Operazioni

mercoledì 29 novembre 2023 19:16

→ OPERAZIONI

def: A insieme, un'operazione binaria su A è una funzione $*: A \times A \to A$

Denotiamo $*(x,y)$ con $x*y$

es:
$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

- Lo stesso vale per somma e prodotto su $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$
- Anche sottrazione e divisione (su $\mathbb{R}^*$) sono operazioni

Un'operazione può soddisfare alcune proprietà:

- PROPRIETÀ COMMUTATIVA $\forall a,b \in A \quad a*b = b*a$
- PROPRIETÀ ASSOCIATIVA $\forall a,b,c \in A \quad a*(b*c) = (a*b)*c$
- ELEMENTO NEUTRO $\exists e \in A$ t.c. $\forall a \in A \quad a*e = e*a = a$

es:

1) $+, \cdot$ soddisfano associativa, commutativa
elemento neutro di $+$ è 0
elemento neutro di $\cdot$ è 1

2) X insieme non vuoto, $A = X^X = \{f : X \to X\}$
$\cdot \; A \times A \to A$
$(f,g) \mapsto g \circ f$
} composizione di funzioni
$\circ$ è associativa, ma non è commutativa (in generale)
esiste un elemento neutro
$Id_X : X \to X$
$f \circ Id = Id \circ f = f$

3) $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \qquad a*b = 2a + 3b$
non è commutativa, non è associativa

4) $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$
$x*y = \sqrt[3]{x+y}$
commutativa, non associativa

→ OPERAZIONI IN $\mathbb{Z}_n$

$\mathbb{Z}_n = \mathbb{Z}/\sim_n$

$x \sim_n y \leftrightarrow x \equiv y \mod n \leftrightarrow x - y = kn \quad k \in \mathbb{Z}$
$\leftrightarrow$ x e y danno lo stesso resto divisi per n

$\overline{n} = \overline{0}, \; \overline{n+1} = \overline{1}$

- $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(\overline{a}, \overline{b}) \longmapsto \overline{a+b}$
} sommo gli interi a e b e prendo la classe modulo n

- $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(\overline{a}, \overline{b}) \longmapsto \overline{a \cdot b}$

$\mathbb{Z}_3 \quad \overline{2} + \overline{1} = \overline{2+1} = \overline{3} = \overline{0}$

[illegible]

$\mathbb{Z}_3 \quad \bar{2}+\bar{1}=\overline{2+1}=\bar{3}=\bar{0}$

$\mathbb{Z}_3 \quad \bar{2}=\bar{5} \quad \bar{1}=\overline{13} \qquad \bar{5}+\overline{13}=\overline{18}=\bar{3}=\bar{0}$

$\bar{a}+\bar{b}=\overline{a+b}$

$\bar{a}\cdot\bar{b}=\overline{a\cdot b}$

$\bar{a}=\{x\in\mathbb{Z} \mid x\equiv a \mod n\}$

verifichiamo che $+$ è ben definita

siano $r,s\in\mathbb{Z}$ t.c. $\bar{a}=\bar{r}$ e $\bar{b}=\bar{s}$

vediamo che $\overline{a+b}=\overline{r+s}$

($\star$) $\bar{a}=\bar{r} \leftrightarrow a\equiv r \mod n \leftrightarrow a-r=kn$

($\star\star$) $\bar{b}=\bar{s} \leftrightarrow b\equiv s \mod n \leftrightarrow b-s=hn$ $\quad k,h\in\mathbb{Z}$

$\overline{a+b}\overset{(\star)}{=}\overline{r+kn+s+hn}=\overline{r+s+(k+h)n}=\overline{r+s}$

$(a+b)-(r+s)=(k+h)n \longrightarrow \overline{a+b}=\overline{r+s}$ perchè la loro differenza è un multiplo di n

Analogamente si verifica che $\overline{a\cdot b}=\overline{r\cdot s}$

vedendo che $ab-rs=$ multiplo di n

es:

