Sudoku, Mathematics and Statistics

Peter J. Cameron

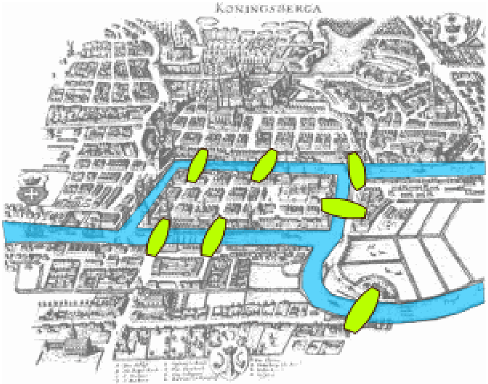
Forder lectures
April 2008

There's no mathematics involved. Use logic and reasoning to solve the puzzle.

Instructions in *The Independent*

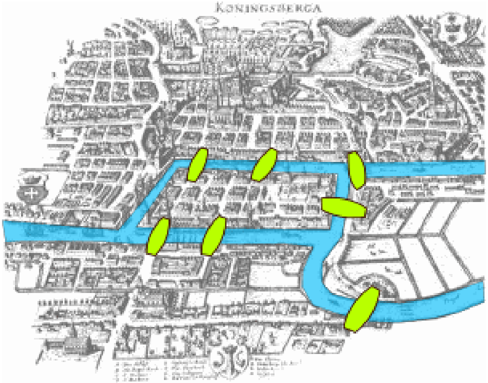
Euler

The bridges of Königsberg



Is it possible to walk around the town, crossing each bridge exactly once?

The bridges of Königsberg



Is it possible to walk around the town, crossing each bridge exactly once?
Euler showed: No!

What is mathematics?

Leonhard Euler, Letter to Carl Ehler, mayor of Danzig, 3 April 1736:

What is mathematics?

Leonhard Euler, Letter to Carl Ehler, mayor of Danzig, 3 April 1736:

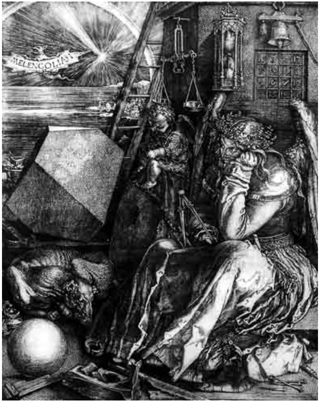
> *Thus you see, most noble Sir, how this type of solution [to the Königsberg bridge problem] bears little relationship to mathematics, and I do not understand why you expect a mathematician to produce it, rather than anyone else, for the solution is based on reason alone, and its discovery does not depend on any mathematical principle ...*

What is mathematics?

Leonhard Euler, Letter to Carl Ehler, mayor of Danzig, 3 April 1736:

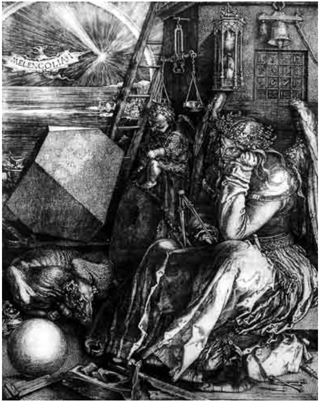
> *Thus you see, most noble Sir, how this type of solution [to the Königsberg bridge problem] bears little relationship to mathematics, and I do not understand why you expect a mathematician to produce it, rather than anyone else, for the solution is based on reason alone, and its discovery does not depend on any mathematical principle ...*
>
> *In the meantime, most noble Sir, you have assigned this question to the geometry of position, but I am ignorant as to what this new discipline involves, and as to which types of problem Leibniz and Wolff expected to see expressed in this way.*

Dürer's *Melancholia*



16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

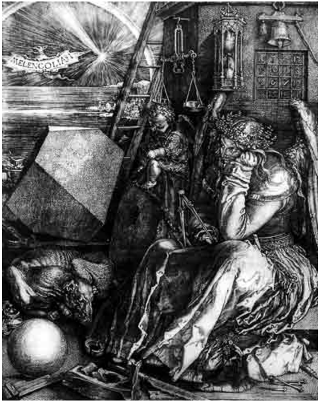
Dürer's *Melancholia*



16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

All rows, columns, and diagonals sum to 34.

Dürer's *Melancholia*



16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

All rows, columns, and diagonals sum to 34. The date of the picture is included in the square.

Euler's construction

Take a Graeco-Latin square of order n.

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

Euler's construction

Take a Graeco-Latin square of order n. Replace the symbols by $0, 1, \ldots, n-1$.

