Integers modulo *n*

Peter Mayr

CU, Discrete Math, April 6, 2020

One important equivalence relation is $\equiv_n$ on $\mathbb{Z}$ for $n \in \mathbb{N}, n > 1$.

Example

The equivalence classes of $\equiv_3$ are

$$\begin{aligned}
[0] &= \{\dots, -3, 0, 3, \dots\} = \{\quad 3z \ : \ z \in \mathbb{Z}\} \\
[1] &= \{\dots, -2, 1, 4, \dots\} = \{1 + 3z \ : \ z \in \mathbb{Z}\} \\
[2] &= \{\dots, -1, 2, 5, \dots\} = \{2 + 3z \ : \ z \in \mathbb{Z}\}
\end{aligned}$$

Note $[0] = [3]$, etc.

Definition

For $n \in \mathbb{N}, n > 1$, the class of $a \in \mathbb{Z}$ modulo n is

$$[a]_n = \{a + zn \ : \ z \in \mathbb{Z}\}.$$

The set of classes

$$\mathbb{Z}_n := \{[0], [1], [2], \dots, [n-1]\}$$

is called the **integers modulo** n.

Computing in $\mathbb{Z}_n$

Define $+, -, \cdot$ on $\mathbb{Z}_n$ by

$$\begin{aligned} [a] + [b] &:= [a + b] \\ -[a] &:= [-a] \\ [a] \cdot [b] &:= [a \cdot b] \end{aligned}$$

Note

These operations are defined via representatives (elements) of classes. But each class has different elements to choose from to do the computation, e.g., in $\mathbb{Z}_3$:

$$[5] = [2], [11] = [2] \quad \text{so} \quad \underbrace{[5] \cdot [11]}_{=[55]} = \underbrace{[2] \cdot [2]}_{[4]}$$

Are the results the same? Yes, $[55] = [1] = [4]$.

Is the result independent of the choice of representatives?

Let $a, b, c, d \in \mathbb{Z}$ such that

$$[a]_n = [c]_n,\ [b]_n = [d]_n$$

We want to show that $[a+b]_n = [c+d]_n$.

Proof.

By assumption $a \equiv_n c, b \equiv_n d$. By a previous Lemma

$$a + b \equiv_n c + d$$
$$ab \equiv_n cd$$

Thus $[a+b]_n = [c+d]_n,\ [ab]_n = [cd]_n$. □

We say the operations $+, \cdot$ on $\mathbb{Z}_n$ are **well-defined** (independent of the choice of representatives for each class).

Theorem

$+, -, \cdot$ on $\mathbb{Z}_n$ for $n > 1$ satisfy the same laws as $+, -, \cdot$ on $\mathbb{Z}$: associativity, commutativity, distributivity, etc.

Proof idea.

This follows since the operations on $\mathbb{Z}_n$ are defined in terms of those on $\mathbb{Z}$.
E.g. to show that $+$ on $\mathbb{Z}_n$ is commutative, consider

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

$\square$

Sometimes one can even divide in $\mathbb{Z}_n$. See HW.

Operation tables on $\mathbb{Z}_4$

To ease notation we drop the brackets [.] for classes and write 0 for [0].
$+, \cdot$ on $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ are represented in the following tables.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1