LA MATEMATICA MODULARE

1. *Operazioni in un insieme*

Nell'insieme **N** dei numeri naturali, la moltiplicazione associa ad *ogni* coppia (ordinata) di numeri naturali, distinti o coincidenti, un ben determinato numero dell'insieme **N** chiamato risultato. Per questo motivo si dice che la moltiplicazione in **N** è una *operazione interna binaria* o una *legge di composizione interna binaria*. Operazione *binaria* perché *due* sono i termini dell'operazione, *interna* perché anche il risultato appartiene all'insieme **N.** Si dice anche che l'insieme **N** è *chiuso* rispetto alla moltiplicazione poiché il prodotto tra numeri naturali è sempre un numero naturale. Se però si eseguono le seguenti sottrazioni

37-40 50-15 5-3 7-4

accade che alcuni risultati non appartengano all'insieme dei numeri naturali, quindi si dice che **N** *non è chiuso* rispetto a tale operazione. In questo caso, si parla di *operazione interna binaria parziale* nell'insieme **N.** Il termine parziale deriva dal fatto che essa ha significato solo per una *parte* delle coppie di numeri naturali. Per contrapposizione, le operazioni non parziali vengono anche chiamate *operazioni totali*. Nell'insieme **D** dei numeri naturali dispari , l'addizione *non è* una operazione (totale o parziale) perché la somma di due numeri dispari è sempre un numero pari.

Nell'insieme **A** di tutti i punti del piano la seguente legge " *ad ogni coppia (ordinata) di punti del piano si associ il punto medio del segmento*" è una operazione interna binaria (totale) poiché ad ogni coppia di elementi di **A** corrisponde un ben determinato elemento appartenente ad **A.**

Nell'insieme **B=**$\{-1,0,1\}$**,** la moltiplicazione è una operazione interna binaria poiché moltiplicando due qualsiasi elementi dell'insieme si ottiene sempre un numero appartenente a **B**

Nell'insieme **N** dei numeri naturali la seguente legge " *dati due numeri naturali scriverne un terzo formato con le cifre dei primi due*" *non è* una operazione poiché ad ogni coppia (ordinata) di elementi di **N** non è associato un unico numero naturale.

Negli esempi proposti una operazione è definita su un insiemi finito, altre su insiemi infiniti, uno tra questi non è un insieme numerico. Pertanto è necessario affrontare lo studio del concetto di *operazione interna binaria* senza specificare la natura degli elementi sui quali si opera.

DEFINIZIONE

Dato un insieme non vuoto E, si dice che è definita in E una operazione (o legge di composizione) interna binaria se ad ogni coppia ordinata (a,b) di elementi di E, distinti o non, resta associato uno e un solo elemento c, appartenente pure ad E.

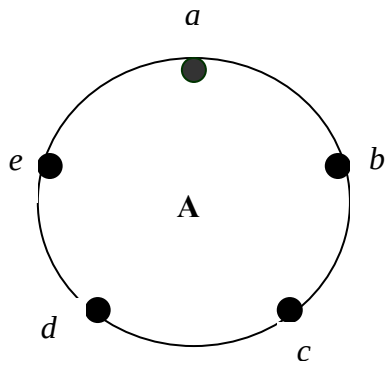
Gli elementi *a,b,c* si dicono, rispettivamente, *primo termine*, *secondo termine* e *risultato* dell'operazione. Per indicare che si compongono due elementi, *a* e *b*, si usano diversi simboli, che variano con i tipi di operazione. Per esempio per indicare l'addizione in un insieme numerico il simbolo adoperato è +, per le operazioni di intersezione tra insiemi si utilizza il simbolo ∩. Di solito quando non interesserà sapere la natura concreta della legge, per indicare l'operazione si usano segni di tipo più generale come $*$. Per indicare che ai termini *a* e *b*, presi nell'ordine, corrisponde il risultato *c,* si scrive $a * b = c$ e si legge " *a composto b uguale c*". L'operazione caratterizzata dal segno $*$ si dice "*l'operazione* $*$"

