CAPITOLO I

NUMERI NATURALI CARDINALI

A. POTENZA DI UN INSIEME

a) ***Definizione di insiemi equipotenti***

Gli insiemi A e B si dicono ***equipotenti*** se ***esiste un'applicazione biiettiva*** ***$f: A \rightarrow B$*** .

Scriveremo per indicare tale circostanza:

$$A \sim B$$

La relazione di ***equipotenza*** è una ***relazione di equivalenza*** sulla categoria di tutti gli insiemi.

b) ***Definizione di numero cardinale o di potenza di un insieme***

Chiameremo ***potenza*** di un insieme A, o ***numero cardinale*** dell'insieme A, la ***classe di tutti gli insiemi equipotenti di A***.

c) ***Definizione di insieme finito***

Un insieme si dice ***finito*** quando ***o è vuoto*** oppure ***non può essere equipotente ad una sua parte propria***.

Si ha :

Teorema.

Dati due insiemi A e B con $A \subseteq B$, allora se A è infinito anche B è infinito e, pertanto, se B è finito anche A è finito.

Dimostrazione

Se A è *infinito* esiste un'applicazione $f: A \rightarrow A'$ biettiva, con A' una parte propria di A . Allora l'applicazione $g: B \rightarrow B'$ definita ponendo :

$$g(x) = \begin{cases} f(x) & \text{se } x \in A \subseteq B \\ x & \text{se } x \in B - A \end{cases}$$

Posto $H = A' \cup (B - A)$, la ***g*** applica B in H ed è biettiva; quindi è *infinito*.
Ora se B è *finito* non può essere A *infinito* poiché ciò implicherebbe B *infinito*.

Dal teorema mostrato discende che:

- se $A \subset B$ e ***pot A = pot B*** $\Rightarrow$ ***B infinito A infinito***

Infatti se ***pot A = pot B*** esiste una ***f : A → B biettiva***, per cui B è ***infinito*** contenendo una parte propria ad esso ***equipotente*** e allora anche A è ***infinito***.

- se $x \not\in A$ e ***A è finito*** $\Rightarrow$ **A ∪ {x} è finito** e ***pot (A ∪ {x}) ≠ pot A***

Risulta **A ⊂ A ∪ {*x*}**. Se fosse $A \cup \{x\}$ ***infinito*** risulterebbe A ***infinito*** il che non è possibile. Allora ***pot (A∪{x}) ≠ pot A***.

c bis) ***Definizione di numero cardinale finito e transfinito***

Si dicono ***numeri cardinali finiti*** o ***naturali*** le ***classi di equipotenza*** relative a insiemi finiti.

Si dicono ***numeri cardinali transfiniti*** le classi di equipotenza di insiemi infiniti.

B. ORDINAMENTO SUI NUMERI NATURALI.

Teorema del confronto per equipotenza

Comunque dati gli insiemi A e B è sempre possibile trovare degli insiemi A' e B' con A' ~ A, B' ~ B e tali che valga una ed una sola delle proprietà:

$$A' \subset B' \quad ; \quad A' \subseteq B' \quad ; \quad A' \supset B'$$

Teorema

Dati comunque gli insiemi A e B non vuoti, se A non è equipotente a B si ha che o A è equipotente ad una parte di B o B è equipotente ad una parte di A.
Qualunque siano le applicazioni:

$$f : A \rightarrow B \quad , \quad g : B \rightarrow A$$

per ipotesi esse non saranno biettive

Dimostrazione
Occorre provare per dimostrare il teorema che se ***non esiste*** una ***f*** iniettiva allora esiste una ***g*** iniettiva.

Infatti se f è iniettiva, non potendo essa essere suriettiva (altrimenti sarebbe biettiva), considerato l' insieme $f(A) \subset B$ esiste un insieme $B' \subset B$ tale che $B' \sim A$.
Se non esiste f ***iniettiva*** una qualsiasi $f: A \to B$ non è iniettiva e può essere o meno ***surriettiva***.

Esiste almeno una f surriettiva?
Supposto che esista una f ***surriettiva*** costruiamo la

$$g: B \to A$$

definita ponendo $\forall\, y \in B \quad g(y) = x$ con x elemento di $f^{-1}(y)$ cioè dell' insieme dei prototipi di y in f.
Da cui $g(B) \subset A$ è tale che $g(B) \sim A$ poiché g per costruzione è ***iniettiva***.
Mostriamo che esiste almeno una f ***surriettiva*** .
Per assurdo non esista una f ***surriettiva*** e non iniettiva .
Allora $\forall\, g$ poiché $g: A \to g(A)$ è ***non iniettiva*** e ***suriettiva***, $g(A)$ è ***equipotente*** ad una parte opportuna A' di A.
Da ciò seguirebbe che tra gli insiemi $A' - A$ e $B - g(A)$, di sicuro non vuoti perché ***g non*** è ***iniettiva*** e ***non surriettiva***, ***non esisterebbero*** applicazioni, il che è assurdo esistendo almeno l' applicazione costante.
Il teorema è completamente dimostrato.

Allora segue che nella ***classe*** dei numeri naturali cardinali può definirsi la ***relazione*** $\leq$ (***minore o uguale***) :

$$pot\, A \leq pot\, B \quad \Leftrightarrow \quad A' \subseteq B'$$

dove A' e B' sono gli insiemi precedentemente introdotti.

La ***relazione*** $\leq$ è ben posta perché
se ***A'' è equipotente ad A, cioè*** $A'' \in pot\, A$ e ***B'' è equipotente a B, cioè*** $B'' \in pot\, B$ risulta $A'' \sim A'$ e $B'' \sim B'$.

La ***relazione*** $\leq$ definita tra potenze è una ***relazione d'ordine***.
Infatti gode, come subito si verifica, delle ***proprietà riflessiva*** e ***transitiva***.

$$\text{se} \quad m \leq n \;\; e \;\; n \leq p \quad \Rightarrow \quad m \leq p \quad \textit{(propietà transitiva)}$$

Dimostrazione

Sia $\quad m = pot\, A \quad n = pot\, B \quad p = pot\, C$
Dall'essere $\quad m \leq n \;\Rightarrow\; pot\, A \leq pot\, B \quad$ cioè $A \subseteq B$ e

$$n \leq p \;\Rightarrow\; pot\, B \leq pot\, C \quad \text{cioè} \;\; B \subseteq C$$

Quindi:

se $A \subseteq B$ e $B \subseteq C$ $\Rightarrow$ $A \subseteq C$ *cioè* pot $A \leq$ pot C

da cui $m \leq p$.

La ***relazione*** $\leq$ gode inoltre della ***proprietà antisimmetrica*** come conseguenza del

Teorema di Cantor – Bernstein.

Dati gli insiemi A e B, se esistono una corrispondenza biunivoca tra A e una parte di B ed una corrispondenza biunivoca tra B ed una parte di A , allora esiste una corrispondenza biunivoca tra A e B cioè A e B sono equipotenti.

pot $A \leq$ pot B, pot $B \leq$ pot A $\Rightarrow$ pot A = pot B (***proprietà antisimmetrica***)

Definiamo inoltre le seguenti ***relazioni***:

pot $A \geq$ pot $B \Leftrightarrow A' \supseteq B'$ ($\geq$, ***maggiore o uguale***)

pot $B <$ pot $A \Leftrightarrow A' \subset B'$ ($<$, ***minore***)

pot $B >$ pot $A \Leftrightarrow B' \supset A'$ ($>$, ***maggiore***)

essendo A' e B' costruiti nel modo indicato nel **teorema del confronto** .

Le ***relazioni*** " $<$ " e " $>$ " definite sui numeri naturali godono inoltre delle seguenti ***proprietà***:

- m non può risultare contemporaneamente

$m > n$ ed $n > m$

Infatti per la ***proprietà transitiva*** si avrebbe

$m > n$ $n > m$ $\Rightarrow$ $m > m$

e ciò è ***assurdo***.

- Comunque si considerino due numeri n, m diversi fra loro risulta

$m > n$ ***oppure*** $n > m$.

Questo segue dal **teorema di confronto**.

C. OPERAZIONI DI PASSAGGIO AL SUCCESSIVO ED AL PRECEDENTE.

Indichiamo i ***numeri naturali finiti*** con lettere latine minuscole e l'insieme costituito da essi con il simbolo $\boldsymbol{N_o}$; indichiamo con $\boldsymbol{N_q}$ l'insieme:

$$\{ h \bullet n \geq q \,,\ \forall\, q \ \in N_o\}$$

La ***classe*** relativa all'***insieme vuoto*** sarà indicata con il simbolo:

0 (zero)

La ***classe*** individuata dall'insieme *A* ***tale che se x*** $\in$ ***A ogni y*** $\neq$ ***x è tale che y*** $\notin$ ***A*** sarà indicata con il simbolo:

1 (uno)

Osserviamo che $0 < 1$ poiché ***l'insieme vuoto è contenuto in* {*x*}**.

Se *A* è un ***insieme finito*** ed **{*x*}** è un ***insieme costituito da un solo elemento*** con $x \notin A$ e se n = ***pot A*** è il numero definito dall'insieme *A*, chiameremo ***numero successivo di n***, e lo indicheremo con il simbolo:

n +1 (n più uno)

la potenza di $A \cup \{x\}$.
In tal modo si definisce ***un'applicazione***:

$$s:\ N_0 \rightarrow N_1$$

detta ***operazione di passaggio al successivo*** ponendo:

$$s\,(n) = n + 1 \qquad n \in N_0$$

Osserviamo che:

a) Lo ***0*** ***non è il successivo di nessuno*** poiché:

$A \cup \{x\} \neq \emptyset$ essendo $\{x\} \neq \emptyset$

b) Il ***numero 1 è il successivo dello 0*** poiché per $A = \emptyset$ si ha:

$$\emptyset \cup \{x\} = \{x\}$$

c) essendo $A \subset A \cup \{x\}$ quando $x \notin A$ si ottiene

$$n < n + 1$$

Dimostriamo la seguente

Proposizione

L'operazione di passaggio al successivo è una applicazione biettiva.

Dimostrazione

Basta dimostrare che:

$$s\,(n) \neq s\,(m) \;\Leftrightarrow\; n \neq m$$

essendo s chiaramente ***suriettiva***

$\Rightarrow$

Sia $s\,(n) \neq s\,(m)$.

Supposto ***per assurdo*** $m = n$, risulterebbe $m = n = pot\, A$ da cui $s\,(m) = s\,(n)$ ***contro l' ipotesi***.

$\Leftarrow$

Sia ora $m \neq n$ ed in particolare $m < n$.

Posti $m = pot\, M$ e $n = pot\, N$ con $M \subset N$, si ha che

se $x \notin N \Rightarrow M \cup \{x\} \subset N \cup \{x\}$

cioè

$$m + 1 < n + 1.$$

Denotiamo con:

$n - 1$ (e si legge ***n meno uno***)

l'***elemento di*** N_0 tale che $s\,(n - 1) = n$.

