ARITMETICA MODULARE (II PARTE)

Proprietà dell'addizione in $\mathbb{Z}_N$ $(N \in \mathbb{N},\ N \geq 2)$.

- <u>ASSOCIATIVA</u>: $\forall\, \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_N \quad (\bar{a}+\bar{b})+\bar{c} = \bar{a}+(\bar{b}+\bar{c})$

  Infatti: $(\bar{a}+\bar{b})+\bar{c} = (\overline{a+b})+\bar{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \bar{a}+(\overline{b+c}) = \bar{a}+(\bar{b}+\bar{c})$

  addizione in $\mathbb{Z}_N$ — addizione in $\mathbb{Z}$ — perché in $\mathbb{Z}$ + è associativa

- <u>EL. NEUTRO</u>: $\forall\, \bar{a} \in \mathbb{Z}_N : \quad \bar{0}+\bar{a} = \bar{a}$ infatti $\bar{0}+\bar{a} = \overline{0+a} = \bar{a}$.

  0 neutro in $\mathbb{Z}$

- <u>COMMUTATIVA</u>: $\forall\, \bar{a}, \bar{b} \in \mathbb{Z}_N : \quad \bar{a}+\bar{b} = \bar{b}+\bar{a}$ infatti $\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a}$.

- <u>OPPOSTO</u>: $\forall\, \bar{a} \in \mathbb{Z}_N \ \exists\, \bar{b} \in \mathbb{Z}_N$ t.c. $\bar{a}+\bar{b} = \bar{0}$ infatti basta prendere $\bar{b} = \overline{-a}$

  e allora $\bar{a}+\overline{-a} = \overline{a-a} = \bar{0}$

<u>Esempio</u>: $\mathbb{Z}_{12}$. Consideriamo $\bar{7}$. Il suo opposto è $\overline{-7} = \bar{5}$.

Infatti $7+5 = 12 \Rightarrow 7+5 \equiv 0 \mod 12 \Rightarrow \bar{7}+\bar{5} = \bar{0}$

Costruiamo la tabella additiva di $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$:

in $\mathbb{Z}_4$

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

ci dice che $\bar{1} + \bar{3} = \bar{0}$ in $\mathbb{Z}_4$

cioè $\bar{3} = -\bar{1}$ in $\mathbb{Z}_4$

Generatori

Es: $\bar{1}$ "genera additivamente" tutto $\mathbb{Z}_N$, infatti $\forall \bar{r} \in \mathbb{Z}_N$ $(0 \le r < N)$ $\bar{r} = \underbrace{\bar{1} + \bar{1} + \bar{1} + \ldots + \bar{1}}_{r \text{ volte}}$

ogni elemento di $\mathbb{Z}_N$ è un multiplo di $\bar{1}$.

Ma non tutti gli elementi di $\mathbb{Z}_N$ lo generano additivamente:

Es: $\bar{2}$ in $\mathbb{Z}_4$: $\bar{2} + \bar{2} = \bar{0}$, $\bar{2} + \bar{2} + \bar{2} = \bar{2}$, $\bar{2} + \bar{2} + \bar{2} + \bar{2} = \bar{0}$ ....

Prop: $\bar{a}$ genera additivamente $\mathbb{Z}_N \iff MCD(a, N) = 1$.

dim: "$\Rightarrow$" Se $\bar{a}$ genera $\mathbb{Z}_N \Rightarrow \exists k$ t.c. $\underbrace{\bar{a} + \bar{a} + \ldots + \bar{a}}_{k \text{ volte}} = \bar{1}$, cioè $\overline{a + a + a + \ldots + a} = \bar{1}$

ma allora $(a + a + a + \ldots + a) - 1 = h \cdot N$ (per un certo $h \in \mathbb{Z}$) $\Rightarrow k \cdot a - h \cdot N = 1$

per l'identità di Bézout, ciò succede solo se $MCD(a, N) = 1$.

"$\Leftarrow$" Se $MCD(a, N) = 1$, per Bézout $\exists x, y \in \mathbb{Z}$ t.c. $ax + Ny = 1$ $\Rightarrow ax \equiv 1 \mod N \Rightarrow \overbrace{\bar{a} + \ldots + \bar{a}}^{x \text{ volte}} = \bar{1}$.

Moltiplicazione in $\mathbb{Z}_N$:

$$\begin{array}{ccc} \mathbb{Z}_N \times \mathbb{Z}_N & \longrightarrow & \mathbb{Z}_N \\ (\bar{a}, \bar{b}) & \longmapsto & \bar{a} \cdot \bar{b} := \overline{ab} \end{array}$$

Mostriamo che è ben definita:

Siano $a, a', b, b' \in \mathbb{Z}$ t.c. $\bar{a} \overset{(1)}{=} \bar{a}'$, $\bar{b} \overset{(2)}{=} \bar{b}'$ in $\mathbb{Z}_N$. Vogliamo mostrare che $\bar{a} \cdot \bar{b} = \bar{a}' \cdot \bar{b}'$

$$\left.\begin{array}{l} (1)\ \exists h \in \mathbb{Z} \text{ t.c. } a - a' = h \cdot N \\ (2)\ \exists k \in \mathbb{Z} \text{ t.c. } b - b' = k \cdot N \end{array}\right\} \Rightarrow a \cdot b = (a' + hN)(b' + kN) = a'b' + a'kN + b'hN + hkN^2$$

$$= a'b' + N \cdot (a'k + b'h + hkN)$$

$$\Rightarrow ab - a'b' = N(a'k + b'h + hkN) \text{ cioè } ab \equiv a'b' \bmod N.$$

Es: $\mathbb{Z}_7$ $\quad \bar{3} \cdot \bar{2} = \overline{3 \cdot 2} = \bar{6}$, $\quad \bar{3} \cdot \bar{4} = \overline{12} = \bar{5}$, $\quad \bar{3} \cdot \bar{5} = \overline{15} = \bar{1}$.

