is, a Latin square!

# Latin squares in experiments

In the above experiment, perhaps one of the treatments is not very effective. The insects could breed up on the plots using that treatment, and spread to neighbouring plots. In order to be fair to all treatments, we could require that, given any pair of treatments, numbers $i$ and $j$ say, treatment $j$ should occur once to the left of $i$, once to its right, once above in the same column, and once below. Such a square is called complete.
Here is an example:

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| 2 | 4 | 1 | 3 |
| 3 | 1 | 4 | 2 |
| 4 | 3 | 2 | 1 |

Another factor needs to be considered if we are using Latin squares to design our experiments.
Suppose the treatments you apply leave some residual effect in the soil. If you want to use the same plots again next year for an experiment, you should see that each treatment next year is paired with all treatments this year.
In other words, choose a Graeco-Latin square, and use the Latin letters this year, the Greek letters next. That guarantees that each of this year's treatments will precede each of next year's just once.

# Keeping secrets

If you want to keep your messages safe from prying eyes, you will need to encrypt them in some way, so that the recipient can decrypt them but an unauthorised interceptor cannot.
One ancient method is the *Caesar cipher*, used by Julius Caesar to send reports on the Gallic Wars back to Rome. To encrypt, you shift each letter forward a fixed number of places in the alphabet; the recipient knows the number of places, so shifts back the right number to get the message. The alphabet is regarded as written around a circle. So for example, if the shift was 10, the message SEND THE NINTH LEGION would be encrypted as COXN DRO XSXDR VOQSYX.
Of course this is very easy to break. There are only 25 shifts to try, and most of them will give nonsense, but one will give the correct message.

# One-time pad

This very simple and inefficient cipher can be tweaked to give something much more serious, called a one-time pad.
Instead of shifting all letters by the same amount, we choose a random shift for each letter. Perhaps we shift the first letter by 10, the second by 21, the third by 4, and so on, obtaining CZR. . . . The random shifts can be specified by choosing random letters of the alphabet, in this case the 10th, 21st, 4th, . . . : so the key is JUD. . . .
This is the only cipher which has been proved to be completely secure if properly used (this means, the key is random, and the interceptor has no access to it). This was done by C. Shannon.
The drawback is, of course, that the key is as long as the message, and must be kept secret from the enemy. So a spy going off into enemy country could take a one-time pad with him (a long list of random letters) and use it to encrypt his messages, destroying each page once used. If he loses it, he cannot encrypt messages any more!

It is said that, during the Cold War, this is the method that spies actually used. Peter Wright, in his book *Spycatcher*, tells of burgling the flats of suspected Soviet spies in London, finding and copying the one-time pads, and glueing them back up again to look untouched.

You can encrypt with the Latin square having rows and columns indexed by the alphabet; look up the message letter by row and the key letter by column, and read off the ciphertext letter from the square. Back at base, this procedure can be reversed.

Now to make things even more difficult for the enemy, you can use an arbitrary Latin square of order 26, rather than the simple cyclic square; this can be changed regularly. This method was used by the Japanese navy in the Second World War.

# Back to statistics

The famous statistician R. A. Fisher worked at Rothamsted for most of his career, and developed methods for experimental design, including the use of Latin squares.
Fisher recommended that, when using a Latin square in an experiment, the experimenter should choose at random from the available squares, to avoid bias. Accordingly, he and his colleague F. Yates produced tables of Latin squares up to order 6. The classification has been continued, though the numbers grow very rapidly. (If you write out the number of $n \times n$ Latin squares, the number of digits required grows faster than $n^2$.)
Two things have made life easier:

- A method for choosing a random Latin square of arbitrary size was developed by M. T. Jacobson and P. Matthews.
- After Fisher, statisticians realised that his method was not required; it was enough to take a single Latin square and pemute its rows, columns and letters.

Here are the numbers of Latin squares of orders up to 11.

