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

Definitions.

(a) *Let $x, y \in \mathbb{Z}$. x is said to be* **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 $k, l \in \mathbb{Z}$ such that
$x - y = kn$ and $y - z = ln$.
Note that $x - z = (x - y) + (y - z) = (k + l)n$,
and $k + l \in \mathbb{Z}$.
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* $\mathbb{Z}_n = \{[x] \mid x \in \mathbb{Z}\}$.
$\mathbb{Z}_n$ *is called as 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 $[x] = [r]$. □

- [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 $s = t$. □

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) $\{x \in \mathbb{Z} : x \in u \text{ for some } u \in \mathbb{Z}_n\} = \mathbb{Z}$

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

(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 $u = [x] = [r]$. □

(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 $u \neq \emptyset$. □

(2) Write $U = \{x \in \mathbb{Z} : x \in u \text{ for some } u \in \mathbb{Z}_n\}$. 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 $\mathbb{Z} \subset U$. □

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) $\{x \in \mathbb{Z} : x \in u \text{ for some } u \in \mathbb{Z}_n\} = \mathbb{Z}$

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

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

H	K	~K	H↔(~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→(~K)]∧[(~K)→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 exits some $x \in \mathbb{Z}$ such that $u = [x]$.

Since $v \in \mathbb{Z}_n$, there exits 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 $u = [x] = [z] = [y] = v$. □

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) $\{x \in \mathbb{Z} : x \in u \text{ for some } u \in \mathbb{Z}_n\} = \mathbb{Z}$

(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 this Handout) in advanced courses (for example, *algebra* and *topology*).

We want to define the function $\alpha: \mathbb{Z}_n^2 \to \mathbb{Z}_n$ through this declaration:
'Define $\alpha: \mathbb{Z}_n^2 \to \mathbb{Z}_n$ by $\alpha([k],[\ell]) = [k+\ell]$ whenever $k, \ell \in \mathbb{Z}$.'
But is this α well-defined as a function?

4. **Theorem (4).**

Define

$$G_\alpha = \left\{ ((u,v),w) \;\middle|\; \begin{array}{l} u,v,w \in \mathbb{Z}_n \text{ and} \\ \text{there exist } k,\ell \in \mathbb{Z} \text{ such that } u=[k], v=[\ell] \text{ and } w=[k+\ell] \end{array} \right\}.$$

Define $\alpha = (\mathbb{Z}_n{}^2, \mathbb{Z}_n, G_\alpha)$.

α is a function from $\mathbb{Z}_n{}^2$ to $\mathbb{Z}_n$.

Proof.

Note that $G_\alpha \subset (\mathbb{Z}_n{}^2) \times \mathbb{Z}_n$. Hence α is a relation from from $\mathbb{Z}_n{}^2$ to $\mathbb{Z}_n$.

(E) [Is each 'input pair' 'assigned' to at least one 'output' by α?]

[Check: For any $u, v \in \mathbb{Z}_n$, there exits some $w \in \mathbb{Z}_n$ such that $((u,v),w) \in G_\alpha$.]

Pick any $u, v \in \mathbb{Z}_n$.
There exit some $k, \ell \in \mathbb{Z}$ such that $u = [k]$ and $v = [\ell]$.
For these $k, \ell \in \mathbb{Z}$, we have $k+\ell \in \mathbb{Z}$. Define $w = [k+\ell]$. We have $w \in \mathbb{Z}_n$.
By definition of G_α, we have $((u,v),w) \in G_\alpha$. □

(U) [Is each 'input pair' 'assigned' to at most one 'output' by α?]

Theorem (4).

Define

$$G_\alpha = \left\{ ((u,v),w) \;\middle|\; \begin{array}{l} u,v,w \in \mathbb{Z}_n \text{ and} \\ \text{there exist } k,\ell \in \mathbb{Z} \text{ such that } u=[k], v=[\ell] \text{ and } w=[k+\ell] \end{array} \right\}.$$

Define $\alpha = ({\mathbb{Z}_n}^2, \mathbb{Z}_n, G_\alpha)$.

α is a function from ${\mathbb{Z}_n}^2$ to $\mathbb{Z}_n$.

Proof.

Note that $G_\alpha \subset ({\mathbb{Z}_n}^2) \times \mathbb{Z}_n$. Hence α is a relation from from ${\mathbb{Z}_n}^2$ to $\mathbb{Z}_n$.

