# Finite arithmetic and Latin squares

Robin McLean

27th January 2018

Can you imagine a world in which there are only a finite number of numbers?... not simply a world with only a finite number of numerals or number symbols

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

but only a finite number of actual numbers.
Is that impossible?

My first mathematical experience was that numbers go on for ever.
Can you prove this?

I claim that we can do arithmetic $(+, -, \times, \div)$ with only a finite number of numbers. Let's start with counting and addition:

$0$

$1$

$1 + 1$

$1 + 1 + 1$

$1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$

$1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1$

. . .

This is an infinite list. Ordinary numbers go on for ever because

(1) we can continue to add 1's, and

(2) when we do this, our numbers get bigger and bigger, so that there are no repetitions in the list.

If we have only a finite number of numbers, there must be repetitions.

Let's invent a system with exactly ten numbers

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

If arithmetic makes sense, then $9 + 1$ must be one of our ten numbers. I claim that $9 + 1 = 0$, for if the answer were some non-zero number, say $9 + 1 = 4$, we could subtract 4 from both sides, giving $5 + 1 = 0$. So $6 = 0$, contradicting the fact that we started with ten distinct numbers. Thus

$$9 + 1 = 0.$$

Now, in ordinary arithmetic, tell me a pair of numbers that add up to zero . . . another pair . . . This suggests that we have negative numbers in our new arithmetic and that -1 $=$ 9 and -9 $=$ 1. Which of our original ten numbers do you think -2 is? Which is -3? . . . Can anyone suggest the answer to $6 + 7$? . . . $3 + 8$? . . . 9 - 3? . . . 3 - 9?

## Arithmetic mod 10

The number system we have invented is *arithmetic modulo 10*, often abbreviated to *arithmetic mod 10*. You have been familiar with it for a long time, for you have used it whenever you have done sums such as

$$\begin{array}{r} 537 \\ +\ 468 \end{array} \qquad\qquad \begin{array}{r} 746 \\ -\ 359 \end{array}$$

In working out what to put in the units column, you were actually doing 7 + 8 and 6 - 9 in arithmetic modulo 10. No doubt you *thought* 7 + 8 = 15 in the first sum and 16 - 9 in the second one, but in arithmetic mod 10, 10 = 0, so we can momentarily forget 10 in the first sum and introduce it to help in the second sum. How do you think we do multiplication in this arithmetic?

. . . What about division?

# Multiplication mod 10

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 2 | 0 | 2 | 4 | 6 | 8 | 0 | 2 | 4 | 6 | 8 |
| 3 | 0 | 3 | 6 | 9 | 2 | 5 | 8 | 1 | 4 | 7 |
| 4 | 0 | 4 | 8 | 2 | 6 | 0 | 4 | 8 | 2 | 6 |
| 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 | 0 | 5 |
| 6 | 0 | 6 | 2 | 8 | 4 | 0 | 6 | 2 | 8 | 4 |
| 7 | 0 | 7 | 4 | 1 | 8 | 5 | 2 | 9 | 6 | 3 |
| 8 | 0 | 8 | 6 | 4 | 2 | 0 | 8 | 6 | 4 | 2 |
| 9 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Here every number is a multiple of 7, so we can always divide by 7.

What numbers can we always divide by?

What numbers can we not always divide by?

## Arithmetic mod $m$

For each integer $m \geq 2$, there is a system of arithmetic mod $m$. For certain values of $m$, division is possible by every number (except 0). I would like to find these values of $m$, for the corresponding number systems are particularly pleasant and useful.

What values of $m$ have this pleasant property? Think about this now.

