# **Modular arithmetic**

#### **Secondary Mathematics Masterclass**

**Gustavo Lau** 

#### Introduction

#### On what day were you born?

Worksheet 1 Going round in circles



#### How to represent time?







Instead of 13 = 1, in modular arithmetic we write  $13 \equiv 1 \pmod{12}$  and read it "13 is congruent to 1 modulo 12" or, to abbreviate, "13 is 1 modulo 12". Examples:  $12 \equiv 0 \pmod{12}$   $17 \equiv 5 \pmod{12}$  $37 \equiv 1 \pmod{12}$   $-1 \equiv 11 \pmod{12}$ In general,  $a \equiv b \pmod{n}$  if a-b is a multiple of n. Equivalently,  $a \equiv b \pmod{n}$  if a and b have the same remainder when divided by n (remainder modulo n).

## **Clock addition table**

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12



In modular arithmetic we use the numbers 0-11 instead of the numbers 1-12. The reason is that 0-11 are the remainders modulo 12.

In general, when we work modulo n we replace all the numbers by their remainders modulo n.

#### Modulo 12 addition table

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

#### Examples:

7 + 8 ≡ 3 (mod 12) 13 + 2 ≡ 3 (mod 12)  $10 + 2 \equiv 0 \pmod{12}$ -1 + 14  $\equiv$  1 (mod 12)

Can we use arithmetic modulo 12 to represent something else?





We can use 0 to represent Day and 1 to represent Night

# Clock with just two numbers





# Modulo 2 1 0 1 0

- 0 and 1 are the remainders modulo 2
- 0 represents the even numbers: 0, 2, 4, 6,...
- 1 represents the odd numbers: 1, 3, 5, 7,...

Algebraically? 2n, any integer n 2n+1, any integer n

Examples:

 $4 \equiv 0 \pmod{2}$  $-6 \equiv 0 \pmod{2}$  $13 \equiv 1 \pmod{2}$  $-1 \equiv 1 \pmod{2}$ 

#### Modulo 2 addition table



+	0	1
0	0	1
1	1	0

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

**Examples:** 

 $0 + 1 \equiv 1 \pmod{2}$  $13 + 2 \equiv 1 \pmod{2}$   $1 + 1 \equiv 0 \pmod{2}$ -1 + 14  $\equiv 1 \pmod{2}$ 

#### Modulo 2 multiplication table



X	0	1
0	0	0
1	0	1

x	Even	Odd
Even	Even	Even
Odd	Even	Odd

Examples:  $0 \ge 1 \equiv 0 \pmod{2}$  $13 \ge 3 \equiv 1 \pmod{2}$ 

 $1 \ge 1 \equiv 1 \pmod{2}$ -1 x 14  $\equiv 0 \pmod{2}$ 





- 0 represents Flood Time
- 1 represents Planting Time
- 2 represents Harvest Time



+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

- 0, 1 and 2 are the remainders modulo 3
- 0 represents the multiples of 3: 0, 3, 6,...
- 1 represents the (multiples of 3) + 1: 1, 4, 7,...
- 2 represents the (multiples of 3) + 2: 2, 5, 8,... 3n+2, any integer n Examples:

 $3 \equiv 0 \pmod{3}$   $-2 \equiv 1 \pmod{3}$   $13 \equiv 1 \pmod{3}$  $2 + 2 \equiv 1 \pmod{3}$   $-1 + 8 \equiv 1 \pmod{3}$   $-2 + 7 \equiv 2 \pmod{3}$ 

Algebraically? 3n, any integer n 3n+1, any integer n 3n+2 any integer n

#### Modulo 3 multiplication table

#### Blackboard

#### Modulo 3 multiplication table

X	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

#### Remainders

Working modulo n is like wearing special glasses that convert each number into its remainder modulo n. For example, to compute the following sum modulo 12 (to find the remainder modulo 12): 19 + 23 + 15 First replace each number by its remainder mod 12:

7 + 11 + 3

then do the sum: 21

and replace the sum by its remainder modulo 12:9

#### Remainders

If today is Sunday, what day will it be in 1000 days? We need to find the remainder of 1000 when divided by 7.

As we don't need the quotient we don't need to do the division. We look for multiples of 7 lower than 1000:

1000 = 700 + 300 = 700 + 280 + 20 = 700 + 280 + 14 + 6

In 6 days, and in 1000 days, it will be Saturday.

# Worksheet 2 Remainders and congruences

#### **Remember:**

- $a \equiv b \pmod{n}$  if a-b is a multiple of n. Equivalently,
- a ≡ b (mod n) if a and b have the same remainder modulo n.

When we work modulo n we replace all the numbers by their remainders modulo n: 0, 1, 2, ..., n-1.

