MATH1050 Integers modulo n

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 $\mathbb{Z}$.

   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*'.

   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) $x \equiv y(\mathsf{mod}\ n)$.
   (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 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) $\{x \in \mathbb{Z} : x \in u \text{ for some } u \in \mathbb{Z}_n\} = \mathbb{Z}$.

(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 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 ones in the Handout *Arithmetic in Integers modulo n*) in advanced courses (for example, *algebra* and *topology*).