$\mathbb{Z}_2=\{\bar{0},\bar{1}\}$

$\bar{0}+\bar{0}=\overline{0+0}=\bar{0}$

$\bar{0}+\bar{1}=\overline{0+1}=\bar{1}$

$\bar{1}\overset{\shortparallel}{+}\bar{0} \quad \overline{1+0}$

$\bar{1}+\bar{1}=\overline{1+1}=\bar{2}=\bar{0}$

$\bar{0}\cdot\bar{0}=\overline{0\cdot0}=\bar{0}$

$\bar{0}\cdot\bar{1}=\overline{0\cdot1}=\bar{0}=\overline{1\cdot0}=\bar{1}\cdot\bar{0}$

$\bar{1}\cdot\bar{1}=\overline{1\cdot1}=\bar{1}$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

oss: $+$ e $\cdot$ in $\mathbb{Z}_n$ sono associativi e commutativi

elemento neutro?

- $\bar{0}$ è neutro per la somma

$\bar{0}+\bar{a}=\overline{0+a}=\bar{a}$ in $\mathbb{Z}_n$

- $\bar{1}$ è neutro per il prodotto

$\bar{1}\cdot\bar{a}=\overline{1\cdot a}=\bar{a}$ in $\mathbb{Z}_n$

es:

$\mathbb{Z}_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$

$\longrightarrow \bar{3}+\bar{1}=\bar{4}=\bar{0}$

$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\rightarrow \bar{3}+\bar{1}=\bar{4}=\bar{0}$

$\bar{3}=\{4k+3 \mid k\in\mathbb{Z}\}=-1$

$\bar{3}+\bar{1}=-\bar{1}+\bar{1}=\overline{-1+1}=\bar{0}$

In generale, dato $\bar{a}\in\mathbb{Z}_n$

$-\bar{a}$ è l'opposto di $\bar{a}$

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

$\mathbb{Z}_4$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\bar{2}\cdot\bar{2}=\bar{4}=\bar{0}$

$\bar{3}\cdot\bar{2}=\bar{6}=\bar{2}$

$\bar{3}\cdot\bar{3}=\bar{9}=\bar{1}$

$\mathbb{Z}_3$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$\bar{2}\cdot\bar{2}=\bar{4}=\bar{1}$

def: La classe $\bar{a}\in\mathbb{Z}_n$ si dice invertibile (rispetto al prodotto) se $\exists\,\bar{b}\in\mathbb{Z}_n$ t.c. $\bar{a}\cdot\bar{b}=\bar{1}$ ($\bar{a}\cdot\bar{b}=\bar{b}\cdot\bar{a}$)

Altrimenti $\bar{a}$ si dice non invertibile

Denotiamo con $U(\mathbb{Z}_n)$ l'insieme degli elementi invertibili di $\mathbb{Z}_n$

$U(\mathbb{Z}_n)=\{\bar{a}\in\mathbb{Z}_n \mid \bar{a} \text{ è invertibile}\}$

A volte si denota con $\mathbb{Z}_n^*$

es:

- $U(\mathbb{Z}_n)=\{\bar{1}\}$ $\mathbb{Z}_2=\{\bar{0},\bar{1}\}$

  $\bar{0}\notin U(\mathbb{Z}_n)$ $\bar{0}$ non è mai invertibile
  $\bar{1}\in U(\mathbb{Z}_n)$ $\bar{1}$ sempre invertibile $\bar{1}\cdot\bar{1}=\bar{1}$
- $U(\mathbb{Z}_3)=\{\bar{1},\bar{2}\}$ $\mathbb{Z}_3\{\bar{0},\bar{1},\bar{2}\}$ $\bar{2}\cdot\bar{2}=\bar{4}=\bar{1}$
- $U(\mathbb{Z}_4)=\{\bar{1},\bar{3}\}$ $\mathbb{Z}_4=\{\bar{0},\bar{1},\bar{2},\bar{3}\}$

  $\bar{2}$ non invertibile in $\mathbb{Z}_4$ $\bar{3}\cdot\bar{3}=\bar{9}=\bar{1}$

$\mathbb{Z}_n=\{\bar{0},\bar{1},\dots,\overline{n-1}\}=\{\bar{n},\overline{n+1},\dots,\overline{n-1}\}$

