Chapter 4

Congruence Classes

Idea. As in the previous Chapter, when we calculate mod 7, say, the integers 2, -5 and 16 are considered to be identical, as are 3, -4 and 17. Thus is makes sense to collect together all those integers that are considered to be identical modulo 7 to form a **congruence class** mod 7.

Goals.

- We will show that there are exactly m congruence classes mod m. The set of these classes is a **finite set** $\mathbb{Z}_m$.
- We will show that $\mathbb{Z}_m$ comes equipped with operations $+$ and $\times$. Thus, $\mathbb{Z}_m$ is a completely new example where **arithmetic is defined on a finite set**.
- We will also introduce the subset $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$. The set $\mathbb{Z}_m^*$ has only one operation, $\times$, but this multiplicative structure is extremely important in modern applications, e.g., cryptography.

Definition (Congruence class)**.** The **congruence class** mod m of $a \in \mathbb{Z}$ is the set of integers congruent to a mod m,

$$[a]_m = \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

Example (Congruence classes modulo 3)**.** With $m = 3$ we have

- $[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$,
- $[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\}$,
- $[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$.

Remark (Initial observations about congruence classes)**.** 1. In the Example we observe that $0 \in [0]_3$, $1 \in [1]_3$ and $2 \in [2]_3$.

Indeed, by Proposition 3.1 congruences are *reflexive*, so $a \equiv a \mod m$ and thus by definition of $[a]_m$ one has $a \in [a]_m$ for all $a \in \mathbb{Z}$. (That is, an integer is an element of the class labelled by that element.)

2. In the example, every integer seems to be in one of these classes, and these classes are disjoint. If we try to construct another congruence class mod 3, for instance

$$[-5]_3 = \{... -11, -8, -5, -3, 1, ...\},$$

we discover that it is **the same set** as $[1]_3$. This is explained by the following fundamental result.

Proposition 4.1 (Congruence classes coincide or are disjoint)**.** For integers a, b,

i) If $a \equiv b \mod m$ then $[a]_m = [b]_m$,

ii) If $a \not\equiv b \mod m$ then $[a]_m \cap [b]_m = \varnothing$.

Since we have exactly one of $a \equiv b$ or $a \not\equiv b \mod m$ we deduce that two congruence classes are either identical (as sets) or disjoint.

Proof. The Proposition will follow from a more general Theorem 5.1 below, so we are not giving a proof at this stage. □

Definition (The set $\mathbb{Z}_m$)**.** We write $\mathbb{Z}_m$ for the set of congruence classes mod m, i.e.,

$$\mathbb{Z}_m = \{[a]_m : a \in \mathbb{Z}\}.$$

Proposition 4.2 (Description of the set $\mathbb{Z}_m$)**.** Let $m \in \mathbb{N}$. The set $\mathbb{Z}_m$ is finite of cardinality m. The m elements of this set are given by

$$\mathbb{Z}_m = \{[r]_m : 0 \leq r \leq m-1\} = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Proof. By Proposition 3.4, each integer each residue class contains a remainder mod m — that is, one of $0, 1, \ldots, m-1$. Hence by Proposition 4.1, every congruence class coincides with one of the $[0]_m, [1]_m, \ldots, [m-1]_m$. These congruence classes are distinct, because by Proposition 3.4, different remainders are incongruent modulo m. Hence there are m distinct congruence classes, as claimed. □

Example (Listing elements of $\mathbb{Z}_3$)**.**

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}.$$

We could equally have written $\mathbb{Z}_3 = \{[3]_3, [7]_3, [-7]_3\}$ since $[3]_3 = [0]_3$, $[7]_3 = [1]_3$ and $[-7]_3 = [2]_3$. Thus, $[2]_3$ and $[-7]_3$ are two different labels for the same set. Arguably, $[2]_3$ is more convenient to use than $[-7]_3$.

Idea. Since we can add and multiply elements of $\mathbb{Z}$, we can define the operations of addition and multiplication on the **finite set** $\mathbb{Z}_m$.

