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

(b) *Define $E_n = \{(x, y) \mid x, y \in \mathbb{Z}$ and $x \equiv y(\text{mod } n)\}$, 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 $\mathbb{Z}$.

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 '$x \equiv y(\text{mod } n)$') as '*student x is in the same class as student y*'.

Now, for each student x, the set $[x]$ is the *set of all classmates of x in the school.* We expect the set $\mathbb{Z}_n$ to be the *set of all classes in the school*, (each class being a set of students).

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

(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 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.] By the Division Algorithm, there exist some (unique) $q, r \in \mathbb{Z}$ such that $x = qn + r$ and $0 \le r < n$. By definition, $r \in [\![0, n-1]\!]$. Also $x - r = qn$ for this $q \in \mathbb{Z}$. 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 $0 \le |s - t| \le n - 1 < n$. 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 $0, 1, \cdots, n-1$.

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) $u \cap v = \emptyset$.

   Proof.

   (0) Pick any $u \in \mathbb{Z}_n$. By definition, there exists some $x \in \mathbb{Z}$ such that $u = [x]$. By Lemma (2), for the same x there exists some $r \in [\![0, n-1]\!]$ such that $[x] = [r]$. Hence $u = [r]$.

   (1) Pick any $u \in \mathbb{Z}_n$. There exists some $x \in \mathbb{Z}$ such that $u = [x]$. Since $(x, x) \in E_n$, we have $x \in [x]$. 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 $U \subset \mathbb{Z}$.
   Pick any $x \in \mathbb{Z}$. We have $x \in [x]$ and $[x] \in \mathbb{Z}_n$. Hence $x \in U$. It follows that $\mathbb{Z} \subset U$.

   (3) Pick any $u, v \in \mathbb{Z}_n$. (A) Suppose $u = v$. Then $u \cap v = u \cap u = u \neq \emptyset$. (B) Suppose $u \cap v \neq \emptyset$. Pick some $z \in u \cap v$. Then $z \in u$ and $z \in v$. Therefore there exist some $x, y \in \mathbb{Z}$ such that $u = [x]$ and $v = [y]$. Since $z \in u = [x]$, we have $[z] = [x]$. Since $z \in v = [y]$, we have $[z] = [y]$. Then $u = [x] = [z] = [y] = v$.

   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. (There is no student-less class.)

   (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'.

   Remark on terminologies.

   (a) In light of Statement (1), Statement (2) and Statement (3) of Theorem (3), we say that $\mathbb{Z}$ 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) $\mathbb{Z}_n = \{[0], [1], \cdots, [n-2], [n-1]\}$ 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*).

4. **Theorem (4).**

   Define

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

   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?]
   Let $u, v \in \mathbb{Z}_n$. There exists some $k, \ell \in \mathbb{Z}$ such that $u = [k]$ and $v = [\ell]$. Take $w = [k + \ell]$. By definition, we have $((u, v), w) \in G_\alpha$.

   (U) [Is each 'input pair' 'assigned' to at most one 'output' by α?]
   Let $u, v, w, w' \in \mathbb{Z}_n$. Suppose $((u, v), w) \in G_\alpha$ and $((u, v), w') \in G_\alpha$. There exist some $k, \ell \in \mathbb{Z}$ such that $u = [k]$, $v = [\ell]$ and $w = [k + \ell]$. There exist some $k', \ell' \in \mathbb{Z}$ such that $u = [k']$, $v = [\ell']$ and $w = [k' + \ell']$.
   Since $[k] = u = [k']$, we have $k \equiv k' (\mathsf{mod}\ n)$. Since $[\ell] = v = [\ell']$, we have $\ell \equiv \ell' (\mathsf{mod}\ n)$.
   $k - k'$, $\ell - \ell'$ are divisible by n. Then $(k + \ell) - (k' + \ell') = (k - k') + (\ell - \ell')$ is divisible by n. Therefore $k + \ell \equiv k' + \ell' (\mathsf{mod}\ n)$. Hence $w = [k + \ell] = [k' + \ell'] = w'$.

   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.

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

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 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. Refer to the Handout *Groups*.

Theorem (5).

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

Proof.

