1. $\mathbb{Z}/n\mathbb{Z}$: The integers modulo n

Definition 1.1 (Equivalence relation)**.** Let X and Y be sets. A **relation** from X to Y is a subset $R \subseteq X \times Y$. If $X = Y$, we say R is a relation *on* X.

Alternative ways to denote the statement $(x, y) \in R$ are

$$xRy, \qquad x \equiv y \mod R, \qquad x \equiv_R y, \qquad x \sim y.$$

Note the last one is the exactly the same as the first, but the symbol $\sim$ has be chosen instead.

Definition 1.2. A **partition** of a set X is a subset $P \subseteq \mathcal{P}(X)$ such that

(i) $X = \bigcup_{A \in P} A$, and

(ii) if $A, B \in P$, then $A \cap B = \varnothing$.

Basically, a partition of a set X is a cover of X by pairwise disjoint sets. Let us present some of the most basic types relations you will encounter in your studies.

Definition 1.3. Let $\sim$ be a relation on a set X. Then

(i) $\sim$ is **reflexive** iff $x \sim x$ for all $x \in X$.

(ii) $\sim$ is **symmetric** iff $x \sim y$ implies $y \sim x$ for all $x, y \in X$.

(iii) $\sim$ is **transitive** iff $x \sim y$ and $y \sim z$ imply $x \sim z$ for all $x, y, z \in X$.

(iv) $\sim$ is an **equivalence relation** on X iff $\sim$ is reflexive, symmetric, and transitive.

Exercise 1. Let $X = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$ and

$$\sim \; = \{((a, b), (c, d)) \in X^2 \mid ad = bc\}.$$

Prove $\sim$ is an equivalence relation on X. How does this relates to the equality of two rational numbers?

Definition 1.4. Let $\sim$ be an equivalence relation on a set X. The **equivalence class** of an element $x \in X$ under $\sim$ is the set

$$\{x' \in X \mid x \sim x'\}$$

denoted by $[x]_\sim$ or simply $[x]$ if $\sim$ is understood from the context. An element of $[x]_\sim$ is said to be equivalent to x. If $x' \in [x]_\sim$, we say x' is a representative of $[x]_\sim$.

Any element of a class can be used as a representative of such class. Evidently, $x \in [x]$ for any x. There is nothing special about the particular element chosen as its representative.

Exercise 2. Let $\sim$ be an equivalence relation on a set X.

(i) Prove

$$x \sim y \iff [x] = [y] \iff [x] \cap [y] \neq \varnothing,$$

for any $x, y \in X$.

(ii) Prove

$$\bigcup_{a \in X} [a] = X \quad \text{and} \quad [x] \cap [y] = \varnothing$$

whenever $x \not\sim y$.

The last exercise shows that an equivalence relation on a set gives rise to a partition of such a set. The elements of this partition are precisely the equivalence classes induced by the equivalence relation. Conversely, any partition induces an equivalence relation in a natural way. Prove this assertion.

Definition 1.5. Let $\sim$ be an equivalence relation on a set X. The **quotient set** of X by $\sim$ is the set

$$\{[x] : x \in X\},$$

denoted $X/\sim$.

Example 1. In Exercise 1. we saw the relation $\sim$ on $\mathbb{Z}^2$ defined by

$$(a, b) \sim (c, d) \iff ad = bc$$

is an equivalence relation on $\mathbb{Z}^2$. It turns out $\mathbb{Q} = \mathbb{Z}^2/\sim$. In other words, the rational numbers can be constructed from integers by means of $\sim$.[1]

1.1. The integers mod n

Fix $n \in \mathbb{Z}^+$. The relation on $\mathbb{Z}$ defined by

$$a \sim_n b \iff n \mid (b - a)$$

is an equivalence relation on $\mathbb{Z}$. We write $a \equiv b \bmod n$ whenever $a \sim_n b$. The equivalence class of an integer a under $\sim_n$ is denoted $\overline{a}$ and it is called the congruence class of a mod n.

Definition 1.6. The set of integers modulo n is the set of congruence classes of $\mathbb{Z}$ under $\sim_n$. It is denoted $\mathbb{Z}/n\mathbb{Z}$.

You will see why we have chosen this notation when we discuss ideals in ring theory. By definition,

$$\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}.$$

Make sure you understand why this is true. There are exactly n congruence classes, namely $[0], [1], \ldots, [n-1]$. Why $[0] = [n]$?

[1] Actually, there may be more than one way to build the rational numbers, but whatever the way we chose to do so, we always end up with a set isomorphic to $\mathbb{Z}^2/\sim$.