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

21	02	10
00	11	22
12	20	01

Euler's construction

Take a Graeco-Latin square of order n. Replace the symbols by $0, 1, \ldots, n-1$. Interpret the result as a two-digit number in base n. Add one.

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

21	02	10
00	11	22
12	20	01

8	3	4
1	5	9
6	7	2

Euler's construction

Take a Graeco-Latin square of order n. Replace the symbols by $0, 1, \ldots, n-1$. Interpret the result as a two-digit number in base n. Add one.

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

21	02	10
00	11	22
12	20	01

8	3	4
1	5	9
6	7	2

Some rearrangement may be needed to get the diagonal sums correct.

Euler's construction

Take a Graeco-Latin square of order n. Replace the symbols by $0, 1, \ldots, n-1$. Interpret the result as a two-digit number in base n. Add one.

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

21	02	10
00	11	22
12	20	01

8	3	4
1	5	9
6	7	2

Some rearrangement may be needed to get the diagonal sums correct.

So for which n do Graeco-Latin squares exist?

Euler's officers

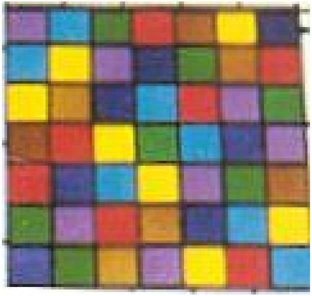
Six different regiments have six officers, each one holding a different rank (of six different ranks altogether). Can these 36 officers be arranged in a square formation so that each row and column contains one officer of each rank and one from each regiment?

Euler's officers

> *Six different regiments have six officers, each one holding a different rank (of six different ranks altogether). Can these 36 officers be arranged in a square formation so that each row and column contains one officer of each rank and one from each regiment?*

Trial and error suggests the answer is "No":

Latin squares in statistics



Latin squares were introduced into statistics by R. A. Fisher.

Latin squares in statistics

A Latin square at Rothamsted Experimental Station.

This Latin square was designed by Rosemary Bailey. Thanks to Sue Welham for the photograph.

Gerechte designs

W. Behrens: What if there is, for example, a boggy patch in the middle of the field?

Gerechte designs

W. Behrens: What if there is, for example, a boggy patch in the middle of the field?

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

Gerechte designs

W. Behrens: What if there is, for example, a boggy patch in the middle of the field?

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

This is a gerechte design (a “fair design”).

Critical sets

John Nelder: A critical set is a partially filled Latin square which can be completed in a unique way to a Latin square, but if any entry is deleted the completion is no longer unique.

1	2		
2			
			3

Sudoku

So a Sudoku puzzle is a partial gerechte design for the partition of a 9×9 square into nine 3×3 subsquares, which contains a critical set.

Sudoku

So a Sudoku puzzle is a partial gerechte design for the partition of a 9×9 square into nine 3×3 subsquares, which contains a critical set.

In fact Sudoku was invented by Howard Garns (a retired New York architect) in the 1980s, under the name "number place", was taken up in Japan and re-names Sudoku, and spread worldwide from there.

How many Sudoku solutions?

We count Sudoku solutions up to

- Permuting the numbers $1, \ldots, 9$;
- Permuting rows and columns preserving the partitions into 3 sets of 3;
- Possibly transposing the grid.

How many Sudoku solutions?

We count Sudoku solutions up to

- Permuting the numbers $1, \ldots, 9$;
- Permuting rows and columns preserving the partitions into 3 sets of 3;
- Possibly transposing the grid.

The number of different solutions of ordinary Sudoku is 5 472 730 538.

How many Sudoku solutions?

We count Sudoku solutions up to

- Permuting the numbers $1, \ldots, 9$;
- Permuting rows and columns preserving the partitions into 3 sets of 3;
- Possibly transposing the grid.

The number of different solutions of ordinary Sudoku is 5 472 730 538.
This was computed by Jarvis and Russell using the Orbit-counting Lemma applied to the group $(S_3 \operatorname{wr} S_3) \operatorname{wr} S_2$ of order $6^8 \cdot 2$.

Robert Connelly's Symmetric Sudoku

Each number from 1 to 9 should occur once in each set of the following types:

- rows;
- columns;
- 3×3 subsquares;
- broken rows (one of these consists of three "short rows" in the same position in the three subsquares in a large column);
- broken columns (similarly defined);
- locations (a location consists of the nine cells in a given position, e.g. middle of bottom row, in each of the nine subsquares).