What can we represent with modulo 4?





- 0 represents Spring
- 1 represents Summer
- 2 represents Autumn
- 3 represents Winter

# Worksheet 3 Addition and multiplication tables

Remember:

When we work modulo n we replace all the numbers by their remainders modulo n: 0, 1, 2, ..., n-1

#### Modulo 4 addition table



+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- 0 denotes 4n: 0, 4, 8, 12,...
- 2 denotes 4n+2: 2, 6, 10, 14,...
  3 denotes:

 $4 \equiv 0 \pmod{4} \quad -2 \equiv 2 \pmod{4} \quad 13 \equiv 1 \pmod{4} \\ 3 + 2 \equiv 1 \pmod{4} \quad -1 + 8 \equiv 3 \pmod{4} \quad -2 + 7 \equiv 1 \pmod{4}$ 

• 1 denotes 4n+1: 1, 5, 9, 13,...

• 3 denotes 4n+3: 3, 7, 11, 15,...

#### Modulo 4 multiplication table



x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

• 1 denotes 4n+1: 1, 5, 9, 13,...

- 0 denotes 4n: 0, 4, 8, 12,...
- 2 denotes 4n+2: 2, 6, 10, 14,...
  3 denotes 4n+3: 3, 7, 11, 15,...
  Examples:

 $4 \equiv 0 \pmod{4}$  $-2 \equiv 2 \pmod{4}$  $13 \equiv 1 \pmod{4}$  $2 \times 2 \equiv 0 \pmod{4}$  $3 \times 2 \equiv 2 \pmod{4}$  $3 \times 3 \equiv 1 \pmod{4}$ 

#### Last digit arithmetic

What is the last digit of 285714 + 571428?

- It is enough to look at the last digits: 4 + 8 = 12
- Then look at the last digit of their sum: 2

*What is the last digit of 142857 x 34745?* 

- It is enough to look at the last digits: 7 x 5 = 35
- Now look at the last digit of their product: 5

How is this related to modular arithmetic?

French Revolution clock



- 0 denotes 10n: 0, 10, 20, 30,... 1 denotes 10n+1: 1, 11, 21, 31,...
- 2 denotes 10n+2: 2, 12, 22, 32,... •
- 4 denotes 10n+4: 4, 14, 24, 34,... •
- 6 denotes 10n+6: 6, 16, 26, 36,... •
- 3 denotes 10n+3: 3, 13, 23, 33,...
  - 5 denotes 10n+5: 5, 15, 25, 35,...
  - 7 denotes 10n+7: 7, 17, 27, 37,...
- 8 denotes 10n+8: 8, 18, 28, 38,...
  9 denotes 10n+9: 9, 19, 29, 39,...
  In general: N ≡ last digit of N (mod 10)

#### Modulo 10 addition table

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Examples:

 $7 + 4 \equiv 1 \pmod{10}$   $19 + 28 \equiv 7 \pmod{10}$   $-2 + 6 \equiv 4 \pmod{10}$ 

#### Modulo 10 multiplication table

x	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

Examples:

 $7 \times 4 \equiv 8 \pmod{10}$   $19 \times 28 \equiv 2 \pmod{10}$   $-2 \times 6 \equiv 8 \pmod{10}$ 

We know that  $10 \equiv 1 \pmod{9}$ Then  $10^2 \equiv 1 \pmod{9}$ ,  $10^3 \equiv 1 \pmod{9}$ , etc. In general:  $10^n \equiv 1 \pmod{9}$  for any n Take any number, say 8794, then we have:  $8794 = 8 \times 1000 + 7 \times 100 + 9 \times 10 + 4$  $\equiv 8 + 7 + 9 + 4 \pmod{9}$ 

In general we have:
 N ≡ sum of digits of N (mod 9)

• In particular, N is divisible by 9 if and only if the sum of its digits is divisible by 9.

 Given that 10 ≡ 1 (mod 3) the same argument proves that N ≡ sum of digits of N (mod 3).

```
We know that
```

 $10 \equiv -1 \pmod{11}$ Then  $10^2 \equiv 1 \pmod{11}$ ,  $10^3 \equiv -1 \pmod{11}$ , etc. In general:  $10^n \equiv 1 \pmod{11}$  if n is even  $10^n \equiv -1 \pmod{11}$  if n is odd Take any number, say 38,794, then we have: 38,794 = 3x10,000 + 8x1,000 + 7x100 + 9x10 + 4 $\equiv 3 - 8 + 7 - 9 + 4 \pmod{11}$ 

• In general we have:

 $N \equiv$  alternate sum of digits of N (mod 11)

 In particular, N is divisible by 11 if and only if the alternate sum of its digits is divisible by 11. Start from the right making the units digit positive. Worksheet 4 Divisibility

Remember:

- N is divisible by 9 if and only if the sum of its digits is divisible by 9.
- N is divisible by 3 if and only if the sum of its digits is divisible by 3.
- N is divisible by 11 if and only if the alternate sum of its digits is divisible by 11. Start from the right making the units digit positive.