- [Associativity?]
  Let $u, v, w \in \mathbb{Z}_n$. There exist some $k, \ell, m \in \mathbb{Z}$ such that $u = [k], v = [\ell], w = [m]$. We have $(u + v) + w = ([k] + [\ell]) + [m] = [k + \ell] + [m] = [(k + \ell) + m] = [k + (\ell + m)] = [k] + [\ell + m] = [k] + ([\ell] + [m]) = u + (v + w)$.
- [Commutativity?]
  Let $u, v \in \mathbb{Z}_n$. There exist some $k, \ell \in \mathbb{Z}$ such that $u = [k], v = [\ell]$. We have $u + v = [k] + [\ell] = [k + \ell] = [\ell + k] = [\ell] + [k] = v + u$.
- [Existence of identity element?]
  Write $0_n = [0]$. Let $u \in \mathbb{Z}_n$. There exists some $k \in \mathbb{Z}$ such that $u = [k]$. We have $0_n + u = [0] + [k] = [0 + k] = [k] = u$, and $u + 0_n = 0_n + u = u$.
- [Existence of inverse element?]
  Let $u \in \mathbb{Z}_n$. There exists some $k \in \mathbb{Z}$ such that $u = [k]$. Take $v = [-k]$. We have $u + v = [k] + [-k] = [k + (-k)] = [0] = 0_n$, and $v + u = u + v = 0_n$.

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.]
  There exist some $k, \ell \in \mathbb{Z}$ such that $u = [k]$, $v = [\ell]$. Take $w = [\ell - k]$. We have $u + w = [k] + [\ell - k] = [k + \ell - k] = [\ell] = v$.
- [Uniqueness argument.]
  Let $w, w' \in \mathbb{Z}_n$. Suppose $u + w = v$ and $u + w' = v$. There exists some $t \in \mathbb{Z}_n$ such that $t + u = 0_n$. Now we have $w = 0_n + w = (t + u) + w = t + (u + w) = t + v = t + (u + w') = (t + u) + w' = 0_n + w' = w'$.

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.

7. **Theorem (7).**

Define

$$G_\mu = \{((u, v), w) \mid u, v, w \in \mathbb{Z}_n \text{ and there exist } k, \ell \in \mathbb{Z} \text{ such that } u = [k], v = [\ell] \text{ and } w = [k\ell]\}.$$

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.

Note that $G_\mu \subset ({\mathbb{Z}_n}^2) \times \mathbb{Z}_n$. Hence μ 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 μ?]
Let $u, v \in \mathbb{Z}_n$. There exists some $k, \ell \in \mathbb{Z}$ such that $u = [k]$ and $v = [\ell]$. Take $w = [k\ell]$. By definition, we have $((u, v), w) \in G_\mu$.

(U) [Is each 'input pair' 'assigned' to at most one 'output' by μ?]
Let $u, v, w, w' \in \mathbb{Z}_n$. Suppose $((u, v), w) \in G_\mu$ and $((u, v), w') \in G_\mu$. There exist some $k, \ell \in \mathbb{Z}$ such that $u = [k]$, $v = [\ell]$ and $w = [k\ell]$. There exist some $k', \ell' \in \mathbb{Z}$ such that $u = [k']$, $v = [\ell']$ and $w = [k'\ell']$.
Since $[k] = u = [k']$, we have $k \equiv k' (\text{mod } n)$. Since $[\ell] = v = [\ell']$, we have $\ell \equiv \ell' (\text{mod } n)$.
$k - k'$, $\ell - \ell'$ are divisible by n. Then $k\ell - k'\ell' = (k - k')\ell + k'(\ell - \ell')$ is divisible by n. Therefore $k\ell \equiv k'\ell' (\text{mod } n)$.
Hence $w = [k\ell] = [k'\ell'] = w'$.

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

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.

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

Multiplication in $\mathbb{Z}_2$

×	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

Multiplication in $\mathbb{Z}_3$

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Multiplication in $\mathbb{Z}_4$

×	[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 $\mathbb{Z}_5$

×	[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 $\mathbb{Z}_6$

×	[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 $\mathbb{Z}_7$

×	[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 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.

(a) Let $u, v \in \mathbb{Z}_n$. There exist some $k, \ell \in \mathbb{Z}$ such that $u = [k], v = [\ell]$. We have $u \times v = [k] \times [\ell] = [k\ell] = [\ell k] = [\ell] \times [k] = v \times u$.

(b) Let $u, v, w \in \mathbb{Z}_n$. There exist some $k, \ell, m \in \mathbb{Z}$ such that $u = [k], v = [\ell], w = [m]$. We have $(u \times v) \times w = ([k] \times [\ell]) \times [m] = [k\ell] \times [m] = [(k\ell)m] = [k(\ell m)] = [k] \times [\ell m] = [k] \times ([\ell] \times [m]) = u \times (v \times w)$.

(c) Note that $[1] \in \mathbb{Z}_n$.

Pick any $u \in \mathbb{Z}_n$. There exists some $k \in \mathbb{Z}$ such that $u = [k]$. We have $[1] \times u = [1] \times [k] = [1 \cdot k] = [k] = u$ and $u \times [1] = [1] \times u = u$.

(d) Let $u, v, w \in \mathbb{Z}_n$. There exist some $k, \ell, m \in \mathbb{Z}$ such that $u = [k], v = [\ell], w = [m]$.