(E) [Is each 'input pair' 'assigned' to at least one 'output' by α? Yes.]

(U) [Is each 'input pair' 'assigned' to at most one 'output' by α?]

[Check: For any $u,v,w,w' \in \mathbb{Z}_n$, if $((u,v),w) \in G_\alpha$ and $((u,v),w') \in G_\alpha$ then $w=w'$.]

Pick any $u,v,w,w' \in \mathbb{Z}_n$. Suppose $((u,v),w) \in G_\alpha$ and $((u,v),w') \in G_\alpha$.

Since $((u,v),w) \in G_\alpha$, there exist some $k,\ell \in \mathbb{Z}$ such that $u=[k]$, $v=[\ell]$ and $w=[k+\ell]$.

Since $((u,v),w') \in G_\alpha$, there exist some $k',\ell' \in \mathbb{Z}$ such that $u=[k']$, $v=[\ell']$ and $w'=[k'+\ell']$.

We have $[k]=u=[k']$. Then $k \equiv k' \pmod n$ by Lemma (1).

We have $[\ell]=v=[\ell']$. Then $\ell \equiv \ell' \pmod n$ by Lemma (1).

$k-k'$, $\ell-\ell'$ are divisible by n. Then $(k+\ell)-(k'+\ell')$ is also divisible by n.

Therefore $k+\ell \equiv k'+\ell' \pmod n$. Hence $w=[k+\ell]=[k'+\ell']=w'$. □

Theorem (4).

Define

$$G_\alpha = \left\{ ((u,v),w) \;\middle|\; \begin{array}{l} u,v,w \in \mathbb{Z}_n \text{ and} \\ \text{there exist } k,\ell \in \mathbb{Z} \text{ such that } u=[k], v=[\ell] \text{ and } w=[k+\ell] \end{array} \right\}.$$

Define $\alpha = (\mathbb{Z}_n{}^2, \mathbb{Z}_n, G_\alpha)$.

α *is a function from* $\mathbb{Z}_n{}^2$ *to* $\mathbb{Z}_n$.

Proof.

Note that $G_\alpha \subset (\mathbb{Z}_n{}^2) \times \mathbb{Z}_n$. Hence α is a relation from from $\mathbb{Z}_n{}^2$ to $\mathbb{Z}_n$.

(E) [Is each 'input pair' 'assigned' to at least one 'output' by α? Yes.]

(U) [Is each 'input pair' 'assigned' to at most one 'output' by α? Yes.]

It follows that α is a function from $\mathbb{Z}_n{}^2$ to $\mathbb{Z}_n$.

Remark.

The function α is called **addition in** $\mathbb{Z}_n$ because of its resemblance with the function 'addition' for other more familiar mathematical objects, such as numbers and matrices.

From now on, we write $\alpha(u,v)$ as $u+v$, and call it the sum of u, v.

By the definition of addition in $\mathbb{Z}_n$, whenever $k, \ell \in \mathbb{Z}$, we have $[k] + [\ell] = \alpha([k],[\ell]) = [k+\ell]$.

(this $+$ happens in $\mathbb{Z}_n$; this $+$ happens in $\mathbb{Z}$.)

5. **Addition table for 'small' values of n:**

$[k] + [\ell] = [k + \ell]$

This happens in $\mathbb{Z}_n$. This happens in $\mathbb{Z}$.

Addition in $\mathbb{Z}_2$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Addition $\mathbb{Z}_3$

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Addition in $\mathbb{Z}_4$

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

Addition in $\mathbb{Z}_5$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

Addition in $\mathbb{Z}_6$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Addition in $\mathbb{Z}_7$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$

Addition table for 'small' values of n:

Addition in $\mathbb{Z}_8$

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

Addition in $\mathbb{Z}_9$

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

6. **Theorem (5).**

$(\mathbb{Z}_n, +)$ *is an abelian group.*

Proof.