$\bar{a}=\bar{b}\leftrightarrow a-b=kn \quad k\in\mathbb{Z}$

$\bar{a}+\bar{b}=\overline{a+b} \quad \bar{a}\cdot\bar{b}=\overline{ab}$

def: $\bar{x}\in\mathbb{Z}_n$ è invertibile se $\exists\,\bar{y}\in\mathbb{Z}_n$ t.c. $\bar{x}\cdot\bar{y}=\bar{1}$

Diciamo che $\bar{y}$ è l'inverso di x, scriviamo $\bar{y}=\bar{x}^{-1}$

$U(\mathbb{Z}_n)=\{\bar{x}\in\mathbb{Z}_n \text{ invertibili}\}$

es:

$\bar{2}$ non invertibile in $\mathbb{Z}_4$

$\bar{2}$ invertibile in $\mathbb{Z}_3$ $\bar{2}\cdot\bar{2}=\bar{4}=\bar{1}$

$\bar{2}^{-1}=\bar{2}$

$\bar{3}$ invertibile in $\mathbb{Z}_4$ $\bar{3}\cdot\bar{3}=\bar{9}=\bar{1}$

$\bar{2}^{-1} = \bar{2}$

$\bar{2}$ invertibile in $\mathbb{Z}_7$ $\quad \bar{2} \cdot \bar{4} = \bar{8} = \bar{1}$

$\bar{2}$ non invertibile in $\mathbb{Z}_8$

teorema: Sia $\bar{x}$ e $\mathbb{Z}_n$. Allora $\bar{x}$ è invertibile $\leftrightarrow MCD(x,n) = 1$

dim: Osserviamo se $y \in \mathbb{Z}$ t.c. $\bar{y} = \bar{x} \rightarrow y = x + kn$, allora $MCD(x,n) = MCD(y,n)$

$MCD(x,n)$ non dipende dal rappresentante di $\bar{x}$

"$\rightarrow$" Sia $\bar{x} \in \mathbb{Z}_n$ invertibile

$\rightarrow \exists \bar{z} \in \mathbb{Z}_n$ t.c. $\bar{x} \cdot \bar{z} = \bar{1}$ in $\mathbb{Z}_n$

$\rightarrow \exists k \in \mathbb{Z}$ t.c. $x \cdot z = 1 + kn$ in $\mathbb{Z}$

$xz - kn = 1$ eq. diofantea

$MCD(x,n) \mid 1 \rightarrow MCD(x,n) = 1$

"$\leftarrow$" $MCD(x,n) = 1 \xrightarrow{BEZOUT} \exists z, k \in \mathbb{Z}$ t.c. $x \cdot z - k \cdot n = 1 \rightarrow xz = 1 + kn \rightarrow \bar{x} \cdot \bar{z} = \bar{1}$ in $\mathbb{Z}_n$ $\square$

es: inverso di $\bar{5}$ in $\mathbb{Z}_{22}$

cerco $\bar{x} \in \mathbb{Z}_{22}$ t.c. $\bar{5} \cdot \bar{x} = \bar{1}$

esiste perchè $MCD(5,22) = 1$

$\bar{5} \cdot \bar{x} = \bar{1} \leftrightarrow 5x = 1 + k \cdot 22 \qquad 5x - 22k = 1$ risolvo l'equazione

- ALGORITMO EUCLIDEO

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + \boxed{1}$ MCD

- BEZOUT

$1 = 5 - 2 \cdot 2 = 5 - 2(22 - 4 \cdot 5) = 9 \cdot 5 - 2 \cdot 22$

$\boxed{x = 9} \quad k = 2$

$\rightarrow \bar{5} \cdot \bar{9} = \bar{1}$

$\quad = \overline{45} = \overline{44 + 1} = \overline{44} + \bar{1} = \bar{0} + \bar{1} = \bar{1}$

def: $m \in \mathbb{Z}$

- $m > 0$ $\quad \bar{a}^m = \underbrace{\bar{a} \cdot \ldots \cdot \bar{a}}_{m \text{ volte}}$ in $\mathbb{Z}_n$

- $m < 0$ $\quad \bar{a}^m = \underbrace{\bar{a} \cdot \ldots \cdot \bar{a}}_{-m \text{ volte}}$

- $\bar{a}^0 = 1$

Quanti sono gli elementi di $U(\mathbb{Z}_n)$?

