1. We assume $n \in \mathbb{N}\backslash\{0,1\}$ throughout this Handout.

Definitions.

(a) *Suppose $x, y \in \mathbb{Z}$. Then we say x is* **congruent to y modulo n** *if $x - y$ is divisible by n.*
We write $x \equiv y (\mathsf{mod}\ n)$.

(b) *Define $E_n = \{(x, y) \mid x, y \in \mathbb{Z}$ and $x \equiv y(\mathsf{mod}\ n)\}$, and $R_n = (\mathbb{Z}, \mathbb{Z}, E_n)$.*
We call R_n the **congruence modulo n relation on $\mathbb{Z}$**.

Remark. R_n is an equivalence relation in $\mathbb{Z}$.

• Is R_n reflexive?

Pick any $x \in \mathbb{Z}$.
Note that
$x - x = 0 = 0 \cdot n$.
Also note that $0 \in \mathbb{Z}$.
Then $x - x$ is divisible by n.
Therefore $x \equiv x \pmod n$.
Hence $(x, x) \in E_n$.

• Is R_n symmetric?

Pick any $x, y \in \mathbb{Z}$. Suppose $(x, y) \in E_n$.
Then $x \equiv y \pmod n$.
Therefore $x - y$ is divisible by n.
Hence there exists some $k \in \mathbb{Z}$ such that $x - y = kn$.
Note that $y - x = (-k) \cdot n$ and $-k \in \mathbb{Z}$.
Then $y - x$ is divisible by n.
Therefore $y \equiv x \pmod n$.
Hence $(y, x) \in E_n$.

• Is R_n transitive?

Pick any $x, y, z \in \mathbb{Z}$.
Suppose $(x, y) \in E_n$ and $(y, z) \in E_n$.
Then $x \equiv y \pmod n$ and $y \equiv z \pmod n$.
Therefore $x - y$ and $y - z$ are divisible by n.
Hence there exist some $k, \ell \in \mathbb{Z}$ such that $x - y = kn$ and $y - z = \ell n$.
Note that $x - z = (x - y) + (y - z) = (k + \ell)n$, and $k + \ell \in \mathbb{Z}$.
Then $x - z$ is divisible by n.
Therefore $x \equiv z \pmod n$.
Hence $(x, z) \in E_n$.

Definitions.

(a) *For any* $x \in \mathbb{Z}$, *define* $[x] = \{y \in \mathbb{Z} : (x, y) \in E_n\}$.
The set $[x]$ *is called the* **equivalence class of** x **under the equivalence relation** R_n.

(b) *Define* $\mathbb{Z}_n = \{[x] \mid x \in \mathbb{Z}\}$.
We call $\mathbb{Z}_n$ *the* **quotient of the set** $\mathbb{Z}$ **by equivalence relation** R_n.

Remark.

This 'school-and-classes' analogy' is intended to help us see the intuitive idea about the definitions above.

Read:

- '*integer* x' as '*student* x',
- '*the set of all integers* $\mathbb{Z}$' as

  '*the school* $\mathbb{Z}$ *(whose elements are exactly all the students of the school)*',
- '$(x, y) \in E_n$' (or equivalently '$x \equiv y (\mathsf{mod}\ n)$') as

  '*student* x *is in the same class as student* y'.

2. **Lemma (1).**

Let $x, y \in \mathbb{Z}$. The following statements are equivalent:

(a) $x - y = qn$ *for some* $q \in \mathbb{Z}$.

(b) $x \equiv y (\mathsf{mod}\ n)$.

(c) $(x, y) \in E_n$.

(d) $y \in [x]$.

(e) $x \in [y]$.

(f) $[x] = [y]$.

Proof. Exercise. (This is nothing but a tedious game of words.)

Remark.

How to interpret Lemma (1) in terms of the 'school-and-classes' analogy'?

Recall that '$(x, y) \in E_n$' is read as '*student x is in the same class as student y*'. Now:

- '$y \in [x]$' reads:

  'Student y is an element of the set of all classmates of student x.'

- '$x \in [y]$' reads

  'Student x is an element of the set of all classmates of student y.'

- '$[x] = [y]$' reads:

  'The set of all classmates of student x is the same as the set of all classmates of student y.'

Each of these is the same as '*x is in the same class as y*'.

Lemma (2).

For any $x \in \mathbb{Z}$, there exists some unique $r \in [\![0, n-1]\!]$ such that $[x] = [r]$.

Proof.

Let $x \in \mathbb{Z}$.

- [Existence argument.]

Apply Division Algorithm:

There exist some $q, r \in \mathbb{Z}$ such that

$x = qn + r$ and $r \in [\![0, n-1]\!]$.

For this $q \in \mathbb{Z}$, we have $x - r = qn$.

Then, by Lemma (1), we have

$$[x] = [r]. \quad \square$$

- [Uniqueness argument?]

Let $s, t \in [\![0, n-1]\!]$.

Suppose $[x] = [s]$ and $[x] = [t]$.

Then $[s] = [x] = [t]$.

By Lemma (1), $s - t$ is divisible by n.

Since $s, t \in [\![0, n-1]\!]$, we have

$$0 \leq |s-t| \leq n-1 < n.$$

Then $|s-t| = 0$. (Why?) Hence $s = t$. $\square$

Remark.

How to interpret Lemma (2) in terms of the 'school-and-classes' analogy'?

No matter which student in the school $\mathbb{Z}$ is picked out, he/she will have exactly one classmate amongst $0, 1, \ldots, n-1$.

3. **Theorem (3).**

The following statements hold:

(0) $\mathbb{Z}_n = \{[0], [1], \cdots, [n-2], [n-1]\}$.

(1) *For any* $u \in \mathbb{Z}_n$, $u \neq \emptyset$.