- [Associativity?] [Check: For any $u,v,w \in \mathbb{Z}_n$, $(u+v)+w = u+(v+w)$.]
  Let $u,v,w \in \mathbb{Z}_n$. There exist some $k,\ell,m \in \mathbb{Z}$ such that $u=[k]$, $v=[\ell]$ and $w=[m]$.
  Then $(u+v)+w = ([k]+[\ell])+[m] = [k+\ell]+[m]$
  $= [(k+\ell)+m] = [k+(\ell+m)] = \ldots = u+(v+w)$. □
- [Commutativity?] [Check: For any $u,v \in \mathbb{Z}_n$, $u+v = v+u$.]
  Let $u,v \in \mathbb{Z}_n$.
  There exist some $k,\ell \in \mathbb{Z}$ such that $u=[k]$ and $v=[\ell]$.
  Then $u+v = [k]+[\ell] = [k+\ell] = [\ell+k] = \ldots = v+u$. □
- [Existence of identity element?] [Check: There exists some $e \in \mathbb{Z}_n$ such that for any $u \in \mathbb{Z}_n$, $u+e = u = e+u$.]
  Define $0_n = [0]$.
  Pick any $u \in \mathbb{Z}_n$. There exists some $k \in \mathbb{Z}$ such that $u=[k]$.
  Then $u+0_n = [k]+[0] = [k+0] = [k] = u$. Also, $0_n+u = \ldots = u$. □
- [Existence of inverse element?] [Check: For any $u \in \mathbb{Z}_n$, there exists some $v \in \mathbb{Z}_n$ such that $u+v = 0_n = v+u$.]
  Let $u \in \mathbb{Z}_n$.
  There exists some $k \in \mathbb{Z}$ such that $u=[k]$. Note that $-k \in \mathbb{Z}$.
  Define $v=[-k]$. Then $u+v = [k]+[-k] = [k+(-k)] = [0] = 0_n$. Also, $v+u = \ldots = 0_n$. □

It follows that $(\mathbb{Z}_n, +)$ is an abelian group.

Corollary (6).

For any $u, v \in \mathbb{Z}_n$, there exists some unique $w \in \mathbb{Z}_n$ such that $u + w = v$.

Proof.

Let $u, v \in \mathbb{Z}_n$.

- [Existence argument.]

  By Theorem (5), there exists some $t \in \mathbb{Z}_n$ such that $u+t = 0_n = t+u$.
  Define $w = t+v$. By definition, $w \in \mathbb{Z}_n$.
  Then $u+w = u+(t+v) = (u+t)+v = 0_n + v = v$. □
  ([Theorem (5)] [Theorem (5)] [Theorem (5)])

- [Uniqueness argument.]

  Let $w, w' \in \mathbb{Z}_n$. Suppose $u+w = v$ and $u+w' = v$.
  Then $u+w = v = u+w'$.
  By Theorem (5), there exists some $t \in \mathbb{Z}_n$ such that $u+t = 0_n = t+u$.
  $w = 0_n + w = (t+u)+w = t+(u+w) = t+(u+w')$
  $= (t+u)+w'$
  $= 0_n + w' = w'$. □
  ([Theorem (5)])

Remark. Here we 'subtract u from v': w is the difference of v from u, and we write $w = v - u$. We write $0_n - u$ as $-u$; it is the unique (additive) inverse of u.

We want to define the function $\mu : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ through this declaration:
"Define $\mu : \mathbb{Z}_n^2 \to \mathbb{Z}_n$ by $\mu([k],[\ell]) = [k\ell]$ whenever $k, \ell \in \mathbb{Z}$."
But is this μ well-defined as a function?

7. **Theorem (7).**
Define

$$G_\mu = \left\{ ((u,v),w) \;\middle|\; \begin{array}{l} u,v,w \in \mathbb{Z}_n \text{ and} \\ \text{there exist } k,\ell \in \mathbb{Z} \text{ such that } u=[k], v=[\ell] \text{ and } w=[k\ell] \end{array} \right\}.$$

Define $\mu = (\mathbb{Z}_n{}^2, \mathbb{Z}_n, G_\mu)$.

μ is a function from $\mathbb{Z}_n{}^2$ to $\mathbb{Z}_n$.

Proof. Exercise. (Imitate the argument for Theorem (4).)

Remark. The function μ is called **multiplication in $\mathbb{Z}_n$** because of its resemblance with the function 'multiplication' for other more familiar mathematical objects, such as numbers and matrices.

From now on, we write $\mu(u,v)$ as $u \times v$, and call it the product of u, v.

By the definition of multiplication in $\mathbb{Z}_n$, whenever $k, \ell \in \mathbb{Z}$, we have $[k] \times [\ell] = \mu([k],[\ell]) = [k \times \ell]$

($[k] \times [\ell]$: this happens in $\mathbb{Z}_n$. $[k \times \ell]$: this happens in $\mathbb{Z}$.)

8. **Multiplication table for 'small' values of n:**

$[k] \times [l] = [k \cdot l]$

This happens in $\mathbb{Z}_n$. This happens in $\mathbb{Z}$.

