

## Definition

We denote by  $\mathbb{Z}_n$  the set  $Z / \sim_n$ , i.e. the set of equivalence classes under  $\sim_n$ .

There are  $n$  equivalence classes:

$$[0], [1], [2], \dots, [n-1]. \quad (1)$$

## Definition

Let us define two operations on  $\mathbb{Z}_n$ ,  $+_n$  and  $*_n$ :

$$[x] +_n [y] = [x + y], \quad [x] *_n [y] = [xy].$$