Nel caso in cui l'operazione agisca su un insieme finito, per rappresentare l'elenco completo dei risultati, si può utilizzare la sua tavola, una griglia formata da un ugual numero di righe e colonne, così costruita:

- nella prima casella in alto a sinistra è indicato il simbolo dell'operazione
- nelle intestazioni delle altre righe e delle colonne sono riportati tutti gli elementi dell'insieme, scritti preferibilmente nello stesso ordine
- nella casella intersezione di una riga e di una colonna viene scritto il risultato dell'operazione eseguita tra gli elementi delle intestazioni corrispondenti

La tavola, che viene anche detta *" tabella operativa"* , evidenzia che il risultato è unico essendo unica la casella intersezione tra una riga e una colonna. Per meglio chiarire il concetto ragioniamo su un esempio.

Sia $A=\{a,b,c,d,e\}$ un insieme di elementi disposti nell'ordine scritto, in senso orario, lungo una circonferenza come in fig.



Indichiamo con "$*$" il segno dell'operazione che ogni coppia ordinata *(x,y)* di elementi di A fa corrispondere l'elemento z di A che si incontra percorrendo la circonferenza in senso orario, a partire da *y*, e spostandosi di tanti intervalli quanti ne intercorrono tra *x* e *y*. La corrispondente tabella operativa è la seguente

$*$	*a*	*b*	*c*	*d*	*e*
a	*a*	*c*	*e*	*b*	*d*
b	*e*	*b*	*d*	*a*	*c*
c	*d*	*a*	*c*	*e*	*b*
d	*c*	*e*	*b*	*d*	*a*
e	*b*	*d*	*a*	*c*	*e*

2. ***Proprietà delle operazioni***

Sia E un insieme non vuoto sul quale sia definita una operazione interna binaria indicata con il simbolo $*$

DEFINIZIONE

Si dice che l'operazione indicata con $*$ gode della ***proprietà commutativa*** *(o,brevemente, che è* ***commutativa****) , se per ogni coppia di elementi x e y di E, risulta*

$$x*y = y*x$$

DEFINIZIONE

Si dice che l'operazione indicata con $*$ gode della ***proprietà associativa*** *(o,brevemente, che è* ***associativa****) , se qualunque siano gli elementi x ,y e z di E, risulta*

$$(x*y) * z = x * (y*z)$$

L'addizione e la moltiplicazione in **N** godono delle proprietà commutativa e associativa

DEFINIZIONE

Un elemento u dell'insieme E si dice ***elemento neutro*** *rispetto all'operazione indicata con $*$, se per ogni elemento x di E, risulta*

$$x*u = u*x = x$$

L'addizione in **N** ha come elemento neutro il numero 0

DEFINIZIONE

E' dato un insieme E non vuoto sul quale sia definita una operazione interna binaria indicata con il simbolo $*$, per la quale esiste un elemento neutro $u \in E$. Si dice che l'elemento $x' \in E$ è ***inverso*** *dell'elemento $x \in E$ rispetto all'operazione(e viceversa),se risulta*

$$x*x' = x'*x = u$$

Nell'insieme **Z** dei numeri interi relativi ogni elemento ammette inverso rispetto all'addizione. Tale inverso si chiama *opposto*

3.*Operazioni in insiemi numerici finiti*

Esempio 1

E' dato l'insieme **A** formato da sei elementi, $\mathbf{A}=\{1,2,3,4,6,12\}$. L'operazione

$$'x \ mcm \ y = m.c.m. \ (x,,y)' con \ x,y \in \mathbf{A}$$

è una legge di composizione interna binaria in A , infatti

- ad ogni coppia di elementi di **A** corrisponde un solo elemento,loro minimo comune multiplo
- questo elemento appartiene ad **A.**

La tabella operativa è la seguente

m.c.m.	1	2	3	4	6	12
1	1	2	3	4	6	12
2	2	2	6	4	6	12
3	3	6	3	12	6	12
4	4	4	12	4	12	12
6	6	6	6	12	6	12
12	12	12	12	12	12	12

Per stabilire se l'operazione è commutativa e ha elemento neutro è sufficiente esaminare con attenzione la tavola.

- L'operazione è commutativa su **A** se $\forall x, y \in A$ si ha x mcm $y = y$ mcm x. Poiché le caselle dove si leggono i risultati dei due calcoli x mcm y *e* y mcm x si trovano in posizione simmetrica rispetto alla diagonale segnata in fig. ne segue che l'operazione è commutativa poiché *tutti* gli elementi presenti nella tavola sono simmetricamente disposti rispetto a tale diagonale. Questo significa che si possono scambiare le righe con le colonne
- L'operazione ammette in **A** elemento neutro se $\exists u \in \mathbf{A} \,/\, x$ mcm $u = u$ mcm $x = x, \ \forall x \in A$. Di conseguenza, l' elemento 1 è neutro poiché tanto la riga quanto la colonna con intestazione 1 sono costituite, nell'ordine, dagli elementi di **A**

Si può osservare che tale operazione gode della proprietà associativa poiché (x mcm y) mcm $z = x$ mcm (y mcm z), $\forall x, y, z \in A$

Esempio 2

E' dato l'insieme **B** formato da sei elementi, $\mathbf{B}=\{0,2,4,6,8\}$. Si definisca un'operazione, chiamata '*addizione speciale'* indicheremo con il simbolo '$\top$ ', nel seguente modo:

il risultato sarà la somma ordinaria finché tale somma sarà minore di 10. Quando, invece, la somma ordinaria risulterà o uguale o maggiore di 10, si prenderà come risultato soltanto la cifra delle unità, trascurando la cifra delle decine

Si avrà, cioè

$0\top 0=0$ $\quad$ $2\top 2=4$
$2\top 0=2$ $\quad$ $4\top 2=6$
$4\top 0=4$ $\quad$ $6\top 2=8$
$6\top 0=6$ $\quad$ $4\top 4=8$
$8\top 0=8$

come nell'addizione ordinaria.

Si avrà, invece

$8\top 2=0$ $\quad$ $6\top 6=2$
$6\top 4=0$ $\quad$ $8\top 6=4$
$8\top 4=2$ $\quad$ $8\top 8=6$

L'operazione è una legge di composizione interna binaria in **B**, infatti

- ad ogni coppia di elementi di **B** corrisponde un solo elemento
- questo elemento appartiene ad **B.**

La tabella operativa è la seguente

$\top$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

Per stabilire se l'operazione è commutativa e ha elemento neutro è sufficiente esaminare con attenzione la tavola.

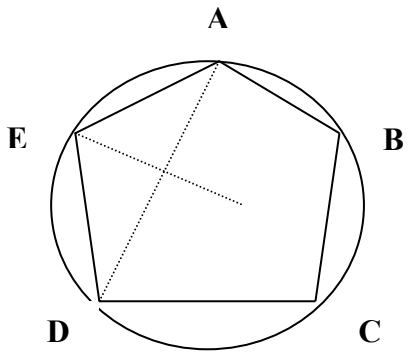
- L'operazione è commutativa su **A** poiché *tutti* gli elementi presenti nella tavola sono simmetricamente disposti rispetto a tale diagonale.
- L'operazione ammette in **A** lo zero come elemento neutro
- In ogni riga della tabella compare l'elemento neutro 0. Ciò significa che dato un qualsiasi elemento $x \in$ **B** $\exists! x' / \quad x \top x' = x' \top x = 0$. L'elemento x' è l'inverso di x rispetto a tale operazione. L'operazione ammette in **A** l'elemento inverso

Si può osservare che tale operazione gode della proprietà associativa poiché, tale proprietà vale, infatti, per l'addizione ordinaria, quindi vale anche per l' *addizione speciale*, nella quale il risultato si ottiene con l'unica variante di limitarlo alla cifra delle unità, variante che non influise sulla proprietà.

esercizi

1) Sia **B** l'insieme formato da sei elementi, $\mathbf{B}=\{0,2,4,6,8\}$. Si definisca un'operazione, chiamata '*moltiplicazione speciale'* , che indicheremo con il simbolo '$\top$ ', nel seguente modo:
il risultato sarà il prodotto ordinario finché tale prodotto sarà minore di 10. Quando, invece, il prodotto ordinario risulterà o uguale o maggiore di 10, si prenderà come risultato soltanto la cifra delle unità, trascurando la cifra delle decine
Costruire la tabella operativa e indicare le caratteristiche di tale operazione

2) Sia $H\{A,B,C,D,E\}$ l'insieme di cinque punti di una circonferenza che sono vertici di un pentagono regolare inscritto.



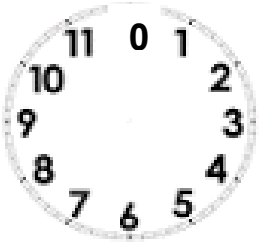
Ad ogni coppia X e Y di punti distinti dell'insieme H si associ quel punto di H che appartiene all'asse del segmento XY. Per $X \equiv Y$ sostituire la corda XY con la tangente in $X \equiv Y$e l'asse con la perpendicolare in $X \equiv Y$a detta tangente. Resta così definita in H una operazione $\perp$della quale si chiede di costruire la tabella operativa.

Esempio 3

Si indichi con $\mathbf{C}_{12}$ l'insieme dei numeri dell'orologio analogico $\mathbf{C}_{12}=\{0,1,2,3,4,5,6,7,8,9,10,11\}$ e si immagini di rappresentare i suoi elementi su un cerchio (il quadrante dell'orologio) che può essere percorso in due versi di rotazione (in generale gli elementi degli insiemi numerici fondamentali sono disposti su una retta infinita nei due versi di percorrenza). In questo insieme si definisca una operazione di '*addizione*', indicata con il simbolo '$\oplus$', secondo i seguenti esempi 'calcolati' sull'orologio
se dalle 10 di sera trascorrono 3 ore si arriva all'una del mattino: $10 \oplus 3=1$
se dalle 9 del mattino trascorrono 2 si arriva alle 11 del mattino: $9 \oplus 2=11$
Il risultato dell'operazione si ottiene, a partire dal primo operando, muovendosi in senso orario di tanti posti quanti indicati dal secondo operando.
L'operazione è una legge di composizione interna binaria in $\mathbf{C}_{12}$, infatti

- ad ogni coppia di elementi di $\mathbf{C}_{12}$ corrisponde un solo elemento
- questo elemento appartiene ad $\mathbf{C}_{12}$

In questo caso non si può parlare di ordinamento totale: infatti confrontando due elementi, per esempio 5 e 7 , si ha $5<7$ perché occorre percorrere due archi per andare da 5 a 7, ma anche $7<5$ perché percorrendo l'arco esplementare del precedente si va da 7 a 5.



0

La tabella operativa è la seguente

$\oplus$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Se si osserva attentamente la tabella, si possono identificare alcune proprietà dell'operazione $\oplus$

- L'operazione è commutativa poiché la tabella è simmetrica rispetto alla diagonale principale
- L'operazione ammette in $\mathbf{C}_{12}$ un elemento neutro, lo 0. La seconda riga della tabella, infatti, è uguale alla prima riga e la seconda colonna è uguale alla prima colonna
- Tale tabella consente di individuare l'inverso di ogni elemento di $\mathbf{C}_{12}$:
  $0 \oplus 0 = 0$: 0 è l'opposto di se stesso
  $3 \oplus 9 = 0$: 3 è l'opposto di 9
  $1 \oplus 11 = 0$: 1 è l'opposto di 11
  Se si osserva il cerchio in fig si capisce meglio il significato di questa proprietà: il numero di intervalli da percorrere in senso orario per raggiungere l'elemento 0 fornisce l'opposto dell'elemento
- L'operazione è associativa

Si consideri ancora l'insieme $\mathbf{C}_{12}$ e si introduca un'operazione di '*moltiplicazione ciclica*', indicata con il simbolo ' $\otimes$', secondo il seguente esempio. Data l'uguaglianza $3 \cdot 5 = 15$, per ottenere il risultato dell'operazione $3 \otimes 5$ si può ragionare in questo modo: si considera il punto corrispondente allo 0 sull'orologio e ci si sposta in senso orario in modo da percorrere 15 intervalli ; ci si troverà nel punto corrispondente a 3 che è il risultato dell'operazione $3 \otimes 5$. Tale operazione è una legge di composizione interna binaria in $\mathbf{C}_{12}$, infatti

- ad ogni coppia di elementi di $\mathbf{C}_{12}$ corrisponde un solo elemento
- questo elemento appartiene ad $\mathbf{C}_{12}$

La tabella operativa è la seguente

$\otimes$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8

5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	8	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Come nel caso dell'addizione $\oplus$, anche la tabella della moltiplicazione $\otimes$ fornisce l'occasione per studiare le proprietà dell'operazione.

- L'operazione è commutativa poiché la tabella è simmetrica rispetto alla diagonale principale
- L'operazione ammette in $\mathbf{C}_{12}$ un elemento neutro, 1 . La terza riga della tabella, infatti, è uguale alla prima riga e la terza colonna è uguale alla prima colonna
- L'operazione è associativa

Maggiore attenzione deve essere invece dedicata all'esistenza dell'elemento inverso di ogni $x \in \mathbf{C}_{12}$: se si osserva la tavola si nota che, per esempio, nella quarta riga non c'è elemento neutro, cioè 1, questo significa che in $\mathbf{C}_{12}$ non esiste inverso dell'elemento 2 , ovvero, che in $\mathbf{C}_{12}$ non esiste un elemento x tale che $2 \otimes x = 1$. La stessa osservazione può essere fatta anche per altri elementi dell'insieme. La moltiplicazione $\otimes$ non possiede elemento inverso. Dalla tabella segue anche che esistono numeri diversi da zero il cui prodotto dà zero, tali numeri vengono chiamati *divisori dello zero*. L'esistenza dei divisori dello zero contraddice il principio di annullamento del prodotto secondo il quale un prodotto è nullo se almeno uno dei fattori è nullo.

Certi orologi hanno sul quadrante soltanto quattro numeri; questo fatto ci suggerisce la possibilità di introdurre le operazioni $\oplus$ *e* $\otimes$ nell'insieme $\mathbf{C}_4 = \{0,1,2,3\}$ in modo analogo a quanto fatto per l'insieme $\mathbf{C}_4$. Si ottengono le seguenti tabelle operative

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Se si osservano le tabelle costruite in $\mathbf{C}_{12}$ e $\mathbf{C}_4$, si può affermare il risultato dell'operazione $x \oplus y$ è anche il *resto della divisione* della somma $x + y$ rispettivamente per 12 o per 4. Analogamente si può affermare il risultato dell'operazione $x \otimes y$ è anche il *resto della divisione* del prodotto $x \cdot y$ rispettivamente per 12 o per 4. Per esempio:

in $\mathbf{C}_4$ $3 \oplus 2 = 1$ che è il resto della divisione di $3 + 2 = 5$ per 4

in $\mathbf{C}_{12}$ $3 \oplus 7 = 9$ che è il resto della divisione di $3 \cdot 7 = 21$ per 12

Questo modo di procedere per costruire le tabelle operative in tali insiemi è più rapido e indica la possibilità di introdurre infiniti insiemi numerici finiti del tipo considerato. Tali insiemi esistono al di fuori dell'orologio e su di essi si opera in un modo che, se pure è stato suggerito da un esempio concreto, sussiste anche al di là di esso.

4. *Aritmetica modulare*

DEFINIZIONE

Si dice che due numeri naturali a e b sono ***congrui modulo n****, e si scrive* $a \equiv b \pmod{n}$ *se le divisioni* $a : n$ *e* $b : n$ *con* $n \in \mathbf{N_0}$ *hanno lo stesso resto.*

Così, per esempio, 2,5,8,11,sono tutti numeri congrui modulo 3 perché ognuno di essi,diviso per 3, dà lo stesso resto 2. Si può allora scrivere $5 \equiv 2 \pmod{3}$; $8 \equiv 2 \pmod{3}$ ecc.

