3 The Congruence Relation and Congruence Classes

In order to extend our knowledge of finite groups, we will consider examples that involve firstly congruence classes and secondly (chapter 4) permutations.

3.1. The Congruence Relation on the Set of Integers

This section concerns itself only with the set **Z** of integers and the set **N** of natural numbers. (**N** is the set of all positive integers).

Definition

Suppose m is any natural number. We say that two integers a and b are *congruent modulo m* if m divides $a - b$ exactly.

If a is congruent to b modulo m we will write $a \equiv b \pmod{m}$.

(Recall that if m divides a–b exactly then we write $m \mid a-b$ and we note that this is exactly the same as saying that $a - b$ is a multiple of m or that $a-b = km$ for some integer k.)
Examples

i) $37 \equiv 17 \pmod 5$ as $37 - 17 = 20$ and $5 \mid 20$.

ii) $19 \equiv -9 \pmod 7$ as $19 - (-9) = 28$ and $7 \mid 28$.

iii) $4 \equiv 4 \pmod 6$ as $4 - 4 = 0$ and $6 \mid 0$. ($0 = 0 \times 6$ so 0 is a multiple of 6).

iv) 13 and 28 are not congruent modulo 4 since $13 - 28 = -15$ which is not divisible by 4.

Properties of the Congruence Relation:

From the definition it is easy to see that

i) $a \equiv a \pmod m$ for all integers a and natural numbers m.

ii) $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$ for all a,b and m.

iii) $a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ for all a,b,c and m.

The only case that is difficult is iii) but we have

$a \equiv b \pmod m$ and $b \equiv c \pmod m \Rightarrow a - b = km,\ b - c = lm$ for some integers k and l.

But then

$$a - c = (a - b) + (b - c) = (k + l)m$$

and so $a \equiv c \pmod m$.

3.2 Congruence Classes

Definition:
Suppose m is any natural number and a is any integer. Then the *congruence class of a modulo m* (written $[a]_m$ or just $[a]$ if it is obvious what m is) is the set of all integers congruent to a modulo m.

Hence

i) $[3]_5$ = set of all integers congruent to 3 modulo 5

= set of all integers which differ from 3 by a multiple of 5

$= \{\ldots, -17, -12, -7, -2, 3, 8, 13, 18, \ldots\}$

ii) $[4]_3$ = set of all integers which differ from 4 by a multiple of 3

$= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

iii) $[1]_3$ = set of all integers which differ from 1 by a multiple of 3

$= \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

We can see from this that the congruence classes $[1]_3$ and $[4]_3$ are actually the same set and so $[1]_3 = [4]_3$. Since there will always be exactly one number in the range 0 to m–1 that can be used to name a particular congruence class and we will normally use this simplest form as the name of the class. Thus the set above would normally be referred to as $[1]_3$.

Exercise 3.2

1. Suppose $A = \{-31, -17, -7, -4, 0, 3, 7, 8, 9, 31\}$.
Write down all the pairs of integers $a, b \in A$ such that

a) $a \equiv b \pmod 4$ b) $a \equiv b \pmod 3$

2. Write down the elements of the following congruence classes.

a) $[3]_5$ b) $[2]_6$ c) $[1]_2$

d) $[13]_3$ e) $[-3]_4$ f) $[-9]_5$

3. Write down the simplest name of each of the following congruence classes

a) $[9]_4$ b) $[15]_3$ c) $[-2]_4$

d) $[-5]_7$ e) $[71]_6$ f) $[-37]_5$

Now consider the different possible congruence classes modulo 3. We have

$$[0] = \{ \ldots, -9, -6, -3, 0, 3, 6, 9, \ldots \}$$

$$[1] = \{ \ldots, -8, -5, -2, 1, 4, 7, 10, \ldots \}$$

$$[2] = \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}$$

Notice that every integer (positive or negative) lies in exactly one of these sets (we say that the three congruence classes *partition* the set **Z** of all integers). Since something similar happens for every natural number m we say that

> There are exactly m different congruence classes modulo m and these can be written $[0], [1], \ldots, [m-1]$ when they are in their simplest form.
>
> The set of all congruence classes modulo m is written $\mathbf{Z}_m$ so we have
> $$\mathbf{Z}_m = \{ [0]_m, [1]_m, \ldots, [m-1]_m \}$$
>
> $\mathbf{Z}_m$ is often called *the set of integers modulo m.*

Also notice that, again working modulo 3

$$[0] = \{ 3k : k\in\mathbf{Z} \} = \{x\in\mathbf{Z} : x \text{ leaves remainder 0 on division by 3}\}$$

$$[1] = \{ 3k+1 : k\in\mathbf{Z} \} = \{x\in\mathbf{Z} : x \text{ leaves remainder 1 on division by 3}\}$$

$$[2] = \{ 3k+2 : k\in\mathbf{Z} \} = \{x\in\mathbf{Z} : x \text{ leaves remainder 2 on division by 3}\}$$

This gives us an alternative way of defining congruence classes. Working modulo m we see that for $0 \le s \le m-1$

$$[s] = \{ mk+s : k\in\mathbf{Z} \} = \{x\in\mathbf{Z} : x \text{ leaves remainder s on division by m}\}$$

3.3 Binary Operations on Congruence Classes

In this section we define two operations on the set $\mathbf{Z}_m$ of congruence classes.

3.3.1 Addition of congruence classes modulo m

Suppose we have two congruence classes $[x]_m$ and $[y]_m$ and that $a \in [x]_m$, $b\in[y]_m$. Then $a-x = km$, $b-y = lm$ for some integers k and l and so we have (adding the two expressions)

$$(a - x) + (b - y) = km + lm$$

or equally

$$(a + b) - (x + y) = km + lm = (k + l)m$$

Hence $a+b \in [x+y]_m$.