Es: $\mathbb{Z}_{12}$ $\quad \bar{3} \cdot \bar{5} = \overline{15} = \bar{3}$, $\quad \bar{6} \cdot \bar{4} = \overline{24} = \bar{0}$.

Proprietà della moltiplicazione in $\mathbb{Z}_N$:

- ASSOCIATIVA: $\forall \bar{a},\bar{b},\bar{c} \in \mathbb{Z}_N \quad (\bar{a}\cdot\bar{b})\cdot\bar{c} = \bar{a}\cdot(\bar{b}\cdot\bar{c})$

  infatti $(\bar{a}\cdot\bar{b})\cdot\bar{c} = (\overline{a\cdot b})\cdot\bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a}\cdot(\overline{bc}) = \bar{a}\cdot(\bar{b}\cdot\bar{c})$
- COMMUTATIVA: $\forall \bar{a},\bar{b} \in \mathbb{Z}_N \quad \bar{a}\cdot\bar{b} = \bar{b}\cdot\bar{a}$ infatti $\bar{a}\cdot\bar{b} = \overline{ab} = \overline{ba} = \bar{b}\cdot\bar{a}$
- EL. NEUTRO: $\forall \bar{a} \in \mathbb{Z}_N \quad \bar{a}\cdot\bar{1} = \bar{a}$ infatti $\bar{a}\cdot\bar{1} = \overline{a\cdot 1} = \bar{a}$.

Inoltre vale la proprietà:

- DISTRIBUTIVA: $\forall \bar{a},\bar{b},\bar{c} \in \mathbb{Z}_N \quad \bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot\bar{b} + \bar{a}\cdot\bar{c}$

  infatti: $\bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot(\overline{b+c}) = \overline{a\cdot(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac} = \bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}$.

  distributività in $\mathbb{Z}$.

($\mathbb{Z}_N$ è anello commutativo unitario)

Proviamo a costruire tabelle moltiplicative:

$\mathbb{Z}_3$:

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

in $\mathbb{Z}_3$: $\bar{2}\cdot\bar{2} = \bar{1}$

$\mathbb{Z}_5$:

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Def: $\overline{a} \in \mathbb{Z}_N$, $\overline{a} \neq \overline{0}$ si dice <u>divisore di zero</u> se $\exists \overline{b} \in \mathbb{Z}_N, \overline{b} \neq \overline{0}$ tale che $\overline{a} \cdot \overline{b} = \overline{0}$.

Es. In $\mathbb{Z}_6$, $\overline{2}$ è divisore di zero, infatti $\overline{2} \cdot \overline{3} = \overline{0}$.

Teorema: Sia $\overline{a} \in \mathbb{Z}_N$, $\overline{a} \neq \overline{0}$.

1) $\overline{a}$ è invertibile $\iff$ $MCD(a,N) = 1$
2) $\overline{a}$ è divisore di zero $\iff$ $MCD(a,N) > 1$

Dim: 1) $MCD(a,N) = 1 \overset{\text{Bézout}}{\iff} \exists x,y \in \mathbb{Z}$ t.c. $ax + Ny = 1 \iff \exists x \in \mathbb{Z}$ t.c. $\overline{ax} = \overline{1}$ in $\mathbb{Z}_N$
$\iff \exists \overline{x} \in \mathbb{Z}_N$ t.c. $\overline{a} \cdot \overline{x} = \overline{1}$, cioè $\overline{a}$ è invertibile in $\mathbb{Z}_N$.

2) Sia $d = MCD(a,N) > 1$, allora $\exists h,k \in \mathbb{Z}$ t.c. $a = d \cdot h$, $N = d \cdot k$ (necessariamente $0 \leq k < N$)
Consideriamo il prodotto $ak = d \cdot h \cdot k = h(dk) = h \cdot N$
allora $\overline{ak} = \overline{0}$ in $\mathbb{Z}_N$ cioè $\overline{a} \cdot \overline{k} = \overline{0}$ in $\mathbb{Z}_N$, inoltre $\overline{k} \neq \overline{0}$
$\Rightarrow$ $\overline{a}$ è divisore di zero.
Viceversa, se $\overline{a}$ è divisore di zero, non può essere invertibile. Infatti, se $\exists \overline{x}$ t.c. $\overline{a} \cdot \overline{x} = \overline{1}$
moltiplicando per $\overline{k}$: $\overline{k}(\overline{a} \cdot \overline{x}) = \overline{k} \Rightarrow (\overline{k} \cdot \overline{a}) \cdot \overline{x} = \overline{k} \Rightarrow \overline{0} \cdot \overline{x} = \overline{k} \Rightarrow \overline{0} = \overline{k}$ ASSURDO
$\Rightarrow$ $\overline{a}$ non è invertibile $\Rightarrow$ $MCD(a,N) \neq 1 \Rightarrow MCD(a,N) > 1$.