Example

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

Example

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

Rows

Example

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

Columns

Example

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

Subsquares

Example

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

Broken rows

Example

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

Broken columns

Example

3	5	9	2	4	8	1	6	7
4	8	1	6	7	3	5	9	2
$\boxed{7}$	2	6	$\boxed{9}$	1	5	$\boxed{8}$	3	4
8	1	4	7	3	6	9	2	5
2	6	7	1	5	9	3	4	8
$\boxed{5}$	9	3	$\boxed{4}$	8	2	$\boxed{6}$	7	1
6	7	2	5	9	1	4	8	3
9	3	5	8	2	4	7	1	6
$\boxed{1}$	4	8	$\boxed{3}$	6	7	$\boxed{2}$	5	9

Locations

Affine geometry

We coordinatise the cells of the grid with F^4, where F is the integers mod 3, as follows:

- the first coordinate labels large rows;
- the second coordinate labels small rows within large rows;
- the third coordinate labels large columns;
- the fourth coordinate labels small columns within large columns.

Affine geometry

We coordinatise the cells of the grid with F^4, where F is the integers mod 3, as follows:

- the first coordinate labels large rows;
- the second coordinate labels small rows within large rows;
- the third coordinate labels large columns;
- the fourth coordinate labels small columns within large columns.

Now Connelly's regions are cosets of the following subspaces:

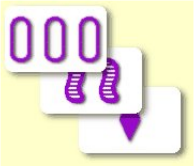
Rows	$x_1 = x_2 = 0$	Columns	$x_3 = x_4 = 0$
Subsquares	$x_1 = x_3 = 0$	Broken rows	$x_2 = x_3 = 0$
Broken columns	$x_1 = x_4 = 0$	Locations	$x_2 = x_4 = 0$

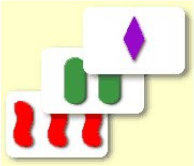
Affine spaces and SET

The card game SET has 81 cards, each of which has four attributes taking three possible values (number of symbols, shape, colour, and shading). A winning combination is a set of three cards on which either the attributes are all the same, or they are all different.

Affine spaces and SET

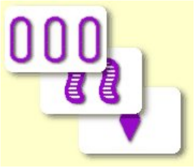
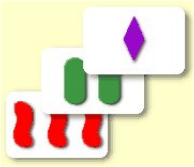
The card game SET has 81 cards, each of which has four attributes taking three possible values (number of symbols, shape, colour, and shading). A winning combination is a set of three cards on which either the attributes are all the same, or they are all different.





Affine spaces and SET

The card game SET has 81 cards, each of which has four attributes taking three possible values (number of symbols, shape, colour, and shading). A winning combination is a set of three cards on which either the attributes are all the same, or they are all different.

Each card has four coordinates taken from F (the integers mod 3), so the set of cards is identified with the 4-dimensional affine space. Then the winning combinations are precisely the affine lines!

Perfect codes

A code is a set C of "words" or n-tuples over a fixed alphabet F. The Hamming distance between two words v, w is the number of coordinates where they differ; that is, the number of errors needed to change the transmitted word v into the received word w.

Perfect codes

A code is a set C of "words" or n-tuples over a fixed alphabet F. The Hamming distance between two words v, w is the number of coordinates where they differ; that is, the number of errors needed to change the transmitted word v into the received word w.

A code C is e-error-correcting if there is *at most* one word at distance e or less from any codeword. [Equivalently, any two codewords have distance at least $2e + 1$.] We say that C is perfect e-error-correcting if "at most" is replaced here by "exactly".

Perfect codes and symmetric Sudoku

- The positions of any symbol in a symmetric Sudoku solution form a perfect code.

Perfect codes and symmetric Sudoku

- The positions of any symbol in a symmetric Sudoku solution form a perfect code.
- So the entire solution is a partition of the affine space into nine perfect codes.

Perfect codes and symmetric Sudoku

- The positions of any symbol in a symmetric Sudoku solution form a perfect code.
- So the entire solution is a partition of the affine space into nine perfect codes.
- Using the SET test, a perfect code is an affine subspace.

Perfect codes and symmetric Sudoku

- The positions of any symbol in a symmetric Sudoku solution form a perfect code.
- So the entire solution is a partition of the affine space into nine perfect codes.
- Using the SET test, a perfect code is an affine subspace.
- So there are only two different symmetric Sudoku solutions.

How hard is a problem?

We measure the complexity of a problem by the smallest number of steps required by the "best possible" solution method.

How hard is a problem?

We measure the complexity of a problem by the smallest number of steps required by the "best possible" solution method.

We imagine that an idealised model of a computer (a Turing machine) is doing the calculation. A Turing machine is a theoretical computer which is

- very simple;

How hard is a problem?

We measure the complexity of a problem by the smallest number of steps required by the "best possible" solution method.

We imagine that an idealised model of a computer (a Turing machine) is doing the calculation. A Turing machine is a theoretical computer which is

- very simple;
- capable of solving any problem that can be solved on any computer yet built or imagined;

How hard is a problem?