#### Powers




#### Powers

What is the last digit of:

a) 
$$4^{13}$$
 ... $4^{5}$ ,  $4^{3}$ ,  $4^{1}$  4  $6^{1}$  6  $4^{2}$ ,  $4^{4}$ ,  $4^{6}$ ...

b) 
$$9^{58}$$
 ...9<sup>5</sup>,  $9^3$ ,  $9^1$  9 1  $9^2$ ,  $9^4$ ,  $9^6$ ...

#### Powers

What is the last digit of:



# Worksheet 5 Powers









x	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

Which of the following are square numbers? 6312, 4553, 9538 Where are the square numbers in the table?

x	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

Which of the following are square numbers? 6312, 4553, 9538 Where are the square numbers in the table?



Where are the square numbers in the table? Why this symmetry?



Where are the square numbers in the table? Why this symmetry?  $1^2=(-1)^2$ 



Where are the square numbers in the table? Why this symmetry?  $1^2=(-1)^2$ ,  $2^2=(-2)^2$ 



Where are the square numbers in the table? Why this symmetry?  $1^2=(-1)^2$ ,  $2^2=(-2)^2$ ,  $3^2=(-3)^2$ 



Where are the square numbers in the table? Why this symmetry?  $1^2=(-1)^2$ ,  $2^2=(-2)^2$ ,  $3^2=(-3)^2$ ,  $4^2=(-4)^2$ 

### Abstraction

#### What is abstraction?



# Abstraction





#### Abstraction Modulo n



In general,  $a \equiv b \pmod{n}$  if a-b is a multiple of n.





#### Modulo 4



Modulo 10



#### Abstraction

What is Mathematics about?

Mathematics is not only about numbers and figures, it is also about patterns, generalizations and abstractions.

<u>http://en.wikipedia.org/wiki/Mathematics</u>: Mathematics is the abstract study of topics such as quantity (numbers), structure, space, and change.



This is an example from Pure Mathematics.

#### Abstraction



Sometimes more abstract is more useful.

#### Abstraction



#### Abstraction helps Unification Modulo n



Gauss, Disquisitiones Arithmeticae, 1801





#### Modulo 2

+	Even	Odd
Even	Even	Odd
Odd	Odd	Even

Modulo 10

Last digit arithmetic

# **Unification in Physics**

Newton's Principia, 1687

Terrestrial Mechanics (Galileo) Celestial Mechanics (Kepler)

Thought experiment: Do you know how to see that the Moon is falling just like an apple?

# **Unification in Physics**

#### Maxwell's Electromagnetism, 1865





# **Unification in Physics** Quantum Mechanics **Einstein's General Relativity**



Concepts are important, e.g. chess, programming.

On which day of the week were you born?

What modulo are we going to use?

# Modulo 7





- 2 represents Tuesday
- 4 represents Thursday
- 6 represents Saturday



- 1 represents Monday
- 3 represents Wednesday
- 5 represents Friday

# Modulo 7





- 0 denotes 7n: 0, 7, 14, 21,...
- 2 denotes 7n+2: 2, 9, 16, 23,...
- 4 denotes 7n+4: 4, 11, 18, 25,...
- 6 denotes 7n+6: 6, 13, 20, 27,...

- 1 denotes 7n+1: 1, 8, 15, 22,...
- 3 denotes 7n+3: 3, 10, 17, 24,...
- 5 denotes 7n+5: 5, 12, 19, 26,...

#### Modulo 7 addition table

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Examples:

 $1 + 4 \equiv 5 \pmod{7} \qquad 2 + 5 \equiv 0 \pmod{7} \qquad 6 + 2 \equiv 1 \pmod{7}$ Monday + 4 = Friday Tuesday + 5 = Sunday Sat + 2 = Monday

# Day of the week

 One way to determine the day of the week of a given date is to assign codes to the years, months and dates such that:

Day of the week  $\equiv$  year code

+ month code

+ date (mod 7)

# Day of the week

 For simplicity let's choose 1 as the code of the year 2001. We start by noticing that 1/January/2001 was a Monday, so we need:  $1 \equiv 1 + \text{January code} + 1 \pmod{7}$ Then, what is the January code?  $0 \equiv January code + 1 \pmod{7}$ January code  $\equiv$  -1 (mod 7)

January code  $\equiv 6 \pmod{7}$ 

This is the January code for non-leap years.