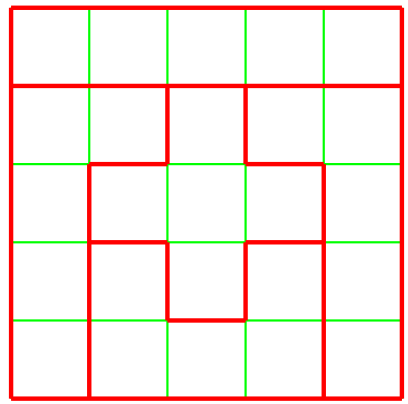
| | |
|---|---|
| 1 | 1 |
| 2 | 2 |
| 3 | 12 |
| 4 | 576 |
| 5 | 161280 |
| 6 | 812851200 |
| 7 | 61479419904000 |
| 8 | 108776032459082956800 |
| 9 | 5524751496156892842531225600 |
| 10 | 9982437658213039871725064756920320000 |
| 11 | 776966836171770144107444346734230682311065600000 |

# Why is it so hard?

There is no simple formula. I will try to indicate why, by looking at the case $n = 4$.
The first row consists of the numbers $1, 2, 3, 4$ in some order. The order doesn't matter, so it is OK to assume that the first row is $\boxed{1}\boxed{2}\boxed{3}\boxed{4}$. Then the second row is a permutation in which no number keeps its original place. Such a permutation is called a derangement, and there are nine of them. (In general, there is a formula for this number.)
But the derangements fall into two types, three of one and six of the other. If we take a derangement of the first type as the second row, there are four ways to complete to a Latin square; but for the second type, there are only two completions.
So the number of Latin squares is $24 \times (3 \times 4 + 6 \times 2) = 576$.
Incidentally, we do know that if you try to construct a Latin square row by row in this way, you will never get stuck; there is always at least one way to proceed.

# Gerechte designs

Two further developments were invented by statisticians. Suppose the field in which the plots are located is not "homogeneous". Perhaps there is a boggy patch in the middle, or there are trees along one side which shade the crops.
W. U. Behrens suggested the following procedure. Divide the square up into relatively homogeneous regions. Then arrange that each treatment occurs once in each region. If $n = 5$:



Can you find a Latin square so that each of the five regions contains all numbers $1, \ldots, 5$? Behrens called these gerechte designs (meaning "fair" or "just" designs).

# Critical sets

At about the same time, J. A. Nelder defined a critical set in a Latin square to be a set of positions such that, if you are given the entries in those positions, there is a unique way to fill in the other positions (but if you leave any of them out, there is more than one solution).

Here is a very simple example, with $n = 3$.

| | | |
|---|---|---|
| | 2 | |
| 3 | | |
| | | |

You can easily see that there is a unique completion. But if, say, we left out the 2, then in any solution we could simply swap the 1s and 2s to get a different solution.

Critical sets have uses in studying how to change one Latin square into another, and how to choose a random Latin square, for example.

Put together the ideas of gerechte design and critical set, and what do you get?

# Sudoku!

The work of Behrens and Nelder was done in the 1950s; statisticians could have come up with Sudoku at any time after that.
But in fact it was Howard Garns, a retired architect in New York, who invented it in 1979. It didn't catch on there, but Maki Kaji introduced it to Japan (where letter puzzles are more difficult to devise given their more complicated characters, so number puzzles are popular) under the name Sudoku in 1986. Then New Zealander Wayne Gould (brother of former British Labour MP Brian Gould) came across it in Japan and spread the word, and very quickly it became as standard a feature of our newspapers as the crossword.
Thus Sudoku asks you to "complete a critical set in the gerechte design formed by dividing a $9 \times 9$ square into $3 \times 3$ subsquares".

# Sudoku and mathematics

But that is not the end of the story, as far as mathematicians are concerned.
Felgenhauer and Jarvis did a big computation to show that the total number of different types of solution to ordinary Sudoku is $6,670,903,752,021,072,936,960$.
Then, using a little group theory (the theory of symmetries), Jarvis and Russell showed that, if we don't care about changing the symbols, or permuting rows and columns, the number of "essentially different" solutions is $5,472,730,538$.

# Symmetric Sudoku

Bob Connelly (who works on the stability of geodesic domes, invented a different form which he called symmetric Sudoku, and showed that there are just two essentially different solutions (so it is less interesting as a puzzle). The proof contained some interesting mathematics, including error-correcting codes and the card game SET®.
David Spiegelhalter, a statistician at Cambridge, turned one of the two solutions into stained glass: