II

Numeri naturali

6. L'INSIEME DEI NUMERI NATURALI

6.1. I numeri naturali: approccio cardinale

Alla fine del XIX secolo, l'intera comunità matematica si trovò impegnata nella puntualizzazione rigorosa dei fondamenti della disciplina: le teorie di George Boole (1815-1864) e di Georg Cantor (1845-1918) e le ricerche logico-matematiche di Gottlob Frege sono testimonianze chiare dello spirito che pervase un ampio settore della ricerca matematica di quel periodo.

Ci siamo già occupati dell'opera di Frege nella presentazione dell'antinomia di Russell; nel 1884, Frege pubblicò *Die Grundlagen der Arithmetik*, l'opera in cui si trova la fondamentale definizione di numero. Egli introduce il numero "zero" facendolo corrispondere al concetto di "diverso da se stesso" (ovvero ad una condizione di impossibilità): potremmo dire che, per Frege, "zero" è la… quantità di elementi che verificano una condizione impossibile.

A partire dallo zero, Frege introduce ricorsivamente ogni altro naturale, ciascuno sulla base del precedente: così il numero 1 è associato al (solo) concetto di "zero" (si tratta dunque di *un* concetto, considerato singolarmente), il numero 2 ai (*due*) concetti di "zero" e di "uno", il numero 3 ai (*tre*) concetti di "zero", di "uno" e di "due", e così via.

Illustreremo una costruzione di **N** sulla base della teoria degli insiemi.

Definizione. Due insiemi A, B si dicono *equipotenti* se sono in corrispondenza biunivoca, cioè quando esiste una funzione biiettiva di dominio A ed insieme delle immagini B.

Esempio. Considerato un triangolo qualsiasi, l'insieme A dei suoi lati e l'insieme B delle sue mediane sono equipotenti.

Per verificare tale affermazione è sufficiente considerare la relazione $R \subseteq A \times B$ che ad ogni lato $a \in A$ fa corrispondere la mediana $b \in B$ avente per estremi il vertice opposto al lato a ed il punto medio dello stesso lato a.

La relazione R è una funzione: infatti, ad ogni lato del triangolo corrisponde, nella relazione introdotta, una ed una sola mediana. Questa funzione è inoltre suriettiva, giacché ogni mediana è corrispondente, nella R, di un lato (quello avente come punto medio l'estremo della mediana non coincidente con un vertice del triangolo); è inoltre iniettiva, in quanto a due lati distinti corrispondono due distinte mediane (i loro estremi non coincidenti con un vertice sono i punti medi di due lati distinti): R è una funzione biiettiva.

In base alla definizione concludiamo che A e B sono equipotenti.

(Contro)esempio. L'insieme I = {0; 1} e l'insieme J = {10; 11; 12} *non* sono equipotenti. Se consideriamo, ad esempio, la funzione f: I→J definita da:

$$x \rightarrow x+10$$

ci rendiamo conto che è una funzione iniettiva ma *non* suriettiva (il suo insieme delle immagini è {10; 11} e *non* coincide con l'intero J), quindi *non* biiettiva.

Non esiste alcuna funzione biiettiva I→J. Gli insiemi I e J non sono dunque equipotenti.

Nel seguito considereremo gli insiemi di cui ci siamo finora occupati (ed altri insiemi che possiamo immaginare) come elementi di un insieme U. Importanti motivazioni ci impediscono però assolutamente di parlare di 'insieme costituito da *tutti* gli insiemi": dunque, l'insieme U dovrà essere considerato soltanto un insieme al quale appartengono, come elementi, altri insiemi, senza alcuna pretesa di totalità.

Osservazione. Tale questione merita sin d'ora un cenno di approfondimento. Indichiamo con #I il cardinale di un insieme I che identificherà l'insieme degli insiemi J equipotenti con I (torneremo più avanti su questa importante nozione). Ad esempio, se:

$$A = \{3; 7\} \qquad B = \{\alpha; \beta\} \qquad C = \{\heartsuit; \spadesuit\}$$

possiamo scrivere:

$$\#A = \#B = \#C$$

Se #D ≤ #E significa che D è equipotente ad un sottoinsieme di E.

Ricordiamo che l'insieme delle parti $\wp(I)$ è l'insieme costituito da tutti i sottoinsiemi di I. A tale proposito, sussiste il *teorema di Cantor*, secondo il quale per ogni insieme I, è: $\#I < \#\wp(I)$.

Immaginiamo ora, per assurdo, di poter parlare dell'*insieme totale* (insieme di 'tutti gli insiemi") T; risulterebbe:

$$\wp(T) \subseteq T$$

(infatti T è l'insieme 'totale"!) e quindi concluderemmo:

$$\#\wp(T) \leq \#T$$

contro il teorema di Cantor, che porta invece a scrivere: $\#T < \#\wp(T)$.

Definiamo in U la relazione di equipotenza, precedentemente introdotta. Verificheremo che essa è una relazione di equivalenza, cioè che è riflessiva, simmetrica e transitiva.

Proposizione. La relazione di equipotenza tra insiemi è una relazione di equivalenza.

Dimostrazione. Verifichiamo direttamente le tre proprietà della relazione di equivalenza.

- La relazione di equipotenza tra insiemi è *riflessiva*. Infatti, ogni insieme $I \in U$ è equipotente a se stesso: si consideri, a tale riguardo, l'identità, ovvero quella relazione che ad ogni elemento di $x \in I$ fa corrispondere x stesso. È semplice verificare che si tratta di una funzione biiettiva (il lettore può farlo, per esercizio): conseguentemente, in base alla definizione 1, ogni insieme I risulta equipotente a se stesso.
- La relazione di equipotenza tra insiemi è *simmetrica*. Infatti, se $I \in U$ è equipotente a $J \in U$, significa (per definizione) che esiste una funzione biiettiva f: $I \to J$; essendo f biiettiva, f risulta invertibile, e la funzione inversa è f^{-1}: $J \to I$, anch'essa biiettiva (ad ogni elemento di J fa corrispondere uno ed un solo elemento di I e viceversa). Pertanto, anche J è equipotente ad I (per la definizione).
- La relazione di equipotenza tra insiemi è *transitiva*. Infatti, se $I \in U$ è equipotente a $J \in U$ ed inoltre $J \in U$ è equipotente a $L \in U$, significa (per definizione) che esistono due funzioni biiettive f: $I \to J$ e g: $J \to L$. Consideriamo la funzione composta $g \bullet f$: $I \to L$: anch'essa è biiettiva (ad ogni elemento di I fa corrispondere uno ed un solo elemento di L e viceversa). Pertanto, anche I è equipotente a L (per la definizione). cvd

Ripercorreremo, in questo paragrafo, la costruzione dell'insieme quoziente. Dovremo inizialmente sviluppare tale procedimento nell'ambito degli insiemi *finiti*; escluderemo quindi dalle nostre considerazioni, in questa prima fase, gli insiemi *infiniti*, dei quali ci occuperemo specificamente in seguito.

L'introduzione dei concetti di insieme finito e di insieme infinito si basa su di una constatazione: in molti casi, un insieme non è equipotente ad un suo sottoinsieme proprio. Il lettore può rendersi conto di ciò verificando direttamente tale impossibilità: ad esempio, non si può definire alcuna funzione biiettiva f: $A \to B$, essendo $A = \{0; 1\}$ e B il suo sottoinsieme proprio $\{1\}$.

Questo comportamento, però, non è caratteristico di *tutti* gli insiemi: esistono infatti insiemi che sono equipotenti ad alcuni loro sottoinsiemi propri.

(Contro)esempio. Consideriamo l'insieme $P = \{0; 2; 4; 6; 8; ...\}$ dei numeri naturali *pari* (considerando pari anche lo zero) ed il suo sottoinsieme $I = \{2; 4; 6; 8; ...\}$ dei numeri naturali *pari e diversi da zero*. Mostreremo che, sebbene I sia un sottoinsieme *proprio* di P, i due insiemi P e I sono equipotenti.

Consideriamo infatti la funzione f: $P \to I$ così definita:

$$f: x \to x+2$$

Tale funzione è biiettiva: ad ogni $x \in P$ corrisponde, infatti, attraverso la funzione f, uno ed un solo $x+2 \in I$; viceversa, ad ogni elemento di I corrisponde uno ed un solo elemento di P attraverso la funzione inversa:

$$f^{-1}: x \to x-2$$

Pertanto P ed I sono equipotenti (per definizione); sottolineiamo ancora che I è un sottoinsieme *proprio* di P: infatti è:

$$P \setminus I = \{0\} \neq \varnothing$$

Le definizioni di insieme finito e di insieme infinito si baseranno proprio sui due diversi comportamenti ora illustrati: in particolare, diremo finito ogni insieme che si comporterà analogamente a $\{0; 1\}$, diremo infinito ogni insieme che si comporterà analogamente a P. Possiamo dunque formalizzare quanto sopra introdotto nella seguente definizione.

Definizione. Un insieme si dice *infinito* se è equipotente ad un suo sottoinsieme proprio. Un insieme si dice *finito* se non è equipotente ad alcun suo sottoinsieme proprio.

Come sopra anticipato, concentriamo la nostra attenzione, in un primo momento, sugli insiemi *finiti*. Se indichiamo, come già sopra fatto, con U un insieme avente per elementi insiemi (finiti ed infiniti), possiamo indicare con $U_f \subseteq U$ un insieme avente per elementi (soltanto) insiemi *finiti*. In U_f consideriamo la relazione di equipotenza tra insiemi: la dimostrazione della proposizione 1 (inizialmente formulata nel caso di insiemi qualsiasi) assicura che tale relazione è una relazione di equivalenza.

La cercata introduzione dell'insieme **N** è ora assai semplice: consideriamo infatti le classi di equivalenza determinate in U_f dalla relazione di equipotenza; e consideriamo, infine, l'insieme quoziente avente tali classi di equivalenza come elementi. Non è difficile identificare ciascuna di tali classi di equivalenza con un numero naturale *n* (intuitivamente: il numero *n* degli elementi appartenenti a ciascuno degli insiemi della classe di equivalenza); si dice che ogni elemento appartenente alla classe di equivalenza in questione ha *potenza* (o *cardinalità*) *n*. L'insieme quoziente può dunque essere interpretato come l'insieme **N** dei numeri naturali.

Il naturale "zero" è dunque identificabile con la classe di equivalenza avente quale unico elemento l'insieme vuoto; potremo dire che l'insieme vuoto ha potenza 0.

Esempio. Il numero naturale 2 si identifica con la classe di equivalenza (riferita alla relazione di equipotenza tra insiemi) alla quale appartiene l'insieme I = {0; 1} e pertanto anche tutti gli insiemi ad esso equipotenti (l'insieme delle lenti di un comune paio di occhiali, l'insieme delle ruote di una bicicletta etc.).

Ogni insieme appartenente alla classe di equivalenza indicata ha potenza 2.

6.2. I numeri naturali: approccio ordinale

Nel paragrafo precedente abbiamo descritto un possibile modo di introdurre l'insieme dei numeri naturali. Esso non è però l'unico: molto interessante, anche per alcune implicazioni applicative, è il seguente, che viene fatto risalire (1891) all'opera di Giuseppe Peano (1858 -1932). Egli propose un'introduzione assiomatica dell'aritmetica, basata su tre concetti primitivi e su sei assiomi.

Nella teoria di Peano, così come essa fu definitivamente enunciata in *Aritmetica*, seconda parte del secondo volume di *Formulaire de mathematiques* (1898), i tre concetti primitivi sono:

- lo *zero*;
- il *numero*;
- il *successivo.*

Gli assiomi sono:

- **Assioma zero.** I numeri formano una classe.
- **Assioma I.** Lo zero è un numero.
- **Assioma II.** Se *a* è un numero, il suo successivo *a*+ è un numero.
- **Assioma III.** Se *s* è una classe contenente lo zero e, per ogni a, se *a* appartiene a *s*, il successivo *a*+ appartiene a *s*, allora ogni numero naturale è in *s* (Peano chiama tale proposizione *principio di induzione*).
- **Assioma IV.** Se *a* e *b* sono due numeri e se i loro successivi *a*+, *b*+ sono uguali, allora *a* e *b* sono uguali.
- **Assioma V.** Se *a* è un numero, il suo successivo *a*+ non è zero.

Osservazione. Sulla necessità dell'Assioma zero notiamo che esso spiega che alla classe dei numeri naturali possiamo applicare il "calcolo delle classi" che Peano stesso aveva sviluppato *precedentemente* nel proprio libro.

La relazione introdotta da Peano è dunque un'applicazione: $a \to a+$ avente per dominio **N** e per codominio **N**\{0}; si può facilmente dimostrare che essa è una biiezione. Dall'esame di tali assiomi, e segnatamente ricordando il concetto di successivo, si può dimostrare che Peano introduce in **N** un ordine stretto.

Applicando opportunamente i propri assiomi, ed approntando le necessarie dimostrazioni, Peano giunse ad introdurre le operazioni aritmetiche con i numeri naturali, nonché a descrivere ed a dimostrare le loro proprietà formali.

Esempio. Sarà interessante osservare che Peano introdusse una simbologia originale. Gli assiomi sopra riportati, in tale simbologia, si scrivono:

$\cdot 0 \quad N_0 \in \mathrm{Cls}$

$\cdot 1 \quad 0 \in N_0$

$\cdot 2 \quad a \in N_0 \mathrel{.\supset.} a+ \in N_0$

$\cdot 3 \quad s \in \mathrm{Cls} \mathrel{.} 0 \in s : a \in s \mathrel{.\supset_a.} a+ \in s : \supset . N_0 \supset s$ Induct

$\cdot 4 \quad a, b \in N_0 \mathrel{.} a+ = b+ \mathrel{.\supset.} a = b$

$\cdot 5 \quad a \in N_0 \mathrel{.\supset.} a+ \mathrel{-=} 0$

Osservazione. Dal punto di vista storico, Campano, nella sua traduzione-edizione degli *Elementi* di Euclide (seconda metà del XIII secolo) introdusse un'interessante assiomatizzazione dei naturali. Nella definizione III del libro VII, l'Autore introduce come "serie naturale dei numeri" la successione

numerica i cui elementi si ottengono per addizione ripetuta dell'unità (*Naturalis series numerorum dicitur, in qua secundum unitatis additionem fit computatio ipsorum*) e ne indica alcune proprietà in quattro *petitiones* (Labella, 2000).

6.3. La rappresentazione dei numeri naturali

La moderna rappresentazione dei numeri naturali, ottenibile mediante le dieci cifre 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, viene detta *posizionale* in base dieci. Ciò significa che il valore di ogni singola cifra che compone la rappresentazione di un numero n dipende dalla posizione di tale cifra in quella rappresentazione; il valore (totale) n del naturale rappresentato da una sequenza ordinata di cifre:

$$\{a_m, a_{m-1}, ..., a_2, a_1, a_0\}$$

è calcolabile mediante l'espressione:

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + ... + a_2 \cdot 10^2 + a_1 \cdot 10^1 + a_0 \cdot 10^0$$

Esempio. Il valore del numero 35206 (scritto in notazione decimale, cioè in base dieci) è dato dalla somma:

$$3 \cdot 10^4 + 5 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10^1 + 6 \cdot 10^0 = 30000 + 5000 + 200 + 0 + 6$$

Osservazione. La storia della matematica registra, lungo il corso dei secoli, il susseguirsi di metodi diversi per la rappresentazione dei naturali. Il sistema di scrittura dei numeri nelle matematiche del mondo antico (con l'eccezione dell'aritmetica babilonese) non si avvale del la notazione posizionale: il valore di un numero risulta semplicemente dalla somma dei valori associati ai simboli che, indicati uno di seguito all'altro, vengono a costituire il numero stesso; tali valori sono fissi, cioè non dipendono (a parte qualche rara eccezione) dalla posizione del simbolo nella scrittura del numero. Una ben nota rappresentazione di questo genere per i numeri naturali, detta *additiva*, è caratteristica dell'aritmetica romana.

Esempio. Ricordando che il valore dei simboli romani M, C, L, X, V, I è rispettivamente 1000, 100, 50, 10, 5, 1, il numero romano scritto nella forma:

MCLXXVIII

è dato, additivamente, da:

$$1000 + 100 + 50 + 10 + 10 + 5 + 1 + 1 + 1 = 1178$$

Prima di chiudere il presente paragrafo, è doveroso riservare un accenno ai sistemi di numerazione posizionale non decimale, ovvero che si avvalgono di basi diverse da dieci. È infatti possibile scegliere come base del sistema di numerazione un numero *b* diverso da dieci (importanti sono, ad esempio per le applicazioni al calcolo automatico, le basi *due* e *sedici*).

Ciò significa che il valore *n* del numero naturale (scritto nella base *b*) rappresentato da una sequenza ordinata di cifre:

$$\{a_m, a_{m-1}, ..., a_2, a_1, a_0\}$$

è calcolabile mediante la formula:

$$n = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + ... + a_2 \cdot b^2 + a_1 \cdot b^1 + a_0 \cdot b^0$$

Esempio. Il valore del numero 35206 scritto in notazione posizionale in base *sette* è dato dalla somma:

$$3 \cdot 7^4 + 5 \cdot 7^3 + 2 \cdot 7^2 + 0 \cdot 7^1 + 6 \cdot 7^0$$

In base *dieci*, tale numero è rappresentato da:

$$3 \cdot 2401 + 5 \cdot 343 + 2 \cdot 49 + 0 \cdot 7 + 6 \cdot 1 = 9022$$

Lasciamo al lettore il compito di verificare che in base *due* tale numero è rappresentato da:

10001100111110

6.4. Proprietà di operazioni aritmetiche e insiemistiche: l'algebra di Boole

Un confronto tra le operazioni aritmetiche di addizione e di moltiplicazione e le operazioni insiemistiche di unione e di intersezione ci consentirà di evidenziare analogie (e differenze) che potranno essere utilmente approfondite in studi ulteriori.

Agli allievi è ben noto, a partire dalle scuole primarie, che le operazioni aritmetiche di addizione e di moltiplicazione godono delle proprietà *associativa* e *commutativa*; cioè per ogni scelta dei numeri naturali a, b, c risulta:

$(a+b)+c = a+(b+c)$	(proprietà associativa dell'addizione)
$a+b = b+a$	(proprietà commutativa dell'addizione)
$(ab)c = a(bc)$	(proprietà associativa della moltiplicazione)
$ab = ba$	(proprietà commutativa della moltiplicazione)

Non sarà inutile ribadire che anche le operazioni insiemistiche di unione e di intersezione godono di analoghe proprietà, come precedentemente visto:

$(A\cup B)\cup C = A\cup(B\cup C)$	(proprietà associativa dell'unione)
$A\cup B = B\cup A$	(proprietà commutativa dell'unione)
$(A\cap B)\cap C = A\cap(B\cap C)$	(proprietà associativa dell'intersezione)
$A\cap B = B\cap A$	(proprietà commutativa dell'intersezione)

Va segnalato che un'analogia tra le operazioni aritmetiche e insiemistiche deve però tenere presente alcune differenze; ad esempio, ricordiamo le due seguenti proprietà che coinvolgono sia l'unione che l'intersezione:

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

solo la seconda ha un analogo in ambito aritmetico (detta *distributiva*):

$$a(b+c) = ab+ac$$

mentre ciò non accade per la prima: infatti $a+bc$ non è (in generale) uguale a $(a+b)(a+c)$.

Quanto ora osservato ci dà l'occasione di introdurre le *algebre di Boole* (dal nome di George Boole).

Come primo esempio, introduttivo ma fondamentale, consideriamo l'insieme $\wp(I)$ delle parti di un insieme I.

Esempio. Sia $(\wp(I), \subseteq)$ l'insieme delle parti di un insieme I, parzialmente ordinato mediante la relazione di inclusione.

Dati due elementi di $\wp(I)$, A e B, possiamo costruire la loro intersezione, $A\cap B$, e la loro unione, $A\cup B$.

Dal punto di vista dell'inclusione, $A \cap B$ è il più grande sottoinsieme di I incluso sia in A che in B; ciò si esprime dicendo che $A \cap B$ è l'unico sottoinsieme di I che soddisfa:

(1) $A \cap B \subseteq A$ e $A \cap B \subseteq B$
(2) per ogni $C \subseteq A$, $C \subseteq B$ si ha che $C \subseteq A \cap B$

Analogamente, $A \cup B$ è il più piccolo sottoinsieme di I in cui sono inclusi sia A che B; ciò si esprime dicendo che $A \cup B$ è l'unico sottoinsieme di I che soddisfa:

(1) $A \cup B \supseteq A$ e $A \cup B \supseteq B$
(2) per ogni $D \supseteq A$, $D \supseteq B$ si ha che $D \supseteq A \cup B$

Analoghe operazioni possono essere introdotte anche in altri insiemi ordinati: ad esempio, nel caso di **N** e della relazione di divisibilità, le operazioni risultano essere il massimo comune divisore e il minimo comune multiplo.

Generalizziamo ora quanto visto e consideriamo un insieme ordinato $(X, \leq)$.

Definizione. In un insieme parzialmente ordinato $(X, \leq)$ si dice *massimo comune minorante* $a \cap b$ per una coppia di elementi $(a; b)$ un elemento tale che: $a \cap b \leq a$, $a \cap b \leq b$ e per ogni $c \leq a$, $c \leq b$ si ha che $c \leq a \cap b$.

Si dice *minimo comune maggiorante* $a \cup b$ un elemento tale che: $a \cup b \geq a$, $a \cup b \geq b$ e per ogni $d \geq a$, $d \geq b$ si ha che $d \geq a \cup b$.

Naturalmente la precedente definizione non assicura l'esistenza, all'interno di un insieme parzialmente ordinato $(X, \leq)$, di un massimo comune minorante e di un minimo comune maggiorante per ogni coppia di elementi di X.

Definizione. Un *reticolo* $(X, \leq, \cap, \cup)$ è un insieme parzialmente ordinato nel quale per ogni coppia di elementi $(a; b)$ esistono un massimo comune minorante $a \cap b$ e un minimo comune maggiorante $a \cup b$.

Applicando le definizioni si verifica facilmente che in un reticolo $(X, \leq, \cap, \cup)$ le due operazioni binarie $\cap$, $\cup$ godono delle seguenti proprietà:

$a \cap a = a$ $\qquad$ $a \cup a = a$
$a \cap b = b \cap a$ $\qquad$ $a \cup b = b \cup a$

$(a \cap b) \cap c = a \cap (b \cap c)$ $\qquad$ $(a \cup b) \cup c = a \cup (b \cup c)$

$a \cap (a \cup b) = a$ $\qquad$ $a \cup (a \cap b) = a$

Le definizioni seguenti introducono importanti tipi particolari di reticoli.

Definizione. Un reticolo $(X, \leq, \cap, \cup)$ si dice *distributivo* se per ogni $a, b, c \in X$:

$(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$

$(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$

Definizione. Un reticolo $(X, \leq, \cap, \cup)$ si dice *complementato* se possiede un minimo che indicheremo con 0, un massimo che indicheremo con 1 e se per ogni $a \in X$ esiste $a' \in X$ (detto *complemento* di a) tale che:

$a \cap a' = 0$ $\qquad$ e $\qquad$ $a \cup a' = 1$

Si può dimostrare (per assurdo) che in un reticolo distributivo con massimo e minimo il complemento a' di un elemento a, se esiste, è unico.

Possiamo ora dare la definizione conclusiva.

Definizione. Si dice *algebra di Boole* un reticolo distributivo complementato.

Esempio. L'insieme $\wp(I)$ delle parti di I con le operazioni di intersezione e di unione, presentato nel precedente esempio. è un'algebra di Boole.

Esempio. L'insieme $\{0; 1\}$ con le operazioni $+$, $\cdot$ definite nel modo seguente è un'algebra di Boole:

$0+0 = 0$ $\qquad$ $0+1 = 1+0 = 1$ $\qquad$ $1+1 = 1$

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

Le stesse regole algebriche valgono per i connettivi logici dei quali ci occuperemo esplicitamente nei prossimi capitoli: infatti se, dato un insieme A consideriamo due suoi sottoinsiemi, definiti mediante proprietà, $X=\{x \in A | P(x)\}$ e $Y=\{y \in A | Q(y)\}$, si avrà:

$X \cap Y = \{z \in A | P(z) \text{ e } Q(z)\}$

$X \cup Y = \{z \in A | P(z) \text{ o } Q(z)\}$

complementare di X $X' = \{ z \in A | \text{ non } P(z)\}$

Lo stesso comportamento si ha per le "porte" dei circuiti logici.
Una *porta or* opera nel modo seguente:

ingressi		uscita
0	0	0
0	1	1
1	0	1
1	1	1

Una *porta and* opera nel modo seguente:

ingressi		uscita
0	0	0
0	1	0
1	0	0
1	1	1

Una *porta not* opera nel modo seguente:

ingresso	uscita
0	1
1	0

Nelle sezioni dedicate alla logica degli enunciati e alla logica dei predicati avremo modo di riprendere queste osservazioni.

7. DIMOSTRAZIONI PER INDUZIONE

7.1. Proposizioni dipendenti da un numero naturale

Frequentemente, in aritmetica, definizioni, esercizi e teoremi dipendono da un numero n variabile nell'insieme $\mathbf{N}$ dei naturali (o in un suo sottoinsieme). Ad esempio, una celebre formula dell'aritmetica è quella che fornisce la *somma di tutti i naturali non maggiori di n*, con n naturale fissato:

$$S_n = \frac{n\cdot(n+1)}{2}$$

Nell'espressione precedente sono riassunte infi nite somme di naturali, una per ciascun indice naturale *n*. Verifichiamo la formula proposta in alcuni casi:

$S_0 = \frac{0\cdot(0+1)}{2} = 0$ essendo: $S_0 = 0$

$S_1 = \frac{1\cdot(1+1)}{2} = 1$ essendo: $S_1 = 0+1 = 1$

$S_2 = \frac{2\cdot(2+1)}{2} = 3$ essendo: $S_2 = 0+1+2 = 3$

$S_3 = \frac{3\cdot(3+1)}{2} = 6$ essendo $S_3 = 0+1+2+3 = 6$

Le considerazioni precedenti provano che la formula proposta è valida fino all'indice $n = 3$; ma appare evidentemente impossibile verificare direttamente *tutte* le (*infinite!*) somme di naturali ottenibili. Una dimostrazione completa della formula proposta dovrebbe però prendere in considerazione *tutti* i casi possibili: essa, quindi, non può essere tentata attraverso una verifica di ogni singolo caso, corrispondente ad ogni indice naturale *n*.

La dimostrazione di tale risultato può essere impostata direttamente, considerando cioè la formula generale, come illustrato nell'esempio seguente.

Esempio. Sia *n* un numero naturale. Dimostriamo che la somma S_n di tutti i numeri naturali non maggiori di *n* è data dalla formula:

$$S_n = \frac{n\cdot(n+1)}{2}$$

Elenchiamo ordinatamente in una prima tabella di una riga tutti i naturali da 1 a *n* (possiamo escludere lo 0, la cui addizione non modifica la somma):

1	2	3	4	...	(*n*–2)	(*n*–1)	*n*

In una seconda riga, elenchiamo i naturali considerati in ordine inverso:

1	2	3	4	...	(*n*–2)	(*n*–1)	*n*
n	(*n*–1)	(*n*–2)	(*n*–3)	...	3	2	1

Se sommiamo in colonna le due righe scritte, otteniamo:

$(n+1)$ $(n+1)$ $(n+1)$ $(n+1)$ ... $(n+1)$ $(n+1)$ $(n+1)$

ovvero: n volte il numero $(n+1)$. La somma di questi n numeri, $n\cdot(n+1)$, è il doppio della quantità S_n cercata, essendo stata ottenuta addizionando due volte ciascun naturale compreso tra 1 e n. Possiamo pertanto concludere che:

$$S_n = \frac{n\cdot(n+1)}{2}$$

Il procedimento illustrato è ricordato in relazione ad un aneddoto riguardante Carl Friedrich Gauss (1777-1855) che, fanciullo, durante un'esercitazione scolastica calcolò velocemente la somma dei naturali da 1 a 100 giungendo a:

$$S_{100} = \frac{100\cdot(100+1)}{2} = 5050$$

Questa dimostrazione elementare non è però l'unica possibile per la formula data.

