

# Prefazione

*Per comprendere la matematica occorre far funzionare il cervello, e questo costa sempre un certo sforzo. Non é possibile fare la matematica "a fumetti", non é possibile trasformare la sua storia in una novellina. Chi é pigro di mente, chi non prova gioia nel far lavorare il suo cervello, é meglio che non cominci neppure a leggere. Chi invece non si spaventa per le fatiche della mente, non si scoraggi se qua e lá, a prima vista, non capisce, e non pretenda di leggere tutto di seguito; ma legga attentamente, un poco per volta, saltando le cose piú difficili, o facendosele spiegare da chi ha studiato piú di lui.*

*Lucio Lombardo Radice*

*("La Matematica da Pitagora a Newton", Prefazione)*

Questi appunti raccolgono gli argomenti delle lezioni del corso di *Algebra 1* per gli studenti dei corsi di laurea in "*Matematica*" e "*Matematica e Informatica*" della Seconda Università degli Studi di Napoli. Essi si presentano spesso schematici e mancano molti dei commenti, dei riferimenti e delle osservazioni indispensabili per una buona presentazione degli argomenti trattati. É, pertanto, consigliabile integrare la loro lettura con quella di un libro.

I testi che abbiamo maggiormente seguito nel preparare le lezioni sono stati:

- M. Curzio, P. Longobardi, M. May, *Lezioni di Algebra*, Liguori Editore;
- S. Franciosi, F. de Giovanni, *Elementi di Algebra*, Aracne Editrice;
- J.A. Gallian, *Contemporary abstract algebra*, D.C. Heath and Company;
- C. Grove, *Algebra*, Academic Press;
- G.M. Piacentini Cattaneo, *Algebra, un approccio algoritmico*, Decibel/Zanichelli.

Per quanto riguarda gli esercizi consigliamo di consultare, oltre ai testi sopraelencati, anche i seguenti:

- M. Curzio, P. Longobardi, M. May, *Esercizi di Algebra*, Liguori Editore;
- S. Franciosi, F. de Giovanni, *Esercizi di Algebra*, Aracne Editrice.

Avvertiamo che nella preparazione del corso, e quindi nella stesura di queste note, sono state tenute presenti alcune delle conoscenze di algebra lineare, analisi matematica e geometria acquisite dagli studenti durante il primo semestre.

Nel concludere, desideriamo ringraziare in anticipo quanti vorranno segnalarci eventuali errori e/o omissioni.

Caserta, febbraio 2002.

Francesco Mazzocca

Figura 1: Pitagora (570 A.C. - 490 A.C.)

# Capitolo 1

## Preliminari e Richiami

### 1.1 Alcune notazioni standard

Nel seguito riterremo che il Lettore abbia familiarità con il linguaggio ed i primi elementi della *teoria elementare degli insiemi* e che conosca le proprietà elementari dei *numeri naturali*, degli *interi relativi*, dei *numeri reali e complessi* e dei *polinomi*. Supporremo, in particolare, noti i concetti di *insieme* e di *elemento* di un insieme.

Ricordiamo le seguenti notazioni standard che useremo sempre nel seguito senza richiamarle esplicitamente.

- $a \in A$  indica che  $a$  è un elemento dell'insieme  $A$ ;
- $a \notin A$  indica che  $a$  non è un elemento dell'insieme  $A$  <sup>1</sup>;
- $\emptyset :=$  insieme vuoto <sup>2</sup>;

Se  $A$  e  $B$  sono insiemi, poniamo

- $A \subseteq B, B \supseteq A \Leftrightarrow A$  è *sottoinsieme* di  $B$ ;
- $A \subset B, B \supset A \Leftrightarrow A$  è sottoinsieme di  $B$  e non è uguale a  $B$  (*sottoinsieme proprio*);
- $A \cup B := \{x : x \in A \text{ o } x \in B\}$  <sup>3</sup> (*unione di  $A$  e  $B$* );
- $A \cap B := \{x : x \in A \text{ e } x \in B\}$  (*intersezione di  $A$  e  $B$* );
- $A \setminus B := \{x : x \in A \text{ e } x \notin B\}$  (*differenza fra  $A$  e  $B$* );
- $A \times B := \{(a, b) : a \in A, b \in B\}$  (*prodotto cartesiano di  $A$  e  $B$* );
- $A_1 \times A_2 \times A_3 \times \cdots \times A_n := \{(a_1, a_2, a_3, \dots, a_n) : a_i \in A_i, i = 1, 2, \dots, n\}$  (*prodotto cartesiano degli insiemi  $A_1, A_2, A_3, \dots, A_n$* );
- $A^n := \{(a_1, a_2, a_3, \dots, a_n) : a_i \in A, i = 1, 2, \dots, n\}$  (*prodotto cartesiano di  $n$  copie di  $A$* );
- $P(A) := \{X : X \subseteq A\}$  (*insieme delle parti di  $A$* ).

---

<sup>1</sup>In generale, il simbolo / sovrapposto ad un altro simbolo indica la negazione di quest'ultimo.

<sup>2</sup>La notazione  $:=$  indica che il simbolo scritto alla sua sinistra è definito da ciò che è scritto alla sua destra.

<sup>3</sup>Il simbolo  $:$  si legge "tale che"; un simbolo equivalente a  $:$  è  $|$ .

**DEFINIZIONE 1.1.1** Due insiemi  $A, B$  si dicono *uguali*, e si scrive  $A = B$ , se risulta  $A \subseteq B$  e  $B \subseteq A$ .  $\diamond$

**OSSERVAZIONE 1.1.2** In virtù della precedente definizione, se si vuole verificare che due insiemi  $A$  e  $B$  sono uguali bisogna provare che *ogni elemento di  $A$  è un elemento di  $B$*  e che *ogni elemento di  $B$  è un elemento di  $A$* .  $\diamond$

Poniamo, inoltre,

- $N_o$  := insieme dei numeri naturali (compreso lo zero);
- $N$  := insieme dei numeri naturali diversi da zero;
- $Z$  := insieme dei numeri interi (relativi);
- $Q$  := insieme dei numeri razionali;
- $R$  := insieme dei numeri reali;
- $C$  := insieme dei numeri complessi;
- $A^* := A \setminus \{0\}$ ,  $A = Z, Q, R, C$ ;
- $A[x]$  := insieme dei polinomi nell'indeterminata  $x$  a coefficienti in  $A$ ,  $A = N_o, Z, Q, R, C$ ;
- $M_{m,n}(A)$  := insieme delle matrici di tipo  $m \times n$  ad elementi in  $A$ ,  $A = N_o, Z, Q, R, C$ ;
- $M_n(A)$  := insieme delle matrici quadrate d'ordine  $n$  ad elementi in  $A$ ,  $A = N_o, Z, Q, R, C$ .

**ESERCIZIO 1.1.3** Siano  $A, B, C$  insiemi. Provare che valgono le seguenti proprietà:

- $A \cup A = A$ ,  $A \cap A = A$ ;
- $A \cup B = B \cup A$ ,  $A \cap B = B \cap A$ ;
- $(A \cup B) \cup C = A \cup (B \cup C)$ ,  $(A \cap B) \cap C = A \cap (B \cap C)$ ;
- $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ ,  $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ .

## 1.2 Richiami sulle funzioni

Una *funzione*, o *applicazione*, è una terna  $(A, B, f)$ , ove  $A$  e  $B$  sono insiemi non vuoti ed  $f$  una legge che ad ogni elemento  $a$  di  $A$  fa corrispondere un ben preciso elemento  $f(a)$  di  $B$ . L'elemento  $f(a)$  si chiama *corrispondente*, o *immagine*, di  $a$  in  $f$ ; gli insiemi  $A, B$  si chiamano rispettivamente *insieme di definizione*, o *dominio*, e *codominio* della funzione. Quando è assegnata una funzione  $(A, B, f)$  si dice anche che è assegnata una *funzione  $f$  di  $A$  in  $B$* , o *fra  $A$  e  $B$* , e ciò si esprime mediante una delle seguenti notazioni:

$$f : A \rightarrow B \quad , \quad A \xrightarrow{f} B \quad , \quad x \in A \rightarrow f(x) \in B .$$

Una funzione, dunque, è caratterizzata da tre oggetti: il dominio, il codominio e la legge di associazione  $f$ ; variando uno di questi tre oggetti, cambia la funzione. Ciò nonostante, con abuso

di notazione, la funzione  $(A, B, f)$  si denota spesso soltanto con il simbolo  $f$ , sottointendendo il dominio e il codominio.

Nel seguito, se non vi é possibilità di equivoci, quando diremo che é assegnata una funzione fra due insiemi sottointenderemo sempre che questi siano non vuoti.

**DEFINIZIONE 1.2.1** Assegnati una funzione  $f : A \rightarrow B$ , un sottoinsieme  $X$  di  $A$  ed uno  $Y$  di  $B$ , il sottoinsieme  $f(X)$  di  $B$  definito da

$$f(X) := \{y \in B : y = f(x), \text{ per qualche } x \in X\}$$

si chiama *immagine di  $X$  in  $f$* , mentre il sottoinsieme  $f^{-1}(Y)$  di  $A$  definito da

$$f^{-1}(Y) := \{x \in A : f(x) \in Y\}$$

si chiama *controimmagine di  $Y$  in  $f$* . L'immagine  $f(A)$  di  $A$  in  $f$  si denota anche con  $Im(f)$ . Se  $Y$  contiene un solo elemento  $b$ , si parla di controimmagine di  $b$  in  $f$ , si scrive  $f^{-1}(b)$  invece di  $f^{-1}(\{b\})$  e, quindi, si ha:

$$f^{-1}(b) := \{x \in A : f(x) = b\}$$

◇

**ESERCIZIO 1.2.2** Sia  $A \xrightarrow{f} B$  una funzione e  $X, Y$  sottoinsiemi di  $A$ . Provare che:

- $f(X \cup Y) = f(X) \cup f(Y)$ ;
- $f(X \cap Y) \subseteq f(X) \cap f(Y)$ ;
- $f(X \setminus Y) \supseteq f(X) \setminus f(Y)$ ;

**ESERCIZIO 1.2.3** Sia  $A \xrightarrow{f} B$  una funzione e  $X, Y$  sottoinsiemi di  $B$ . Provare che:

- $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$ ;
- $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$ ;
- $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$ ;

**DEFINIZIONE 1.2.4** Assegnate le funzioni  $f : A \rightarrow B$  e  $g : B \rightarrow C$ , la funzione  $g \circ f$  definita da

$$g \circ f : x \in A \rightarrow g(f(x)) \in C$$

prende il nome di *funzione composta*, o *composizione*, di  $f$  e  $g$ . Nel seguito porremo quasi sempre  $fg := g \circ f$ , cioè

$$(fg)(x) = g(f(x)), \text{ per ogni } x \in A.$$

◇

**DEFINIZIONE 1.2.5** Una funzione  $f : A \rightarrow B$  si dice *iniettiva* se vale la seguente proprietà

$$a, b \in A, \quad a \neq b \Rightarrow f(a) \neq f(b)$$

o, equivalentemente,

$$a, b \in A, \quad f(a) = f(b) \Rightarrow a = b.$$

◇

**ESERCIZIO 1.2.6** Sia  $A \xrightarrow{f} B$  una funzione. Provare che

$$f \text{ iniettiva} \Leftrightarrow f^{-1}(f(X)) = X, \text{ per ogni } X \subseteq A.$$

**DEFINIZIONE 1.2.7** Una funzione  $f : A \rightarrow B$  si dice *suriettiva* se risulta  $f(A) = B$ , cioè se vale la seguente proprietà

per ogni elemento  $b \in B$ , esiste almeno un elemento  $a \in A$  tale che  $f(a) = b$

o, equivalentemente,

$$f^{-1}(b) \neq \emptyset, \text{ per ogni } b \in B.$$

◇

**ESERCIZIO 1.2.8** Sia  $A \xrightarrow{f} B$  una funzione. Provare che

$$f \text{ suriettiva} \Leftrightarrow f^{-1}(f^{-1}(Y)) = Y, \text{ per ogni } Y \subseteq B.$$

**DEFINIZIONE 1.2.9** Una funzione  $f : A \rightarrow B$  si dice *biiettiva*, o *biunivoca*, se risulta iniettiva e suriettiva, cioè se vale la seguente proprietà

per ogni elemento  $b \in B$ , esiste un unico elemento  $a \in A$  tale che  $f(a) = b$ .

Nell'ipotesi che  $f$  sia biunivoca, la funzione fra  $B$  ed  $A$  che ad ogni elemento  $b \in B$  associa l'unico elemento  $a \in A$  tale che  $f(a) = b$  si chiama *inversa* della  $f$  e si denota con  $f^{-1}$ . Una funzione biunivoca si dice anche *invertibile*. ◇

**ESERCIZIO 1.2.10** Siano  $A \xrightarrow{f} B$  e  $B \xrightarrow{g} C$  due funzioni. Provare che:

- $A \xrightarrow{f} B$  iniettiva  $\Rightarrow A \xrightarrow{f} f(A)$  biunivoca.
- $f, g$  iniettive (resp. suriettive, biunivoche)  $\Rightarrow fg$  iniettiva (resp. suriettiva, biunivoca).
- $fg$  iniettiva  $\Rightarrow f$  iniettiva.
- $fg$  suriettiva  $\Rightarrow g$  suriettiva.
- $fg$  biunivoca  $\Rightarrow f$  iniettiva e  $g$  suriettiva.

**ESERCIZIO 1.2.11** Siano  $A \xrightarrow{f} B$ ,  $B \xrightarrow{g} C$  e  $C \xrightarrow{h} D$  tre funzioni. Provare che risulta

$$(fg)h = f(gh).$$

**DEFINIZIONE 1.2.12** Una funzione biunivoca di un insieme non vuoto  $A$  su se stesso prende il nome di *permutazione* su  $A$ . L'insieme di tutte le permutazioni su  $A$  si denota con  $Perm(A)$  o  $Symm(A)$ .

La funzione che ad ogni  $a \in A$  associa l'elemento  $a$  stesso é una permutazione che si chiama *funzione o permutazione identica*, o anche *identitá*, e si denota con  $i_A$ , o semplicemente con  $i$  se non vi é luogo ad equivoci.  $\diamond$

**ESERCIZIO 1.2.13** Sia  $A \xrightarrow{f} B$  una funzione. Provare che:

$$fi_B = i_A f.$$

**ESERCIZIO 1.2.14** Sia  $A \xrightarrow{f} B$  una funzione iniettiva. Provare che esiste una funzione  $B \xrightarrow{g} A$  tale che

$$fg = i_A.$$

**ESERCIZIO 1.2.15** Sia  $A \xrightarrow{f} B$  una funzione suriettiva. Provare che esiste una funzione  $B \xrightarrow{g} A$  tale che

$$gf = i_B.$$

**ESERCIZIO 1.2.16** Sia  $A \xrightarrow{f} B$  una funzione e supponiamo che esistano due funzioni  $B \xrightarrow{g} A$  e  $B \xrightarrow{h} A$  tali che

$$fg = i_A \quad e \quad hf = i_B.$$

Provare che  $f$  é biunivoca e risulta  $h = g = f^{-1}$ .

### 1.3 Proprietá fondamentali degli interi relativi

Consideriamo l'insieme  $Z$  dei numeri interi (relativi) con le usuali operazioni di *addizione* e *moltiplicazione* e con la usuale relazione  $\leq$  di *minore o uguale*. Le seguenti proprietá, ove  $a, b, c \in Z$ , sono (*apparentemente*) ovvie.

1.  $a + b$  e  $ab$  sono elementi di  $Z$ .
2.  $a + b = b + a$  e  $ab = ba$ .
3.  $(a + b) + c = a + (b + c)$  e  $(ab)c = a(bc)$ .
4. Esiste un elemento 0 (lo *zero*) tale che  $a + 0 = a$ . Esiste un elemento 1 (l'*unitá*) tale che  $a1 = a$ .
5.  $a(b + c) = ab + ac$ .
6. Per ogni  $a$  esiste un elemento  $-a$  (l'*opposto di a*) tale che  $a + (-a) = 0$ .
7.  $a \neq 0$  e  $ab = ac \Rightarrow b = c$ .
8. La relazione  $\leq$  é d'ordine totale in  $Z$  (- *riflessiva*:  $a \leq a$ , per ogni  $a \in Z$ ;

- antisimmetrica:  $a \leq b, b \leq a \Rightarrow a = b$ ;
- transitiva:  $a \leq b \leq c \Rightarrow a \leq c$ ;
- $a, b \in Z \Rightarrow a \leq b$  o  $b \leq a$ .)

9.  $a \leq b \Rightarrow a + c \leq b + c$ .

10.  $a \leq b$  e  $0 \leq c \Rightarrow ac \leq bc$ .

11. (*principio di induzione*) Sia  $S$  un insieme di elementi di  $Z$  e  $h$  un elemento di  $S$ . Se vale la proprietá

$$h \leq k \quad , \quad k \in S \Rightarrow k + 1 \in S,$$

allora  $S$  contiene tutti gli interi maggiori o uguali ad  $h$ .

**OSSERVAZIONE 1.3.1** Le undici proprietá ricordate sono *fondamentali* nel senso che a partire da esse é possibile dimostrare tutte le proprietá degli interi. Assumeremo, pertanto, queste proprietá come gli **assiomi** che definiscono  $Z$ . Il Lettore interessato potrà approfondire lo studio sulle costruzioni assiomatiche di  $N_o$  e di  $Z$  consultando un testo universitario di Algebra o di Analisi matematica.  $\diamond$

**DEFINIZIONE 1.3.2** L'intero  $a + (-b)$  si denota con  $a - b$  e si chiama *differenza* fra  $a$  e  $b$ . L'operazione che ad ogni coppia di interi  $(a, b)$  associa la loro differenza  $a - b$  prende il nome di *sottrazione*.  $\diamond$

Valgono le seguenti proprietá, che il Lettore puó provare a dimostrare per esercizio.

- $a + b = a \Rightarrow b = 0$ .
- $ab = a, a \neq 0 \Rightarrow b = 1$ .
- $a - (-b) = a + b$ .
- $a0 = 0$ .
- $a, b > 0$  o  $a, b < 0 \Leftrightarrow ab > 0$ .
- $a, b$  uno positivo e l'altro negativo  $\Leftrightarrow ab < 0$ .
- $ab = 0 \Rightarrow a = 0$  oppure  $b = 0$  (*legge di annullamento del prodotto*).
- $a \leq b \Rightarrow -b \leq -a$ .
- $0 \leq a^2$ .
- $a \leq a + 1$  (*principio di Archimede*).

**PROPOSIZIONE 1.3.3 (principio di buon ordinamento)** Ogni sottoinsieme non vuoto  $X$  di  $Z$  che sia inferiormente limitato<sup>4</sup> possiede l'elemento minimo<sup>5</sup>.

<sup>4</sup> $X$  é inferiormente limitato se esiste un intero  $a$  tale che  $a \leq n$ , per ogni  $n \in X$ .

<sup>5</sup>Un elemento  $m \in X$  si dice *minimo* di  $X$ , se risulta  $m \leq n$ , per ogni  $n \in X$ . Si prova che se  $X$  ammette un minimo  $m$  esso é unico.

**DIMOSTRAZIONE.** L'insieme  $S$  degli interi  $a$  tali che  $a \leq x$ , per ogni  $x \in X$ , é non vuoto perché  $X$  é inferiormente limitato. Si deve, dunque, provare che  $S$  contiene un elemento di  $X$ . Nell'ipotesi contraria, cioè  $S \cap X = \emptyset$ , detto  $h$  un elemento di  $S$ , risulta

$$h \leq k \quad , \quad k \in S \quad \Rightarrow \quad k + 1 \in S,$$

ed  $S$ , per il principio d'induzione, contiene tutti gli interi maggiori o uguali ad  $h$  e, quindi,  $X$ . Ciò é evidentemente assurdo e l'asserto é così provato.  $\diamond$

**OSSERVAZIONE 1.3.4** Se negli assiomi che definiscono  $Z$  si sostituisce il principio di induzione con quello di buon ordinamento, é facile provare che quest'ultimo implica il primo. I due principi, dunque, sono equivalenti.  $\diamond$

## 1.4 Varianti del principio di induzione

I teoremi che seguono sono due varianti del principio d'induzione; la loro dimastrazione é immediata ed é lasciata come esercizio al Lettore.

**PROPOSIZIONE 1.4.1** Sia  $S$  un sottoinsieme di  $N_o$  con le seguenti proprietá:

$$(i) \quad 0 \in S \quad e \quad (ii) \quad k \in S \Rightarrow k + 1 \in S.$$

Allora risulta  $S = N_o$ .

**PROPOSIZIONE 1.4.2** Sia  $P(k)$  una proposizione definita per ogni intero  $k \geq h$ . Se

$$P(h) \text{ é vera}$$

e se

$$P(k) \text{ vera, con } k \geq h \Rightarrow P(k + 1) \text{ vera,}$$

allora  $P(k)$  é vera per ogni  $k \geq h$ .

**OSSERVAZIONE 1.4.3** L'ultima versione del principio di induzione é particolarmente utile perché fornisce un importante metodo di dimostrazione (*dimostrazione per induzione*) che, in alcuni casi, permette di ridurre soltanto a due un numero non finito di prove da effettuare: se vogliamo provare che tutte le proposizioni (in numero non finito)  $P(n)$  sono vere per ogni  $n \geq h$ , basta dimostrare soltanto che  $P(h)$  é vera e che, se  $P(n)$  é vera per  $n > h$ , allora  $P(n + 1)$  é vera. Gli esercizi che seguono mostrano alcune semplici applicazioni di questa tecnica.  $\diamond$

**ESERCIZIO 1.4.4** Provare che, per ogni intero non negativo  $n$ , l'intero  $2^{2n} - 1$  é divisibile<sup>6</sup> per 3.

<sup>6</sup>Dati due interi  $a, b$ , con  $b \neq 0$ , si dice che  $a$  é divisibile per  $b$  se esiste un intero  $c$  tale che  $a = bc$ .

**SOLUZIONE.** L'asserto é banalmente vero per  $n = 0$ . Denotiamo con  $S$  l'insieme di tutti gli interi non negativi  $k$  tali che  $2^{2k} - 1$  sia divisibile per 3; ovviamente  $0 \in S$ . Ora, se assumiamo che un intero  $n$  appartenga ad  $S$ , abbiamo

$$2^{2(n+1)} - 1 = 4 \cdot 2^{2n} - 1 = 4 \cdot 2^{2n} - 4 + 3 = 4(2^{2n} - 1) + 3,$$

da cui ricaviamo che  $2^{2(n+1)} - 1$  é divisibile per 3 e cioè  $n + 1 \in S$ . Il principio di induzione assicura allora che  $S = N_o$ ; cioè che il nostro asserto é vero.  $\diamond$

**ESERCIZIO 1.4.5 (formula di de Moivre)** *Provare che, per ogni intero non negativo  $n$  e per ogni numero reale  $\theta$ , risulta*

$$(\cos \theta + i \operatorname{sen} \theta)^n = \cos n\theta + i \operatorname{sen} n\theta, \quad (1.1)$$

ove  $i = \sqrt{-1}$  é l'unità immaginaria del campo complesso.