We measure the complexity of a problem by the smallest number of steps required by the "best possible" solution method.

We imagine that an idealised model of a computer (a Turing machine) is doing the calculation. A Turing machine is a theoretical computer which is

- very simple;
- capable of solving any problem that can be solved on any computer yet built or imagined;
- not too much slower (in terms of number of computation steps required) than any computer yet built.

How hard is a problem?

We measure the complexity of a problem by the smallest number of steps required by the "best possible" solution method.

We imagine that an idealised model of a computer (a Turing machine) is doing the calculation. A Turing machine is a theoretical computer which is

- very simple;
- capable of solving any problem that can be solved on any computer yet built or imagined;
- not too much slower (in terms of number of computation steps required) than any computer yet built.

The last statement would become false if a quantum computer were to be built.

Complexity measures

We measure the size of a problem by the number of bits of information needed to specify it.

Complexity measures

We measure the size of a problem by the number of bits of information needed to specify it.

A type of problem is polynomial-time, or in the class P, if an n-bit instance can be solved in a number of steps polynomial in n. (Informally these are the problems which can be solved "efficiently".

Complexity measures

We measure the size of a problem by the number of bits of information needed to specify it.

A type of problem is polynomial-time, or in the class P, if an n-bit instance can be solved in a number of steps polynomial in n. (Informally these are the problems which can be solved "efficiently".

A type of problem is non-deterministic polynomial time, or in the class NP, if we can recognise a solution in a polynomial number of steps.

Complexity measures

It is widely believed that the classes P and NP are not equal, since NP contains some well-known hard problems like the travelling salesman problem. The Clay Institute have offered a prize of a million dollars for proof or disproof of $\mathsf{P} = \mathsf{NP}$.

Complexity measures

It is widely believed that the classes P and NP are not equal, since NP contains some well-known hard problems like the travelling salesman problem. The Clay Institute have offered a prize of a million dollars for proof or disproof of P $=$ NP.

According to Cook's Theorem, there is a class of problems called NP-complete, which are the "hardest" problems in NP; if one of them could be solved in polynomial time, then all could.

Complexity measures

It is widely believed that the classes P and NP are not equal, since NP contains some well-known hard problems like the travelling salesman problem. The Clay Institute have offered a prize of a million dollars for proof or disproof of $\mathsf{P} = \mathsf{NP}$.

According to Cook's Theorem, there is a class of problems called NP-complete, which are the "hardest" problems in NP; if one of them could be solved in polynomial time, then all could.

In other words, if a problem is NP-complete, then no known algorithm solves it efficiently, and we suspect that no efficient solution can exist.

Example

Given a graph G,

- the problem of walking round the graph so that every edge is traversed exactly once is in P (this is Euler's bridges of Königsburg in disguise);

Example

Given a graph G,

- the problem of walking round the graph so that every edge is traversed exactly once is in P (this is Euler's bridges of Königsburg in disguise);
- the problem of walking round the graph so that each vertex is visited exactly once is NP-complete (this is Hamilton's Icosian game).

What about Sudoku?

Sudoku seems to be hard:

What about Sudoku?

Sudoku seems to be hard:

- Deciding whether a partly filled $n^2 \times n^2$ Sudoku grid can be completed is an NP-complete problem;

What about Sudoku?

Sudoku seems to be hard:

- Deciding whether a partly filled $n^2 \times n^2$ Sudoku grid can be completed is an NP-complete problem;
- Deciding whether an empty gerechte grid can be filled is an NP-complete problem.

What about Sudoku?

Sudoku seems to be hard:

- Deciding whether a partly filled $n^2 \times n^2$ Sudoku grid can be completed is an NP-complete problem;
- Deciding whether an empty gerechte grid can be filled is an NP-complete problem.

Several problems remain, for example:

- What about empty gerechte grids where the regions are contiguous?

What about Sudoku?

Sudoku seems to be hard:

- Deciding whether a partly filled $n^2 \times n^2$ Sudoku grid can be completed is an NP-complete problem;
- Deciding whether an empty gerechte grid can be filled is an NP-complete problem.

Several problems remain, for example:

- What about empty gerechte grids where the regions are contiguous?
- Is there a test for completability short of actually trying to do it?

What about Sudoku?

Sudoku seems to be hard:

- Deciding whether a partly filled $n^2 \times n^2$ Sudoku grid can be completed is an NP-complete problem;
- Deciding whether an empty gerechte grid can be filled is an NP-complete problem.

Several problems remain, for example:

- What about empty gerechte grids where the regions are contiguous?
- Is there a test for completability short of actually trying to do it?
- What about finding an orthogonal mate to a Latin square (one which extends it to a Graeco-Latin square)?