7.2. Dimostrazioni per induzione

La regolarità osservata nel precedente paragrafo delle "infinite dimostrazioni" che servirebbero a provare una proprietà (o delle infinite espressioni che servirebbero a fornire una definizione) sui numeri naturali ha portato a formulare un principio generale che va sotto il nome di *Principio di induzione*. In sostanza esso afferma che se una proprietà vale per il primo numero e, valendo per un certo numero, allora vale anche per il successivo, allora vale per tutti i numeri (analogamente per le definizioni). Usiamo un tale principio anche nella logica di tutti i giorni quando ci riferiamo all'infinito come in frasi del tipo:

Il mio bambino sa contare
che vuol dire
Tutti i numeri naturali sono conosciuti dal mio bambino

Naturalmente ciò non vuol dire che il mio bambino abbia effettivamente nominato tutti i numeri naturali, e nemmeno li abbia pensati; ma egli è in grado di cominciare la serie e, se qualcuno gli nomina un numero, di dire il

successivo. Conosce, cioè, lo schema che permette di nominare qualunque numero a partire dal precedente. La permanenza dello schema al variare del numero considerato, permette di ridurre gli infiniti passaggi necessarii a due soltanto.

Indichiamo dunque con il simbolo $P(n)$ una proposizione che vogliamo provare, sottolineando in tale modo che si tratta di un'affermazione dipendente dall'indice $n \in \mathbf{N}$. Presenteremo ora la dimostrazione per induzione di $P(n)$ in due fasi distinte, *entrambe indispensabili*:

- *prima fase:* si verifica direttamente la verità di $P(0)$; nel caso in cui la proposizione da dimostrare valga per $n \geq n_0 > 0$, si verifica che essa valga per il minimo degli indici, $n = n_0$;
- *seconda fase:* si ammette la verità di $P(n-1)$ e, sulla base di ciò, si dimostra che la proposizione P è vera anche per l'indice n; ovvero: si prova che la validità della proposizione per un indice (qualsiasi) comporta la validità per l'indice successivo.

Se è possibile completare la verifica di *entrambi* i punti sopra illustrati, la proposizione $P(n)$ può dirsi dimostrata (per *tutti* gli indici $n \in \mathbf{N}$): la prima fase, infatti, ci consente di affermare che la proposizione $P(n)$ è vera per $n = 0$; sulla base di ciò, la seconda fase ci assicura che $P(n)$ è vera anche per $n = 1$ (ovvero per il successivo di 0). Appurato ciò, possiamo affermare che $P(n)$ è vera anche per $n = 2$ (per il successivo di 1) e così di seguito per tutti gli indici naturali.

Illustriamo il procedimento dimostrativo attraverso un esempio nel quale proporremo una dimostrazione alternativa della formula sopra provata.

Esempio. Sia n un numero naturale. Dimostriamo che la somma S_n di tutti i numeri naturali non maggiori di n è data dalla formula (già proposta e giiustificata nel precedente esempio):

$$S_n = \frac{n \cdot (n+1)}{2}$$

Procediamo per induzione sull'indice n.

Prima fase: mostriamo che la formula è verificata per il naturale $n = 0$. Risulta, in questo caso: $S_0 = 0$, e nella formula proposta: $S_0 = \frac{0 \cdot (0+1)}{2} = 0$.

Seconda fase: ammettiamo ora che la formula in questione sia verificata per l'indice $(n-1)$; ammettiamo cioè che sia vera:

$$S_{n-1} = \frac{(n-1)\cdot n}{2}$$

Dovremo, sulla base di ciò, provare la validità della formula anche per l'indice n. Ricaviamo dunque S_n (utilizzando quanto sopra ammesso):

$$S_n = S_{n-1} + n = \frac{(n-1)\cdot n}{2} + n = \frac{(n-1)\cdot n + 2n}{2} = \frac{n\cdot(n+1)}{2}$$

Pertanto la validità della formula per l'indice $(n-1)$ comporta la validità della formula per l'indice n. Ciò, unito alla provata validità della formula per $n = 0$, completa la dimostrazione per induzione.

Nella sezione precedente abbiamo anticipato una proprietà dell'insieme delle parti di un insieme dato, proprietà che riprendiamo nell'esempio seguente.

Esempio. Sia I un insieme al quale appartengono n elementi (avente cardinalità n). Dimostriamo che l'insieme delle parti di I, $\wp(I)$, contiene 2^n elementi (ha cardinalità 2^n).

Per comodità di notazione, indichiamo con #(I) la cardinalità dell'insieme I; procediamo per induzione su n.

Prima fase: se $n = 0$, allora è: $I = \varnothing$ e dunque $\#(\wp(I)) = \#(\{\varnothing\}) = 1 = 2^0$. La tesi è quindi valida per questo primo caso.

Seconda fase: Ammettiamo la validità della tesi da dimostrare qualora I sia costituito da $n-1$ elementi, dunque quando sia $\#(I) = n-1$; cioè ammettiamo che sia $\#(\wp(I)) = 2^{n-1}$.

Sia ora $a \notin I$; consideriamo quindi l'insieme $I \cup \{a\}$ la cui cardinalità è n. Qual è la cardinalità di $\wp(I \cup \{a\})$?

Ricordiamo che $\wp(I \cup \{a\})$ è costituito da tutti i sottoinsiemi (propri e impropri) di $I \cup \{a\}$. Elenchiamo tali sottoinsiemi in una tabella nel modo seguente: nella prima colonna scriviamo tutti i sottoinsiemi di $I \cup \{a\}$ ai quali non appartiene a (in pratica: tutti e soltanto i sottoinsiemi di I): $\varnothing$, B, C, D, ..., I; in una seconda colonna, scriviamo i sottoinsiemi di $I \cup \{a\}$ ai quali appartiene a, con un criterio assai semplice: uniamo a ciascun sottoinsieme della prima colonna l'insieme $\{a\}$.

Otteniamo:

$\varnothing$	$\varnothing \cup \{a\}$
B	$B \cup \{a\}$
C	$C \cup \{a\}$

D	D$\cup\{a\}$
...	...
I	I$\cup\{a\}$
(2^{n-1} sottoinsiemi)	(2^{n-1} sottoinsiemi)

Quanti sono, dunque, i sottoinsiemi di I$\cup\{a\}$?

Nella prima colonna ne abbiamo elencati 2^{n-1}, in quanto abbiamo ammesso che sia $\#(\wp(\mathrm{I})) = 2^{n-1}$; nella seconda colonna ne troviamo altrettanti. I sottoinsiemi di I$\cup\{a\}$ sono $2\cdot 2^{n-1}$. Quindi:

$$\#(\wp(\mathrm{I}\cup\{a\})) = 2^n$$

e ciò completa la cercata dimostrazione per induzione su n.

Notiamo infine che se non fossimo ancora convinti che il principio di induzione ci permette di raggiungere tutti i casi possibili, potremmo ragionare come segue: supponiamo che esista un numero m per il quale, nonostante la dimostrazione per induzione, $P(m)$ non sia valida. Intanto m non può essere lo 0, perché sappiamo che P(0) è vera per la prima condizione. Allora $P(m)$ non sarebbe vera per un numero più grande di 0; ma allora non sarebbe vera nemmeno per il caso precedente, diciamo $P(m-1)$, perché la seconda condizione ci assicura che la verità di $P(m-1)$ implica la verità di $P(m)$. Così, a ritroso, *dopo un numero finito di passi*, proveremmo la falsità di $P(0)$.

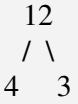
Come si vede, il principio di induzione si fonda sul fatto che nei numeri naturali si può andare sempre avanti con la funzione successore, ma dato un numero, da questo si torna allo 0 in un numero finito di passi.

Questa osservazione ci permette di formulare il principio in modo diversi, ma che sottintendono sempre in realtà la struttura dei numeri naturali.

Una prima apparente generalizzazione è il seguente principio: 'Se vale $P(0)$ e, se per ogni $n<m$, la validità di $P(n)$ implica la validità di $P(m)$, allora vale $P(k)$ per ogni k'. In questo caso l'ipotesi è più debole perché il predecessore di n è soltanto uno dei numeri più piccoli di n, perciò è evidente che questo principio implica il precedente (la dimostrazione formale si potrà fare come esercizio una volta studiato il calcolo degli enunciati). In realtà sui numeri naturali i due principi sono equivalenti.

Abbiamo un altro caso che utilizzeremo spesso in logica, che introdurremo con l'esempio seguente.

Esempio. Supponiamo di dover provare che ogni numero è decomponibile in un prodotto di fattori primi. In questo caso l'induzione non può essere applicata direttamente ai numeri in quanto tali, perché nel passaggio da un numero al successore la situazione e la dimostrazione cambiano drasticamente. Dovremo allora trattare i nostri numeri come oggetti ai quali è assegnato un altro numero che deve variare in modo da rendere parametrica la dimostrazione. Possiamo pensare di associare ad ogni numero un "albero di decomposizione", cioè porre il numero alla radice dell'albero e, se possibile, generare due "figli", usando una possibile decomposizione non banale del numero:



Abbiamo due possibilità: o il numero è già primo e ci fermiamo al primo nodo (radice), o si può decomporre in due fattori diversi da 1 e da lui stesso; a questo punto il gioco si ripete per i due fattori e deve terminare prima o poi perché i fattori ogni volta sono strettamente minori del numero dato e perciò, prima o poi ci fermeremo.

Abbiamo così costruito in un numero finito di passi un albero binario con il numero dato alla radice. Associamo allora al numero originario un altro numero, l'altezza dell'albero, cioè il numero massimo dei passi che occorrono per andare dalla radice ad una foglia (nodo senza figli); proviamo allora che qualunque sia l'altezza dell'albero, il numero dato è il prodotto dei numeri primi che sono sulle foglie. Se dunque l'albero associato al numero ha altezza 0 vuol dire che il numero dato era già primo e siamo arrivati; supponiamo che la proprietà sia vera per numeri che hanno un albero di decomposizione di altezza n e dimostriamolo per per numeri che hanno un albero di decomposizione di altezza n+1. Per un tale numero n esistono due numeri più piccoli r ed s tali che $n = rs$ ed essi hanno un albero di decomposizione di altezza al più n. Quindi per essi vale il fatto che sono decomponibili in numeri primi; ma allora il prodotto delle due decomposizioni sarà una decomposizione di n.

Questo modo di procedere si dice per *induzione strutturale* ed opera sostanzialmente associando ad oggetti (non necessariamente numeri) che sono decomponibili in oggetti più semplici, un numero naturale che ne rappresenta la complessità, in modo che le componenti abbiano un numero più piccolo. La dimostrazione avverrà poi per induzione su questi indici di complessità. Talvolta, quando la diminuzione della complessità sarà evidente, si potrà addirittura omettere di specificare l'indice.

8. I NUMERI PRIMI

8.1. Divisibilità e numeri primi

In questa sezione presenteremo le principali nozioni collegate ai numeri primi ed indicheremo alcune dimostrazioni; in particolare, daremo la definizione di numero primo e illustreremo il crivello di Eratostene; mostreremo quindi l'esistenza e l'unicità della scomposizione in fattori primi di un numero naturale.

Inoltre ci occuperemo di alcuni importanti problemi: "quanti" sono i numeri primi? Come essi sono distribuiti nella sequenza dei numeri naturali? Daremo quindi alcuni risultati: una condizione necessaria di primalità (teorema di Fermat) ed infine una condizione necessaria e sufficiente di primalità (teorema di Wilson). In un'appendice presenteremo alcuni problemi aperti, come le congetture di Goldbach e dei primi gemelli.

Iniziamo a presentare la nozione di divisibilità.

Definizione. Un naturale a si dice *divisibile* per un naturale b se esiste un naturale c tale che $a = b \cdot c$. Si dice allora che b è un *divisore* di a. Si scrive: $b|a$.

Si tratta di una nozione elementare: su di essa si basano tecniche e concetti di primaria importanza. La illustreremo con alcuni esempi.

Esempio. Dimostriamo che la somma di cinque numeri naturali consecutivi è sempre divisibile per 5.

Indicati infatti i numeri in questione con: a, $a+1$, $a+2$, $a+3$, $a+4$, la loro somma è:

$$a+(a+1)+(a+2)+(a+3)+(a+4) = 5 \cdot a+10 = 5 \cdot (a+2)$$

e tale naturale, avendo 5 come fattore, è divisibile per 5.

Esempio. Dati tre numeri naturali non nulli tali che la differenza tra il secondo ed il primo e la differenza tra il terzo ed il secondo sia 2, dimostrare che uno di essi è divisibile per 3.

Siano n, $n+2$, $n+4$ i tre naturali in questione, con $n \neq 0$.

La dimostrazione può essere scritta sinteticamente utilizzando le congruenze (ricordiamo che $a \equiv b \pmod{n}$ significa che n divide $b-a$):

se $n \equiv 0 \pmod 3$, allora la tesi è subito provata
se $n \equiv 1 \pmod 3$, allora $n+2 \equiv 0 \pmod 3$
se $n \equiv 2 \pmod 3$, allora $n+4 \equiv 0 \pmod 3$

Altrimenti è necessario esprimere diversamente il ragionamento (la dimostrazione può apparire meno chiara): se n è divisibile per 3, la tesi è subito provata. Se n non è divisibile per 3, effettuando tale divisione avremo un resto non nullo che potrà essere $r = 1$ oppure $r = 2$. Se è $r = 1$, allora $n+2$ è divisibile per 3; se è $r = 2$, allora $n+4$ è divisibile per 3.

Esempio. Per alcuni naturali non nulli n, m, è possibile che n sia divisore di m e contemporaneamente m sia divisore di n: ciò accade se (e solo se) è $n = m$.

Se n è divisore di m e m è divisore di n scriviamo:

$$m = b \cdot n \quad \text{e} \quad n = a \cdot m \tag{1}$$

con a, b naturali (diversi da zero, essendo, per ipotesi, diversi da zero i naturali dati n, m). Scriviamo allora:

$$n \cdot m = (a \cdot m) \cdot (b \cdot n) = a \cdot b \cdot m \cdot n \quad \Rightarrow \quad a \cdot b = 1$$

Tale prodotto di naturali è verificato solamente nel caso: $a = b = 1$. Possiamo concludere allora, sostituendo nella formula (1), che: $n = m$.

Esempio. Siano a, b due naturali multipli del naturale n ($n \neq 0$): dimostriamo che ogni naturale della forma $\alpha \cdot a + \beta \cdot b$, con α, β naturali, è anch'esso multiplo di n.

Se a e b sono multipli di n, esistono due naturali h, k tali che:

$$a = h \cdot n \qquad b = k \cdot n$$

e perciò:

$$\alpha \cdot a + \beta \cdot b = \alpha \cdot h \cdot n + \beta \cdot k \cdot n = n \cdot (\alpha \cdot h + \beta \cdot k)$$

Quindi il naturale $\alpha \cdot a + \beta \cdot b$ è divisibile per n secondo il fattore $\alpha \cdot h + \beta \cdot k$.

Definizione. Il naturale p si dice *primo* se è maggiore di 1 ed è divisibile soltanto per 1 e per se stesso. Un naturale maggiore di 1 non primo si dice *composto*.

Un'antica tecnica per individuare i numeri primi minori di un limite prefissato è illustrata nell'esempio seguente.

Esempio. Crivello di Eratostene per trovare i primi *minori di 50*:

...	2	3	…	5	…	7	…	9	…
11	…	13	…	15	…	17	…	19	…
21	…	23	…	25	…	27	…	29	…
31	…	33	…	35	…	37	…	39	…
41	…	43	…	45	…	47	…	49	…

Iniziamo a prendere in considerazione il naturale 2 ed affermiamo che si tratta di un primo. Ne segue che tutti i multipli di 2 saranno composti (li cancelliamo).

Il procedimento deve essere ripetuto considerando successivamente tutti i naturali non maggiori della radice quadrata della limitazione assegnata, ovvero di $\sqrt{50}$ (perché? Il lettore è invitato a rispondere per iscritto, per esercizio).

Esempio. I numeri primi tra i naturali: una tabella (a parte la prima riga, i primi sono contenuti nella prima e nella quinta colonna: perché? Il lettore è invitato a formulare la semplice risposta):

(1)	**2**	**3**	(4)	**5**	(6)
7	(8)	(9)	(10)	**11**	(12)
13	(14)	(15)	(16)	**17**	(18)
19	(20)	(21)	(22)	**23**	(24)
(25)	(26)	(27)	(28)	**29**	(30)
31	(32)	(33)	(34)	(35)	(36)
37	(38)	(39)	(40)	**41**	(42)
43	(44)	(45)	(46)	**47**	(48)
(49)	(50)	(51)	(52)	**53**	(54)
(55)	(56)	(57)	(58)	**59**	(60)
61	(62)	(63)	(64)	(65)	(66)
67	(68)	(69)	(70)	**71**	(72)
73	(74)	(75)	(76)	(77)	(78)
79	(80)	(81)	(82)	**83**	(84)

8.2. La scomposizione in fattori primi

Proposizione. Esistenza della scomposizione in fattori primi. Ogni numero naturale maggiore di 1 è un prodotto di numeri primi.

Dimostrazione. Sia n un numero naturale: o n è un primo, nel qual caso la tesi è provata, oppure n ha divisori compresi tra 1 e n.

Se m è il minimo di questi divisori, m è primo in quanto, se m avesse un divisore k compreso tra 1 e m stesso, k sarebbe divisore anche di n, contro la minimalità di m. Quindi il naturale n è primo oppure è divisibile per un numero primo, che chiameremo p_1:

$$n = p_1 n_1$$

con $1<n_1<n$. Ripetiamo il ragionamento su n_1: esso o è primo o è divisibile per un primo $p_2<n_1$. Iterando il procedimento, otteniamo una sequenza decrescente di numeri (non primi):

$$n, n_1, n_2, ..., n_{k-1}$$

finché uno di loro sarà primo, $n_k = p_k$. Scriveremo allora:

$$n = p_1 p_2 ... p_k \quad \text{cvd}$$

Proposizione. Unicità della scomposizione in fattori primi. La scomposizione in fattori primi di un numero naturale è *unica*. A parte permutazioni di fattori, un naturale può essere espresso come prodotto di primi *in un solo modo*.

Dimostrazione (Lindemann). Chiamiamo *numeri anormali* i numeri che possono essere fattorizzati in prodotti di primi in più modi (a parte permutazioni). Sia n il minimo numero anormale.

Lo stesso primo p non può apparire in due diverse fattorizzazioni di n: se così fosse n/p sarebbe anormale e $n/p < n$, contro la minimalità di n. Allora:

$$n = p_1 p_2 p_3 \ldots = q_1 q_2 q_3 \ldots$$

dove i p e i q sono primi, nessun p è uguale a un q e nessun q è uguale a un p.

Sia p_1 il minimo dei p; risulta: $p_1^2 \leq n$.

Sia q_1 il minimo dei q; risulta: $q_1^2 \leq n$.

Da ciò, ricordando che $p_1 \neq q_1$: $p_1 q_1 < n$.

Se poniamo $N = n - p_1 q_1$ è $0 < N < n$ e dunque N non è un numero anormale.

Ora, $p_1 | n$ e dunque $p_1 | N$. Inoltre $q_1 | n$ e dunque $q_1 | N$. Ciò significa che p_1 e q_1 appaiono entrambi nell'(unica) fattorizzazione di N e che $p_1 q_1 | N$.

Da questo segue che $p_1 q_1 | n$ e quindi che $q_1 | n/p_1$. Ma n/p_1 è minore di n e dunque ammette l'unica fattorizzazione $p_2 p_3 \ldots$ Dato che q_1 non è un p, è impossibile. Dunque non possono esistere *numeri anormali*. cvd

Esempio. Nel piano cartesiano chiamiamo *punti primi* i punti P(m, n) aventi entrambe le coordinate appartenenti all'insieme dei numeri primi {2; 3; 5; 7; 11; …}. Si dimostra che nessuna retta passante per l'origine degli assi, ad eccezione della bisettrice del primo quadrante, può passare per più un punto primo. Lasciamo al lettore la stesura della dimostrazione.

Esempio. Dimostriamo che se un numero primo p è divisore di un prodotto ab, allora p deve dividere a o b.

Procediamo per assurdo, se p non dividesse a né b, il prodotto dei fattori primi di a e di b porterebbe ad una scomposizione di ab…Lasciamo al lettore di formulare la semplice conclusione.

8.3. "Quanti" sono i numeri primi?

Proposizione (XX, Libro IX degli *Elementi*). I numeri primi sono sempre più di ogni assegnata quantità di primi.

Dimostrazione. Sia $p_1, p_2, \ldots, p_r$ un'assegnata quantità di numeri primi. Poniamo: $P = p_1 p_2 \ldots p_r + 1$ e sia p un numero primo che divida P; allora p non può essere alcuno dei $p_1, p_2, \ldots, p_r$, altrimenti p dividerebbe la differenza $P - p_1 p_2 \ldots p_r = 1$ che è impossibile. Dunque questo p è un altro primo, e $p_1, p_2, \ldots, p_r$ non sono tutti i numeri primi. cvd

Proposizione (Euler). La serie dei reciproci dei numeri primi diverge.

Ciò permette di far seguire immediatamente il risultato euclideo: se l'insieme dei numeri primi fosse finito, tale sarebbe anche la somma dei reciproci di tutti i primi (la dimostrazione di L. Euler che riporteremo nell'appendice C si può trovare in: Tenenbaum & Mendès France, 1997; per un'elegante dimostrazione di P. Erdös si può vedere: Aigner & Ziegler, 1998).

Un classico problema riguarda la distribuzione dei primi tra i numeri naturali. Per ogni naturale n, sia A_n il numero di primi non maggiori di n:

$A_1 = 0$	(nessun primo è minore o uguale a 1)	
$A_2 = 1$	il primo considerato è 2	
$A_3 = 2$	i primi considerati sono 2, 3	
$A_4 = 2$	i primi considerati sono 2, 3	
$A_5 = 3$	i primi considerati sono 2, 3, 5	etc.

Consideriamo ad esempio la successione di n 10^3, 10^6, 10^9, …e la tabella:

n	A_n/n	$1/\log n$	$(A_n/n)/(1/\log n)$
10^3	0,168…	0,145…	1,159…
10^6	0,078…	0,062…	1,084…
10^9	0,050…	0,048…	1,053…

Sulla base di una verifica empirica Gauss ipotizzò che:

$$\lim_{n\to+\infty} \frac{A_n / n}{1 / \log n} = 1$$

La dimostrazione di ciò risale al 1896 (da Hadamard e de la Vallée Poussin).

8.4. Condizioni di primalità

Enunciamo ora alcune classiche condizioni di primalità.

Una condizione necessaria affinché un numero naturale sia primo è espressa dal *piccolo teorema di Fermat* (dimostrato da Euler).

Proposizione. Se a è un intero e p è un numero primo: $a^p - a \equiv 0 \pmod{p}$.

Dunque: se p è un primo, $a^p - a$ è un multiplo di p. Una sua diversa formulazione: se p è un primo che non divide a, allora $a^{p-1} - 1$ è un multiplo di p (il lettore è invitato a fare qualche verifica).

La precedente condizione è necessaria, ma non sufficiente: dunque tutti i numeri primi certamente soddisfano quanto espresso dal piccolo teorema di Fermat, ma non tutti i numeri che soddisfano tale condizione sono primi.

Una condizione necessaria e sufficiente è espressa dal *teorema di Wilson* (risalente al 1770, poi dimostrato da Lagrange e da Euler):

Proposizione. $(p-1)!+1 \equiv 0 \pmod{p}$ se e solo se p è un numero primo.

Dunque: $(p-1)!+1$ è un multiplo di p se e soltanto se p è un primo.

Può essere interessante fare qualche verifica. Occupiamoci ad esempio del numero primo 7: $(7-1)!+1 = 721$ è un multiplo di 7 ($7 \cdot 103$); ma già la verifica relativa ai primi successivi (11, 13) appare difficoltosa per il calcolo del fattoriale (il lettore provi a calcolare 10! e 12!). E nel caso di applicazione a primi più grandi, il calcolo del fattoriale si rivela un ostacolo molto serio.

Il teorema di Wilson quindi è un risultato elegante e importante, ma praticamente ben poco utile, in quanto *non conosciamo alcun algoritmo in grado di calcolare il fattoriale con "sufficiente" rapidità!* Da ciò segue che la velocità di un test di primalità basato sul teorema di Wilson sarebbe minore di quella di un test basato sul crivello di Eratostene.

Molte formule sono basate sul teorema di Wilson; ad esempio la formula di Willans (1964) fornisce il numero primo n-esimo:

$$p_n = 1 + \sum_{k=1}^{2^n} \left\lfloor \left(\frac{n}{\sum_{j=1}^{k} \left\lfloor \cos^2 \pi \frac{(j-1)!+1}{j} \right\rfloor} \right)^{\frac{1}{n}} \right\rfloor$$

ma le difficoltà applicative precedentemente menzionate restano.

Ricordiamo che nella storia dell'informatica le verifiche di primalità sono stati i primi procedimenti ad essere condotti su elaboratori. E tuttora sono considerati validissimi test per valutare l'efficienza di una macchina.

9. CONFRONTO DI INSIEMI INFINITI

9.1. La potenza del numerabile

Ricordiamo che due insiemi si dicono equipotenti se possono essere posti in corrispondenza biunivoca. Il concetto di equipotenza ha consentito di formulare una definizione di insieme infinito; finora, però, non sono stati trattati gli

insiemi infiniti: abbiamo introdotto **N** considerando le classi di equivalenza determinate, in un insieme U_f costituito da insiemi finiti, dalla relazione di equipotenza. Ora ci occuperemo invece specificamente degli insiemi *infiniti*: dato che la relazione di equipotenza è definita anche per questi insiemi, è spontaneo considerare il problema dell'estensione del concetto di potenza di un insieme anche agli insiemi infiniti. E la potenza di tali insiemi, per quanto visto, non potrà essere data da un numero naturale: dovremo quindi introdurre ed utilizzare denominazioni nuove.

A tale riguardo si presenta una questione fondamentale: possiamo affermare che tutti gli insiemi infiniti hanno la *stessa* potenza? Sarebbe corretto, ad esempio, concludere che la potenza di insiemi come **N**, **Z**, **Q**, **R** è indicabile con il termine "infinito", senza ulteriori specificazioni? Come vedremo, una delle massime conquiste della teoria degli insiemi di Georg Cantor sarà proprio identificabile in un'inedita possibilità di "confrontare" (di "classificare") gli insiemi infiniti.

Dimostriamo innanzitutto che l'insieme **N** dei numeri naturali è un insieme infinito. Per fare ciò, proveremo che **N** è equipotente ad un suo sottoinsieme proprio.

Proposizione. L'insieme $P \subseteq \mathbf{N}$ dei numeri naturali pari è equipotente a **N**.