(2) $\{x \in \mathbb{Z} : x \in u$ *for some* $u \in \mathbb{Z}_n\} = \mathbb{Z}$.

(3) *For any* $u, v \in \mathbb{Z}_n$, *exactly one of the following statements hold:*

(3a) $u = v$. (3b) $u \cap v = \emptyset$.

Remark.

How to interpret Theorem (3) in terms of the 'school-and-classes' analogy'?

(0) The classes $[0], [1], \cdots, [n-1]$ are exactly all the classes in the school $\mathbb{Z}$.

(1) In every class in the school, there is at least one student.

(2) Lunch break; all classes dismissed. But every student is still somewhere in the school campus.

(3) Any two copies of 'class namelists' in the school are either 'identical' or 'totally disjoint'.

Theorem (3).

The following statements hold:

(0) $\mathbb{Z}_n = \{[0], [1], \cdots, [n-2], [n-1]\}$.

(1) *For any* $u \in \mathbb{Z}_n$, $u \neq \emptyset$.

(2) $\{x \in \mathbb{Z} : x \in u$ *for some* $u \in \mathbb{Z}_n\} = \mathbb{Z}$.

(3) *For any* $u, v \in \mathbb{Z}_n$, *exactly one of the following statements hold:*

(3a) $u = v$. (3b) $u \cap v = \emptyset$.

Proof.

(0) Pick any $u \in \mathbb{Z}_n$.

By the definition of $\mathbb{Z}_n$, there exists some $x \in \mathbb{Z}$ such that $u = [x]$.

By Lemma (2), there exists some $r \in [\![0, n-1]\!]$ such that $[x] = [r]$.

Then for this $r \in [\![0, n-1]\!]$, we have $u = [x] = [r]$. $\square$

(1) Pick any $u \in \mathbb{Z}_n$.

By the definition of $\mathbb{Z}_n$, there exists some $x \in \mathbb{Z}$ such that $u = [x]$.

By reflexivity, $(x, x) \in E_n$. By Lemma (1), $x \in [x] = u$. Then $u \neq \emptyset$. $\square$

(2) Write $U = \{x \in \mathbb{Z} : x \in u$ for some $u \in \mathbb{Z}_n\}$. By definition, we have $U \subset \mathbb{Z}$.

[Ask: Is it true that $\mathbb{Z} \subset U$?

Check: 'For any object x, if $x \in \mathbb{Z}$ then $x \in U$'.]

Pick any object x. Suppose $x \in \mathbb{Z}$. We have $x \in [x]$ and $[x] \in \mathbb{Z}_n$. Then $x \in U$.

It follows that $\mathbb{Z} \subset U$. $\square$

Theorem (3).

The following statements hold:

(0) $\mathbb{Z}_n = \{[0], [1], \cdots, [n-2], [n-1]\}$.

(1) *For any* $u \in \mathbb{Z}_n$, $u \neq \emptyset$.

(2) $\{x \in \mathbb{Z} : x \in u$ *for some* $u \in \mathbb{Z}_n\} = \mathbb{Z}$.

(3) *For any* $u, v \in \mathbb{Z}_n$, *exactly one of the following statements hold:*

(3a) $\underbrace{u = v}_{H}$. (3b) $\underbrace{u \cap v = \emptyset}_{K}$.

H	K	$\sim K$	$H \leftrightarrow (\sim K)$
T	T	F	F
T	F	T	T
F	T	F	T
F	F	T	F

Proof.

(3) Pick any $u, v \in \mathbb{Z}_n$. [What to deduce? '$[H \rightarrow (\sim K)] \wedge [(\sim K) \rightarrow H]$' is true. Why? Truth table?]

(A) Suppose $u = v$.

Then $u \cap v = u \cap u = u \neq \emptyset$ by Statement (1).

(B) Suppose $u \cap v \neq \emptyset$.

Pick some $z \in u \cap v$. We have $z \in u$ and $z \in v$.

Since $u \in \mathbb{Z}_n$, there exists some $x \in \mathbb{Z}$ such that $u = [x]$.

Since $v \in \mathbb{Z}_n$, there exists some $y \in \mathbb{Z}$ such that $v = [y]$.

We have $z \in u = [x]$. Then $[z] = [x]$ by Lemma (1).

We have $z \in v = [y]$. Then $[z] = [y]$ by Lemma (1).

Then $u = [x] = [z] = [y] = v$. $\square$

Theorem (3).
The following statements hold:

(0) $\mathbb{Z}_n = \{[0], [1], \cdots, [n-2], [n-1]\}$.

(1) *For any* $u \in \mathbb{Z}_n$, $u \neq \emptyset$.

(2) $\{x \in \mathbb{Z} : x \in u$ *for some* $u \in \mathbb{Z}_n\} = \mathbb{Z}$.

(3) *For any* $u, v \in \mathbb{Z}_n$, *exactly one of the following statements hold:*
(3a) $u = v$. (3b) $u \cap v = \emptyset$.

Remark on terminologies.

(a) $\mathbb{Z}$ is **partitioned** into the n pairwise disjoint non-empty sets $[0]$, $[1]$, ..., $[n-2]$, $[n-1]$. We may simply refer to the set (of sets) $\mathbb{Z}_n$ as a **partition of** $\mathbb{Z}$.

(b) Because such a partition of $\mathbb{Z}$ arises ultimately from the equivalence relation R_n, we refer to $\mathbb{Z}_n$ as the **quotient of $\mathbb{Z}$ by the equivalence relation** R_n.

You will encounter more of these ideas and terminologies (and 'natural consequences' of these ideas, such as the rest of the Handout *Arithmetic in Integers modulo* n) in advanced courses (for example, *algebra* and *topology*).