University Undergraduate Lectures in Mathematics
A First Year Course

GROUP THEORY

The Mathematics of Symmetry

G R O U P T H E O R Y I

Lecture 1

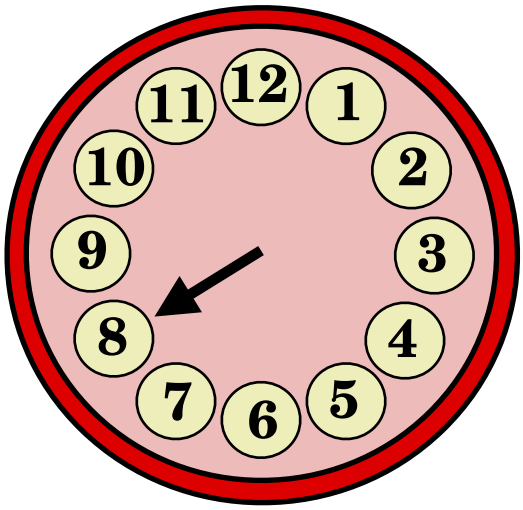
University Undergraduate Lectures in Mathematics
A First Year Course
Group Theory I

1.1 Introduction

Welcome to the world of Group Theory.
In this series of lectures, the underlying theme is “symmetry”, a familiar idea from schoolwork where, for example, reflections and rotations of simple shapes are studied. However, other mathematical entities can have “symmetry”.
For example, a carefully chosen set of numbers or functions.
To tease out the underlying symmetry of such seemingly different entities, mathematics uses a powerful tool; Group Theory.
These lectures are suitable for new undergraduate students, for they assume only competence with GCSE mathematics. A second set of Lectures, Group Theory II, is for study towards the end of a first year at University.

1.2 Clock Arithmetic

Imagine an analogue clock that works fine, but has lost its minute hand.
It reads 8 O'clock.
Exactly five hours later, it will read 1 O'clock.



It would be confusing to write the following statement as a description of the situation just considered;

$$8 + 5 = 1$$

And yet, for our clock, this is true !

The way a mathematician would write the calculation is like so;

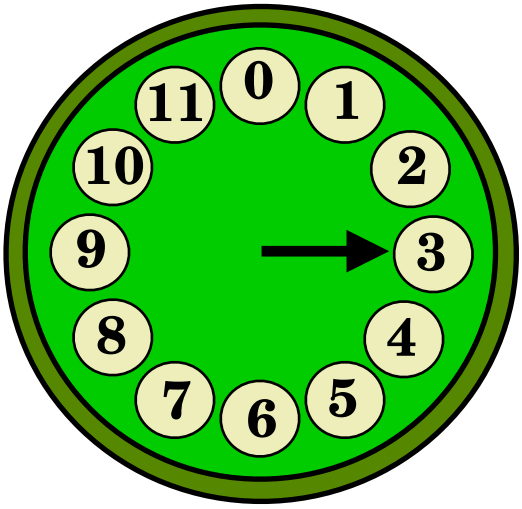
$$8 + 5 \equiv 1 \pmod{12}$$

and they would say, “Eight plus five is congruent to one, modulo twelve”
The word “modulo” is often simply said “mod”.

1.3 A Mathematician Quirk

In measuring time, a traditional clock face features the integers 1 to 12 inclusive. However, in the world of modulo 12 arithmetic, mathematicians' prefer to work with the following set of integers;

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$



Have you spotted the mathematicians' quirk ?

Rather than write,

$$3 + 9 \equiv 12 \pmod{12}$$

a mathematician would write,

$$3 + 9 \equiv 0 \pmod{12}$$

The set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ is termed the least residues modulo 12

1.4 Exercise

Solve the following congruence equations modulo 12

Answers should be given as elements from the set of least residues modulo 12

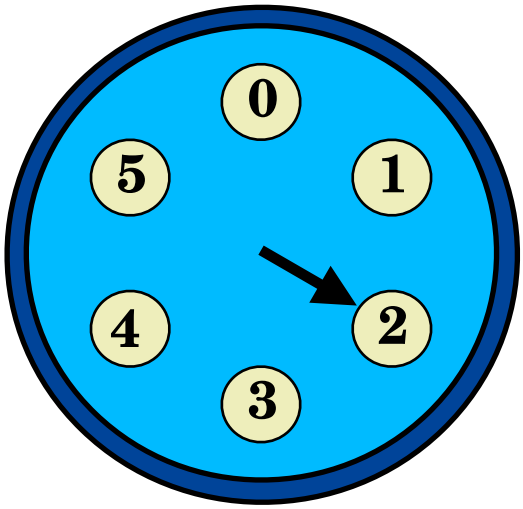
(i) $6 + 9 \equiv x \pmod{12}$ **(ii)** $10 + x \equiv 5 \pmod{12}$