Dimostrazione. Sia P l'insieme dei numeri naturali pari:

$$P = \{m \in \mathbf{N}: m = 2 \cdot n \text{ e } n \in \mathbf{N}\}$$

Per dimostrare che P, sottoinsieme proprio di **N**, è equipotente a **N**, è necessario individuare una funzione biiettiva f: $P \to \mathbf{N}$. Tale funzione è:

$$f: x \to x/2$$

Mostriamo ora che f è biiettiva (ovvero che gli insiemi P e **N** sono posti, attraverso f, in corrispondenza biunivoca): rappresentiamo tale relazione nel modo seguente:

	0	2	4	6	8	10	12	14	...	(P)
	↑	↑	↑	↑	↑	↑	↑	↑		
f	|	|	|	|	|	|	|	|	...	
	↓	↓	↓	↓	↓	↓	↓	↓		
	0	1	2	3	4	5	6	7	...	(**N**)

Ad ogni elemento di P corrisponde dunque uno ed un solo elemento di **N** (e viceversa): ciò prova quanto affermato. cvd

Possiamo ora introdurre una specifica denominazione per la potenza di tutti quegli insiemi che (come P) sono equipotenti a **N**.

Definizione. Un insieme equipotente a **N** si dice avente la *potenza del numerabile*.

L'insieme $P \subseteq \mathbf{N}$ dei naturali pari ha dunque la potenza del numerabile. La prossima proposizione darà un importante esempio di insieme equipotente a **N**.

Proposizione. L'insieme **Z** ha la potenza del numerabile.

Dimostrazione. Per dimostrare che **Z** ha la potenza del numerabile dobbiamo dimostrare che **Z** è equipotente a **N**, ovvero individuare una funzione biiettiva g: $\mathbf{Z} \to \mathbf{N}$. Tale funzione è così rappresentata schematicamente:

	0	1	–1	2	–2	3	–3	4	...	(**Z**)
	↑	↑	↑	↑	↑	↑	↑	↑		
g	|	|	|	|	|	|	|	|	...	
	↓	↓	↓	↓	↓	↓	↓	↓		
	0	1	2	3	4	5	6	7	...	(**N**)

N		**Z**
0	↔	0
$2n+1$	↔	$n+1$
$2n$	↔	$-n$

Ad ogni elemento di **Z** corrisponde dunque uno ed un solo elemento di **N** (e viceversa). cvd

Quanto stabilito da queste due proposizioni potrebbe apparire sorprendente: un'interpretazione eccessivamente libera ed "intuitiva" del problema potrebbe infatti suggerire conclusioni ben diverse sulla "quantità" di elementi appartenenti agli insiemi esaminati. Ad esempio, l'insieme dei numeri naturali pari potrebbe sembrare costituito dalla "metà" degli elementi appartenenti all'insieme **N**; analogamente, l'insieme **Z** potrebbe sembrare costituito dal "doppio" degli elementi appartenenti a **N**. Invece queste ultime "constatazioni", nonostante la loro apparente plausibilità, non hanno alcun significato, in

matematica. I tre insiemi **N**, l'insieme P dei naturali pari, **Z**, sono semplicemente equipotenti.

Occupiamoci ora dell'insieme **Q** dei razionali. Intuitivamente, se confrontato con l'insieme dei numeri interi, **Q** appare costituito da "moltissimi" elementi; potrebbe sembrare, a prima vista, che i razionali siano "molto più numerosi" dei naturali (e degli interi): ad esempio tra due naturali stanno infiniti razionali!

Esempio. Proveremo che, dati due razionali a, b, con $a<b$, esiste sempre un razionale q tale che $a<q<b$. Dall'ipotesi $a<b$ possiamo trarre:

$$a+a < a+b \text{ e } a+b < b+b$$
$$2\cdot a < a+b \text{ e } a+b < 2\cdot b$$
$$2\cdot a < a+b < 2\cdot b$$

infine: $a < \frac{1}{2}\cdot(a+b) < b$

Pertanto la frazione $\frac{1}{2}\cdot(a+b)$ è il numero razionale cercato.

Le considerazioni sino ad ora esposte potrebbero intuitivamente far supporre che l'insieme **Q** sia "molto più numeroso" dell'insieme **N**. Eppure...

Proposizione. L'insieme **Q** ha la potenza del numerabile.

Dimostrazione. Analogamente a quanto fatto nelle dimostrazioni precedenti, dobbiamo "allineare" in un'unica fila tutti gli elementi di **Q**: fatto ciò, sarà possibile mettere in corrispondenza biunivoca gli elementi di **Q** e quelli di **N**.

Scriviamo gli elementi di $\mathbf{Q}^+$ (le frazioni positive) nella tabella seguente:

1/1	1/2	1/3	1/4	1/5	1/6	...
2/1	2/2	2/3	2/4	2/5	2/6	...
3/1	3/2	3/3	3/4	3/5	3/6	...
4/1	4/2	4/3	4/4	4/5	4/6	...
5/1	5/2	5/3	5/4	5/5	5/6	...
6/1	6/2	6/3	6/4	6/5	6/6	...
...	...	...	...	...	...	...

Grazie a questa tabella, possiamo scrivere una "fila" di razionali:

- scriviamo innanzitutto l'elemento 0 (non compreso nella tabella), che sarà il primo elemento della "fila";
- partiamo dall'elemento 1/1 (che si trova, nella tabella, in alto a sinistra);
- "percorriamo" la tabella procedendo a zig -zag, ovvero secondo una serpentina che, da 1/1, individua successivamente:

  1/1 1/2 2/1 3/1 2/2 1/3 1/4 2/3 3/2 4/1...

- consideriamo esclusivamente le frazioni, tra quelle così individuate, che non risultano equivalenti ad una frazione già considerata; ad esempio, una volta accettato l'elemento 1/1, dobbiamo trascurare 2/2, 3/3, 4/4... (frazioni che sono tutte equivalenti a 1/1);
- nella "fila" di elementi di **Q**, dopo 0, per ciascuna delle frazioni m/n così individuate, scriviamo sia la frazione positiva, $+m/n$, che la frazione negativa, ovvero $-m/n$.

Otteniamo, pertanto, quanto inizialmente voluto: l'intero insieme **Q** (il lettore si renderà conto che *tutti* i razionali compaiono nella tabella sopra considerata!) risulta ordinato nella "fila" precedente; **Q** può quindi essere messo in corrispondenza biunivoca con **N** mediante la funzione biiettiva h: $\mathbf{Q} \rightarrow \mathbf{N}$ rappresentata da:

	0	+1/1	−1/1	+1/2	−1/2	+2/1	−2/1	+3/1	...	(**Q**)
	↑	↑	↑	↑	↑	↑	↑	↑		
h	|	|	|	|	|	|	|	|	...	
	↓	↓	↓	↓	↓	↓	↓	↓		
	0	1	2	3	4	5	6	7	...	(**N**)

Ad ogni elemento di **Q** corrisponde dunque uno ed un solo elemento di **N** (e viceversa). cvd

Ricapitoliamo: abbiamo verificato che **N** e tutti gli altri insiemi infiniti considerati (l'insieme dei naturali pari, **Z** e **Q**) hanno la potenza del numerabile.

9.2. La potenza del continuo

Quanto affermato nel paragrafo precedente propone una questione centrale: *tutti* gli insiemi infiniti hanno la potenza del numerabile? La risposta è: *no*.La

proposizione seguente, dovuta a Cantor, motiva questa risposta.

Proposizione. L'insieme **R** *non* ha la potenza del numerabile.

Dimostrazione. Ammettiamo, per assurdo, che **R** abbia la potenza del numerabile: dovrebbe allora essere possibile, analogamente a quanto fatto nelle dimostrazioni precedenti, "allineare" in un'unica lista tutti gli elementi di **R**. Inizieremo a scrivere questa fila elencando tutti i reali x con $0<x<1$ scritti in forma decimale (per evitare malintesi collegati alla notazione usata, possiamo scegliere di non considerare successioni costituite, da un certo punto in poi, da una fila illimitata di sole cifre 9: com'è noto, ad esempio, 0,74999999…è 0,75 e in quest'ultima rappresentazione, dopo la cifra 5, può seguire un'illi mitata sequenza di cifre 0):

$x_1 = 0,a_1a_2a_3a_4a_5a_6a_7a_8a_9...$
$x_2 = 0,b_1b_2b_3b_4b_5b_6b_7b_8b_9...$
$x_3 = 0,c_1c_2c_3c_4c_5c_6c_7c_8c_9...$
$x_4 = 0,d_1d_2d_3d_4d_5d_6d_7d_8d_9...$
$x_5 = 0,e_1e_2e_3e_4e_5e_6e_7e_8e_9...$ etc.

Ogni allineamento decimale può essere illimitato o limitato (nel qual caso, come sopra accennato, può essere considerato seguito da un'illimitata fila di zeri). Dimostreremo che una *qualsiasi* "fila" come quella sopra indicata *non* può contenere tutti i reali compresi tra 0 e 1. Infatti, consideriamo il reale α:

$\alpha = 0,\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5\lambda_6\lambda_7...$

tale che sia: $\lambda_1 \neq a_1$ $\lambda_2 \neq b_2$ $\lambda_3 \neq c_3$ $\lambda_4 \neq d_4$ $\lambda_5 \neq e_5$ $\lambda_6 \neq f_6$ $\lambda_7 \neq g_7$ ...
Il reale α non può appartenere alla 'fila" sopra introdotta; infatti:

- $\alpha \neq x_1$ perché ha la prima cifra decimale diversa;
- $\alpha \neq x_2$ perché ha la seconda cifra decimale diversa;

e, in generale:

- α *è diverso da* x_n *perché ha la n-esima cifra decimale diversa.*

Possiamo pertanto concludere che è impossibile "elencare" in un'unica "fila" tutti i numeri reali compresi tra 0 e 1 e, di conseguenza, è impossibile "elencare" in un'unica "fila" tutti gli elementi di **R**. Quindi **R** *non* può essere messo in corrispondenza biunivoca con **N** e *non* ha la potenza del numerabile. cvd

Osservazione. Il lettore noti che la dimostrazione precedente non funziona se si considera **Q** al posto di **R**. Lo invitiamo a cercare di spiegarsi il perché di ciò.