L'applicazione

$$p = f^{-1} : \; N_1 \rightarrow N_0$$

definita ponendo

$$p\,(n) = n - 1$$

prende il nome di ***passaggio al precedente.***

Fissato $a \in N_0$ si consideri $s(a)$; a ed $s(a)$ si dicono ***successivi consecutivi***.
Si ha allora:

$$\textit{non esiste}\quad m \in N_0 \quad \text{tale che} \quad a < m < s(a).$$

Infatti:
sia A tale che $pot\, A = a$ con $x \in A$.
Allora è $A \subset A \cup \{x\}$.
Considerato un M tale che $A \subseteq M \subseteq A \cup \{x\}$ si verifica che

$$x \in M \quad \text{oppure} \quad x \notin M$$

da cui

$$M = A \cup \{x\} \quad \text{oppure} \quad M = A.$$

TEOREMI DI INDUZIONE MATEMATICA

Lemma

Dato N_q se $S \subseteq N_q$ ed è tale che $q \in S$
Se $\forall\ n \in S$ $(n + 1) \in S \Rightarrow$

$$S \equiv N_q$$

Dimostrazione
Sia ***m il primo elemento dell'insieme ordinato N_q***
Per assurdo sia $m \notin S$; di sicuro è $m > q$ poiché ***per ipotesi*** $q \in S$
Consideriamo $f^{-1}(m) = h \in N_q$ risulta allora $h \in S$. Pertanto, essendo $m = h + 1$, $m \in S$.

I° Teorema di induzione matematica

Ad ogni $n \in N_q$ associamo una affermazione E_n
Ogni affermazione E_n è vera se
a) E_q è vera
b) E_k vera $\Rightarrow E_{k+1}$ vera. $\forall\ k \in N_q$.

Dimostrazione
Sia $S = \{\, n \in N_q \ : E_n \text{ è vera} \,\}$
Allora se $q \in S$, $n \in S \Rightarrow n + 1 \in S$.
Quindi per il ***lemma precedente*** risulta $S \equiv N_q$.

II° Teorema di induzione di matematica.

Sia E_n una proposizione associata ad ogni $n \in N_q$ e $n > q$.
Se
a) ***E_q vera***
b) ***E_k vera*** ***per $q \leq k < m$*** e ***$k \in N_q - N_m$ si ha*** ***E_m è vera***
allora

$$E_n \text{ è vera} \qquad \text{per ogni } n$$

Dimostrazione
Supponiamo che esista ***$n \in N_m$*** tale che ***E_n è falsa*** e sia ***h il più piccolo di tali interi valori positivi***.
Risulterà allora ***E_n vera*** per ogni ***$q \leq n < h$.***
Ma ***per l'ipotesi (b)*** ciò implica ***E_h vera.***

Nota: *I simboli I° e II° si leggono "primo" e "secondo" e per noi hanno solo carattere distintivo.*

Concetto di primi $x + 1 = s(x)$ numeri naturali

Scriveremo ***0, 1,.., x, …*** per indicare i numeri ottenuti da 0 operando successivamente con l'***applicazione s*** in maniera del tutto arbitraria.
Risulta chiaramente:

$$0 < 1 < s(1) < s(s(1)) < \ldots < p(x) < x < s(x) < \ldots$$

I numeri ***i*** ed ***s(i)*** sono detti ***successivi consecutivi*** e ***tra essi non vi sono altri numeri***.

Questo ***insieme*** così costruito viene detto ***insieme dei primi x + 1, dei primi s(x) numeri naturali***.

Esso è ***complementare di N_{x+1}*** e lo si indicherà con:

$$\ell N_{x+1}$$

Infatti poiché si è posto

$$N_{x+1} = \{y : y \geq x + 1\}$$

Risultando invece

$$\ell N_{x+1} = \{y : y \in N_0, \; y \leq x\}$$

esso è proprio l'***insieme dei naturali minori di x + 1.***

D. CONCETTO DI MASSIMO E DI MINIMO E TEOREMI RELATIVI

a) ***Definizione di minimo***

Sia $S \neq \emptyset$ un insieme tale che $S \subseteq N_0$,
allora un elemento $m \in S$ si dice ***un minimo di S*** se

$$m \leq x \qquad \forall x \in S$$

Osservazione

Se m ed $\overline{m}$ sono ***entrambi minimi di S*** risulta $m \leq \overline{m}$, $\overline{m} \leq m$ da cui

$$m = \overline{m}.$$

b) ***Definizione di massimo***

Sia $S \neq \emptyset$ un insieme tale che $S \subseteq N_0$,
allora un elemento $M \in S$ si dice ***un massimo di S*** se

$$M \geq x \qquad \forall x \in S$$

Osservazione

Se M ed $\overline{M}$ sono ***entrambi massimi di S*** risulta $M \leq \overline{M}$, $\overline{M} \leq M$ da cui

$$M = \overline{M}.$$

Si fa osservare che per ***definizione*** di ***max*** e di ***min*** l'***insieme*** ℓN_{x+1} ha ***per massimo x*** e ***per minimo 0***.

Teorema di esistenza del minimo

Ogni sottoinsieme non vuoto di N_0 ha minimo

Dimostrazione

Sia $S \subset N_0$ un ***sottoinsieme di S*** ed $S \neq \emptyset$
Consideriamo l'***insieme***:

$$\{x : x \in N_0 ;\ x < y \ \ \forall y \in S\}$$

Se ***S non*** ha ***minimo*** allora

$$\forall \ y \in S, \qquad \exists \ y_0 \in S : \ y_0 < y$$

I ***numeri inferiori a y*** sono ***elementi*** dell'***insieme***

$$\ell \ N_y = \{0, 1, \ldots\ldots, y\}$$

Risulta $\ell N_{y0} \subset \ell N_y$
Consideriamo allora gli ***insiemi***:

$$\emptyset \subset \ell N_1 \subset \ell N_{1+1} \subset \ldots \subset \ell N_{y0} \subset \ell N_y$$

Se ***S* non ha minimo** deve avere ***intersezione non vuota con ciascuno di questi insiemi.***
In particolare:

$$S \cap \ell N_1 = \{ 0 \}$$

Ma ***se S contiene lo 0 ha minimo***.

Un insieme $S \subset N_0$ con $S \neq \emptyset$ si dice ***limitato superiormente*** $\Leftrightarrow$

$$\exists\ l \in N_0 : x \leq l \qquad \forall\ x \in S$$

Osservazione
Tale ***definizione differisce da quella di massimo*** per il fatto che ***non è richiesto che*** $l \in S$

Teorema di esistenza del massimo
Ogni sottoinsieme non vuoto di n—limitato superiormente ha massimo.

$$\exists\ l \in N_0 : \forall\ x \in S \Rightarrow x < l$$

Dimostrazione
Consideriamo l'***insieme*** $T = \{y : y < l \ \ e \ \ y \geq x, \ \ \forall\ x \in S\}$
Tale ***insieme*** ha ***minimo***: infatti ***non essendo vuoto contiene almeno l'elemento l***.
Il ***minimo di T***, allora, per ***definizione di massimo***, è il ***massimo di S***.

Definizione
Un ***insieme A ordinato*** si dice ***ben-ordinato*** $\Leftrightarrow$ ***ogni sottoinsieme non vuoto*** (ivi compreso ***A***) ***ha minimo***.

Ne segue che l'***insieme ordinato totalmente*** $(N_0, \geq)$ è ***ben ordinato***.

E. OPERAZIONI SUI NUMERI NATURALI

a) ***Definizione di somma di naturali***
Dati i ***naturali*** $m = pot\ A$, $n = pot\ B$ siano $M \sim A$, $N \sim B$ con $M \cap N = \emptyset$
Chiameremo ***somma di m ed n*** il ***numero naturale*** $pot\ (M \cup N)$ e lo denoteremo con

$$m + n.$$

b) ***Definizione di addizioni di naturali***
Chiameremo ***addizioni di naturali*** l'***applicazione***

$$S : N_0 \times N_0 \to N_0$$

definita ponendo $\forall (m, n) \in N_0^{\times 2}$

$$S(m, n) = m + n$$

c) ***Definizione di prodotto di naturali***

Dati i naturali $m = pot\ A$, $n = pot\ B$ chiameremo ***prodotto di m ed n*** il ***numero naturale pot (A x B)*** e lo indicheremo con

$$m \cdot n$$

d) ***Definizione di moltiplicazione di naturali***

Chiameremo ***moltiplicazione di naturali*** l'***applicazione*** :

$$P : N_0 \times N_0 \to N_0$$

definita ponendo $\forall (m, n) \in N_0^{\times 2}$

$$P(m, n) = m \cdot n$$

Osservazione

$\forall\ n \in N_0$ si ha $s(n) = n+1$. L'***applicazione s***, detta ***operazione*** di ***passaggio al successivo*** è la ***restrizione*** di ***S*** all'***insieme*** $N_0 \times \{1\}$, per cui è giustificata la ***notazione*** per $s(n)$ di $n+1$.

F. PROPRIETA' DELLE OPERAZIONI.

L'***addizione*** e la ***moltiplicazione*** definite in N_0 godono delle seguenti ***proprietà***

a) ***Proprietà commutativa***

$$(i) \quad m + n = n + m \qquad \forall\ m, n \in N_0$$

$$(ii) \quad m \cdot n = n \cdot m \qquad \forall\ m, n \in N_0$$

Infatti se $m = pot\ A$, $n = pot\ B$ con $A \cap B \neq \emptyset$ risulta nel caso additivo:

$$pot\ (A \cup B) = pot\ (B \cup A)$$

perché l'***unione*** gode della ***proprietà commutativa***.

Nel caso moltiplicativo dobbiamo far vedere che

$$Pot\ (A \times B) = pot\ (B \times A)$$

Sappiamo che il ***prodotto cartesiano non*** gode della ***proprietà commutativa***, però se consideriamo un'***applicazione*** che realizza l'***equipotenza*** tra $A \times B$ ***e*** $B \times A$, allora le ***potenze*** dei due insiemi ***sono eguali*** e di conseguenza vale la ***proprietà commutativa***.

b) ***Proprietà associativa***

$$(m + n) + h = m + (n + h) \qquad \forall m, n, h, \in N_0$$
$$(m \cdot n) \cdot h = m \cdot (n \cdot h) \qquad \forall m, n, h, \in N_0$$

Infatti, se $m = pot\ A$, $n = pot\ B$, $h = pot\ C$ e $A \cap B = \emptyset$ $B \cap C = \emptyset$ $A \cap C = \emptyset$,
nel caso additivo risulta:

$$pot\ ((A \cup B) \cup C) = pot\ (A \cup (B \cup C))$$

perché, come sappiamo dalla teoria degli insiemi

$$(A \cup B) \cup C = A \cup (B \cup C).$$

Nel caso moltiplicativo dobbiamo far vedere che

$$Pot\ ((A \times B) \times C) = pot\ (A \times (B \times C))$$

Sappiamo che il ***prodotto cartesiano non*** gode della ***proprietà associativa*** e quindi i due insiemi ***non*** sono ***uguali*** ma l'***applicazione*** chiaramente ***biiettiva***:

$$f : (A \times B) \times C \to A \times (B \times C)$$

definita ponendo

$$f((a, b), c) = (a, (b, c)) \qquad \forall a \in A, \forall b \in B, \forall c \in C$$

mostra l'***equipotenza*** degli insiemi considerati.

c) ***Significato delle proprietà associativa***

Sia

$$\{m_i\}_{i \in I} \qquad I = \ell\ N_{q+1} \quad q \in N_1$$

una ***famiglia*** indicata di ***naturali***.

