Part IV

Modular World and Modular Dynamics

Congruence and modulus

Definition 4.1.1

Let m be a positive integer (called the *modulus*). We say two integers a and b are *congruent modulo* m, written as

$$a \equiv b \pmod{m},$$

if $m \mid a - b$.

Theorem 4.1.2

Fix a modulus m. "Being congruent module m" is an equivalence relation on $\mathbb{Z}$. Namely,

- *(reflexivity) for all integer $a \in \mathbb{Z}$, $a \equiv a \pmod{m}$;*
- *(symmetry) for all integers $a, b \in \mathbb{Z}$, if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;*
- *(transitivity) for all integers $a, b, c \in \mathbb{Z}$, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*

Definition 4.1.3

For any integer $a \in \mathbb{Z}$, the set of integers congruent to a modulo m is called the *congruence class (modulo m)* with *representative* a, written as $[a]_m$, or simply $[a]$ or $\bar{a}$ if the modulus m is clear.

Definition 4.1.3

For any integer $a \in \mathbb{Z}$, the set of integers congruent to a modulo m is called the *congruence class (modulo m)* with *representative* a, written as $[a]_m$, or simply $[a]$ or $\bar{a}$ if the modulus m is clear.

Example 4.1.4

Take 2 to be the modulus. $[0]_2$ is the set of even numbers, while $[1]_2$ is the set of odd numbers.

Definition 4.1.5

The *residue set modulo* m, written as $\mathbb{Z}/m$, is the quotient set of $\mathbb{Z}$ up to congruence modulo m. Namely, $\mathbb{Z}/m$ is the set of congruence classes modulo m.

Definition 4.1.5

The *residue set modulo* m, written as $\mathbb{Z}/m$, is the quotient set of $\mathbb{Z}$ up to congruence modulo m. Namely, $\mathbb{Z}/m$ is the set of congruence classes modulo m.

A priori, every integer defines a congruence class. But many of them turn out to be the same.

Example 4.1.6

It turns out that $\mathbb{Z}/2$ consists of only two classes: $[0]_2$, the even numbers, and $[1]_2$, the odd numbers.

Definition 4.1.7

Let x be an integer and m be a modulus.
The *natural representative of* x *modulo* m is the remainder r left under the division

$$x = q \cdot m + r, \quad 0 \leqslant r < m, \quad q \in \mathbb{Z}.$$

Definition 4.1.7

Let x be an integer and m be a modulus.
The *natural representative of* x *modulo* m is the remainder r left under the division

$$x = q \cdot m + r, \quad 0 \leqslant r < m, \quad q \in \mathbb{Z}.$$

Example 4.1.8

- The natural representative of $1234567 \pmod{10}$ is 7.
- The natural representative of $7^{2023} \pmod{2}$ is 1.

Definition 4.1.7

Let x be an integer and m be a modulus.
The *natural representative of* x *modulo* m is the remainder r left under the division

$$x = q \cdot m + r, \quad 0 \leqslant r < m, \quad q \in \mathbb{Z}.$$

Note that $x \equiv r \pmod{m}$. Hence, $[r]_m = [x]_m$. Namely, r is a representative of the congruence class $[x]_m$. Moreover, the natural representative depends only on the congruence class $[x]_m$, rather than the integer x.

Theorem 4.1.8

The set $\mathbb{Z}/m$ is finite. In fact, it is bijective to the set of remainders dividing m: $\{0, \cdots, m-1\}$.

Proof. The following process gives a bijection from $\mathbb{Z}/m$ to $\{0, \cdots, m-1\}$: for any congruence class $[x]_m$, take the natural representative r of it. $\square$