$\rightarrow$ LA FUNZIONE φ DI EULERO

$\varphi: \mathbb{N}^* \rightarrow \mathbb{N}^*$

$\varphi(n) = \#\{m \in \mathbb{N}^* \mid m \leq n, MCD(m,n) = 1\}$

teor $|U(\mathbb{Z}_n)|$

p primo $\quad \varphi(p) = p - 1$

p primo $\varphi(p) = p-1$

ogni intero $1 \leq x \leq p-1$ è coprimo con p

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	4	2	6	4	6

proprietà

1) $MCD(n,m) = 1$ $\quad \varphi(m \cdot n) = \varphi(m \cdot \varphi(n))$

φ MOLTIPLICATIVA

2) $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ $\quad p_i$ primi distinti,

$\alpha_i \in \mathbb{Z} + \mathbb{N}^* \rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$

è difficile computazionalmente calcolare $\varphi(n)$ se non si conosce la fattorizzazione di n

es:

$n = 2^3 \cdot 5 = 8 \cdot 5 = 40$

$\varphi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = \cancel{40}^{4} \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{4}^{2}}{\cancel{5}} = 4 \cdot 4 = 16$

teorema di Eulero

$n, x \in \mathbb{Z}$, $MCD(x,n) = 1$, $n \geq 2$

$\bar{x}^{\varphi(n)} = \bar{1}$ in $\mathbb{Z}_n \rightarrow \underbrace{\bar{x} \cdot \dots \cdot \bar{x}}_{\varphi(n) \text{ volte}}$

oss: $\bar{x} \cdot \bar{x}^{\varphi(n)-1} = \bar{x}^{\varphi(n)} = \bar{1}$ in $\mathbb{Z}_n \rightarrow \bar{x}^{-1} = \bar{x}^{\varphi(n)-1}$

es:

$\mathbb{Z}_7 \quad \varphi(7) = 6$

$\bar{3}$ in $\mathbb{Z}_7$ $\quad \bar{3}$ invertibile

$\bar{3}^6 = \bar{3}^2 \cdot \bar{3}^2 \cdot \bar{3}^2 = \bar{2} \cdot \bar{2} \cdot \bar{2} = \bar{8} = \bar{1}$

$\bar{3}^2 = \bar{9} = \bar{2}$

es:

$\mathbb{Z}_{22} \quad \bar{5}^{13003} = ?$

eulero $\quad \bar{5}^{\varphi(22)} = \bar{1} \rightarrow \bar{5}^{10} = \bar{1}$ in $\mathbb{Z}_{22}$

$\bar{5} \in U(\mathbb{Z}_{22})$ vero $MCD(5,22) = 1$

$22 = 2 \cdot 11 \rightarrow \varphi(22) = \varphi(2) \cdot \varphi(11) = 1 \cdot 10 = 10$

$\bar{5}^{10} = \bar{1} \rightarrow \bar{5}^{10 \cdot k} = \bar{1} \qquad k \in \mathbb{Z}$

$13003 = 13000 + 3 = 1300 \cdot 10 + 3$

$\bar{5}^{13003} = \bar{5}^{1300 \cdot 10 + 3} = (\bar{5}^{10})^{1300} \cdot \bar{5}^3 = \bar{1}^{1300} \cdot \bar{5}^3 = \bar{5} \cdot \bar{5} \cdot \bar{5} = \overline{25} \cdot \bar{5} = \bar{3} \cdot \bar{5} = \overline{15}$

teorema di Fermat

p primo, $x \in \mathbb{Z}$, $MCD(x, p) = 1$

Allora $\bar{x}^{p-1} = \bar{1}$ in $\mathbb{Z}_p$

dim: segue da Eulero perchè $\varphi(p) = p-1$ $\square$