Definition (Arithmetic operations on the set $\mathbb{Z}_m$)**.** For $a, b \in \mathbb{Z}$ define

$$[a]_m + [b]_m = [a+b]_m, \qquad [a]_m \times [b]_m = [a \times b]_m. \tag{†}$$

Example. In $\mathbb{Z}_{10}$,

$$\begin{aligned}
&[7]_{10} + [8]_{10} = [15]_{10} = [5]_{10} \\
&[7]_{10} \times [8]_{10} = [56]_{10} = [6]_{10} \\
&[2]_{10} \times [0]_{10} = [0]_{10} \text{ and } [2]_{10} \times [5]_{10} = [0]_{10} \\
&[2]_{10} \times [1]_{10} = [2]_{10} \text{ and } [2]_{10} \times [6]_{10} = [2]_{10} \qquad \text{etc.}
\end{aligned}$$

This definition of addition and multiplication on $\mathbb{Z}_m$ might seem to depend on the choice of labels for the classes. The next result shows this is not the case. The following result is, in fact, simply a reinterpretation of the earlier result known as Modular Arithmetic.

Proposition 4.3 (Addition and multiplication on the set $\mathbb{Z}_m$ are well-defined)**.** If $[a]_m = [a']_m$ and $[b]_m = [b']_m$ then $[a]_m + [b]_m = [a']_m + [b']_m$ and $[a]_m \times [b]_m = [a']_m \times [b']_m$.

Thus for the arithmetic operations on $\mathbb{Z}_m$ it does not matter what label we choose for a class.

Proof. Since different labels for the same congruence class are congruent mod m we have

$$[a]_m = [a']_m \implies a \equiv a' \mod m, \qquad [b]_m = [b']_m \implies b \equiv b' \mod m.$$

The earlier Proposition 3.2 on Modular Arithmetic implies $a + b \equiv a' + b' \mod m$ which in turn implies $[a+b]_m = [a'+b']_m$. Then

$$\begin{aligned}
[a]_m + [b]_m &= [a+b]_m && \text{by (†)} \\
&= [a'+b']_m && \text{by the above} \\
&= [a']_m + [b']_m && \text{again by (†).}
\end{aligned}$$

The argument for multiplication is similar and is omitted. □

If we express the result of addition or multiplication as a class $[r]_m$ with label $0 \leq r \leq m-1$ we can write all results in a **multiplication table** (even if the operation is addition!).

Example.

$(\mathbb{Z}_4, +)$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

$(\mathbb{Z}_4, \times)$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

Remark (Divisors of zero)**.** In the latter table we see something never seen in $(\mathbb{Z}, \times)$, namely that we can multiply two non-zero objects and get zero! For example $[2]_4 \times [2]_4 = [0]_4$. Here, $[2]_4$ is an example of **divisors of zero**.

Exercise (not given in the lectures because of size)**.** Check the multiplication table for $(\mathbb{Z}_8, \times)$:

$\times$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$	$[0]_8$
$[1]_8$	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[2]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[3]_8$	$[0]_8$	$[3]_8$	$[6]_8$	$[1]_8$	$[4]_8$	$[7]_8$	$[2]_8$	$[5]_8$
$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$	$[0]_8$	$[4]_8$
$[5]_8$	$[0]_8$	$[5]_8$	$[2]_8$	$[7]_8$	$[4]_8$	$[1]_8$	$[6]_8$	$[3]_8$
$[6]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$	$[0]_8$	$[6]_8$	$[4]_8$	$[2]_8$
$[7]_8$	$[0]_8$	$[7]_8$	$[6]_8$	$[5]_8$	$[4]_8$	$[3]_8$	$[2]_8$	$[1]_8$

Note that we again have divisors of zero, i.e. $[2]_8$, $[4]_8$ and $[6]_8$.

We are ready to define the important subset $\mathbb{Z}_m^*$ of $\mathbb{Z}_m$.

Definition (Invertible elements of $\mathbb{Z}_m$)**.** An element $[a]_m$ of $\mathbb{Z}_m$ is **invertible** if there exists $[a']_m$ such that $[a]_m[a']_m = [1]_m$. Such $[a']_m$ is the **(multiplicative) inverse** of $[a]_m$ and is denoted $[a]_m^{-1}$.

Definition (The zet $\mathbb{Z}_m^*$)**.** $\mathbb{Z}_m^*$ is the set of all invertible elements in $\mathbb{Z}_m$.

