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) $\{x \in \mathbb{Z} : x \in u$ *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) 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**.

   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.

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

   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 $k \equiv k'(\text{mod } n)$. Since $[\ell] = v = [\ell']$, we have $\ell \equiv \ell'(\text{mod } n)$.

   $k - k'$, $\ell - \ell'$ are divisible by n. Then $(k + \ell) - (k' + \ell') = (k - k') + (\ell - \ell')$ is divisible by n. Therefore $k + \ell \equiv k' + \ell'(\text{mod } n)$. 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.

2. **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]

3. Refer to the Handout *Abelian groups, integral domains and fields.*

   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.

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.]
     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.

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

6. **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 $\mathbb{Z}_8$

×	[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 $\mathbb{Z}_9$

×	[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.

(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.

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* $xy \equiv 1(\text{mod } p)$ *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 $xy \equiv 1(\text{mod } p)$.

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 $(\mathbb{C}, +, \times)$.

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 $u \times v = 0_n$.

   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**.

10. 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.*)