Exercise 3. Prove or disprove $\mathbb{Z}/n\mathbb{Z} \subseteq \mathbb{Z}/m\mathbb{Z}$ for integers $n < m$. Find a necessary and sufficient condition on m and n so that $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$.

Note there is always a smallest nonnegative integer contained in $[k]$. In order to find such representative, we use the division algorithm. Recall n is fixed. There are integers $q, r \in \mathbb{Z}$ such that

$$k = nq + r \qquad \text{with } 0 \leq r < n.$$

Then $nq = k - r$, and so $n \mid k - r$. Therefore $\overline{k} = \overline{r}$.

Exercise 4. List all the elements of $\mathbb{Z}/4\mathbb{Z}$.

1.2. Modular operations in $\mathbb{Z}/n\mathbb{Z}$

There are two basic operations we can do in $\mathbb{Z}$, namely add and multiply integers. Based up on these operations we can endow $\mathbb{Z}/n\mathbb{Z}$ with an addition and a multiplication too. Define $+, \cdot \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

for any $a, b \in \mathbb{Z}$. Note, for instance, the sum of the congruence classes two integers is the congruence class of their sum. Likewise for the multiplication.

Theorem 1.7. *The binary operations $+$ and $\cdot$ are well-defined. More precisely, If $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then*

$$\overline{a} + \overline{b} = \overline{a'} + \overline{b'} \quad \textit{and} \quad \overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}.$$

Proof. Classwork. □

Example 2. In $\mathbb{Z}/2\mathbb{Z}$, we have $\overline{1} + \overline{1} = \overline{0}$. In $\mathbb{Z}/5\mathbb{Z}$, $\overline{3} \cdot \overline{4} = \overline{2}$. In $\mathbb{Z}/20\mathbb{Z}$, $\left(\overline{8} + \overline{2}\right) \cdot \overline{3} = \overline{10}$.

1.3. An application in number theory

Let us see how to compute the last two digits of 9^{1500}, using the modular operations we have defined. The key observation to make is that computing the last two digits of an integer corresponds to computing its residue after division by 100. (Why?)

We have

$$\begin{aligned}
9 &\cong 9 \mod 100 & 9^6 &\cong 41 \mod 100 \\
9^2 &\cong 81 \mod 100 & 9^7 &\cong 69 \mod 100 \\
9^3 &\cong 29 \mod 100 & 9^8 &\cong 21 \mod 100 \\
9^4 &\cong 61 \mod 100 & 9^9 &\cong 89 \mod 100 \\
9^5 &\cong 49 \mod 100 & 9^{10} &\cong 1 \mod 100
\end{aligned}$$

Each computation is based on the previous line, after multiplying by 9. Finally, note that

$$9^{1500} \cong (9^{10})^{150} \cong 1 \mod 100.$$

Thus, the last two digits of 9^{1500} are 01.

1.4. The units of $\mathbb{Z}/n\mathbb{Z}$

The congruence classes mod$n$ that have a *multiplicative inverse*[2] is called the set of units of $\mathbb{Z}/n\mathbb{Z}$. It is defined by

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{a \in \mathbb{Z}/n\mathbb{Z} \mid a \cdot b = 1 \text{ for some } c \in \mathbb{Z}/n\mathbb{Z}\}.$$

Exercise 5. Prove

(i) $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under $\cdot$.

(ii) $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$.

(iii) $\text{card}(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$ (Recall φ is Euler's totient function.)

Example 3. Let us compute the multiplicative inverse of 3 in $(\mathbb{Z}/10\mathbb{Z})^\times$. We know 3 and 10 only share 1 as positive common divisor, so they are coprime. This guarantees that 3 indeed has a multiplicative inverse in $(\mathbb{Z}/10\mathbb{Z})^\times$. In order to compute its multiplicative inverse, we use the Euclidean algorithm. Note $10 = 3 \cdot 3 + 1$, so $10 - 3 \cdot 3 = 1$. Then, since $\overline{10} = \overline{0}$, taking congruence class mod10, we have $\overline{-3} \cdot \overline{3} = \overline{1}$. Thus $\overline{-3}$ is the inverse of $\overline{3}$. To find the smallest positive representative of $\overline{-3}$ we simply add $\overline{0}$ as many times as needed:

$$\overline{-3} = \overline{-3} + \overline{10} = \overline{7}.$$

Therefore $\overline{3} \cdot \overline{7} = \overline{1}$.

Exercise 6. (i) Show $(\mathbb{Z}/10\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

(ii) Compute $(\mathbb{Z}/7\mathbb{Z})^\times$.

[2] We will define precisely what we mean by a multiplicative inverse when we arrive at group theory.