Let $n$ be an integer, in the range $0 < n < m$, whose multiples (mod $m$) are not all different. Then there are integers $x, y$ such that

$$\begin{gathered} 0 \leq y < x < m \\ \text{and} \quad nx \equiv ny \pmod{m} \\ \text{So} \quad n(x-y) \equiv 0 \pmod{m} \text{ and } 0 < x-y < m. \end{gathered}$$

There must be a smallest integer $s$ such that

$$ns \equiv 0 \pmod{m} \text{ and } 0 < s < m. \tag{1}$$

Moreover, $s \neq 1$, for $n$ (which is less than $m$) cannot be divisible by $m$. So $1 < s < m$. Let $q$ be the quotient and $r$ the remainder when $m$ is divided by $s$. Then $m = qs + r$ and $0 \leq r < s$. Thus $qs + r \equiv 0 \pmod{m}$. Multiplying by $n$ and using (1) gives $nr \equiv 0 \pmod{m}$. Now $r$ cannot be positive (by our definition of $s$), so $r = 0$ and $m = qs$, which is not prime. Obviously, if $m$ is not prime, there is a number whose multiples are not all different. Hence division in arithmetic mod $m$ by every number ($\neq 0$) is possible if and only if $m$ is prime.

## Fields

When *p* is any prime number, all four operations (+, -, × and ÷) are always possible (except division by zero) *within* the system of arithmetic mod *p*. Such a system of numbers is called a *field*. The integers (+ve & -ve) do not form a field because, although +, - and × can always be done, division is not always possible (e.g. $2 \div 3$ is not an integer). We have to extend the integers to include all +ve and -ve fractions in order to get a field, You are already familiar with this field, called the field of rational numbers, and the much larger field of real numbers (corresponding to points on a number line) that includes such numbers as $\sqrt{2}$ and $\pi$.

# Addition and multiplication tables in arithmetic mod 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 | 2 | 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 |

Note that $2^2 = 3^2 = 4 = -1$ in this arithmetic, so -1 has two square roots.

3 has no square root in this field of 5 numbers. If we wish, we can add $\sqrt{3}$ to this field and construct a field of 25 numbers:

| | | | | |
|---|---|---|---|---|
| $0$ | $\sqrt{3}$ | $2\sqrt{3}$ | $3\sqrt{3}$ | $4\sqrt{3}$ |
| $1$ | $1+\sqrt{3}$ | $1+2\sqrt{3}$ | $1+3\sqrt{3}$ | $1+4\sqrt{3}$ |
| $2$ | $2+\sqrt{3}$ | $2+2\sqrt{3}$ | $2+3\sqrt{3}$ | $2+4\sqrt{3}$ |
| $3$ | $3+\sqrt{3}$ | $3+2\sqrt{3}$ | $3+3\sqrt{3}$ | $3+4\sqrt{3}$ |
| $4$ | $4+\sqrt{3}$ | $4+2\sqrt{3}$ | $4+3\sqrt{3}$ | $4+4\sqrt{3}$ |

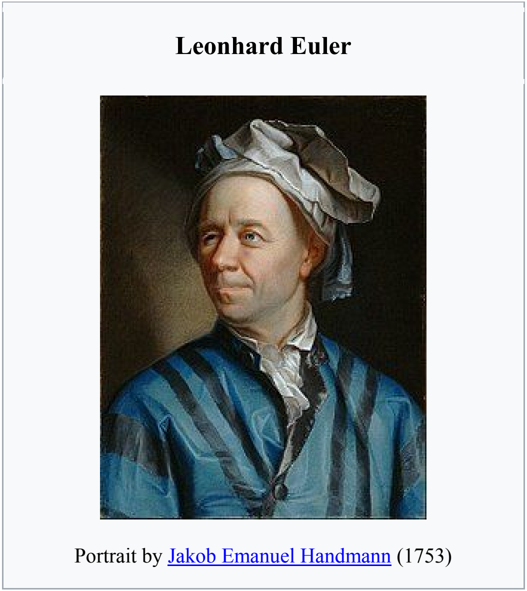
## Finite fields

It can be shown that here is a finite field with exactly $n$ numbers if and only if $n$ is a power of a prime (e.g. $n = 5^2$). For each such value of $n$ there is essentially one field with this number of elements. These fields are often called *Galois fields* after a young French mathematician Évariste Galois (1811-1832) who was killed in a duel.

### Problem (1725)

Take all the Aces, Kings, Queens and Jacks from a pack of cards. Can you arrange them in a $4 \times 4$ array so that no suit occurs twice in any row or column and, similarly, that no single kind of a card, such as Kings, occurs twice in any row or column?

