II
Insiemi con struttura

6. I NUMERI NATURALI

6.1. L'insieme dei numeri naturali

Alla fine del XIX secolo, l'intero mondo matematico è impegnato nella puntualizzazione rigorosa dei fondamenti della disciplina: le teorie di George Boole (1815-1864) e di Georg Cantor (1845-1918) e le approfondite ricerche logico-matematiche di Gottlob Frege sono testimonianze chiare dello spirito che pervade 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 pubblica *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.

Ricordiamo che, sette anni dopo la pubblicazione del trattato di Frege, un grande matematico italiano propone per l'aritmetica una sistemazione di tipo assiomatico. Con il lavoro *Sul concetto di numero*, del 1891, Giuseppe Peano (1858-1932) introduce un'impostazione dell'aritmetica basata su tre concetti primitivi e su sei postulati (la formulazione originale della teoria di Peano assume quali concetti primitivi l'*unità*, il *numero* ed il *successivo*; all'*unità* lo stesso Peano sostituirà, in un secondo momento, il concetto primitivo *zero*). Illustreremo una costruzione di **N** sulla base della teoria degli insiemi.

6.2. Gli assiomi di Peano: un approccio ordinale

Nel capitolo precedente avevamo introdotto l'insieme dei numeri naturali in maniera intuitiva e mettendo in risalto l'aspetto quantitativo, cioè la cardinalità. Possiamo ora considerarli in maniera più rigorosa in base all'opera di Giuseppe Peano. Egli propose un'introduzione assiomatica dell'aritmetica, basata su tre concetti primitivi e su sei assiomi che tiene piuttosto conto della struttura ordinale dei numeri stessi.

Nella teoria di Peano, così come essa fu definitivamente enunciata in *Aritmetica*, seconda parte del secondo volume di *Formulaire de mathématiques*

(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 "successivo" introdotta da Peano è dunque un'applicazione s: $a \rightarrow a+$ avente per dominio **N** e per codominio **N**\{0}; si può facilmente dimostrare che, così definita, 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, cioè la chiusura transitiva dell'applicazione *s* pensata come relazione.

Applicando opportunamente gli 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 (v. più avanti).

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

0. $N_0 \in Cls$
1. $0 \in N_0$
2. $a \in N_0 . \supset . a+ \in N_0$
3. $s \in Cls . 0 \in s : a \in s . \supset . a+ \in s . \supset . N_0 \supset s$ Induct
4. $a, b \in N_0 . a+ = b+ . \supset . a = b$
5. $a \in N_0 . \supset . a+ \neq 0$

Osservazione. Dal punto di vista storico, Campano da Novara (seconda metà del XIII secolo), nella sua traduzione/edizione degli *Elementi* di Euclide, aveva già introdotto 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].

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 **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 infinite somme di naturali, una per ciascun indice naturale n. Verifichiamo la formula proposta in alcuni casi:

$$S_0 = \frac{0 \cdot (0+1)}{2} = 0 \quad \text{essendo} \quad S_0 = 0$$
$$S_1 = \frac{1 \cdot (1+1)}{2} = 1 \quad \text{essendo} \quad S_1 = 0+1 = 1$$
$$S_2 = \frac{2 \cdot (2+1)}{2} = 3 \quad \text{essendo} \quad S_2 = 0+1+2 = 3$$
$$S_3 = \frac{3 \cdot (3+1)}{2} = 6 \quad \text{essendo} \quad S_3 = 0+1+2+3 = 6$$

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

$$(n+1)\ \ (n+1)\ \ (n+1)\ \ (n+1)\ \ \ldots\ \ \ (n+1)\ \ (n+1)\ \ (n+1)$$

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 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. 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 $P(n)$ la proposizione da provare per tutti i numeri naturali, 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 dimostrata 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.

Si può verificare che se l'insieme I è costituito da n elementi (cioè di *cardinalità* n), l'insieme delle parti di I è costituito da 2^n elementi (ovvero: la cardinalità di $\wp(\mathrm{I})$ è 2^n).

Esempio. Consideriamo l'insieme (avente cardinalità 3): I = {5; *w*; *z*}. I suoi sottoinsiemi propri sono:

{5}, {*w*}, {*z*}, {5; *w*}, {5; *z*}, {*w*; *z*}

I suoi sottoinsiemi impropri sono: ∅ e {5; *w*; *z*}. L'insieme delle parti (proprie e improprie) dell'insieme I ha cardinalità $2^3 = 8$ ed è, in rappresentazione tabulare:

$\wp$(I) = {∅, {5}, {*w*}, {*z*}, {5; *w*}, {5; *z*}, {*w*; *z*}, {5; *w*; *z*}}

Applichiamo ora il procedimento induttivo alla dimostrazione di 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). Ricordiamo che #I denota la cardinalità dell'insieme I; procediamo per induzione su *n*.

Prima fase: se *n* = 0, allora è: I = ∅ e dunque #I = #∅ = 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* ∉ I; consideriamo quindi l'insieme I∪{*a*} la cui cardinalità è *n*.

Qual è la cardinalità di $\wp$(I∪{*a*})?

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

∅	∅∪{*a*}
B	B∪{*a*}
C	C∪{*a*}
D	D∪{*a*}
...	...
I	I∪{*a*}
(2^{n-1} sottoinsiemi)	(2^{n-1} sottoinsiemi)

Quanti sono, dunque, i sottoinsiemi di I∪{*a*}?

Nella prima colonna ne abbiamo elencati 2^{n-1}, in quanto abbiamo ammesso che sia #$\wp$(I) = 2^{n-1}; nella seconda colonna ne troviamo altrettanti. I sottoinsiemi di I∪{*a*} sono $2 \cdot 2^{n-1}$. Quindi, #$\wp$(I∪{*a*}) = 2^n e ciò completa la cercata dimostrazione per induzione su *n*.

Il lettore faccia attenzione all'esempio seguente.

(Contro)esempio. Vogliamo dimostrare, per induzione, che per ogni numero naturale n è:

$$(n+1)^2-(n-1)^2 = 4n$$

Ammettiamo che la formula sia valida per $m = n-1$, ovvero che sia:

$$(m+1)^2-(m-1)^2 = (n-1+1)^2-(n-1-1)^2 = n^2-(n-2)^2 = 4(n-1)$$

Risulta

$$(n-n+2)(n+n-2) = 4n-4 \quad \Rightarrow \quad 2(2n-2) = 4n-4$$
$$\Rightarrow \quad 2(2n-2)+4 = 4n \quad \Rightarrow \quad 2(2n) = 4n$$

da cui infine

$$[(n+1)-(n-1)][(n+1)+(n-1)] = 4n \quad \Rightarrow \quad (n+1)^2-(n-1)^2 = 4n$$

che è la formula che si doveva dimostrare.

La precedente dimostrazione è ancora inaccettabile in quanto è incompleta: manca infatti l'*indispensabile* verifica della formula da provare per $n = 0$. Verifichiamo la formula proposta per $n = 0$:

$$(0+1)^2-(0-1)^2 = 1-1 = 0 = 4\cdot 0$$

La tesi è dunque verificata in questo primo caso. A quest'ultima verifica può essere fatto seguire quanto sopra stabilito: ciò completa la dimostrazione per induzione su n.

Osservazione. La formula proposta in quest'ultimo esempio avrebbe potuto essere dimostrata anche direttamente, senza ricorrere alla dimostrazione per induzione (sarebbe stato infatti sufficiente sviluppare i quadrati al primo membro).

Il procedimento dimostrativo dell'induzione si basa sul terzo assioma di Peano, perché, se S è l'insieme degli indici k per i quali P(k) è vero, allora, una volta provati i due passi dell'induzione (caso base e passo induttivo), avremo dimostrato che $0 \in S$ e, se $n \in S$, allora anche $n+ \in S$; questo, per il suddetto assioma, equivale a dire che S coincide con **N** e, cioè, P(n) vale per ogni n numero naturale.

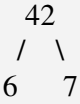
Notiamo infine che, se non fossimo ancora convinti che il principio di induzione ci permette di raggiungere tutti i casi possibili, potremmo ragionare come segue: supponiamo che esista un numero m per il quale, nonostante la dimostrazione per induzione, $P(m)$ non sia valida. Intanto m non può essere lo 0, perché sappiamo che P(0) è vera per la prima condizione. Allora $P(m)$ non sarebbe valida per un qualche m più grande di 0; ma allora non sarebbe vera nemmeno per il caso precedente, diciamo $P(m\text{-}1)$, perché la seconda condizione ci assicura che la verità di $P(m\text{-}1)$ 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 quello che si chiama in matematica 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 dimostriamola 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.

Per quanto riguarda la prova del caso base, non è necessario che questo venga identificato con lo 0. Immaginiamo una proprietà che valga per i naturali a partire da 25. Il caso base dovrà essere per forza 25, ma ciò non costituisce problema perché potremo etichettare 25 con 0, 26 con 1, ecc.; ossia porre una corrispondenza biunivoca f tra $\mathbf{N}\backslash\{0,\ldots,25\}$ ed $\mathbf{N}$, definendo $f(n)= n–25$. La prova per induzione, lavorando sugli indici, avrà 0 come caso base.

La precedente osservazione ci consente di lavorare con l'induzione su ogni insieme numerabile I, purché sia esplicitamente fornita la corrispondenza biunivoca tra I ed **N**. Ad esempio sul prodotto cartesiano $\mathbf{N}\times\mathbf{N}$, dove, una volta definito l'ordinamento lessicografico, è facile dare un'effettiva numerazione delle coppie.

7.3. Definizioni per induzione

Il principio di induzione può essere utilizzato non soltanto per dimostrare proprietà indicizzate sui numeri naturali, ma anche per dare definizioni, qualora queste risultino variare "con regolarità" sui numeri naturali. Anche in questo caso la definizione dovrà essere esibita per un caso base e poi, supponendola data per un caso generico, dovrà essere esibita per il successivo. In questo modo vengono definite le usuali operazioni aritmetiche.

Definizione. Fissato un naturale n, la somma con n è così definita:
$n+0 = n$
$n+m^+ = (n+m)^+$

Con questa definizione si può facilmente dimostrare che $n^+ = n+0^+$, cioè $n^+ = n+1$.

Analogamente, per la moltiplicazione.

Definizione. Fissato un naturale n, la moltiplicazione per n è così definita:
$n \cdot 0 = 0$
$n \cdot m^+ = (n \cdot m)+n$

Usando il principio di induzione si possono anche provare per queste operazioni le ben note proprietà. Il procedimento non è difficile, ma un po' noioso. Vale la pena di provarne effettivamente almeno una come esercizio.

7.4. 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 e 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:

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

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 della 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 rare eccezioni) dalla posizione del simbolo nella scrittura del numero. Una rappresentazione di questo genere per i naturali, detta *additiva*, è caratteristica dell'aritmetica romana.

Esempio. Ricordando che il valore dei simboli romani M, C, L, X, V e 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 naturale (in 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 sarebbe rappresentato da:

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

8. OPERAZIONI ARITMETICHE ED INSIEMISTICHE

8.1. Proprietà

Un confronto tra le operazioni aritmetiche di addizione e di moltiplicazione da un lato e le operazioni insiemistiche di unione e di intersezione dall'altro ci consentirà di evidenziare analogie (e differenze) che potranno essere utilmente riprese in studi ulteriori.

Abbiamo già visto che le operazioni aritmetiche di addizione e di moltiplicazione su **N** godono delle proprietà *associativa* e *commutativa*; cioè per ogni scelta dei numeri naturali n, m e k risulta:

$(n+m)+k = n+(m+k)$	(proprietà associativa dell'addizione)
$n+m = m+n$	(proprietà commutativa dell'addizione)
$(nm)k = n(mk)$	(proprietà associativa della moltiplicazione)
$nm = mn$	(proprietà commutativa della moltiplicazione)

Non sarà inutile ribadire che anche le operazioni insiemistiche di unione e di intersezione fra sottoinsiemi di un insieme X godono di analoghe proprietà, come abbiamo 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*):

$$n(b+k) = nm+nk$$

mentre ciò non accade per la prima: infatti $n+mk$ non è (in generale) uguale a $(n+m)(n+k)$.

Ancora a proposito di analogie possiamo citare l'esistenza di elementi neutri in tutti i casi:

$$n+0 = n$$
$$n1 = n$$

e così

$$A\cup\emptyset = A$$
$$A\cap X = A$$

Anche la funzione di annullatore dello 0 è riproducibile per l'insieme Ø:

$n\ 0 = 0$

$A \cap \emptyset = \emptyset$

Tuttavia nel caso dei sottoinsiemi di X si ha anche la formula simmetrica (duale)

$A \cup X = X$

che non corrisponde a nulla in **N**. Continuando con le diversità, possiamo notare che in $\wp(X)$ valgono ancora equazioni del tipo:

$A \cup A = A$ (idempotenza dell'unione)

$A \cap A = A$ (idempotenza dell'unione)

ed esiste, per ogni A, un altro sottoinsieme di X, A^c, il suo complemento, tale che

$A \cup A^c = X$

$A \cap A^c = \emptyset$

D'altra parte, **N** risulta un insieme totalmente ordinato rispetto alla relazione $\leq$ così definita

$n \leq m$ sse esiste k tale che $n+k=m$

mentre $\wp(X)$ risulta un insieme parzialmente ordinato rispetto alla relazione di inclusione $\subseteq$.

8.2. Algebre di Boole

Ai filosofi ed ai matematici che si proponevano di ridurre il calcolo delle classi al calcolo dei numeri (più noto tra tutti G. Leibniz), le ultime proprietà che abbiamo osservato nel precedente paragrafo sembrarono bizzarre e passò molto tempo finché vennero accettate come proprietà ammissibili per delle operazioni. Tuttavia l'analogia tra il calcolo delle classi ed il calcolo delle proprietà con i connettivi sintattici, che abbiamo osservato nel precedente capitolo, spingeva ad uno studio astratto delle operazioni di unione, intersezione, complemento, ecc. Si arrivò così all'introduzione dell'algebra di Boole (dal nome di George Boole).

Proposizione. Sia dato un insieme parzialmente ordinato $(B,\leq)$ nel quale, per ogni coppia di elementi (a,b) esista un massimo comune minorante $a \bullet b$ ed un minimo comune maggiorante $a+b$.

• e + sono due operazioni che godono delle seguenti proprietà :

0.	$a \bullet a = a$	$a+a=a$
1.	$a \bullet b = b \bullet a$	$a+b=b+a$
2.	$(a \bullet b) \bullet c = a \bullet (b \bullet c)$	$(a+b)+c=a+(b+c)$
3.	$a \bullet (a+b) = a$	$a+(a \bullet b)=a$

Dimostrazione. Le proprietà 0,1 e 2 sono immediate dalla definizione; per la 3, procediamo come segue. Per definizione, $a \bullet b \leq a$ e, per 0, $a + a \bullet b \leq a$; inoltre, per definizione, $a \leq a + a \bullet b$. Pertanto, $a+(a \bullet b)=a$; simili ragionamenti per $a \bullet (a+b)=a$.

Si noti inoltre che la proprietà 0 è anche conseguenza dalla 3: ponendo $b = a$ nella seconda legge del punto 3., abbiamo che $a + a \bullet a = a$; ponendo $b = a \bullet a$ nella seconda legge del punto 3., abbiamo che $a \bullet (a + a \bullet a) = a$, cioè $a \bullet a = a$. Simile per $a+a=a$.■

Proposizione. Sia $(B,\bullet,+)$ un insieme con due operazioni che godono delle proprietà 1., 2. e 3. della precedente proposizione, allora è possibile definire su B una relazione d'ordine $\leq$ in modo che • dia il massimo comune minorante e + il minimo comune maggiorante.

Dimostrazione. Si pone $a \leq b$ se e soltanto se $b+a=b$ o, equivalentemente, $a \bullet b=a$. La riflessività discende dalla 0., l'antisimmetria dalla 1., la transitività dalla 2.. La massimalità di $a \bullet b$ tra i minoranti di a e di b è provata osservando che, per la 3., si tratta di un minorante; inoltre, se $x \leq a$ e $x \leq b$ (cioè, $x \bullet a=x$ e $x \bullet b=x$), per la 2., $x=(x \bullet a) \bullet b=x \bullet (a \bullet b)$, cioè $x \leq a \bullet b$ (dualmente per +).■

Definizione. Si dice *algebra di Boole* (B,•,+) un insieme con due operazioni che godono delle proprietà 1., 2. e 3. sopra enunciate, ma anche:

4. $a \bullet (b+c)=(a \bullet b)+(a \bullet c)$ $\qquad a+(b \bullet c)=(a+b) \bullet (a+c)$

Inoltre, visto che un'agebra di Boole può essere visto come un insieme parzialmente ordinato (vedi Prop. precedente), richiediamo inoltre che

5. un minimo *0* ed un massimo *1*, e
6. per ogni elemento a esista un a' (complemento), tale che:

$a \bullet a'=0$ $\qquad a+a'=1$

Esempio. $(\wp(X), \subseteq, \cap, \cup, (\,)^c)$ è un'algebra di Boole per ogni insieme X.

Proposizione. In un'algebra di Boole valgono le seguenti proprietà:

$(a \bullet b)'=a'+b'$ $\qquad (a+b)'=a' \bullet b'$ $\qquad$ (leggi di De Morgan)

$(a')'=a$

$a \leq b$ *sse* $b' \leq a'$

Tra le algebre di Boole riveste particolare importanza l'algebra **2**, costruita sull'insieme B={0,1} con 0≤1. Diamo innanzitutto le tavole per le operazioni in **2**, indicando con + e • rispettivamente il minimo comune maggiorante ed il massimo comune minorante

+	0	1
0	0	1
1	1	1

•	0	1
0	0	0
1	0	1

Naturalmente i due elementi, 0 ed 1, sono l'uno complementare dell'altro.

L'insieme delle parti di un insieme X, $\wp(X)$, è in corrispondenza biunivoca con le funzioni $X \to \mathbf{2}$, perché ad ogni sottinsieme di X possiamo associare la sua *funzione caratteristica* e viceversa. Infatti, considerato un sottoinsieme A di X, possiamo definire la funzione $\chi_A: X \to \mathbf{2}$ che associa 1 agli elementi di X che sono in A e 0 agli altri. Viceversa, data una funzione f: $X \to \mathbf{2}$, possiamo considerare il sottoinsieme di X costituito dalle controimmagini di 1. Ciò significa in particolare nel caso finito (ma la cosa si può estendere anche al caso generale), che ad ogni sottinsieme di un X con n elementi viene associata una n-upla di 0 e di 1. L'unione, l'intersezione ed il complementare possono allora essere calcolati punto per punto usando le tavole delle operazioni di **2** come nel seguente esempio.

Esempio. Siano X={a,b,c,d,e}, A={a,c,d}, B={b,d}, χ_A =(10110) e χ_B =(01010). Allora

1 0 1 1 0 +	1 0 1 1 0 •	
0 1 0 1 0 =	0 1 0 1 0 =	(1 0 1 1 0)'
$\chi_{A \cup B}$ = 1 1 1 1 0	$\chi_{A \cap B}$ = 0 0 0 1 0	χ_{A^c} = 0 1 0 0 1

Avremo quindi che $A+B=\{a,b,c,d\}$, $A \bullet B=\{d\}$ e $A'=\{b,e\}$. Si osservi che le somme ed i prodotti sono quelli delle algebre di Boole e, pertanto, operaro cifra a cifra; quindi, nessun tipo di riporto o nozioni collegate sono da assumere.

Una delle più importanti e classiche applicazioni della teoria delle algebre di Boole riguarda la costruzione e la semplificazione di circuiti. Naturalmente si tratta di circuiti in senso astratto perché quanto diremo sarà altrettanto bene riferibile sia a circuiti elettrici o elettronici, che a circuiti idraulici o di traffico, ecc.. La caratteristica peculiare di questi circuiti dovrà essere la presenza di interruttori a due soli valori: "aperto" e "chiuso"; questo fatto significa che un circuito sia una funzione $\mathbf{2}^n \to \mathbf{2}$. Infatti il passaggio o meno del "flusso di corrente" attraverso il circuito sarà determinato dai valori assunti dagli interruttori.

La "somma" ed il "prodotto" di interruttori sarà rispettivamente la loro messa in parallelo o in serie: infatti nel primo caso la corrente passerà se almeno passa per uno dei due; nell'altro caso, la corrente passerà se passa per ambedue. Detto in altre parole, la funzione somma assume valore 1 se almeno uno dei due addendi assume valore 1, mentre la funzione prodotto assume valore 1 se ambedue i fattori assumono valore 1.

Abbiamo già accennato alla relazione tra le operazioni in $\wp(X)$ ed i connettivi logici dei quali ci occuperemo nel prossimo capitolo; a questo punto è chiaro che questi ultimi potranno essere caratterizzati anche da circuiti elementari che prendono il nome di *porte logiche*.

9. * I NUMERI PRIMI

9.1. Divisibilità e numeri primi

In questo paragrafo presenteremo le principali nozioni collegate ai numeri primi ed indicheremo alcune dimostrazioni; in particolare:

- ci chiederemo innanzitutto: che cosa sono i numeri primi? Daremo la definizione e illustreremo il crivello di Eratostene. Mostreremo l'esistenza e l'unicità della scomposizione in fattori primi di un numero naturale.
- inoltre, quanti sono i numeri primi? Come sono distribuiti nella sequenza dei numeri naturali?
- daremo quindi alcuni risultati: una condizione necessaria di primalità (teorema di Fermat); una condizione necessaria e sufficiente di primalità (teorema di Wilson).
- presenteremo infine 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:

$$m = b\cdot n \quad \text{e} \quad n = a\cdot m \qquad (*)$$

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 (*), 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)

9.2. 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:

$$n = p_1 p_2 ... p_k \quad \blacksquare$$

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: $p_1^2 \le n$.

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

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

Se poniamo $N = n - p_1 q_1$ abbiamo che $0<N<n$ 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*. $\blacksquare$

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.

9.3. 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: $P = p_1p_2 \ldots p_r+1$ 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 $P - p_1p_2 \ldots p_r = 1$ che è impossibile. Dunque questo p è un altro primo, e $p_1, p_2, \ldots, p_r$ non sono tutti i numeri primi. ■

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 si può trovare in: Tenenbaum & Mendès France, 1997; per un'elegante dimostrazione di P. Erdös si può vedere: Aigner & Ziegler, 1998).

Dimostrazione. Consideriamo innanzitutto che ogni intero positivo n può essere scritto in forma unica nome prodotto di un numero q privo di fattori quadrati e di un numero m^2. Indicando con q un numero privo di fattori quadrati, possiamo scrivere:

$$\sum_{n\le x}\frac{1}{n}=\sum_{q\le x}\left(\frac{1}{q}\sum_{m\le\sqrt{x/q}}\frac{1}{m^2}\right)\le\sum_{q\le x}\left(\frac{1}{q}\sum_{m=1}^{+\infty}\frac{1}{m^2}\right)$$

(la prima uguaglianza potrebbe non apparire subito evidente: suggeriamo al lettore di prendere confidenza con essa facendo qualche prova; ad esempio con $x = 20$). La seguente minorazione non richiede particolari commenti:

$$\sum_{m=1}^{+\infty}\frac{1}{m^2}\le 1+\sum_{m=2}^{+\infty}\frac{1}{(m-1)m}=1+\sum_{m=2}^{+\infty}\left(\frac{1}{m-1}-\frac{1}{m}\right)=2$$

(la serie $\displaystyle\sum_{m=2}^{+\infty}\frac{1}{(m-1)m}=\sum_{m=2}^{+\infty}\left(\frac{1}{m-1}-\frac{1}{m}\right)=1$, è detta "telescopica") da cui:

$$\sum_{n\le x}\frac{1}{n}\le 2\sum_{q\le x}\frac{1}{q}$$

Consideriamo ora la $\sum_{q\le x}\frac{1}{q}$ e indichiamo con p un primo:

$$\sum_{q\le x}\frac{1}{q}\le\prod_{p\le x}\left(1+\frac{1}{p}\right)\le\exp\left\{\sum_{p\le x}\frac{1}{p}\right\}$$

La prima minorazione si ottiene sviluppando $\prod_{p\le x}\left(1+\frac{1}{p}\right)$; la seconda notando che è: $1+a \le e^a$ (tale disequazione può essere un utile esercizio) e ponendo quindi in questa formula: $a = 1/p$. Possiamo dunque scrivere:

$$\sum_{n\le x}\frac{1}{n}\le 2\exp\left\{\sum_{p\le x}\frac{1}{p}\right\}$$

Occupiamoci del primo membro della disuguaglianza. Da $\frac{1}{n}\ge\int_{n}^{n+1}\frac{dt}{t}$, risulta:

$$\sum_{n\le x}\frac{1}{n}\ge\sum_{n\le x}\int_{n}^{n+1}\frac{dt}{t}\ge\log x$$

e ciò ci permette di scrivere:

$$\log x\le\sum_{n\le x}\frac{1}{n}\le 2\exp\left\{\sum_{p\le x}\frac{1}{p}\right\}$$

$$\sum_{p\le x}\frac{1}{p}\ge\log\log x-\log 2$$

Considerando che $\lim_{x\to+\infty}\log x=+\infty$ possiamo affermare che la serie dei reciproci dei numeri primi diverge. ■

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. Ad esempio:

$A_1 = 0$	(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 completa di ciò venne data nel 1896 (da Hadamard e de la Vallée Poussin).

9.4. 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* (introdotto nel 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.

9.5. Numeri primi e problemi aperti

Uno dei più celebri problemi aperti della teoria dei numeri è la congettura di Goldbach, suggerita (ma non provata) in uno scambio di lettere tra Christian Goldbach (1690-1764) e Leonhard Euler (1707-1783) nel giugno 1742, secondo la quale *tutti i naturali pari maggiori di 2 sono somme di due numeri primi* (non necessariamente distinti).

Esempio. La congettura di Goldbach è facilmente verificabile per alcuni pari:

4 = 2+2
6 = 3+3
8 = 3+5
10 = 3+7 = 5+5 etc.

Ma ciò vale per *tutti* i numeri pari? Nessuno finora (2002) è stato capace di dimostrarlo né di trovare un naturale pari maggiore di 2 che *non* sia esprimibile come somma di due numeri primi.

La teoria additiva dei numeri si è sviluppata a partire dalla fine del XVIII secolo. Risultato fondamentale per tale teoria è il teorema seguente:

Proposizione (Lagrange). Ogni naturale è la somma di quattro quadrati.

Un insieme B di naturali è detto base di ordine *h* se ogni naturale può essere scritto come somma di *h* elementi di B (non necessariamente distinti). Ad esempio, il teorema di Lagrange stabilisce che l'insieme $\{n \in \mathbf{N}: n = x^2 \text{ e } x \in \mathbf{N}\}$ è una base di ordine 4.

Il problema fondamentale della teoria additiva dei numeri è stabilire se un assegnato sottoinsieme di N è una base di ordine finito.

La congettura di Goldbach esprime il problema analogo applicato ai naturali pari maggiori di 2, con la base di ordine due costituita dall'insieme dei primi.

Proposizione (1919-1920, Brun). Ogni intero non negativo pari abbastanza grande è la somma di due numeri aventi ciascuno non più di nove fattori primi.

Proposizione (1930, Shrinel'man). Ogni intero maggiore di 1 è la somma di un limitato numero di primi.

Proposizione (1937, Vinogradov). Ogni intero dispari abbastanza grande o è primo o è la somma di tre primi.

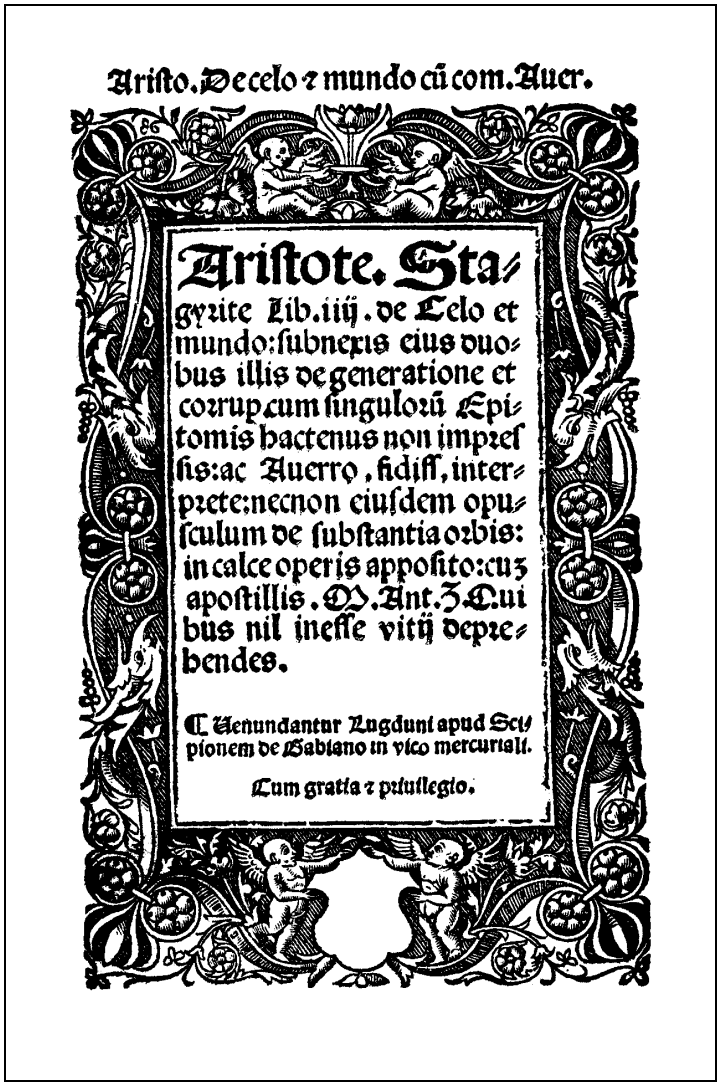
Proposizione (1966-1978, Chen). Ogni intero pari abbastanza grande può essere scritto come somma di un primo dispari e di un numero che o è primo o è il prodotto di due primi.

Un'altra celebre congettura a tutt'oggi non provata è detta *dei primi gemelli*. Alcune coppie di numeri primi sono costituite da p e da $p+2$ (primi gemelli):

3, 5 11, 13 17, 19 etc.

Ebbene, esistono infinite coppie di primi gemelli? Ancora una volta il problema è aperto (2002).

Osservazione. La presenza di questi e di altri problemi aperti riguardanti i primi (anche apparentemente semplici: esistono infiniti primi della forma n^2+1?) induce a qualche riflessione. C'è una forte asimmetria tra l'*addizione* e la *moltiplicazione*. Rispetto alla *moltiplicazione* (elemento neutro 1), infatti, esistono infiniti elementi "atomici": i primi. La scomposizione di un naturale in un prodotto di naturali "atomici rispetto alla *moltiplicazione*" è interessante, semplifica la trattazione del numero dato. Invece rispetto all'*addizione* (elemento neutro 0) esiste un solo elemento atomico: 1. La scomposizione di un naturale in un prodotto di naturali "atomici rispetto all'*addizione*" è banale (1+1+ …+1) e non semplifica la trattazione del numero dato.



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