Example. In the previous chapter we found that 56 had inverse 5 modulo 93. Thus $[56]_{93} \in \mathbb{Z}_{93}$ is invertible with inverse $[5]_{93}$, i.e. $[56]_{93}^{-1} = [5]_{93}$. Hence $[56]_{93} \in \mathbb{Z}_{93}^*$. Similarly $[5]_{93} \in \mathbb{Z}_{93}^*$.

Question. How to describe the set $\mathbb{Z}_m^*$?

Proposition 4.4 (description of the set $\mathbb{Z}_m^*$)**.** $[a]_m \in \mathbb{Z}_m^*$ if, and only if, $\gcd(a, m) = 1$.

Proof. Since, by definition of $\mathbb{Z}_m^*$, "$[a]_m \in \mathbb{Z}_m^*$" means "$[a]_m$ is invertible", this is exactly Proposition 3.5 proved earlier. □

Corollary. We can therefore write

$$\mathbb{Z}_m^* = \{[r]_m : \ 0 \leq r \leq m-1, \ \gcd(r,m) = 1\}.$$

Example (The set $\mathbb{Z}_5^*$)**.** $\mathbb{Z}_5^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ and the multiplication table for $(\mathbb{Z}_5^*, \times)$ is

$\times$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

It is easy to read off inverses from a table, so

$$[1]_5^{-1} = [1]_5, \qquad [2]_5^{-1} = [3]_5, \qquad [3]_5^{-1} = [2]_5, \qquad [4]_5^{-1} = [4]_5.$$

Example (The set $\mathbb{Z}_8^*$)**.** $\mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ and the multiplication table for $(\mathbb{Z}_8^*, \times)$ is

$\times$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[1]_8$	$[1]_8$	$[3]_8$	$[5]_8$	$[7]_8$
$[3]_8$	$[3]_8$	$[1]_8$	$[7]_8$	$[5]_8$
$[5]_8$	$[5]_8$	$[7]_8$	$[1]_8$	$[3]_8$
$[7]_8$	$[7]_8$	$[5]_8$	$[3]_8$	$[1]_8$

Looking at the main diagonal of this table, we see that every element of $\mathbb{Z}_8^*$ is a **self-inverse**. So in some fundamental way the tables for $(\mathbb{Z}_8^*, \times)$ and $(\mathbb{Z}_5^*, \times)$ are different.

Remark. What of the tables for $(\mathbb{Z}_5^*, \times)$ and $(\mathbb{Z}_4, +)$, written as

$\times$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

and

$+$	$[0]_4$	$[1]_4$	$[3]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[3]_4$	$[2]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[0]_4$	$[3]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[2]_4$	$[1]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[1]_4$	$[0]_4$

do they not have the same "form"? Such questions are analysed at a much more conceptual level in future courses on Algebraic Structures.

Definition (closed under multiplication)**.** A subset X of $\mathbb{Z}_m$ is **closed under multiplication** if for all $[a]_m$, $[b]_m \in X$ one has $[a]_m[b]_m \in X$.

Proposition 4.5 ($\mathbb{Z}_m^*$ is closed under multiplication)**.** For all $m \in \mathbb{N}$, $\mathbb{Z}_m^*$ is a subset of $\mathbb{Z}_m$ closed under multiplication.

Proof. Let $[a]_m, [b]_m \in \mathbb{Z}_m^*$. This means they have inverses, i.e. there exist $[a]_m^{-1}$ and $[b]_m^{-1} \in \mathbb{Z}_m^*$ for which $[a]_m[a]_m^{-1} = [1]_m$ and $[b]_m[b]_m^{-1} = [1]_m$. Consider

$$\begin{aligned}([a]_m[b]_m)([b]_m^{-1}[a]_m^{-1}) &= [a]_m([b]_m[b]_m^{-1})[a]_m^{-1} \\ &= [a]_m[1]_m[a]_m^{-1} \\ &= [a]_m[a]_m^{-1} \\ &= [1]_m.\end{aligned}$$

Thus $[a]_m[b]_m$ has an inverse $[b]_m^{-1}[a]_m^{-1}$, and is therefore invertible. Hence $[a]_m[b]_m \in \mathbb{Z}_m^*$. □

Remark. The above result means that multiplication, $\times$, is well-defined on $\mathbb{Z}_m^*$.