0. This is a continuation of the Handout *Integers modulo n*.

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

R_n is the equivalence relation in $\mathbb{Z}$ with graph $E_n = \{(x, y) \mid x, y \in \mathbb{Z} \text{ and } x \equiv y (\text{mod } n)\}$.

We call R_n the **congruence modulo n relation on $\mathbb{Z}$**.

Recall Lemma (1), Theorem (3) and terminologies associated to Theorem (3).

Lemma (1).

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

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

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

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

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

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

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

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**.

We are going to introduce two functions, called 'addition in $\mathbb{Z}_n$' and 'multiplication in $\mathbb{Z}_n$' respectively.

These two functions possess properties which are analogous to usual addition and usual multiplication for integers respectively.

'Addition in $\mathbb{Z}_n$' makes $\mathbb{Z}_n$ an abelian group.

'Addition in $\mathbb{Z}_n$' and 'multiplication in $\mathbb{Z}_n$' together maks $\mathbb{Z}_n$ a commutative ring with unity. For certain values of n, they in fact make $\mathbb{Z}_n$ a field.

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?

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

Then 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 exists some $w \in \mathbb{Z}_n$ such that $((u,v),w) \in G_\alpha$.]

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

There exist 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 $((u,v),w) \in G_\alpha$. $\square$

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

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?

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

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

Then 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 $\mathbb{Z}$.

2. **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 in $\mathbb{Z}_3$

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

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

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

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]

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

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

3. **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 $(u+v)+w = ([k]+[\ell])+[m] = [k+\ell]+[m]$

  $= [(k+\ell)+m] = [k+(\ell+m)] = \dots = u+(v+w)$. □

- [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 $u + v = [k]+[\ell] = [k+\ell] = [\ell+k] = \dots = v+u$. □

- [Existence of identity element?] [Check: There exits 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 exits some $k \in \mathbb{Z}$ such that $u = [k]$.

  Then $u + 0_n = [k]+[0] = [k+0] = [k] = u$. Also, $0_n + u = \dots = u$. □

- [Existence of inverse element?] [Check: For any $u \in \mathbb{Z}_n$, there exits some $v \in \mathbb{Z}_n$ such that $u+v = 0_n = v+u$.]

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

  There exits 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, $v+u = \dots = 0_n$. □

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

4. **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 $u+w = u+(t+v) \underset{[\text{Theorem (5)}]}{=} (u+t)+v \underset{[\text{Theorem (5)}]}{=} 0_n + v \underset{[\text{Theorem (5)}]}{=} v$. $\square$

- [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 $u+t = 0_n = t+u$.

$w = 0_n + w = (t+u)+w = t+(u+w) = t+(u+w')$
$= (t+u)+w'$
$= 0_n + w' = w'$. $\square$

[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?

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

Then 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 $[k] \times [\ell] = \mu([k],[\ell]) = [k \times \ell]$

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

6. **Multiplication table for 'small' values of n:** $[k] \times [\ell] = [k \cdot \ell]$

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 in $\mathbb{Z}_3$

$\times$	[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: $[k] \times [\ell] = [k \cdot \ell]$

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

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]

7. **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.

8. 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.)

9. 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**.

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

Theorem (13).

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

Proof.

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

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.*)