La proposizione ora dimostrata richiede evidentemente che la potenza di **R** venga denominata con un'espressione diversa da "potenza del numerabile": la definizione seguente stabilisce tale nuova denominazione.

Definizione. Un insieme equipotente a **R** si dice avente la *potenza del continuo*.

Abbiamo potuto constatare direttamente che non tutti gli insiemi infiniti hanno la stessa potenza, in particolare che non tutti gli insiemi infiniti sono equipotenti a **N**: la potenza dell'insieme **R** è diversa dalla potenza del numerabile e viene detta potenza del continuo. A questo punto, è spontaneo porsi il problema: esistono insiemi infiniti non equipotenti né a **N** né a **R**?

La matematica contemporanea ha dato risposta affermativa a questa domanda: è possibile costruire un numero qualsiasi di altri insiemi infiniti aventi potenze sempre diverse (intuitivamente, sempre più "numerosi"). Indichiamo con il simbolo $\aleph_0$ (*Aleph con zero*) la potenza del numerabile e con $\aleph_1$ (*Aleph con uno*) la potenza del continuo: essi sono detti *numeri transfiniti*; è possibile definire i transfiniti $\aleph_0$, $\aleph_1$, $\aleph_2$...: l'insieme dei transfiniti è, a sua volta, infinito.

Ma esistono numeri transfiniti compresi tra $\aleph_0$ e $\aleph_1$? Esiste cioè un insieme infinito $I \subseteq \mathbf{R}$ che non abbia né la potenza del numerabile né la potenza del continuo? Non è stata data una risposta a questa domanda; in particolare, è stata formulata la seguente ipotesi: *Ogni sottoinsieme infinito di* **R** *non avente la potenza del numerabile ha la potenza del continuo.* Essa, detta *ipotesi del continuo*, equivale a negare l'esistenza di transfiniti intermedi tra $\aleph_0$ e $\aleph_1$. Nel 1962, Paul Joseph Cohen (nato nel 1934) dimostrò che l'ipotesi del continuo appartiene ad una particolare classe di questioni, denominate *indecidibili*.

Esercizi sul Capitolo 2

2.1. Dimostrare per induzione che per ogni intero positivo n il numero $5^n+2\cdot 3^{n-1}+1$ è divisibile per 8.

2.2 Dimostrare per induzione che per ogni naturale $n\geq 2$ risulta: $n^3 \geq n+6$.

2.3. Dimostrare per induzione che per ogni intero positivo n è: $3n^3-n^2 \geq 2$.

2.4. Dimostrare per induzione che per ogni naturale $n\geq 1$ risulta: $5^n \geq n+4$.

2.5. Dimostrare per induzione che per ogni numero intero positivo m la somma dei primi m interi positivi dispari è m^2.

2.6. Dimostrare per induzione che per ogni intero positivo m si ha: $2^1+...+2^m = 2^{m+1}-2$.

2.7. Dimostrare per induzione che in un ricevimento in cui sono presenti m persone, con m intero maggiore di 1, se ognuno stringe una sola volta la mano di ciascuna persona presente si hanno esattamente $m(m-1)/2$ strette di mano.

2.8. Siano $D = \{x\in \mathbf{R}: 0<x<1\}$, $\mathbf{R}^+$ l'insieme dei reali positivi e $\mathbf{Q}^+$ l'insieme dei razionali positivi. Indicare un esempio di funzione biiettiva f: $\mathbf{R}^+\rightarrow D$ ed un esempio di funzione biiettiva g: $\mathbf{R}^+\rightarrow\mathbf{Q}^+$.

2.9. Dimostrare che un sottoinsieme di $\mathbf{Z}$ non può avere la potenza del continuo.

Soluzioni degli esercizi sul Capitolo 2

2.1. Per $n = 1$, $5^n+2\cdot\ 3^{n-1}+1 = 5+2+1 = 8$ ed è divisibile per 8. Ammettiamo ora che esista un k intero positivo per cui: $5^n+2\cdot\ 3^{n-1}+1 = 8k$; allora si ha: $5(5^n+2\cdot\ 3^{n-1}+1) = 5\cdot\ 8k$; da cui: $5^{n+1}+10\cdot\ 3^{n-1}+5 = 40k$; quindi: $5^{n+1}+2\cdot\ 3^n+1 = 40k-10\cdot\ 3^{n-1}+2\cdot\ 3^n-4$; infine: $5^{n+1}+2\cdot\ 3^n+1 = 40k-4(3^{n-1}-1)$. Essendo $3^{n-1}-1$ pari, esiste un intero positivo h per cui $5^{n+1}+2\cdot\ 3^n+1 = 8h$ e ciò completa la dimostrazione.

2.2 Per $n = 2$, $n^3 \geq n+6$ porta a $8 \geq 8$. Ammettiano che sia $n^3 \geq n+6$. Risulta allora: $n^3+3n^2+3n+1 \geq 3n^2+4n+7$, quindi: $(n+1)^3 \geq (n+1)+6+3n^2+3n$ ma essendo $n\geq 2$: $(n+1)^3 \geq (n+1)+6+3n(n+1) \geq (n+1)+6$ per transitività e ciò completa la dimostrazione.

2.3. Per $n = 1$, $3n^3-n^2 \geq 2$ porta a $2 \geq 2$. Ammettiamo che sia: $3n^3-n^2 \geq 2$...

2.4. Per $n = 1$, $5^n \geq n+4$ porta a $5 \geq 5$. Ammettiamo che sia: $5^n \geq n+4$...

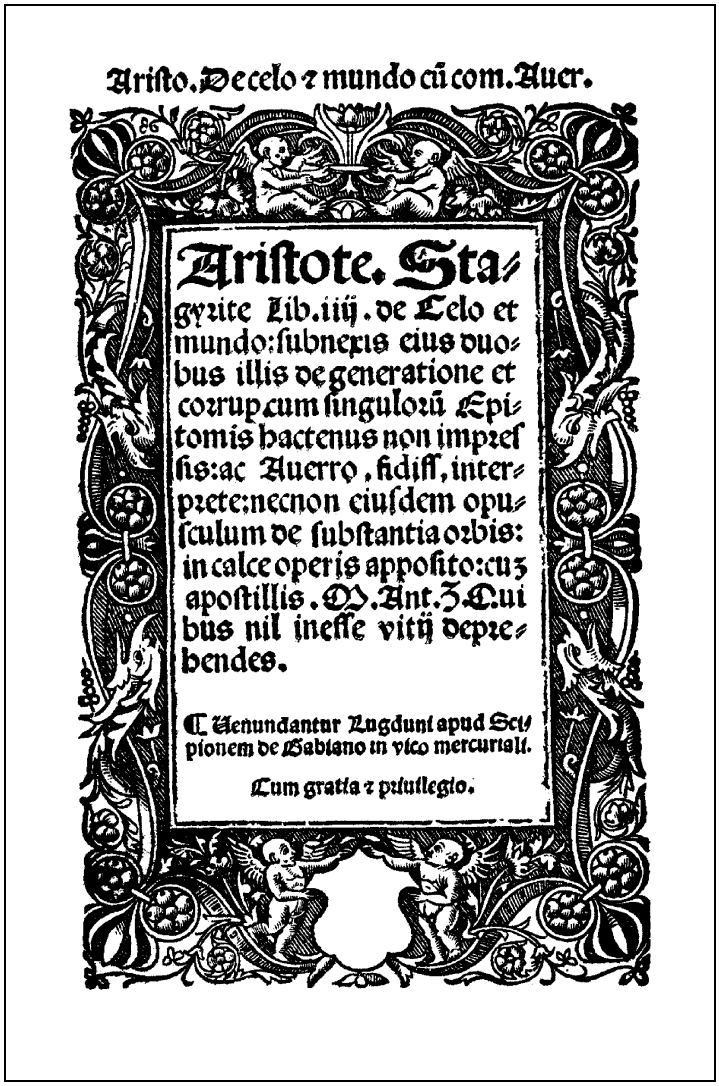
2.5. Per $m = 1$...

2.6. Per $m = 1$ si ha $2^1 = 2^{1+1}-2 = 2$. Per...

2.7. Per $m = 2$ sia ha una stratta di mano. Ammettiamo valida la tesi per...

2.8. f: $x\rightarrow 1/(1+x^2)$; non può esistere alcuna funzione g biiettiva, g: $\mathbf{R}^+\rightarrow\mathbf{Q}^+$, in quanto $\mathbf{R}^+$ ha la potenza del continuo mentre $\mathbf{Q}^+$ ha la potenza del numerabile.

2.9. Si può procedere per assurdo dimostrando che se $I\subseteq\mathbf{Z}$ avesse la potenza del continuo anche $\mathbf{Z}$ avrebbe la potenza del continuo, mentre è noto che $\mathbf{Z}$ ha la potenza del numerabile.



Il frontespizio di un'edizione di *De Coelo* e *De Mundo*
con i commenti di Averroé stampata a Lione nel 1529