# Leonhard Euler (1707 - 1783)

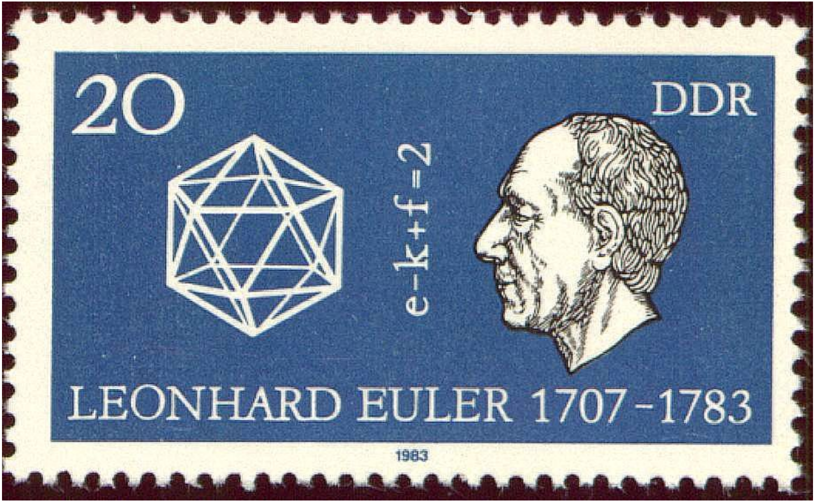


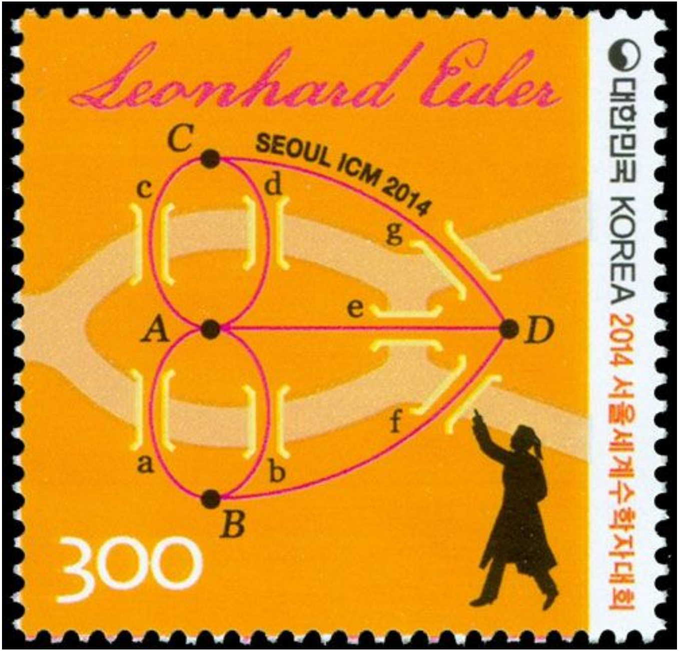
**Leonhard Euler**

Portrait by Jakob Emanuel Handmann (1753)

## Some of Euler's mathematics

Euler could calculate “just as men breathe, as eagles sustain themselves in the air”.
The seven bridges of Königsberg.
Polyhedra: $V - E + F = 2$.
The most beautiful formula in mathematics: $e^{i\pi} + 1 = 0$.
Latin squares . . .


20
DDR
e-k+f=2
LEONHARD EULER 1707-1783
1983


Leonhard Euler
SEOUL ICM 2014
C
c
d
g
e
A
D
f
a
b
B
300
대한민국 KOREA
2014 서울세계수학자대회

## Euler's problem (1779)

36 officers of 6 different ranks and taken from 6 different regiments, one of each rank in each regiment, are to be arranged, if possible, in a solid $6 \times 6$ formation, so that each row and each column contains one and only one officer of each rank and one and only one officer from each regiment.