Consideriamo i ***numeri*** costruiti con il seguente procedimento:

$m_0 + m_1 = S_1$ $\qquad m_0 \cdot m_1 = P_1$

$S_1 + m_{S(1)} = S_{S(1)}$ $\qquad P_1 \cdot m_{s(1)} = P_{S(1)}$

.... $\qquad$ ....

$S_r + m_{s(r)} = S_{s(r)}$ $\qquad P_r \cdot m_{s(r)} = P_{s(r)}$

I due ***numeri*** S_q e P_q che si denotano anche con i simboli:

$$S_q = \sum_{i \in I} m_i = \sum_{1}^{r}{}_i\ m_i$$

$$P_q = \prod_{i \in I} m_i = \prod_{1}^{r}{}_i\ m_i$$

vengono chiamati rispettivamente ***somma*** e ***prodotto*** dei ***naturali della famiglia*** .

La ***proprietà associativa*** permette in sostanza di dire che P_q e S_q ***non dipendono*** dalla scelta dell'ordine degli indici.

d) ***Proprietà distributiva della moltiplicazione rispetto all'addizione***

$$m \cdot (n + h) = m \cdot n + m \cdot h \qquad \forall\, m, n, h, \in N_0$$

Infatti, se $m = pot\ A$, $n = pot\ B$, $h = pot\ C$, risulta

$$Pot\ A \cdot (pot\ B + pot\ C) = pot\ A \cdot pot\ B + pot\ A \cdot pot\ C$$

Supposto $B \cap C = \emptyset$, il che non è restrittivo, si ha:

$$A \times (B \cup C) = (A \times B) \cup (A \times C)$$

da cui segue l'asserto.

e) ***Significato della proprietà distributiva***

La ***proprietà distributiva*** afferma che

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Si prova con esempi che invece

$$a + (b \cdot c) \neq (a + b) \cdot (a + c)$$

ESEMPIO

$$a = 1 \qquad b = 0 \qquad c = 1$$

$$a + (b \cdot c) = 1 + (0 \cdot 1) = 1$$

$$(a + b) \cdot (a + c) = (1 + 0) \cdot (1 + 1) = 1 \cdot 2 = 2$$

Ne segue che può scriversi senza ambiguità $a + b \cdot c$ eseguendo ***prima*** la ***moltiplicazione*** e ***successivamente*** l'***addizione***.

Dalla definizione di ***parentesi*** si deduce che ***in ogni espressione numerica*** occorre operare sui calcoli ***a partire dalle parentesi più interne*** ed in esse eseguire ordinatamente prima moltiplicazioni e poi addizioni.

Teorema

$(N_1, S, P, <)$ ***è archimedeo*** $\Leftrightarrow$ ***dati***

$$a, b \in N_1\ \exists\ n \in N_1 :\ b < a \cdot n$$

Dimostrazione

Se $a = 1$ posto $n = b^*$ risulta

$$b < b^* = 1 \cdot b^* = a \cdot n$$

Se $a \neq 1$ supposto $a > 1 \quad \exists\ c \in N_1 : 1 + c = a$

posto allora $n = b$ si ha

$$b < b + b \cdot c = b \cdot (1 + c) = a \cdot n$$

Si può ***osservare*** che se $a = 0$ la ***proprietà non vale*** quando $b \in N_1$ essendo

$$b > a \qquad \forall\, b \in N_1$$

f) ***Deduzione del prodotto dalla somma.***

Dalle ***proprietà associativa*** e ***distributiva*** si ha, applicando prima la ***distributiva***, che:

$$m \cdot n = \sum_{i \in CN_{m+1}} n_i = \sum_{j \in CN_{n+1}} m_j \qquad \forall\ m, n \in N_{1*}$$

e

$$n_i = n \qquad m_j = m$$

Infatti:

$$m \cdot n = (n + n + \ldots\ldots\ldots + n) = \qquad \text{(per m addendi)}$$
$$= n \cdot (1+1+\ldots\ldots+1) = n \cdot m =$$
$$= m\,(1+1+\ldots\ldots+1) = (m+n+\ldots..+m) \qquad \text{(per n addendi)}$$

Si pone infine

$$1 \cdot n = n \qquad 0 \cdot n = 0$$

Conseguono dalle ***proprietà distributiva*** ed ***associativa*** le:

g) ***Proprietà dei multipli***

$$m \cdot a + m \cdot b = m \cdot (a + b)$$
$$m \cdot a + n \cdot a = (m + n) \cdot a$$
$$m \cdot (n \cdot a) = (m \cdot n) \cdot a$$

h) ***Potenze***

Indicheremo con il simbolo a^n un ***prodotto*** del tipo

$$a^n = \prod a_i$$

con

$$\begin{cases} i \in N_{n+1} \\ a_i = a \\ n \in \ell N_{1*} \end{cases}$$

e porremo per ***definizione***

$$a^1 = a \qquad a^0 = 1$$

i) ***Proprietà delle potenze***

Siano $a, b \in N_0 \quad m, n \in N_0 \quad (a, n) \neq (0, 0) \quad (b, m) \neq (0, 0)$

risulta

$$a^m \cdot b^m = (a \cdot b)^m$$

$$a^m \cdot a^n = a^{m+n}$$
$$(a^m)^n = a^{m \cdot n}$$

Le dimostrazioni sono ovvie.

1) ***Elementi neutri rispetto alle operazioni***

I ***naturali*** 0 e 1, già introdotti, sono tali che:

$$\left.\begin{aligned} n + 0 &= n \\ n \cdot 1 &= n \end{aligned}\right. \qquad \forall\, n \in N_0$$

come risulta immediato.

Infatti

$$pot\ A + pot\ \emptyset = pot\ (A + \emptyset) = pot\ A$$

e

$$pot\ A \cdot pot\ \{x\} = pot\ (A \times \{x\}) = pot\ A$$

perchè l'***applicazione***

$$f: A \times \{x\} \to A$$

definita ponendo $\forall\, x \in A$

$$f(a, x) = a$$

è ***biiettiva***.

Struttura algebrica di (N_0, S, P)

Le **proprietà a (i), b), d)** garantiscono che

(N_0, S, P) è un **semianello**

che è inoltre **commutativo** per la **a (ii)** e dotato di ***elementi neutri*** .

m) **Proprietà degli elementi neutri.**

Si ha intanto dalle precedenti scambiando **S** con **P**:

$$\left. n \cdot 0 = 0 \right\}$$

$$\forall\ n \in N_0$$
$$n+1 = s(n)$$

Dimostrazione
Facciamo vedere, essendo l'altra già nota, che $n \cdot 0 = 0$.
Posto
$n = pot\ A \quad 0 = pot\ \emptyset$
segue:
$$n \cdot 0 = potA \cdot pot\ \emptyset = potA \times \emptyset = pot\ \emptyset = 0$$

Si hanno inoltre le seguenti:

Legge di annullamento del prodotto
$$m \cdot n = 0 \Rightarrow \{m = 0\} \vee \{n = 0\} \vee \{m = n = 0\}$$
ciascuna di queste possibilità escludendo le altre.

Dimostrazione
Posto $m = pot\ M$ e $n = pot\ N$ $m \cdot n$ si può scrivere:
$$pot\ (M \times N) = pot\ \emptyset = O,$$
e quindi
$$M \times N \sim \emptyset,$$
cioè per definizione di ***equipotenza***
$$M \times N = \emptyset$$
onde poiché
$$M \times N = \emptyset \Rightarrow \{M = \emptyset\} \vee \{N = \emptyset\} \vee \{M = N = \emptyset\}$$
l'asserto è provato.

n) **Legge di annullamento della somma**.
$$m+n=0 \Rightarrow m = n = 0$$

Dimostrazione
Posto $m = pot\ M,\ n = pot\ N$, dalla ***definizione di somma*** segue:
$$pot\ (M \cup N) = 0 = pot\ \emptyset$$
Quindi dalla ***definizione di unione*** segue:
$$M = \emptyset \text{ ed } N = \emptyset$$
cioè l'asserto.

Per completezza **dimostriamo** che:

$$m \cdot n = 1 \Rightarrow m = n = 1$$

$$m + n = 1 \Rightarrow \begin{cases} 0 \cdot m = 0 \quad e \quad n = 1 \\ 0 \cdot m = 1 \quad e \quad n = 0 \end{cases}$$

Dimostrazione

Posto $m = pot\ A \quad n = pot\ B$ con $A \cap B = \emptyset$,

si ha per ipotesi:

$$m \cdot n = pot\ (A \times B) = 1$$

da cui se

$$(a, b) \in A \times B \qquad \forall\ (c, d) \neq (a, b) \ \ e \quad (c, d) \notin A \times B$$

risulta

$$A = \{a\} \qquad B = \{b\}$$

onde

$$m = n = 1.$$

$$m + n = pot\ (A \cup B) = pot\ \{x\} \Rightarrow A \cup B = \{x\}$$

Essendo $A \cap B = \emptyset$

se $x \in A$

si ha che

$$A = \{x\} \quad e \quad B = \emptyset$$

da cui l'asserto.

Analogamente si ragiona se $b \in B$.

Considerazioni algebriche sugli elementi neutri.

La ***legge di annullamento del prodotto*** garantisce che

(A, S, P) è ***privo di divisori dello zero***.

La ***legge di annullamento della somma*** dice che

il semimodulo (A, S) ha il gruppo delle unità (o elementi regolari) costituito dal solo 0

o anche che

nessun elemento non nullo è dotato di opposto.

Il fatto che

$$m \cdot n = 1 \Rightarrow m = n = 1 \qquad se \quad A_0 = A - \{0\}$$

dice che

il semigruppo (A_0, P) ha il gruppo delle unità moltiplicative costituite dal solo elemento unitario 1

o, in altre parole, che

nessun elemento diverso da 0 e da 1 è dotato di inverso.

Inoltre, come è evidente

$$\mathbf{1}\ \text{ha per inverso se stesso}$$

$$\text{lo } \mathbf{0} \text{ non può avere inverso}$$

essendo

$$n \cdot 0 = 0 \neq 1 \qquad \forall\ n \in N_0$$

G. STABILITA'DELLE OPERAZIONI RISPETTO ALL'ORDINAMENTO

Teorema di compatibilità di S e P con l'ordinamento

Risulta:

$$(i) \quad \begin{cases} m > n \\ a \geq b \end{cases} \quad \Rightarrow \quad \begin{cases} m + a > n + b \quad \forall \quad m, n \in N_0 \\ m \cdot a > n \cdot b \quad \forall \quad a^n, b \in N_1 \end{cases}$$

Osserviamo inoltre che risulta

$$a \geq b \iff \exists\ x \in N_0 : a = b + x$$

Dimostrazione

Sia $a \geq b$, $a = pot\ A$ $b = pot\ B$ con $A \supseteq B$.

Posto $X = C_A B = A - B$, il numero $x = pot\ X$ è tale che

$$a = pot\ A = pot\ [(A - B) \cup B] = pot\ X + pot\ B = x + b.$$

Inversamente se $\exists\ x \cdot a = b + x$,

e se $b = pot\ B$

sia $X \cap B = \emptyset$ in modo tale che $x = pot\ X$.

Considerato $A = B \cup X$

risulta

$$B \subseteq A$$

Da cui

$$pot\ B \leq pot\ A.$$

E' inoltre chiaro che è

$$a = b \quad \text{quando e solo quando} \quad X = \emptyset.$$

Ne segue che se $m = n + x$ con $x \in N_1$ e $a = b + y$ con $y \in N_1$

risulta:

$$m + a = (n + b) + (x + y) \quad \text{con} \quad x + y \in N_1$$

da cui

$$m + a > n + b$$

Risulta inoltre :

$$m \cdot a = n \cdot b + (n y + b x + x y)$$

con

$$n\, y + b\, x + x\, y \in N_1$$

Osservazione.

Ricordando ora che la ***relazione*** $\geq$ è di ***ordine totale*** e che quindi risulta

$$m > n \quad o \quad n > m \qquad \forall \quad m, n \in N_0 \text{ con } m \neq n$$

ciascuna possibilità *escludendo l'altra*, risulta che è possibile una almeno delle due equazioni:

$$(i\ i) \qquad \begin{matrix} m + x = n \\ m \neq 0 \\ m = n + y \end{matrix} \qquad \forall \quad m, n \in N_0 \quad \text{con}$$

H. REGOLA DI SEMPLIFICAZIONE.

Si ha che:

$$a + b = a + c \Leftrightarrow b = c$$
$$a + b > a + c \Leftrightarrow b > c$$
$$a \cdot b = a \cdot c,\ a \neq 0 \quad \Leftrightarrow \quad b = c$$
$$a \cdot b > a \cdot c\ ,\ a \neq 0 \quad \Leftrightarrow \quad b > c$$

Dimostrazione

Per dimostrare che

$$a + b = a + c \quad \Leftrightarrow \quad b = c$$

basta osservare che presi tre insiemi ***A, B, C*** tali che

$$a + b = pot\ (A \cup B) = pot\ (A \cup C) = a + c$$

per la ***sottrazione tra insiemi*** risulta

$$pot\ (A \cup B - A) = pot\ (A \cup C - A)$$

da cui, poiché gli insiemi ***A, B*** e ***A, C*** sono ***disgiunti***, segue

$$pot\ B = pot\ C$$

e quindi

$$b = c\ .$$

Sia ora $a + b > a + c$. Non potendo essere $b = c$, sia $b < c$.

Poiché risulta $a \leq a$ seguirebbe

$$a + b < a + c$$

contro l'Hp , da cui è

$$b > c.$$

Mostriamo ora che:

$$a \cdot b = a \cdot c \quad \text{con} \ \ a \neq 0 \quad \Rightarrow \quad b = c$$

Sappiamo che esistono certamente gli insiemi ***A, B, C*** tali che:

$$A \times B \sim A \times C$$

con $a = pot\ A$, $b = pot\ B$, $c = pot\ C$

Se $A \neq \emptyset$, l'***applicazione biiettiva***

$$f: A \times B \to A \times C$$

certamente esistente per l'***equipotenza*** dei due ***prodotti cartesiani***, permette di costruire l'applicazione:

$$g : B \to C$$

definita fissando un qualsiasi $a \in A$ e associando ad ***ogni*** $x \in B$ il ***secondo elemento della coppia (a, c) corrispondente alla coppia (a, b)***[1].

L'applicazione g è chiaramente ***biiettiva***, per cui

$$B \sim C$$

e quindi

$$b = c$$

Se $A = \emptyset$, non esistendo a, ***la g non è definibile***.

H (bis). OPERAZIONI PARZIALI INVERSE IN N_0

a) *Nozione di operazione parziale.*

Ricordiamo che

un'operazione parziale in A è ***una applicazione***

$$f: H \to A$$

ove $H \subseteq A \times A$.

Se $H = A \times A$ si ha ***un'operazione***, altrimenti ***un'operazione parziale***.

L'insieme H definisce una ***relazione R su A*** e si ha che :

$$\forall\ a, b \in A\ ,\ \exists\ \ f(a, b) \Leftrightarrow a\ R\ b.$$

b) *Operazione di sottrazione*.

In ***(G - b)*** dati $m, n \in N_0$ se $m \neq n$ è possibile

$$(i) \qquad m + x = n$$

o

$$(ii) \qquad m = n + y.$$

In ***H*** si è provata la ***regola di semplificazione***

$$a + x \Rightarrow x = y$$

---

[1] Ricordiamo che una coppia (a, b) è per ***definizione*** l'***insieme*** $\{\{a\},\{a, b\}\}$. Gli ***elementi*** dell'***insieme coppia*** sono insiemi $A = \{a\}$ e $B = \{a, b\}$ con la ***proprietà*** che $A \subseteq B$ .L'***elemento di A*** si dice il "***primo***" elemento della coppia, l'***elemento di*** $A \cap B$ si dice il "***secondo***" elemento della coppia. Nel simbolo ***(a, b)*** si scrive a sinistra il ***primo*** elemento e a destra il ***secondo***.

ne segue ovviamente che quando sono ***valide*** o la ***(i)*** o la ***(ii)*** la ***soluzione*** è necessariamente ***unica***.

Infine se ***m = n*** è ***possibile*** sia la ***(i)*** che la ***(ii)*** avendo come ***unica soluzione lo 0***.

Diamo ora la

definizione di differenza di numeri naturali.

Se l'equazione m + x = n è possibile la sua unica soluzione è detta differenza fra m e n ed è denotata con il simbolo

$$m - n$$

Si ha subito dalle considerazioni iniziali che:

Condizione necessaria e sufficiente perché n > m esista è che

$$n > m$$

Dimostrazione

Ovvia.

Si ha inoltre che:

Se esiste n - m allora esiste anche m - n se e solo se

$$n = m$$

Dimostrazione

Ovvia.

Ed ancora:

Comunque presi m, n $\in N_0$ o esiste n-m o esiste m - n ciascuna possibilità escludente l'altra se m $\neq$ n.

Consideriamo ora il ***sottoinsieme*** $H \subset N_0^{x2}$ costituito dalle coppie ***(n, m)*** con ***n $\geq$ m***.

Definizione di sottrazione di numeri naturali.

Chiameremo ***sottrazione del naturale n per il naturale m l'applicazione***

$$D: H \rightarrow N_0$$

definita ponendo:

$$D(n, m) = n - m \qquad \forall (n, m) \in H$$

c) ***Operazione di divisione esatta.***

Se $n \in N_1 \quad m \in N_0$ definiamo ***una relazione R*** tale che:

$$n \; R \; m \iff \exists K \in N_0 : m = K n$$

Per indicare

$$n \, R \, m$$

scriveremo n / m e leggeremo ***n divide m***

La ***relazione R*** è individuata da un opportuno ***sottoinsieme H di*** $N_1 \times N_0$.

<u>Teorema.</u>

La relazione R è una relazione di ordine parziale in N_1.

Dimostrazione

Si ha che

$$a/a \qquad \forall a \in N_1$$

essendo $a = 1 \cdot a$

Se risulta che

$$a/b \quad \text{e contemporaneamente} \quad b/a$$

essendo

$$b = Ka \qquad a = hb$$

si ha

$$b = h\,Kb \qquad \text{con} \; b \in N_1$$

da cui segue

$$hK = 1$$

cioè

$$h = K = 1$$

e pertanto

$$a = b.$$

E' inoltre vero che

$$a/b \, , \, b/c \Rightarrow a/c$$

Infatti da

$$b = Ka, \; c = hb$$

si deduce

$$c = hKa.$$

E' immediato che la ***relazione*** sia d'***ordine parziale.***

Infatti se $n > 1$ non si può avere ad esempio che $n/1$ poiché ciò implicherebbe

$$1 = hn \qquad \text{con} \quad n > 1.$$

Si **prova** inoltre che:

$$\left.\begin{array}{l} n/a \\ \\ \end{array}\right\} \quad \left\{\begin{array}{l} n/a + b \\ \\ \end{array}\right.$$

$$n/b \quad \Rightarrow \quad n/a - b$$
$$a > b \qquad\qquad n/h \cdot a + k \cdot b$$

Dimostrazione
Infatti da $a = 1 \cdot n\,,\ b = m \cdot n$
segue

$$a + b = (l + m)\, n$$

cioè

$$n/a + b\,.$$

Inoltre se n/a
ne segue che

$$n/\,h\,a \qquad \forall\ h \in N_1$$

poiché se $a = l\,n$ è $h\,a = (\,h \cdot l)\,n$
da cui

$$n/h\,a + K\,b.$$

Inoltre posto $a - b = x$ cioè $a = b + x$
da

$$n/\,b + x \quad \text{ed} \quad n/b$$

segue

$$b = m \cdot n\,, \quad b + x \neq l \cdot n\,,$$

per cui

$$l \cdot n = x + m \cdot n$$

e pertanto esiste

$$l \cdot n - m \cdot n = x$$

ma essendo $m \cdot n < l$ esiste

$$y = l - m.$$

Dalle relazioni

$$l \cdot n = x + m \cdot n \quad e \quad m + y = l$$

si deduce

$$n \cdot y = x^2$$

onde

$$a - b = y \cdot n.$$

Si osservi ora che per la ***regola di semplificazione moltiplicativa***, l'elemento ***k associato alla coppia (m , n)*** $\in H$ è ***unico***.

Definizione

---

[2] Si è così incidentalmente provato che

$$n\,(1 - m) = n \cdot y = x = n \cdot 1 - n \cdot m$$

L'elemento k associato a (n, m) $\in$ H si chiama quoziente esatto di m ed n e si scrive $k = \frac{n}{m}$.

Definizione

L'applicazione

$$Q : H \to N_0$$

definita ponendo

$$Q\,(n, m) = \frac{n}{m}, \qquad (n, m) \in H$$

si chiama operazione parziale di divisione esatta.

Le ***coppie*** di ***H*** sono le ***coppie (m, n)*** tali che

$$n = k \cdot m$$

ovvero come ***si suol dire*** sono ***quelle coppie per cui n è multiplo di m***.

Premettiamo il seguente

Lemma

Se $m \in N_0$ $n \in N_1$ allora o m è multiplo di n o è compreso tra due multipli di n.

Dimostrazione

Se $n = 1$ risulta $m = m \cdot 1$

Se $n \in N_2$ l'insieme $\{k \cdot n\}_{k \in N_0}$ contiene $0 < n$ e contiene $m \cdot n > m$.

L'insieme $\{k \cdot n \;:\; kn < m\}$ essendo limitato superiormente ha ***massimo***

$$q \cdot n \leq m$$

ed è

$$(q + 1) \cdot m > m$$

Teorema della divisione con resto

Dati comunque $m \in N_0$ $n \in N_1$ esistono $q, r\ n \in N_0$ con $r < n$ tali che sussista la relazione

$$m = q \cdot n + r$$

e tale decomposizione è unica.

Dimostrazione

Per il ***Lemma*** precedente esiste un q tale che

$$q \cdot n \leq m < (q + 1)\, n.$$

Si ponga $m = q \cdot n + r$; essendo $q \cdot n + r < q \cdot n + n$

Per la ***regola di semplificazione*** risulta

$$r < n.$$

Sia ora $m = q' \cdot n + r'$; risulta

$$q \cdot n + r = q' \cdot n + r'.$$

Se è $r = r'$ allora è anche $q = q'$ e ***viceversa***.

Supponiamo dunque $q \neq q'$ ed $r \neq r'$.
Si arriva ad un assurdo.
Infatti sia $q > q'$ non può essere $r > r'$ né $r = r'$ per cui è $r' > r$.
Risulta pertanto

$$q = q' + x \quad \text{e} \quad r' = r + y$$

da cui

$$(q' + x) \cdot n + r = q' \cdot n + r + y$$

e quindi

$$x \cdot n = y.$$

poichè $x, y, \in N_1$, è anche $y \geq n$
e da $r' = r + y$
si ha l'***assurdo*** essendo $r' \geq n$.
Analogamente si ragiona se $q \geq q'$.

Definizione
L' applicazione

$$D_r : N_o \times N_1 \rightarrow N_o \times N_o$$

ottenuta ponendo

$$D_r(n, m) = (q, r), \quad \forall\ n \in N_o, m \in N_1,$$

con la coppia (q, r) definita dal teorema precedente , ***esiste ed è unica***; ***essa si chiama divisione con resto***

I. SISTEMI DI NUMERAZIONE IN N_O.

Per il seguito valga la seguente notazione:
dato il naturale ***n***, indicheremo con ***n**** il ***naturale successivo di n***, con ***n***** il ***naturale successivo di n**** e così via.

Dimostriamo il seguente
Lemma (1)
Dati i numeri naturali a, n si ha sempre, per qualsiasi valore di a>1 e di n>1

$$\textbf{(b)} \qquad a^n > 1 + (a - 1)n$$

Dimostrazione
Fissato $a > 1$, procediamo per induzione rispetto ad n.
Sia $\overline{N}$ l'***insieme formato dai naturali n*** per i quali è ***valida*** la relazione **(b)** per ogni valore di $a > 1$ fissato.
All' insieme $\overline{N}$ appartiene il naturale $1^* = 1 + 1$.
Infatti, per $n = 1^*$ per il ***secondo membro della relazione*** **(b)** si ha :

$$1 + (a - 1) \cdot 1^* = 1 + (a - 1) \cdot (1 + 1) = [1 + (a - 1)] + (a-1) = a + (a - 1)$$

ed inoltre risulta:

$$a \cdot a = a^{1+1} = a^{1^*}$$

Per essere ***valida*** la ***disuguaglianza*** si deve mostrare :

$$a + (a - 1) < a \cdot a.$$

Osserviamo che ***per qualunque valore di*** $a > 1$ la disuguaglianza :

$$(a - 1) < a(a - 1)$$

è ***vera***, avendosi, se $a > 1$,

$$a - 1 \geq a - 1 \Rightarrow a(a - 1) > (a - 1).$$

Per la ***proprietà distributiva della differenza*** la disuguaglianza

$$(a - 1) < a(a - 1)$$

può scriversi nella seguente maniera:

$$a - 1 < a \cdot a - a$$

da cui segue

$$a + (a - 1) < a \cdot a.$$

Abbiamo dunque verificato che per $n = 1^*$ la relazione :

$$a^{1^*} > 1 + (a - 1) \cdot 1^*$$

è ***vera***.

Supponiamo che $\overline{N}$ contenga il naturale n.
Avremo che la relazione

$$a^n > 1 + (a - 1)n$$

è ***vera*** e quindi, moltiplicando per a ambo i membri, è ***vera*** anche la relazione

(c) $$a \cdot a^n = a^{n+1} > a \cdot [1 + (a - 1)n] = a + (a - 1)\, a \cdot n.$$

Essendo $a > 1$, $n > 1$, sarà anche $a - 1 \geq 1$ da cui ne segue $n(a - 1) > 1$.
Sarà allora

$$an > n + 1$$

e pertanto, per il secondo membro della relazione **(c)**, vale la ***disuguaglianza*** :

$$a + (a - 1) \cdot an > 1 + (a - 1)(n + 1)$$

La relazione **(c)** quindi diventa :

$$a \cdot a^n = a^{n+1} > a + (a - 1) \cdot an > 1 + (a - 1)(n + 1)$$

e, in definitiva

$$a^{n+1} > 1 + (a - 1)(n + 1)$$

All' insieme $\overline{N}$ appartiene allora, insieme ad ***n***, anche il ***suo successivo n+1*** e, per il ***principio di induzione matematica***, la relazione:

$$a^n > 1 + (a - 1)\, n,$$

fissato ***a > 1***, è ***vera per ogni naturale n > 1***.

Lemma

Siano 0, 1, ……, x dei simboli, detti fondamentali, associati ai primi numeri naturali.

Fissato x≥1 ed indicato x* il suo successivo, per qualsiasi naturale a>1 è possibile trovare un naturale n in modo che risulti :

$$(d) \qquad (x^*)^n \le a < (x^*)^{n+1}$$

Dimostrazione

Fissato il ***naturale x***, se risulta ***a < x***, il **lemma** è ***vero*** per ***n = 0***.

Se risulta invece ***a > x****, per determinare il ***naturale n*** che soddisfi alla:

$$(x^*)^n \le a < (x^*)^{n+1}$$

procediamo nella seguente maniera.
Cominciamo a determinare il ***naturale m*** tale che sia $a \le (x^*)^m$.
Tale naturale ***esiste sempre***.
Sappiamo infatti dal **lemma (1)** che
per il ***naturale x* > 1*** e per qualsiasi ***naturale h > 1*** è valida la relazione:

$$1 + (x^* - 1)\, h < (x^*)^h$$

Se vogliamo quindi che sia $a < (x^*)^m$, basterà determinare il ***naturale m*** in modo che si abbia :

$$a < 1 + (x^* - 1)\cdot m \;\Rightarrow\; a < (x^*)^m$$

e, cioè, in modo che sia :

$$a - 1 < (x^* - 1)\cdot m$$

Tale relazione è ***sempre soddisfatta*** se si pone $m = q + 1$, dove q è il ***quoziente*** della ***divisione con resto*** di $(a - 1)$ per $(x^* - 1)$, divisione ***sempre possibile*** perché risulta $x^* - 1 \in N_1$ e dalla quale si ottiene ***un quoziente*** $q \in N_1$ perché è $a > x^*$ da cui

$$a - 1 > x^* - 1.$$

Fissato in tale maniera il ***naturale*** m, si confronti il ***naturale*** a con le s***uccessive potenze di*** $(x^*)^m$, con m determinato in modo anzidetto, e cioè con:

$$x^*,\ (x^*)^{1^*},\ (x^*)^{1^{**}},\ \ldots\ldots\ldots\ldots\ldots,\ (x^*)^m$$

La ***prima*** delle ultime disuguaglianze è ***minore di*** a per ***ipotesi***, l'***ultima*** è ***maggiore di*** a per ***costruzione***.
Essendo gli ***esponenti crescenti da*** 1 ***a*** m, esiste un ***unico naturale***, compreso tra 1 ed m, e sia $n+1$, tale che sia il ***più piccolo dei naturali*** k, compresi tra 1 ed m, per i quali valga $(x^*)^k > a$.
Risulta allora

$$(x^*)^n \leq a \leq (x^*)^{n+1}$$

<u>Teorema fondamentale di rappresentazione</u>
Siano 0, 1, …, x dei simboli associati ai primi numeri naturali.
Fissato $x \geq 1$***, ogni naturale*** $a > x^*$ ***si decompone in una somma di prodotti dei naturali rappresentati dai simboli fondamentali 0, 1, …, x, per tutte le potenze di*** x^* ***decrescenti da n a 0, dove il naturale n soddisfa la relazione***

$$(x^*)^n \leq a \leq (x^*)^{n+1}$$

Dimostrazione
Occorre dimostrare che, dati i ***naturali*** a e x, con $a > x^*$ e $x \geq 1$, per il ***naturale*** a vale una decomposizione del tipo:

$$\textbf{(d)} \qquad a = a_0 \cdot (x^*)^n + a_1 \cdot (x^*)^{n-1} + \ldots + a_{n-1} \cdot x^* + a_n$$

con $0 \leq a_i \leq x$ (i = 0, 1,…, n-1, n)
e dove ogni naturale a_i resta determinato in ***modo univoco***.
Procediamo ***per induzione*** rispetto ad h, essendo h ***un naturale*** tale che

$$(x^*)^h \leq a \leq (x^*)^{h+1}$$

La **(d)** è ***vera*** per i ***naturali*** a che soddisfano la seguente disuguaglianza

$$x^* \leq a \leq (x^*)^{1^*}.$$

Infatti, dividendo ***a per*** x^* ed indicando con a_0 il ***quoziente*** e con r il ***resto della divisione***, risulta

$$a = a_0 \cdot x + r \qquad con \quad 0 < a_0 \quad ed \quad r < x^*.$$

Inoltre, dalla relazione

$$a < (x^*)^{1^*} = (x^*)^{1+1} = x^* \cdot x^*$$

segue

$$a = a_0 \cdot x^* + r < x^* \cdot x^*$$

e quindi anche

$$(*) \qquad a_0 \cdot x^* < x^* \cdot x^*$$

da cui infine

$$a_0 < x^*$$

Posto $r = a_1$, si ha, in definitiva

$$a = a_0 \cdot x^* + a_1 \quad \text{con} \quad 0 < a_0 < x^* \quad \text{e} \quad 0 \le a < x^*$$

e la ***decomposizione*** è ***unica*** essendo a ed a_1 rispettivamente ***quoziente*** e ***resto*** di una divisione.
Ammettiamo ora che la proprietà **(d)** valga per l'***insieme dei naturali a*** per i quali risulta

$$\textbf{(e)}\ x^* \le a < (x^*)^n, \qquad \text{con } n > 1^*$$

e cioè sia $a = .\ .\ .\ .\ .$ la ***decomposizione*** di a che supponiamo ***esistente*** ed ***unica***, e dimostriamo che essa vale anche per l'***insieme dei naturali a*** per i quali risulti

$$(x^*)^n \le a < (x^*)^{n+1}$$

Essendo $(x^*)^n \le a$ possiamo dividere a per $(x^*)^n$.
Indicando con a_0 il ***quoziente*** e con r il ***resto della divisione***, abbiamo:

$$\textbf{(f)} \quad a = a_0 \cdot (x^*)^n + r \qquad \text{con } 0 < a_0,\ 0 \le r < (x^*)^n\ ;$$

dalla relazione $a < (x^*)^{n+1}$, segue allora:

$$a = a_0 \cdot (x^*)^n + r < (x^*)^{n+1}$$

da cui si ricava

$$a_0 \cdot (x^*)^n < (x^*)^{n+1} = x^* \cdot (x^*)^n$$

e quindi

$$a_0 < x^*.$$

Ora, se $r < x^*$, posto $r = a_n$, la **(f)** può scriversi :

$$a = a_0 \cdot (x^*)^n + 0 \cdot (x^*)^{n-1} + \ldots + 0 \cdot x^* + a_n$$

con $0 < a_0 < x^*$ e $0 \leq a_n < x^*$

e la proprietà **(d)** è dimostrata.

Se risulta invece:

$$x^* \leq r < (x^*)^n$$

la proprietà **(d)** vale per il ***naturale*** r per l'***ipotesi*** **(e)** e quindi, essendo

$$a = a_0 \cdot (x^*)^n + r$$

la proprietà **(d)** vale anche per il ***naturale a*** e si può scrivere:

$$a = a_0 \cdot (x^*)^n + a_1 \cdot (x^*)^{n-1} + \ldots + a_{n-1} \cdot x^* + a_n$$

con $0 < a_0 < x^*$ e $0 \leq a_i < x^*$ (i = 1,1*, 1**, . . , n - 1, n).

Ammesso che il teorema ***valga*** per i ***numeri naturali a*** della classe che verificano la **(e)** abbiamo così dimostrato che esso vale anche per i ***naturali a*** della classe verificante la:

$$(x^*)^n \leq a < (x^*)^{n+1}$$

e dunque il teorema, per il ***secondo principio d'induzione***, è ***valido*** per ***tutti i naturali***.

Per ottenere per via ***algoritmica*** la rappresentazione, di cui al teorema precedente, si procede nella maniera seguente:
fissato il ***naturale x*** ed il ***naturale a*** che si vuole scomporre, si determina il ***naturale n*** che soddisfi la:

$$(x^*)^n \leq a < (x^*)^{n+1}$$

Dopo di ciò si ha via via:

$$a = a_0 \cdot (x^*)^n + r_0 \qquad con\ 0 \le r_0 < (x^*)^n,\ 0 < a_o < x^*$$

$$r_0 = a_1 \cdot (x^*)^{n-1^*} + r_1 \qquad con\ 0 \le r_1 < x^{*n-1},\ 0 \le a_1 < x^*$$

....

....

$$r_i = a_{i^*} \cdot (x^*)^{n-i^*} + r_{i^*} \qquad con\ 0 \le r_{i^*} < (x^*)^{n-i^*},\ 0 \le a_{i^*} < x^*$$

....

....

$$r_{n-1^*} = a_{n-1} \cdot x^* + r_{n-1} \qquad con\ 0 \le r_{n-1} < x^*,\ 0 \le a_{n-1} < x^*$$

Sostituendo nella divisione di a per $(x^*)^n$, ad r_0 la sua ***espressione*** data dalla ***divisione di r_0 per $(x^*)^{n-1}$*** e procedendo così sino alla ***divisione di r_{n-1^*} per x^****, posto ancora $r_{n-1} = a_n$ si ottiene la rappresentazione:

$$a = a_0 \cdot (x^*)^n + a_1 \cdot (x^*)^{n-1^*} + \ldots + a_{n-1} \cdot x^* + a_n$$

dove, ricordiamo, $a_0, a_1, a_{1^*}, \ldots, a_{n-1}, a_n$ sono ***numeri naturali*** rappresentati dai ***simboli fondamentali*** $0, 1, \ldots, x$ e dove le ***potenze di*** x^* possono essere espresse come ***somme*** di ***simboli fondamentali***.

Convenendo di scrivere il numero naturale a come una ***sequenza ordinata*** di ***simboli fondamentali*** che rappresentano i naturali che compaiono davanti alle potenze di x^*, in ordine decrescente, si ottiene la ***rappresentazione abbreviata*** del ***naturale*** a:

$$a = (a_0, a_1, a_{1^*}, \ldots, a_{n-1}, a_n)_{x+1}.$$

Con tale sistema siamo in grado di ***rappresentare un qualsiasi numero naturale usando solo alcuni simboli fondamentali.***

Tale metodo costituisce ciò che viene detto ***sistema di numerazione***.

Il ***numero naturale*** rappresentato dal simbolo

$$x^* = x + 1$$

è chiamato ***base*** del ***sistema di numerazione***.

ESEMPI

Numerazione in base dieci o decimale

In tale ***sistema di numerazione*** i ***simboli fondamentali*** si indicano con

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

in cui il ***simbolo*** ***2*** (due) rappresenta il ***naturale successivo*** di ***1***
in cui il ***simbolo*** ***3*** (tre) rappresenta il ***naturale successivo*** di ***2***
in cui il ***simbolo*** ***4*** (quattro) rappresenta il ***naturale successivo*** di ***3***
in cui il ***simbolo*** ***5*** (cinque) rappresenta il ***naturale successivo*** di ***4***
in cui il ***simbolo*** ***6*** (sei) rappresenta il ***naturale successivo*** di ***5***
in cui il ***simbolo*** ***7*** (sette) rappresenta il ***naturale successivo*** di ***6***
in cui il ***simbolo*** ***8*** (otto) rappresenta il ***naturale successivo*** di ***7***
in cui il ***simbolo*** ***9*** (nove) rappresenta il ***naturale successivo*** di ***8***
e dove la ***base*** del ***sistema di numerazione*** è il ***numero successivo*** a ***9***, ***9+1*** al quale si dà il nome di ***numero dieci***.

Un ***numero naturale*** ***a*** tale che:

$$a = 4 \cdot (9 + 1)^5 + 7 \cdot (9 + 1)^4 + 0 \cdot (9 + 1)^3 + 1 \cdot (9 + 1)^2 + 9 \cdot (9 + 1) + 5$$

si rappresenta con l'***allineamento*** dei ***simboli fondamentali*** ***4, 7, 0, 1, 9, 5*** e si scrive

$$a = (470195)_{9+1}$$

o, semplicemente,

$$a = 470195.$$

<u>Sistema di numerazione binaria</u>

In questo ***sistema di numerazione*** i ***simboli fondamentali*** sono ***0***, ***1***, che rappresentano i ***numeri naturali*** ***zero*** e ***uno***.
La ***base*** del ***sistema di numerazione*** è il s***uccessivo di*** ***1***, ***1 + 1***.
Si hanno, per i primi casi, le seguenti rappresentazioni:

$(0)_{1+1} = 0$

$(1)_{1+1} = 1$

$(10)_{1+1} = 1 \cdot (1 + 1) + 0$

$(11)_{1+1} = 1 \cdot (1 + 1) + 1$

$(100)_{1+1} = 1 \cdot (1 + 1)^{1+1} + 0 \cdot (1 + 1) + 0$

$(101)_{1+1} = 1 \cdot (1 + 1)^{1+1} + 0 \cdot (1 + 1) + 1$

$(110)_{1+1} = 1 \cdot (1 + 1)^{1+1} + 1 \cdot (1 + 1) + 0$ …

che, tradotte nella ***numerazione decimale***, rappresentano ordinatamente i ***naturali***:

$$0, 1, 2, 3, 4, 5, 6, \ldots$$

Il vantaggio di tale ***sistema di numerazione*** è che esso adopera solo i ***simboli fondamentali*** ***0***, ***1*** ma, se si vuole utilizzare tale vantaggio, si deve accettare in cambio il fatto che le ***rappresentazioni binarie*** di ***numeri naturali***, anche più piccoli, sono molto lunghe.

Così, per esempio, il ***numero naturale*** $(198)_{9+1}$ si rappresenta, nel ***sistema binario***, come

$$(11000110)_{1+1}$$

Nomenclatura o simbolismo nella base 10

La ***base*** maggiormente usata per rappresentare un ***numero naturale*** è la ***base*** costituita dai ***simboli***

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

che abbiamo chiamato ordinatamente: ***zero***, ***uno***, ***due***, ***tre***, ***quattro***, ***cinque***, ***sei***, ***sette***, ***otto***, ***nove***.

Essendo $x = 9$ porremo $x^* = 10 = 9 + 1$ e lo chiameremo ***dieci***.

Allora ogni ***naturale*** n si potrà scrivere in ***uno e un solo modo*** nella forma:

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_0$$

dove i simboli $a_m, \ldots, a_0$ sono ***elementi*** della ***base***.

Abbiamo convenuto allora di ***rappresentare*** il ***numero*** n ***scrivendo uno dopo l'altro i simboli della combinazione delle potenze del dieci*** e cioè

$$n = a_m\, a_{m-1} \ldots a_0$$

chiameremo tale scrittura ***posizionale*** e i ***simboli*** della scrittura verranno dette ***cifre del numero n***.
Si dirà anche che

il numero n è scritto nella base 10 o decimale.

Sorge ora il problema di dare un nome ad ogni numero che sia formato da più di una cifra ed è evidente che non si può assegnare un nome diverso per ogni numero, ma occorre dare delle regole generali che permettano l'assegnazione di un nome.

Tali regole generali almeno per i primi numeri che si incontrano presentano delle eccezioni almeno per i numeri a due cifre mentre per i numeri di cifre superiori vi sono poche regole come vedremo. Cominciamo quindi a trattare il ***caso*** dei ***numeri a due cifre***.

Nomenclatura dei numeri con due cifre.

Consideriamo nella ***base 10*** i numeri del tipo $a_1 a_0$.
Tra questi alcuni hanno un nome speciale.
Essi sono i numeri del tipo $1a_0$ ed a_10, tali numeri li scriveremo nell'ordine e scriveremo sotto ciascuno di essi il relativo nome:

Numeri $1a_0$

10 , 11 , 12 , 13 , 14 , 15
dieci, undici, dodici, tredici, quattordici, quindici
16 , 17 , 18 , 19
sedici , diciassette , diciotto , diciannove

Numeri a_10

20 , 30 , 40 , 50
venti , trenta , quaranta , cinquanta
60 , 70 , 80 , 90
sessanta , settanta , ottanta , novanta .

i rimanenti numeri a due cifre, tranne pochissimi di cui diremo, si leggono come segue:

il numero $a_1 a_0 = a_10 + a_0$ si legge con il nome di $a_1 0$ seguito dal nome di a_0.

Esempi:

$22 = 20 + 2$ (***venti – due***)
$37 = 30 + 7$ (***trenta – sette***)
$95 = 90 + 5$ (***novanta – cinque***)

Fanno eccezione i numeri del tipo:

$a_11 \ , a_18$

per i quali ***non*** si legge l'***ultima lettera di a_10*** e la parola si fonde con le parole ***uno*** ed ***otto***.

Esempi:

$21 = 20 + 1$ (***vent – uno***)
$41 = 40 + 1$ (***quarant – uno***)
$38 = 30 + 8$ (***trent – otto***)
$98 = 90 + 8$ (***novant – otto***)

Nomenclatura dei numeri a tre cifre.

Siamo così pervenuti al ***più grande numero*** a due cifre posizionali che è ***99 = 90 + 9*** (***novantanove***) il ***successivo*** del quale si indica con:

$$100 = 1 \cdot 10^2 + 0 \cdot 10 + 0 \quad (cento) .$$

Ogni ***numero a tre cifre*** è del tipo:

$$a_2\, a_1\, a_0 \;=\; a_2\, 0\, 0 \;+ a_1\, a_0$$

e si legge a_2 - ***cento*** seguito dal ***nome di*** $a_1\, a_0$ se $a_1 \neq 0$ e dal nome di a_0 se $a_1 = 0$.

Esempi:

327	(***tre – cento – ventisette***)
402	(***quattro – cento – due***)
542	(***cinque – cento – quarantadue***)

Nomenclatura dei numeri da quattro a sei cifre.

Il ***più piccolo numero*** a quattro cifre è ***1000*** che si legge "***mille***".
Per i rimanenti aventi un ***numero di cifre da 4 a 6*** si procede come segue.
Scritto il numero in forma posizionale

$$a_5 \;\; a_4 \;\; a_3 \;\; a_2 \;\; a_1 \;\; a_0$$

a partire da destra ***si staccano le prime tre cifre*** onde si legge:

nome di $a_5\ a_4\ a_3$ seguito dalla ***parola mila*** e di seguito si legge il nome di $a_2\, a_1\, a_0$ con la convenzione che se a_5 o a_4 oppure a_2 o a_1 sono ***nulli*** si esegue la lettura senza tenere conto ***dello zero,*** con la sola ***eccezione*** nel caso $1\, a_2\, a_1\, a_0$ che si legge ***mille*** seguito dal nome di $a_2\, a_1\, a_0$.

Si ha così:

27˙235	(***ventisette – mila – duecentotrentacinque***)
1˙125	(***mille – cento – venticinque***)
312˙711	(***trecentododici – mila – settecento – undici***)
70˙000	(***settanta – mila***)
800˙000	(***ottocento – mila***)
999˙999	(***novecento – novanta – nove – mila – novecento – novanta – nove***).

Vediamo ora di renderci conto come si prosegue nella ***nomenclatura*** secondo la seguente partizione:

insieme dei *numeri ad 1 cifra o unità semplici*
" " " *a 2 cifre o decine semplici*
" " " *a 3 cifre o centinaia semplici*

Insieme delle unità semplici

" " " *a 4 cifre o unità di migliaia*
" " " *a 5 cifre o decine di migliaia*
" " " *a 6 cifre o centinaia di migliaia*

Insieme delle migliaia

" " " *a 7 cifre o unità di milione*
" " " *a 8 cifre o decine di milione*
" " " *a 9 cifre o centinaia di milione*

Insieme dei milioni

Il *numero ad 8 cifre*

12˙712˙158

si legge

dodici milioni – settecento – dodici – mila - cento - cinquantotto.

i successivi *insiemi della partizione* prendono il nome di insieme dei:

bilioni o miliardi	(*10 – 11 – 12 cifre*)
tri – lioni	(*13 – 14 – 15 cifre*)
quadri – lioni	(*16 – 17* – 18 cifre)
quinti – lioni	(*19 – 20 – 21 cifre*)
sesti - lioni	(*22 – 23 – 24 cifre*)
septi – lioni	(*25 – 26 – 27 cifre*)
opti – lioni	(*28 – 29 – 30 cifre*)
novi – lioni	(*31 – 32 – 33 cifre*)
deci – lioni	(*34 – 35 – 36 cifre*) ;

onde si prosegue a partire da ***undici – lioni*** leggendo il nome davanti a ***lioni*** ***secondo il numero che esso rappresenta***. Si arriva così ad esempio ad un ***milione – lioni*** che si legge un milione di lioni e così via ma penso che nessuno sia mai arrivato a contare tanto.

Ad esempio si voglia leggere il numero

3˙102˙311˙122˙142˙002˙005

Essendo di *19 cifre* esso appartiene all' insieme dei ***quintilioni*** e si legge:
tre quintilioni – centodue quadrilioni – trecentoundici trilioni – centoventidue miliardi – centoquarantadue milioni – duemila – cinque.

Giustificazione delle operazioni elementari.

a) ***Ricerca della somma di due numeri***

Dati

$$n = a_p (x_*)^p + . . + a_0 \qquad m = b_q (x_*)^q + . . + b_0$$

qualora sia $p > q$ per le ***proprietà associativa e distributiva*** risulta:

$$n + m = a_p(x_*)^p + . . + (a_q + b_q) (x_*)^q + . . + (a_0 + b_0) = h_p (x_*)^p + . . + h_0$$

Ora $a_0 + b_0$ è un ***numero a due cifre*** del tipo

$$a_0 + b_0 = c_0 x_* + d_0 = (c_0 d_0)_x$$

pertanto si ha che $h_o = d_0$.
Il ***coefficiente di*** x_* è invece $a_1 + b_1 + c_0$ che è ancora un ***numero a due cifre*** del tipo

$$c_1 x_* + d_1$$

e sarà

$$h_1 = d_1.$$

Tale procedimento è ***ricorrente*** nel senso che determinato il coefficiente di $(x_*)^i$ con $i < q$ da

$$a_i + b_i + c_{i-1} = c_i x_* + d_i$$

si avrà

$$h_i = d_i.$$

Pertanto si avrà

$$\begin{array}{r} a_p . . . a_{q+1} a_q . . . a_1 a_0 + \\ b_q . . . b_1 b_0 = \\ \hline c_p d_p . . . d_{q+1} d_q . . . d_1 d_0 \end{array}$$

$$a_0 + b_0 = c_0 \cdot d_0$$

$$c_0 + a_1 + b_1 = c_1 \cdot d_1$$

. . . .

$$c_{q-1} + a_q + b_q = c_q \cdot d_q$$

$$c_q + a_{q+1} = c_{q+1} \cdot d_{q+1}$$

. . . .

$$c_{p-1} + a_p = c_p \cdot d_p .$$

b) ***Ricerca del prodotto di due numeri.***

Posto $\boldsymbol{n \cdot m = h_r \cdot (x_*)^r + .. + h_0}$

si ha:

$$\boldsymbol{n \cdot m = a_0 \cdot m + a_1 \cdot m \cdot x^* + .. + a_p \cdot m \cdot (x_*)^p} =$$

$$= \boldsymbol{(a_i \cdot (x_*)^i)\ (b_0 + b_1 \cdot X_* + .. + b_q \cdot (x_*)^q)} =$$

$$= \boldsymbol{a_i \cdot b_0 \cdot (x_*)^i + a_i \cdot b_1 \cdot (x_*)^{i+1} + .. + a_i \cdot b_q \cdot (x_*)^{q+1}} =$$

$$= \boldsymbol{h_r \ldots h_{i+1}\, 0_i \ldots 0_1}$$

ove le ***cifre*** si trovano con procedimento analogo a quello della somma essendo $\boldsymbol{a_i \cdot b}$ un ***numero a due cifre***.

Si ha il quadro :

$$\begin{array}{rrrrrrr} \boldsymbol{b_q} & . & . & . & & \boldsymbol{b_0} & \\ & \boldsymbol{a_i} & \boldsymbol{0_{i-1}} & . & . & . \ \boldsymbol{0_1} & = \\ \hline \hline . & . & \boldsymbol{d_1\ d_o} & \boldsymbol{0_{i-1}} & . & \ldots\ \boldsymbol{0_1} & \end{array}$$

$\boldsymbol{a_i . b_0 = c_0 . x^* + d_0}$

$\boldsymbol{c_0 + a_i . b_i = c_1 . x^* + d_i}$

…………………………

etc.

E' importante quindi conoscere il ***prodotto*** dei ***simboli fondamentali*** che si ricavano dalla tabella :

	0	1	…..	x
0	0	0		0
1	0	1		x
…	…	…	…	…
x	0	x		

che prende il nome di ***Tavola Pitagorica***.

NUMERI ORDINALI FINITI

Se ***A*** è un insieme non vuoto , ed ***R*** è una ***relazione di ordine*** su ***A*** , la coppia

$$(A, R)$$

si dice ***insieme ordinato*** .

Se inoltre rispetto alla ***R*** ogni ***sottoinsieme non vuoto*** di ***A*** ha ***minimo*** la coppia ***(A , R)*** si dice ***insieme bene ordinato***.

Poniamo le seguenti ***definizioni*** :

Dati ***due insiemi bene ordinati (A, R) , (B, S)*** ed un'***applicazione***

$$f : A \rightarrow B ,$$

diremo che ***f*** è una ***similitudine*** di ***(A, R) su (B, S)*** se :

- ***a) f è una biiezione ;***
- ***b) $\forall a , b \in A$ si ha $a R b \Leftrightarrow f(a) \; S \; f(b)$.***

Diremo inoltre che ***(A, R)*** e ***(B, S) bene ordinati*** sono ***isotoni*** (o ***simili***) , e scriveremo :

$$(A, R) \sim (B, S)$$

se tra essi è definita una similitudine .

La ***relazione " ~ "*** di ***isotonia*** tra ***insiemi bene ordinati*** é una ***relazione di equivalenza sulla classe degli insiemi bene ordinati***.

Chiameremo tipo di ordinale o numero ordinale dell'insieme bene ordinato (A, R) la classe di isotonia dell'insieme (A, R) .

Chiameremo ***numeri ordinali naturali*** o ***ordinali finiti*** le ***classi di isotonia di insiemi ben ordinati*** il cui sostegno ***A sia finito*** .

Chiameremo ***tipi di ordinali trasfiniti*** o ***ordinali trasfiniti*** le ***classi di isotonia di insiemi bene ordinati*** il cui sostegno ***A sia infinito*** .

Sussiste il seguente

Teorema

Se A e B sono insiemi finiti non vuoti , allora quali che siano gli insiemi bene ordinati (A, R) , (B, S) si ha :

$$(A, R) \sim (B, S) \Leftrightarrow A \sim B$$

Dimostrazione

C.N. $\Rightarrow$
Per ***ipotesi*** ***(A, R) ~ (B, S)***.
Allora la ***similitudine f*** esistente tra gli ***insiemi ordinati*** è una ***biiezione tra A e B*** da cui

$$A \sim B .$$

C. S. $\Leftarrow$
Per ***ipotesi A e B sono finiti e equipotenti*** .
Sia $n = pot\ A = pot\ B$, con $n \in N_1$.
Siano a_0 e b_0 i ***minimi di A e B*** .
Siano a_1 e b_1 i ***minimi di*** $A_1 = A - a_0$ e di $B_1 = B - b_0$.
Siano ora A_h e B_h due ***sottoinsiemi di A e B***, indicheremo con a_{h+1} e b_{h+1} i ***minimi di*** A_h ***e*** B_h.
Se al ***naturale h*** diamo successivamente i valori $1 , 2 , ... , n-1$ si otterranno gli insiemi

$$\{a_0 \ , ... , a_{n-1}\} = A \ , \qquad \{b_0 , ... , b_{n-1}\} = B .$$

L′ applicazione $f : A \rightarrow B$ definita ponendo :

$$f(a_h) = b_h \qquad \forall\ h \in N_0 - N_n$$

è una ***similitudine*** tra ***(A, R) e (B, S)*** poiché se $\forall h < k$ è $a_h < a_k$ è anche per costruzione

$$b_h < b_k$$

Significato dei numeri ordinali finiti .
In virtù del **teorema** precedente ***ad ogni sottoinsieme di un insieme finito si può associare un ordinale***, per cui ***ad ogni numero naturale non nullo si può associare un ordinale***.