(iii) $4 - 7 \equiv x \pmod{12}$ **(iv)** $42 - x \equiv 8 \pmod{12}$

[8 marks]

1.5 A Modulo Six Clock

There is no particular reason why a modulo clock has to have twelve integers upon its face. Here is a modulo six clock;



For the modulo six clock the set of least residues is {0, 1, 2, 3, 4, 5}

1.6 Example

Solve the following congruence equation modulo 6.
Any answers should be given as elements from the set of least residues modulo 6.

$$3x + 14 \equiv 5 \pmod 6$$

Teaching Video : http://www.NumberWonder.co.uk/v9108/1.mp4

[6 marks]

1.7 Exercise

Marks Available : 50

Question 1

Working modulo 12, what are the following congruent to ?

(i) 29 **(ii)** -7 **(iii)** 145

(iv) $47 + 21$ **(iv)** $3 - 19$ **(vi)** 5^3

[4 marks]

Question 2

(a) Write down the set of least residues modulo 4.

[1 mark]

(b) Working modulo 4, what are the following congruent to ?
Answers should be elements from the set of least residues modulo 4.

(i) 7^0 **(ii)** 7^1 **(iii)** 7^2

(iv) 7^3 **(v)** 7^4 **(vi)** 7^5

[3 marks]

(c) From the pattern suggested in part (b), and still working modulo 4,
what are the following congruent to ?

(i) 7^{758} **(ii)** 7^{433} **(iii)** $7^{501} + 7^{383}$

[3 marks]

Question 3

Solve the following congruence equations modulo 8.
Answers should be given as elements from the set of least residues modulo 8.

(i) $6 + 4 \equiv x \pmod 8$ **(ii)** $3 + x \equiv 1 \pmod 8$

(iii) $4 - 19 \equiv x \pmod 8$ **(iv)** $37 - x \equiv 8 \pmod 8$

[8 marks]

Question 4

Solve the following congruence equation modulo 6.

Any answers should be given as elements from the set of least residues modulo 6.

$$2x + 11 \equiv 1 \pmod 6$$

[6 marks]

Question 5

Consider integer addition modulo 5.

As any integer what-so-ever is congruent to an element in the set of least residues modulo 5, all possible modulo 5 additions can be captured in one simple table.

Here is that table;

$+_5$	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

Highlighted is the addition, $3 + 4 \equiv 2 \pmod 5$

Produce a similar table for multiplication modulo 5;

$\times_5$	0	1	2	3	4
0					
1					
2					
3					
4					

[4 marks]

Question 6

5! is said "5 factorial"

5! means $5 \times 4 \times 3 \times 2 \times 1$

Your calculator will tell you that 5! = 120

However, $5! \equiv 1 \pmod 7$ because $120 = 17 \times 7 + 1$

(a) Working modulo 7, what are the following congruent to ?

(i)	1!	**(ii)**	2!	**(iii)**	3!
(iv)	4!	**(v)**	5!	**(vi)**	6!
(vii)	7!	**(viii)**	8!	**(ix)**	9!

[3 marks]

(b) **(i)** From part (a), Lilibet conjectures that.

$n! \equiv 0 \pmod 7$ for $n \geqslant 7$ where $n \in \mathbb{Z}^+$

Lilibet is correct. Explain why.

[2 marks]

Question 7

(a) Working modulo 9, what are the following congruent to ?

(i)	13	**(ii)**	572	**(iii)**	334
(iv)	85507	**(v)**	1002001	**(vi)**	9994999

[3 marks]

(b) There is a quick "trick" for working out the answers to part (a)
Explain what this "trick" is and use it to determine the value of,

12345678987654321 (mod 9)

[2 marks]

Question 8

Find the remainder when $1! + 2! + 3! + 4! + ... + 100!$ is divided by 15.
In other words, find the value of,

$$1! + 2! + 3! + 4! + ... + 100! \pmod{15}$$

[5 marks]

Question 9

The serial number of a certain currency is 11 digits long.
The first 10 digits of the serial number are followed by a security check digit.
For the note to pass the security check, the 10 digit number will be congruent to the check digit modulo 9.
For each of these serial numbers, determine is they pass the security check.

(i) 51177875501 **(ii)** 88100245327

[2 marks]

Question 10

Determine the value of,

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 + 6^2 + ... + 100^2 \pmod{4}$$

[4 marks]