# Somma e prodotto di classi di resto

Leonardo Bizzoni

October 19, 2023

Siano $[a]_n, [b]_n \in \mathbb{Z}_n$ 2 classi di equivalenza modulo $n$.
Poniamo:

- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n * [b]_n = [ab]_n$

## 1 Esempi

$[1]_5 + [3]_5 = [4]_5$
$[2]_5 + [3]_5 = ([5]_5 = [0]_5)$
$[2]_5 * [3]_5 = ([6]_5 = [1]_5)$

## 2 Proprietà $(\mathbb{Z}_n,\ +)$

- Associativa: $\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ si ha che:

$$([a]_n + [b]_n) + [c]_n = [(a+b)+c]_n = [a+(b+c)]_n = [a]_n + ([b]_n + [c]_n)$$

- Commutativa: $\forall [a]_n, [b]_n \in \mathbb{Z}_n$ si ha che:

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

- **Elemento neutro** $[0]_n$ per la definizione di somma
- **Inverso**: $\forall [a]_n \in \mathbb{Z} \mid \exists [n-a]_n \in \mathbb{Z}_n$ tale che:

$$[a]_n + [n-a]_n = [0]_n$$

$(\mathbb{Z}_n,\ +)$ è quindi un gruppo abeliano/commutativo.

## 3 Proprietà $(\mathbb{Z}_n,\ *)$

- Associativa: $\forall [a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ si ha che:

$$([a]_n * [b]_n) * [c]_n = [(ab)c]_n = [a(bc)]_n = [a]_n * ([b]_n * [c]_n)$$

- Commutativa: $\forall [a]_n, [b]_n \in \mathbb{Z}_n$ si ha che:

$$[a]_n * [b]_n = [b]_n * [a]_n$$

- **Elemento neutro** $[1]_n$ per la definizione di prodotto

$(\mathbb{Z}_n,\ *)$ è quindi un monoide abeliano/commutativo.