

## 0.1 Congruence relation (an equivalence relation)

two integers  $a$  and  $b$  are congruent modulo  $n$ :  $a \equiv b \pmod{n}$ , with  $(a - b)/n = z$ , where  $z \in \mathbb{Z}$ .  $n$  is the “modulus” of the congruence (imagine a clock, 12 is the modulus).

## 0.2 Congruence classes (the equivalence class)

The equivalent class of the integer  $a$  is  $\bar{a}_n := \{\dots, a - 2n, a - n, a, a + n, a + 2n, \dots\}$ .

## 0.3 Integers modulo $n$

**Def:** The set of all congruence classes of the integers for a modulus  $n$

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a}_n | a \in \mathbb{Z}\}. \quad (1)$$

When  $n \neq 0$

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}_n, \bar{1}_n, \dots, \overline{n-1}_n\}. \quad (2)$$

When  $n = 0$ ,  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to  $\mathbb{Z}$ .