## Latin squares

An $n \times n$ array of $n$ symbols is called a *Latin square* if each symbol appears exactly once in each row and exactly once in each column. For example

$$\begin{array}{ccc} A & B & C \\ B & C & A \\ C & A & B \end{array}$$

is a Latin square (Euler's name, because he used the Latin alphabet). He was particularly interested in what he called Graeco-Latin squares. Here is an example:

$$\begin{array}{ccc} A\alpha & B\beta & C\gamma \\ B\gamma & C\alpha & A\beta \\ C\beta & A\gamma & B\alpha \end{array}$$

Here the Greek letters also form a Latin square, so we have two Latin squares superimposed.

Latin squares turn up in some surprising contexts.

1960 ROMA OLİMPİYATLARI
TÜRKİYE CUMHURİYETİ POSTALARI
30
KURUŞ
1960 ROMA
IMPRESSION COURVOISIER S.A. LA CHAUX-DE-FONDS (SUISSE)

32 USA
1893 Duryea
1898 Columbia
1901 White
1894 Haynes
1899 Winton
S1111
PLATE POSITION

Bridges | Ponts
Bridges | Ponts
Canada
50
Bridges | Ponts
Bridges | Ponts

# Orthogonal Latin squares

Look again at our example of one of Euler's Graeco-Latin squares:

$$\begin{array}{ccc} A\alpha & B\beta & C\gamma \\ B\gamma & C\alpha & A\beta \\ C\beta & A\gamma & B\alpha \end{array}$$

Here the Greek letters also form a Latin square, so we have two Latin squares superimposed. They are superimposed in a particularly neat way, because each combination of a Latin letter and a Greek letter occurs exactly one. When this happens, the two Latin squares are said to be *orthogonal*. The squares need not actually be superimposed to be orthogonal. They might be shown separately:

$$\begin{array}{ccc} A & B & C \\ B & C & A \\ C & A & B \end{array} \qquad \begin{array}{ccc} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{array}$$

## A Latin square in the design of a French experiment in 1788

Cretté de Palluel did an experiment on feeding 4 types of food to 4 different breeds of sheep for 4 different lengths of time. He took 4 sheep of each breed and fed them for the number of months shown in the table, weighing each sheep before and after the experiment.

| | potatoes | turnips | beets | corn |
|---|---|---|---|---|
| Ile de France | 1 | 2 | 3 | 4 |
| Beauce | 4 | 1 | 2 | 3 |
| Champagne | 3 | 4 | 1 | 2 |
| Picardy | 2 | 3 | 4 | 1 |

Even though only 16 sheep were used, not 64, the experiment could have tested duration of feed against diet or duration of feed against breed in addition to how it was used - for diet against breeds.

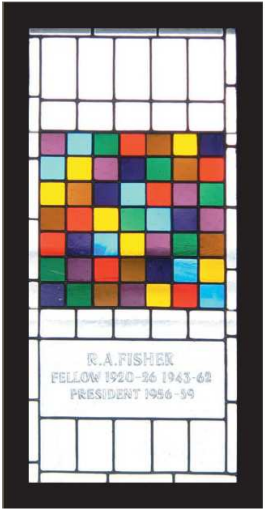


Figure: The memorial window to R.A.Fisher in the hall of Gonville and Caius College, Cambridge, UK. The Latin square of colours appeared on the dustcover of Fisher's book "The design of experiments". This photograph by Derek Ingram is reproduced by kind permission of his executors.

## How orthogonal squares are used in experiments

Suppose we wished to compare the yields from 4 different varieties of wheat (A, B, C, D) when they are treated with 4 different types of fertilizer $(\alpha, \beta, \gamma, \delta)$. We could divide a field into an array of $4 \times 4 = 16$ plots. and plant it according to the square:

$$\begin{array}{cccc} A\alpha & B\beta & C\gamma & D\delta \\ D\gamma & C\delta & B\alpha & A\beta \\ B\delta & A\gamma & D\beta & C\alpha \\ C\beta & D\alpha & A\delta & B\gamma \end{array}$$

We could even bring include a third variable and compare 4 types of insecticide (0, 1, 2, 3), using them on the plots as shown