La relazione di congruenza tra naturali è una relazione di equivalenza, detta di **congruenza modulo n,** in quanto gode delle tre proprietà riflessiva, simmetrica e transitiva. Questa relazione permette di ripartire l'insieme dei numeri naturali in classi di equivalenza dette **classi resto modulo n** .
La relazione di congruenza nell'insieme dei naturali si estende anche all'insieme **Z** degli interi relativi. Ad esempio:
il numero -17,diviso per 3, dà il quoziente -6 e il resto 1, infatti, dalla proprietà fondamentale della divisione, segue $3\cdot(-6)+1=-18+1=-17$**;**
il numero -14, diviso per 3, dà il quoziente -5 e il resto 1, infatti $3\cdot(-5)+1=-15+1=-14$**;**
il numero -11, diviso per 3, dà il quoziente -4 e il resto 1, infatti $3\cdot(-4)+1=-12+1=-11$**.**
Si deduce quindi che -17 e -14 sono congrui mod.3 poiché i resti delle loro divisioni per 3 sono uguali. Per individuare il *resto positivo* della divisione per *n* di un intero negativo *a* si assume come quoziente l'intero negativo il cui valore assoluto è il quoziente per eccesso, a meno di una unità, della divisione di $|a|$ per *n*. Nell'esempio precedente, dati i due numeri interi -17,-14, i resti positivi delle loro divisioni per 3 si ottengono con le seguenti operazioni

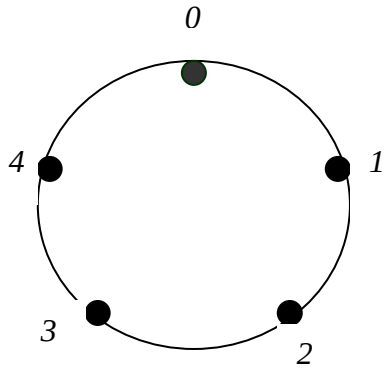
$$\begin{array}{rr} -17 & 3 \\ \hline -(-18) & -6 \\ \hline +1 & \end{array} \qquad \begin{array}{rr} -14 & 3 \\ \hline -(-15) & -5 \\ \hline +1 & \end{array} \qquad \begin{array}{rr} -11 & 3 \\ \hline -(-12) & -4 \\ \hline +1 & \end{array}$$

Quindi nella partizione di **Z** (mod.3) i numeri 2,5,8,11 appartengono alla *classe 2*; i numeri -17,-14, -11 appartengono alla *classe 1.*
L'aritmetica modulare è una particolare aritmetica in cui gli "elementi" su cui si opera sono le classi resto (mod.*n*).
Se ad esempio *n*=5 , l'insieme **Z** viene ripartito in 5 classi
$[0]$indica la classe dei numeri interi relativi che divisi per 5 danno il resto 0, costituita dagli elementi dell'insieme $\{....-25,-20,-15,-10,-5,0,5,10,15,20,25,...\}$
$[1]$indica la classe dei numeri con resto 1, costituita dagli elementi dell'insieme
$\{....-14,-9-4,1,6,11,16,....\}$
$[2]$indica la classe dei numeri con resto 2, costituita dagli elementi dell'insieme
$\{...-13,-8,-3,2,7,12,17,...\}$
$[3]$indica la classe dei numeri con resto 3, costituita dagli elementi dell'insieme
$\{...-12,-7,-2,3,8,13,18,....\}$
$[4]$indica la classe dei numeri con resto 4, costituita dagli elementi dell'insieme
$\{...-11,-6,-1,4,9,14,19,....\}$
Ogni elemento di ciascuna classe è chiamato rappresentante della classe a cui appartiene. Per esempio 7,12 sono alcuni rappresentanti della classe 2 di cui 2 è il più piccolo rappresentante
Si consideri allora l'insieme $\mathbf{Z}_5$ delle classi di congruenza (mod.5).I suoi elementi sono le classi $[0],[1],[2],[3],[4]$. $\mathbf{Z}_5=\{[0],[1],[2],[3],[4]\}$ è un insieme finito di 5 elementi, ma i suoi elementi sono insiemi infiniti, in altre parole $\mathbf{Z}_5$ è un insieme finito di insiemi infiniti, ossia è un insieme contenente un numero finito di elementi, ma ciascun elemento è, a sua volta, una classe che non è un semplice numero ma un insieme di infiniti numeri che sono stati chiamati classe. Per brevità di scrittura si omette di scrivere le parentesi quadrate e si indica con $\mathbf{Z}_5$ l'insieme. In $\mathbf{Z}_5$ si può definire un'*addizione* tra classi, indicata con $\oplus$, con la seguente regola
la 'somma' di due classi è la classe resto a cui appartiene la somma aritmetica di due suoi rappresentanti
Ad esempio $[4]\oplus[2]=[1]$, per brevità di scrittura si omette di scrivere le parentesi quadrate e si scrive $4\oplus2=1$. Il risultato è 1 perché 4+2 =6 e 6 appartiene alla classe resto $[1]$. Il risultato dell'operazione è indipendente dalla scelta dei rappresentanti. Come si può dimostrare da quanto segue