How do we find the February code? February code ≡ January code + number of days in January (mod 7) February code  $\equiv 6 + 31 \pmod{7}$ February code  $\equiv$  37 (mod 7) February code  $\equiv 2 \pmod{7}$ This is the February code for non-leap years. Please now compute the March to December codes for a non-leap year.

In general, to find the month codes we list the number of days in each month in a non-leap year: Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 31 28 31 30 31 30 31 31 30 31 30 31 Look at them modulo 7:



#### *How to remember the month codes?*

Month	Number	Mnemonic		
January	6	WINTER has 6 letters		
February	2	February is the 2 <sup>nd</sup> month		
March	2	March 2 the beat.		
April	5	APRIL has 5 letters		
Мау	0	MAY-0		
June	3	Jun (Jun has 3 letters)		
July	5	The SHARD (5) opened on July 5		
August	1	August begins with A, the 1 <sup>st</sup> letter		
September	4	First TERM (4 letters) at school		
October	6	SIX or treat!		
November	2	11 <sup>th</sup> month (11 => II or 1+1=2)		
December	4	LAST (or XMAS) has 4 letters		

*How to remember the month codes?* 

#### Remember this number: 622-503-514-624

Or one of these tables:

May C	_					_
Aug 1	2	Mar	2	Feb	6	Jan
Feb, Mar, Nov 2	3	Jun	0	May	5	Apr
Jun 3	4	Sep	1	Aug	5	Jul
Sep, Dec 4	Λ	Dec	2	Nov	6	Oct
Apr, Jul 5	-	Dec	۷		0	OCI

Jan, Oct 6

Exception: in a leap year the January code is 5 and the February code is 1.

Remember that leap years (almost always) are the years that are multiples of 4.

#### Year codes

If your birthday fell on a Sunday this year, what day will it fall on next year? How do we find the 2002 code?  $2002 \text{ code} \equiv 2001 \text{ code}$ + number of days in 2002 (mod 7)  $2002 \text{ code} \equiv 1 + 365 \pmod{7}$  $2002 \text{ code} \equiv 1 + 1 \pmod{7}$  $2002 \text{ code} \equiv 2 \pmod{7}$ 

#### Year codes

In general, to find the year codes we list the number of days in each year: 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 365 365 365 366 365 365 365 366 365 365 Look at them modulo 7:



Please now find the 2011-14 codes.

#### Year codes

What about the 20<sup>th</sup> century?

- The codes are like the 21<sup>st</sup> century except that we need to add 1 to the year code. E. g. given that 2001 has code 1, 1901 has code 2.
- We can also deduce codes for previous years: 1995 1996 1997 1998 1999 2000 2001 365 366 365 365 365 366 365  $1 \ 2 \ 1 \ 1 \ 1 \ 2 \ 1 \ 0 \ 2 \ 3 \ 4 \ 5 \ 0 \ 1$
### Year codes

- It helps to remember the years with code 0:
- 1905 Albert Einstein's annus mirabilis
- 1911, 22, 33, 44 First four multiples of 11
- 1916 4<sup>2</sup>
- 1939 World War II started
- 1950 Brazil '50 World Cup (<u>Maracanazo</u>)
  - 1961Berlin Wall started
    - The year after 1966!
  - 1972Munich '72 Olympics
    - Argentina '78 World Cup
      - Berlin Wall ended
    - Netscape IPO (Internet boom started)

• 1995

1967

1978

1989

 $\bullet$ 

### Year codes

How do we find the 1971 code?

Remember that 1967, the year after England won the World Cup, has code 0.

1971 code ≡ 71-67 + number of leap years in 1968-1971 (mod 7)

1971 code  $\equiv 4 + 1 \pmod{7}$ 1971 code  $\equiv 5 \pmod{7}$ 

### Year codes

 It also helps is to remember years with code equal to its last digit: 1964-1966

2000-2003

- Year codes in Excel
- Examples thinking aloud

# Worksheet 6 Day of the week

Find the day of the week in which a classmate was born.

Remember: Day of the week ≡ year code + month code + date (mod 7)

# 60 points going around a circle

- Imagine 60 points going around in concentric circles clockwise and starting at 3pm.
- The first, and outermost, point goes around at 1 rpm, the second at 2 rpm and so on until the 60<sup>th</sup> which goes around at 60 rpm.
- Where will they be after a minute?
- Where will they be after 1/2 minute?
- Where will they be after 1/3 minute?
- Where will they be after 1/4 minute?

## 60 points going around a circle

http://whitneymusicbox.org/whitneyMinute.swf

### Pendulum waves

- Something similar can be done with pendulums.
- Each successive shorter pendulum is adjusted so that it executes one additional oscillation in a 1 minute period.
- Video taken from <u>http://www.youtube.com/watch?v=yVkdfJ9PkRQ</u>