We have $u \times (v + w) = [k] \times ([\ell] + [m]) = [k] \times [\ell + m] = [k(\ell + m)] = [k\ell + km] = [k\ell] + [km] = ([k] \times [\ell]) + ([k] \times [m]) = (u \times v) + (u \times w)$.

Also, $(u + v) \times w = w \times (u + v) = (w \times u) + (w \times v) = (u \times w) + (v \times w)$.

Remark on terminologies.

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

By virtue of Theorem (4), Theorem (5), Theorem (7) and Theorem (8), we refer to $(\mathbb{Z}_n, +, \times)$ as 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.

Proof.

Pick any $x \in \mathbb{Z}$. Suppose x is not divisible by p. Then $\gcd(x, p) = 1$. By Bezôut's Identity, there exist some $y, t \in \mathbb{Z}$ such that $yx + tp = 1$. We have $xy - 1 = tp$. Then $xy - 1$ is divisible by p. Therefore $xy \equiv 1 (\mathsf{mod}\ p)$.

We verify that y is not divisible by p.

- Suppose it were true that y was divisible by p. Then there would exist some $s \in \mathbb{Z}$ such that $y = sp$. We would have $(sx + t)p = yx + tp = 1$. Therefore 1 would be divisible by p. Contradiction arises.

  Hence y is not divisible by p in the first place.

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 $v \times u = u \times v = 1_p$.

Proof.

Let $u \in \mathbb{Z}_p$. Suppose $u \neq 0_p$.

There exists some $k \in \mathbb{Z}$ such that $u = [k]$. Since $u \neq 0_p$, we have $k \notin [0]$. Therefore k is not divisible by p. (Why?)

Now there exists some $\ell \in \mathbb{Z}$ such that $k\ell \equiv 1 (\text{mod } p)$ and ℓ is not divisible by p.

Take $v = [\ell]$. Since ℓ is not divisible by p, we have $v \neq 0_p$. We have $u \times v = [k] \times [\ell] = [k\ell] = [1] = 1_p$. Also $v \times u = u \times v = 1_p$.

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 $u \times w = v$.

Proof.

Let $u, v \in \mathbb{Z}_p$. Suppose $u \neq 0_p$ and $v \neq 0_p$.

- [Existence argument.]
  There exists some $\tilde{u} \in \mathbb{Z}_p \backslash \{0_p\}$ such that $u \times \tilde{u} = \tilde{u} \times u = 1_p$.
  Take $w = \tilde{u} \times u$. We have $u \times w = u \times (\tilde{u} \times v) = (u \times \tilde{u}) \times v = 1_p \times v = v$.
  We verify that $w \neq 0_p$:
  - Suppose it were true that $w = 0_p$.
    There exists some $k \in \mathbb{Z}_p$ such that $u = [k]$. Now we would have $v = u \times w = [k] \times [0] = [k \times 0] = [0] = 0_p$.
    But $v \neq 0_p$. Contradiction arises.
    Hence $w \neq 0_p$ in the first place.
- [Uniqueness argument.]
  Let $w, w' \in \mathbb{Z}_p \backslash \{0_p\}$. Suppose $u \times w = v$ and $u \times w' = v$. Then $u \times w = u \times w'$.
  There exist some $k, m, m' \in \mathbb{Z}$ such that $u = [k]$, $w = [m]$ and $w' = [m']$. Now $[km] = [k] \times [m] = [k] \times [m'] = [km']$. Then $km \equiv km' (\text{mod } p)$. Therefore $k(m - m') \equiv 0 (\text{mod } p)$. $k(m - m')$ is divisible by p.
  Recall that $u \neq 0_p$. Then k is not divisible by p. By Euclid's Lemma, $m - m'$ is divisible by p. Therefore $m \equiv m' (\text{mod } p)$. Hence $w = [m] = [m'] = w'$.

Remark on terminologies.

By virtue of Theorem (10), we refer to $(\mathbb{Z}_p, +, \times)$ as a **field**. Because $\mathbb{Z}_p$ has only finitely many elements, $(\mathbb{Z}_p, +, \times)$ is a **finite field**, in contrast to 'infinite' fields like $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ and $(\mathbb{C}, +, \times)$.

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 $u \times v = 0_n$.

Proof.

Suppose n is not a prime number. Then there exists some positive integers h, k such that $1 < h < n$ and $1 < k < n$ and $hk = n$. By the definition of multiplication in $\mathbb{Z}_n$, we have $[h] \times [k] = [n] = 0_n$. But since $1 < h < n$ and $1 < k < n$, we also have $[h] \neq 0_n$ and $[k] \neq 0_n$.

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.*)