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{array}$$

## How to construct mutually orthogonal $n \times n$ Latin squares (when $n$ is a power of a prime)

In this case there is a finite field with exactly $n$ numbers. We can construct $n - 1$ mutually orthogonal squares as follows. Here we take $n = 5$ and construct 4 squares. Start with the multiplication table for arithmetic mod 5.

| × | 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 |

Take each of its last 4 columns as the first column of one of our orthogonal squares. Keep the first row as 0, 1, 2, 3, 4 in each case. At this stage we have numbers in each first row and in each first column.

| 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |

| 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 2 | | | | |
| 4 | | | | |
| 1 | | | | |
| 3 | | | | |

| 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 3 | | | | |
| 1 | | | | |
| 4 | | | | |
| 2 | | | | |

| 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 4 | | | | |
| 3 | | | | |
| 2 | | | | |
| 1 | | | | |

To complete each square we add border numbers mod 5.

|  |  |  |  |  |
|---|---|---|---|---|
| 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 |

|  |  |  |  |  |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 2 | 3 | 4 | 0 | 1 |
| 4 | 0 | 1 | 2 | 3 |
| 1 | 2 | 3 | 4 | 0 |
| 3 | 4 | 0 | 1 | 2 |

|  |  |  |  |  |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 3 | 4 | 0 | 1 | 2 |
| 1 | 2 | 3 | 4 | 0 |
| 4 | 0 | 1 | 2 | 3 |
| 2 | 3 | 4 | 0 | 1 |

|  |  |  |  |  |
|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 |
| 4 | 0 | 1 | 2 | 3 |
| 3 | 4 | 0 | 1 | 2 |
| 2 | 3 | 4 | 0 | 1 |
| 1 | 2 | 3 | 4 | 0 |

## Why each square is Latin

As an example, take our third square. It is

$$\begin{array}{ccccc}
3\times 0 & 3\times 0+1 & 3\times 0+2 & 3\times 0+3 & 3\times 0+4 \\
3\times 1 & 3\times 1+1 & 3\times 1+2 & 3\times 1+3 & 3\times 1+4 \\
3\times 2 & 3\times 2+1 & 3\times 2+2 & 3\times 2+3 & 3\times 2+4 \\
3\times 3 & 3\times 3+1 & 3\times 3+2 & 3\times 3+3 & 3\times 4+4 \\
3\times 4 & 3\times 4+1 & 3\times 4+2 & 3\times 4+3 & 3\times 4+4
\end{array}$$

The numbers in each row are different. (Remember we are working mod 5.) The numbers in the 3 times table are all different because arithmetic mod 5 is a field, so the numbers in each column are different. Hence there is one copy of each number in each row and in each column, so our number square is Latin.

## Why, for example, the 1st and 4th Latin squares are orthogonal

Suppose that the same pair of numbers (one from the 1st square, one from the 4th) occur together in position (row $r_1$, column $c_1$) and in (row $r_2$, column $c_2$) when the squares are superimposed. Then

$$\begin{array}{rrcl} & 1 \times r_1 + c_1 & = & 1 \times r_2 + c_2 \\ \text{and} & 4 \times r_1 + c_1 & = & 4 \times r_2 + c_2 \\ \text{Subtracting,} & (4-1)r_1 & = & (4-1)r_2 \end{array}$$

Now arithmetic mod 5 is a field in which $4 - 1 \neq 0$, so we can divide by 4 - 1, getting $r_1 = r_2$. Substituting in an earlier equation, $c_1 = c_2$. Hence the 1st and 4th Latin squares are orthogonal. Similarly every pair of these 4 squares are orthogonal.

## What is known

For each integer $n \geq 2$, there are no more than $n - 1$ mutually orthogonal Latin squares.

When $n$ is a power of a prime number, there is a finite field of $n$ numbers and a set of $n - 1$ orthogonal squares can be constructed.

When $n = 6$, there is no pair of orthogonal squares. (Euler's officers problem.)

For each $n \neq 6$, there is at least one pair of orthogonal Latin squares.

## What is not known

How many pairs of orthogonal Latin squares are there when $n$ is not a power of a prime number?