Thus any element of [x] added to any element of [y] gives an element of [x+y] and so it makes sense to define an operation (called *addition of congruence classes modulo m* and represented by the symbol $\oplus$) by the rule

$$[x] \oplus [y] = [x+y]$$

Thus as examples we see that

$$[2]_4 \oplus [3]_4 = [5]_4 = [1]_4$$

$$[3]_5 \oplus [2]_5 = [5]_5 = [0]_5$$

and we notice that while $[5]_4 = [1]_4$ we should always write our answer in the simplest possible form. This will mean that $\oplus$ is a closed binary operation on the set of congruence classes modulo m. Since there will only be a finite number of congruence classes we can construct an operation table for the operation.

For example the operation table for addition of congruence classes modulo 4 has the form:

⊕	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

3.3.2 Multiplication of congruence classes modulo m

Now suppose we have two congruence classes $[x]_m$ and $[y]_m$ and that $a \in [x]_m$, $b \in [y]_m$. Then $a-x = km$, $b-y = lm$ for some integers k and l and so we have

$$a = x + km, \quad b = y + lm$$

or equally

$$(ab) = xy + xlm + ykm + klm^2$$

Hence $ab - xy = m(xl + yk + klm)$ and so $ab \in [xy]_m$.

Thus any element of [x] multiplied by any element of [y] gives an element of [xy] and so it makes sense to define an operation (called *multiplication of congruence classes modulo m* and represented by the symbol $\odot$) by the rule

$$[x] \odot [y] = [xy]$$

Thus as before we have examples and for instance

$$[2]_4 \odot [3]_4 = [6]_4 = [2]_4$$

$$[3]_5 \odot [4]_5 = [12]_5 = [2]_5$$

where again we should always write our answer in the simplest possible form. Again this means that $\odot$ is a closed binary operation on the set of congruence classes modulo m and we can construct an operation table for it. The operation table for multiplication of congruence classes modulo 4 is given by

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

and so we see again that the operation is closed.

Exercise 3.3

1. Write down the operation tables for $\mathbf{Z}_5$ and $\mathbf{Z}_6$ when the operation is addition of congruence classes.

2. Write down the result of the following sums and products of congruence classes in their simplest form.

a) $[3]_2 \oplus [4]_2$ b) $[-3]_4 \oplus [6]_4$

c) $[5]_5 \oplus [7]_5$ d) $[23]_6 \oplus [-44]_6$

e) $[3]_2 \odot [4]_2$ f) $[-3]_4 \odot [6]_4$

g) $[5]_5 \odot [7]_5$ h) $[23]_6 \odot [-44]_6$

3. Write down the multiplication tables for $\mathbf{Z}_5$, $\mathbf{Z}_6$ and $\mathbf{Z}_3$ when the operation is multiplication of congruence classes.

4. Suppose a and b are non-zero natural numbers less than m and consider the product $[a]_m \odot [b]_m$.

a) Can the answer ever be $[0]_m$? (I.e. can two non-zero congruence classes be multiplied together to give the congruence class of zero?)

b) For what values of m can the answer [0] be found for the product of non-zero congruence classes.

5. Prove that addition of congruence classes modulo *m* is associative. (*Hint.* Use the fact that addition of integers is associative) Prove a similar result for multiplication.

3.4 Congruence Classes and Groups.

You should have proved Ex 3.3 no 5 that both addition and multiplication of congruence classes is associative.
We can now ask the question, do any of the tables drawn up in Ex 3.3, Nos 1 and 3 exhibit group structure, ie checking the axioms of closure, identity and inverse from these tables? Certainly all the tables exhibit closure.

The tables in no 1, also demonstrate the existence of an identity and an inverse for every element. *(For an identity to exist, there must be a row and column inside the table which is exactly the same as the input row and input column. For every element to have an inverse the identity must be present on each row and column of the inside of the table - this will be proved in Section 5)*

When we observe the tables for No 3, it appears that [1] could be an identity element. However we then observe that [0] has no inverse, so the tables for No 3 do not exhibit group structure.

Let us next consider the table for $\mathbf{Z}_5 - [0]_5$

$\odot$	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]
[2]	[2]	[4]	[1]	[3]
[3]	[3]	[1]	[4]	[2]
[4]	[4]	[3]	[2]	[1]

The above table is closed, [1] is the identity element and the inverses for [2], [3], [4] are [3], [2], [4] respectively. Note the identity is self inversing.

Exercise 3.4

Note in any of the following examples you may assume that addition and multiplication of congruence classes is associative.

1. Complete the structure tables for the following sets and associated operations

   a) $\mathbf{Z}_4 - [0]_4$ multiplication of congruence classes modulo 4

   b) $\mathbf{Z}_7 - [0]_7$ multiplication of congruence classes modulo 7

   Do either of these sets and binary operations give rise to a group?

2. Show $\{[2]_{14}, [4]_{14}, [8]_{14}\}$ forms a group w.r.t. multiplication of congruence classes modulo 14. Which element is the identity element? Redraw your table with the identity first.

3. Show $\{[2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$ forms a group w.r.t. multiplication of congruence classes modulo 10. Find the identity element and hence find inverse for each of the elements.

4. Which of the following sets of congruence classes mod 13 forms a group w.r.t. $\odot$ mod 13?
   i) $\{ [1], [2], [4], [6], [8], [10], [12] \}$
   ii) $\{ [1], [5], [8], [12] \}$

5. Try to complete a structure table for $\odot$ mod 18, which contains the elements [2], [4], [8]. What extra elements do you need to add to the set in order to have a group?