- gli elementi della classe $[4]$ sono del tipo *5k+4*
- gli elementi della classe $[2]$ sono del tipo *5h+2*
- addizionando due elementi generici otteniamo
  5k+4+5h+2=5(k+h)+6 =5(k+h)+5+1=5(k+h+1)+1

Il risultato è quindi un multiplo di 5 addizionato a 1 cioè un elemento generico della classe $[1]$

Si opera, in sostanza, come se le classi di congruenza modulo 5 fossero rappresentate lungo una circonferenza sulla quali vengono segnati 5 punti a intervalli regolari, facendo corrispondere a ogni punto una classe.



Così $4 \oplus 2 = 1$ perché, "spostandosi" di 2 posti a partire da 4 (in verso orario) si "arriva" a 1. L'operazione $\oplus$ agisce ciclicamente e quindi il risultato appartiene ancora a $\mathbf{Z}_5$ che risulta chiuso rispetto a essa.
In modo analogo si può definire in $\mathbf{Z}_5$ una *moltiplicazione* indicata con il simbolo $\otimes$
il 'prodotto' di due classi è la classe resto a cui appartiene il prodotto aritmetico di due suoi rappresentanti
Ad esempio $3 \otimes 4 = 2$, perché $3 \cdot 4 = 12$ e 12 appartiene alla classe resto $[2]$
Oppure, sulla circonferenza, $3 \otimes 4 = 2$, perché "spostandosi" di 12 posti a partire da 0 (in verso orario) si "arriva" a 2. Anche l'operazione $\otimes$ agisce ciclicamente e quindi il risultato appartiene ancora a $\mathbf{Z}_5$ che risulta chiuso rispetto a essa.
Le tabelle operative sono le seguenti

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	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

E' facile verificare dalle tabelle operative le proprietà commutativa, associativa, l'esistenza dell'elemento neutro
Qualunque sia $n \in \mathbf{N}$, in $\mathbf{Z}_n$ si possono sempre definire sia un'addizione che una moltiplicazione ciclica.
Si dice 'somma' di due classi, nella partizione di $\mathbf{Z}$ *(mod.n), la classe resto a cui appartiene la somma aritmetica di due suoi rappresentanti*
Si dice 'prodotto' di due classi, nella partizione di $\mathbf{Z}$ *(mod.n), la classe resto a cui appartiene il prodotto aritmetico di due suoi rappresentanti*
L'insieme $\mathbf{Z}_n(\oplus)$:

1. è chiuso rispetto rispetto all'operazione $\oplus$
2. $\oplus$ è commutativa e associativa
3. 0 è l'elemento neutro
4. ogni elemento ha il suo inverso, l'inverso di a è n-a

Se con Θ si indica l'operazione inversa dell'addizione ciclica, per in eseguire $\mathbf{C}_5$ l'operazione
$2 \Theta 4$ basta operare 'direttamente' con l'elemento inverso di 4 $2 \Theta 4 = 2 \oplus 1 = 3$
Se ne deduce dunque che è quindi risolubile, in $\mathbf{Z}_n$ ogni equazione del tipo $a \oplus x = b$ con a e $b \in \mathbf{Z}_n$

L'insieme $\mathbf{Z}_n(\otimes)$:

1. è chiuso rispetto rispetto all'operazione $\otimes$
2. $\otimes$ è commutativa e associativa
3. 1 è l'elemento neutro