Esiste quindi un'***applicazione naturale biiettiva*** :

$$a : N_1 \rightarrow M_1$$

con M_1 ***insieme degli ordinali finiti***, definita ponendo

$$a(n) = [A, R] \qquad \forall n \in N_1,$$

classe di isotonia di ***(A, R)*** , dove ad esempio risulta $A = \ell\ N_n$ (rispetto ad N_0) con la ***relazione di buon ordinamento naturale*** .

Ora osserviamo che
dato un ***qualsiasi insieme finito*** e ***bene ordinato*** ***(A, R)*** con $pot\ A = n$ tale insieme è sempre ***isotono all'insieme bene ordinato***

$$(N , \leq) = (\ell_{N1}N_{n+1} , \leq) .$$

Pertanto ***ad ogni elemento di (A, R)*** si può ***associare*** mediante la relativa ***similitudine*** un ***numero naturale*** e di conseguenza l'***ordinale corrispondente***; cioè, se ***ad*** $x \in A$ ***finito associamo*** un certo ***cardinale*** $h \in N_1$, ***ad h associamo*** l'***ordinale a(h)***.

L'elemento ***a(h) associato*** ad ***h*** ed ad $x \in A$ si usa come un *aggettivo* e si legge con il ***nome del cardinale h*** in cui si sopprime l'ultima lettera seguito da

-esimo , ***-esima*** , ***-esimi*** , ***-esime***

a seconda che l'***oggetto x*** sia *maschile singolare*, *femminile singolare*, *maschile plurale*, *femminile plurale*.

Se in un ***sistema di numerazione*** è nota la lettura e la scrittura di ***n*** si porrà :

$$a(n) = n^{o}$$

usandosi per il simbolo ***'*** ^{o} ***'*** un simbolo ***diverso dallo 0*** (zero), come dimensione .

Fanno ***eccezione*** alla lettura degli ***ordinali corrispondenti*** agli ***elementi*** di $N_1 - N_{11}$ che si leggono come nella seguente tabella :

- ***a(1)*** ***primo – prima – primi – prime***
- ***a(2)*** ***secondo - seconda- secondi-seconde***
- ***a(3)*** ***terzo – terza - terzi - terze***
- ***a(4)*** ***quarto – quarta – quarti - quarte***
- ***a(5)*** ***quinto – quinta – quinti - quinte***
- ***a(6)*** ***sesto – sesta – sesti - seste***
- ***a(7)*** ***settimo – settima – settimi - settime***
- ***a(8)*** ***ottavo – ottava – ottavi - ottave***
- ***a(9)*** ***nono – nona – noni - none***
- ***a(10)*** ***decimo – decima – decimi - decime***

In matematica si suole considerare anche l'aggettivo ***zeresimo***, ***zeresima***, ***zeresimi***, ***zeresime*** che può essere considerato ***numero ordinale*** qualora si consideri l'***applicazione*** :

$$b = a\ s: N_0 \rightarrow M_1$$

definita ponendo $a\,s(n) = a\,(n+1)$, pertanto l' aggettivo introdotto è il ***simbolo***

b(0) .

Esempi di ***ordinali*** li abbiamo già incontrati a [pag.1] per i simboli distintivi dei ***due* teoremi *di induzione matematica*** .

L′ ***insieme dei due teoremi*** è ***ordinato*** in quanto ***una dimostrazione precede l'altra .***
Ai due ***sottoinsiemi non vuoti { I } {I, II}*** e ***bene ordinati*** abbiamo associato i nomi ***primo*** e ***secondo*** . Così nella ***definizione di coppia*** , si definisce il simbolo ***(a, b)*** che è dato dall'insieme ***{{a}, {a, b}} ben ordinato*** naturalmente ***rispetto all'inclusione*** .

Le cifre romane il simbolismo degli ordinali finiti

Vogliamo qui esporre brevemente la ***numerazione romana***, i cui simboli sono spesso oggi usati per indicare gli ***ordinali finiti*** e non già i ***cardinali*** .

I ***simboli fondamentali*** di questa ***numerazione*** sono :

I, V, X, L, C, D, M,

corrispondenti ai nostri ***ordinali***:

1°, 5°, 10°, 50°, 100°, 500°, 1000°.

Regole di formazione per più cifre.

a) ***Le cifre eguali si sommano.***

Esempi: XX = 20°; III = 3°; CCC = 300°.

b) ***Le cifre si sommano se la maggiore è a sinistra della minore, si sottraggono se la maggiore è a destra della minore***.

Esempi: MIII = 1003° CXV = 135°
IC = 99° XCC = 190°.

c) ***Una lineetta sovrapposta al simbolo romano moltiplica per 1˙000 il cardinale corrispondente***.

d) Il ***simbolo*** $\boxed{\quad\quad}$ ***entro cui si scrive il numero moltiplica il cardinale corrispondente per 100˙000.***

Esempi : $\overline{\text{MCIII}}$ = 1˙103˙000° (unmilionecentotremila-esimo)

$\boxed{\text{DILIII}}$ = [(500+40+3)·(100˙000)]°=(54˙300˙000)° (cinquecentoquarantatremil-esimo)

e) ***La seguente facoltativa convenzione permette di eliminare due simboli fondamentali.***

Si ponga: ***D = I*** ***M = CI*** da cui

a) ogni) posta a destra del simbolo I moltiplica il cardinale corrispondente per 10,

b) ***il cardinale corrispondente al segno CI si moltiplica per 10,100,1000 a seconda che si pongano una C a sinistra e una) a destra, due C a sinistra e due) a destra , tre C a sinistra***

Considerazioni didattiche sui numeri naturali,

Le questioni che vengono esposte nel seguente paragrafo costituiscono una indicazione su alcuni modi di introdurre i numeri naturali nelle scuole secondarie, evitando s'intende un'esposizione pressoché completa

Infatti penso che leggendo le pagine precedenti, chiunque si convinca, come una tale esposizione è in primo luogo fuori posto in una scuola secondaria, in secondo luogo i discenti alle prime armi verrebbero spaventati dalla imponente mole di ***proprietà*** e ***teoremi*** al punto tale di odiare la matematica *più di quanto già non facciano.*

In ogni caso a mio avviso pur dando per ***primitivo*** (cioè a tutti noto) il ***concetto di numero naturale*** e il ***concetto di zero***, nonché delle ***operazioni S*** e ***P*** e della ***relazione d'ordine***, *è a mio parere* importante insistere sulle ***proprietà delle operazioni*** e della ***relazione d'ordine***, *più che dimostrando* illustrando le ***numerose proprietà*** con molteplici esempi e rimandando a più tardi ***l'iniziazione alle dimostrazioni.***

L'esigenza di semplificare la trattazione dei numeri naturali aumenta se pensiamo che attualmente i numeri naturali sono introdotti nella Scuola Media Inferiore ed alle Superiori sono soltanto richiamati.
Un po' diverso sarà il discorso a proposito degli ***interi relativi***.

Propongo qui tre vie per introdurre i numeri naturali con ordine crescente di difficoltà.

A. Si inizia dicendo che i ***numeri naturali*** sono i ***simboli*** ben noti:

$$0 , 1 , 2 , \ldots , n , \ldots$$

ed è noto il significato della scrittura

$$0 < 1 < \ldots < n < \ldots$$

$$\ldots > n > n-1 > \ldots > 1 > 0 .$$

Si elencano quindi le proprietà più note delle ***operazioni di addizione e moltiplicazione***, corredandole di numerosi esempi

A mio avviso, secondo la classe, il Docente potrà farne un numero maggiore o minore.

Indi, dopo aver posto il problema delle ***operazioni inverse***, si può passare al concetto di ***Massimo Comune Divisore***, ***minimo comune multiplo*** e di ***divisione con resto*** nonché al ***concetto di numero primo*** ed all'***enunciato del teorema fondamentale dell'aritmetica***.

Un breve cenno sul ***teorema di rappresentazione***, sulla ***nomenclatura dei numeri***, sulla ***numerazione binaria*** può concludere lo studio dei numeri.
Punti importanti su cui battere sono le ***proprietà associativa e commutative*** illustrandone ampiamente il significato, della ***proprietà distributiva*** e dell'***uso delle parentesi***, il tutto per spiegare la risoluzione delle espressioni. Occorre mettere ben in rilievo il fatto che le ***operazioni inverse non sono sempre possibili.***

B. Il punto di partenza dell'esposizione di tipo A. può essere ampliato se sono verificate le seguenti condizioni:

a) La classe è costituita da elementi piuttosto svegli.
b) L'insegnante ritiene che fin dalla *prima media* debbono essere introdotti, almeno dal punto di vista intuitivo, i primi elementi di ***Teoria degli insiemi***.
Sotto queste condizioni si può tentare una via che permette una definizione di ***numero naturale*** procedendo nel modo seguente.

Sia $\{a\}$ un insieme costituito dal ***solo elemento a.***
Considero ***tutti gli insiemi di tale tipo,*** chiamo ***numero 1*** il ***quid comune a questi insiemi***, o anche la ***totalità di tutti gli insiemi*** di tale tipo.
Se a e b sono tali che $a \neq b$ chiamo ***2*** il ***simbolo*** associato all'***insieme***
$\{a\} \cup \{b\}$ e così via.

Si possono a questo punto definire anche le ***operazioni S*** e ***P*** mediante $\cup$ e $\cdot$ nonché il ***simbolo*** $>$ mediante $\supset$.

Consiglio in questo caso molti ***esempi*** per vedere le operazioni e il confronto a partire da insiemi dati nonché la collaborazione del Professore di disegno per preparare tavole illustrative mediante ***diagrammi di Venn***.

C. Se la classe è in media particolarmente dotata si può tentare un'altra strada. Tale strada è particolarmente feconda qualora la si usi nelle prime classi del superiore per esporre dei richiami. Tale metodo è applicabile dagli insegnanti che intendono premettere, oltre alle prime nozioni di teoria degli insiemi, anche nozioni sulle ***strutture algebriche*** ed in particolare: ***operazioni binarie su insiemi, proprietà delle operazioni, concetto di semigruppo, gruppo, anello, campo.***

A tale proposito i ***naturali*** possono essere richiamati come esempio di ***semigruppo**** e, in questo ordine, di idee si presentano abbastanza spontanee le ***proprietà delle operazioni inverse*** che ***non sono sempre definite***, mostra come esistono ***semigruppi che non sono gruppi***.

Praticamente interessanti da questo punto di vista sono le ***classi resto modulo un naturale ≥ 2*** poiché mediante esse possono mostrarsi esempi di tutte le strutture sopra indicate nonché ***esempi di divisori dello zero***.

Spero che queste pagine, direi di consigli, possano essere utili a qualche neo – insegnante che desideri insegnare modernamente la matematica, senza lasciarsi influenzare da coloro che invece parlano di insegnare la matematica moderna come se si trattasse di una matematica diversa da quella che si è sempre insegnata e che pertanto ritengono di non dover cambiare.