Multiplication in $\mathbb{Z}_2$

$\times$	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Multiplication $\mathbb{Z}_3$

$\times$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Multiplication in $\mathbb{Z}_4$

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

Multiplication in $\mathbb{Z}_5$

$\times$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Multiplication in $\mathbb{Z}_6$

$\times$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

Multiplication in $\mathbb{Z}_7$

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

Multiplication table for 'small' values of n:

Multiplication in $\mathbb{Z}_8$

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

Multiplication in $\mathbb{Z}_9$

$\times$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[2]	[0]	[2]	[4]	[6]	[8]	[1]	[3]	[5]	[7]
[3]	[0]	[3]	[6]	[0]	[3]	[6]	[0]	[3]	[6]
[4]	[0]	[4]	[8]	[3]	[7]	[2]	[6]	[1]	[5]
[5]	[0]	[5]	[1]	[6]	[2]	[7]	[3]	[8]	[4]
[6]	[0]	[6]	[3]	[0]	[6]	[3]	[0]	[6]	[3]
[7]	[0]	[7]	[5]	[3]	[1]	[8]	[6]	[4]	[2]
[8]	[0]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

9. **Theorem (8).**

The following statements hold:

(a) *For any* $u, v \in \mathbb{Z}_n$, $u \times v = v \times u$.

(b) *For any* $u, v, w \in \mathbb{Z}_n$, $(u \times v) \times w = u \times (v \times w)$.

(c) *There exists some* $e \in \mathbb{Z}_n$, *namely* $e = [1]$, *such that* $e \times u = u \times e = u$.

(d) *For any* $u, v, w \in \mathbb{Z}_n$, $u \times (v+w) = (u \times v) + (u \times w)$ *and* $(u+v) \times w = (u \times w) + (v \times w)$.

Proof. Exercise. (Imitate the argument for Theorem (5).)

Remark on terminologies.

Because of Statement (c), it is natural for us to write $[1]$ as 1_n.

$(\mathbb{Z}_n, +, \times)$ is a **commutative rings with unity** with additive identity 0_n and multiplicative identity 1_n.

10. For the moment, assume n is a prime number. Write $n = p$.

Lemma (9).
For any $x \in \mathbb{Z}$, if x is not divisible by p then there exists some $y \in \mathbb{Z}$ such that $xy \equiv 1 (\mathsf{mod}\ p)$ and y is not divisible by p.

Theorem (10).
Let $u \in \mathbb{Z}_p$. Suppose $u \neq 0_p$.
Then there exists some unique $v \in \mathbb{Z}_p \backslash \{0_p\}$ such that $v \times u = u \times v = 1_p$.

Corollary (11).
Let $u, v \in \mathbb{Z}_p$. Suppose $u \neq 0_p$ and $v \neq 0_p$.
Then there exists some unique $w \in \mathbb{Z}_p \backslash \{0_p\}$ such that $u \times w = v$.

Remarks on terminologies.
$(\mathbb{Z}_p, +, \times)$ is a **field**.
$(\mathbb{Z}_p, +, \times)$ is a **finite field** .

As a consequence of Theorem (10), for any $s, t \in \mathbb{Z}_p$, if $s \times t = 0_p$ then $s = 0_p$ or $t = 0_p$. (Why? Exercise.)

11. What if n is definitely not a prime number?

Theorem (12).

Suppose n is not a prime number.

Then there exist some $u, v \in \mathbb{Z}_n \backslash \{0_n\}$ such that $u \times v = 0_n$.

Remark.

Such elements u, v of $\mathbb{Z}_n \backslash \{0_n\}$ which satisfy $u \times v = 0_n$ are called **zero divisors**.

12. The result below holds whether n is a prime number or not.

Theorem (13).

$\underbrace{1_n + 1_n + \cdots + 1_n}_{n \text{ times}} = 0_n$.

Proof.

By definition, $\underbrace{1_n + 1_n + \cdots + 1_n}_{n \text{ times}} = \underbrace{[1] + [1] + \cdots + [1]}_{n \text{ times}} = [\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}] = [n] = 0_n$.

Remark.

We do not obtain the integer 0 by adding up many copies of the integer 1 together.

The commutative ring with unity $(\mathbb{Z}_n, +, \times)$ is some mathematical object which possesses many properties common to $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, but which is **decisively different** from them. (*This is one of the starting points of MATH2070.*)