4. non sempre tutti gli elementi possiedono inverso. Se ne deduce dunque che è non sempre è risolubile, in $\mathbf{Z}_n$ ogni equazione del tipo $a \otimes x = b$ con a e $b \in \mathbf{Z}_n$

TEOREMA 1 *di Wilson*

Un elemento $a \in \mathbf{Z}_n$ *possiede inverso rispetto all'operazione* $\otimes$ *se e solo se a è primo con n*

TEOREMA 2

Se il modulo n è un numero primo, allora ogni elemento di $\mathbf{Z}_n$*, esclusa la classe* $[0]$ *possiede inverso rispetto all'operazione* $\otimes$

Il teorema 1 consente di precisare che ogni equazione del tipo $a \otimes x = b$ con a e $b \in \mathbf{Z}_n$ è risolubile, in $\mathbf{Z}_n$ e ammette un'unica soluzione solo a condizione che a sia non nullo e primo con n. Solo in questo caso infatti a possiede un unico inverso rispetto all'operazione $\otimes$.Se a non è primo con n l'equazione $a \otimes x = b$ con o è impossibile oppure a e $b \in \mathbf{Z}_n$ o è impossibile oppure ammette più di una soluzione. Inoltre il teorema 2 porta a concludere che se il modulo n è un numero primo, ogni equazione del tipo $a \otimes x = b$ con a e $b \in \mathbf{Z}_n - \{0\}$ è dunque sempre risolubile in $\mathbf{Z}_n - \{0\}$, con un'unica soluzione.

Un'ulteriore osservazione riguarda il caso in cui il numero n non sia primo. Esaminando le tavole di moltiplicazione su $\mathbf{Z}_n$, con n non primo, si nota che esistono degli elementi, non necessariamente nulli, il cui prodotto è la classe $[0]$ esistono, cioè, divisori dello zero. Si conclude, quindi, che se il modulo n è primo, non sempre è valida la legge di annullamento del prodotto.

Infatti, confrontando le tabelle operative di moltiplicazione in $\mathbf{Z}_4$, $\mathbf{Z}_5$, $\mathbf{Z}_{12}$ con le seguenti, rispettivamente in $\mathbf{Z}_2$ e $\mathbf{Z}_3$

$\otimes$	0	1
0	0	0
1	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

si osserva che i divisori dello zero compaiono nelle congruenze mod.12 e mod.4 ma non in quelle mod.2, mod.3,mod.5, il perché si può comprendere ragionando come segue. I divisori dello zero sono numeri, minori del modulo, che contengono dei divisori del modulo poiché il prodotto aritmetico di due di essi deve risultare un multiplo del modulo. Così

per il mod.4 è $2 \otimes 2 = 0$

per il mod.12 è $4 \otimes 6 = 0$

Se invece il modulo è un numero primo, non ha divisori propri e quindi non può mai capitare che il prodotto aritmetico di due numeri minori del modulo sia un multiplo del modulo. Quando non esistono divisori dello zero, nelle tavole di moltiplicazione modulare l'unità compare in tutte le righe quindi ciascun elemento della classe possiede inverso .

Esercizi

Per risolvere, ad esempio, l'equazione $2 \otimes x = 1$ nell'insieme delle classi resto mod.3 si procede come segue. L'inverso di 2 in tale insieme è 2, perciò moltiplicando ambo i membri dell'uguaglianza per 2 si ottiene $2 \otimes 2 \otimes x = 2$ da cui $x = 2$. Se si vuole risolvere la stessa equazione nell'insieme $\mathbf{Z}_5$ si devono moltiplicare ambo i membri dell'uguaglianza per 3 (poiché l'inverso di 2 è 3) e si ottiene $2 \otimes 3 \otimes x = 3$ da cui $x = 3$

Nell'aritmetica mod.5 si ha $4^4 = 3^4 = 2^4 = 1$, cioè la quarta potenza di qualsiasi numero è 1

Nell'aritmetica mod.3 $1 \ominus 2 = 2$, quindi la sottrazione è sempre possibile senza ricorrere ai numeri negativi.