**SOLUZIONE.** L'asserto é vero per  $n = 0$ . Se supponiamo che sia vero per un intero  $n > 0$ , abbiamo:

$$\begin{aligned} (\cos \theta + i \operatorname{sen} \theta)^{n+1} &= (\cos \theta + i \operatorname{sen} \theta)^n (\cos \theta + i \operatorname{sen} \theta) = \\ &= (\cos n\theta + i \operatorname{sen} n\theta)(\cos \theta + i \operatorname{sen} \theta) \\ &= \cos n\theta \cos \theta - \operatorname{sen} n\theta \operatorname{sen} \theta + i(\operatorname{sen} n\theta \cos \theta + \operatorname{sen} \theta \cos n\theta) \\ &= \cos (n+1)\theta + i \operatorname{sen} (n+1)\theta. \end{aligned}$$

Allora l'asserto segue dal principio di induzione.  $\diamond$

Figura 1.1: A. de Moivre (1667-1754)

**ESERCIZIO 1.4.6** *Supponiamo di giocare a poker avendo a disposizione solo fiches da 5 e 8 euro. E' facile rendersi conto che in queste condizioni non é possibile fare puntate di*

1, 2, 3, 4, 6, 7, 9, 11, 12, 14, 17, 19, 22, 27

*euro. Provare che é possibile fare puntate di  $n$  euro, per ogni  $n > 27$ .*

**SOLUZIONE.** Basta provare che ogni intero  $n > 27$  può scriversi nella forma  $a5 + b8$ , con  $a, b$  interi positivi. Ovviamente  $28 = 4 \cdot 5 + 1 \cdot 8$  é di questo tipo.

Supponiamo ora che un intero  $n > 28$  sia del tipo  $n = a5 + b8$  e osserviamo che  $a$  e  $b$  non possono essere entrambi minori di 3. Allora abbiamo:

$$a \geq 3 \Rightarrow$$

$$n + 1 = (a5 + b8) + (-3 \cdot 5 + 2 \cdot 8) = (a - 3)5 + (b + 2)8,$$

cioé  $n + 1$  é del tipo desiderato;

$$b \geq 3 \Rightarrow$$

$$n + 1 = (a5 + b8) + (5 \cdot 5 - 3 \cdot 8) = (a + 5)5 + (b - 3)8$$

e anche in questo caso  $n + 1$  é del tipo desiderato. Il principio di induzione assicura allora che il nostro asserto é vero.  $\diamond$

## 1.5 Equipotenza di Insiemi e Cardinalità

*Il tutto é maggiore della somma di sue parti.*

*Aristotele ("Metaphysica")*

*...nel numero infinito, se concepir lo potessimo, bisognerebbe dire, tanti essere i quadrati quanti tutti i numeri insieme.*

*Galileo Galilei*

*("Discorsi e dimostrazioni matematiche intorno a due nuove scienze")*

Se  $n, m \in \mathbb{Z}$  sono due interi, con  $n \leq m$ , denoteremo con  $[n, m]$  l'intervallo chiuso di estremi  $m$  ed  $n$ , cioé

$$[n, m] = \{a \in \mathbb{Z} : n \leq a \leq m\}.$$

**DEFINIZIONE 1.5.1** Due insiemi  $A, B$  si dicono *equipotenti* se esiste tra essi una funzione biunivoca<sup>7</sup>. Se due insiemi sono equipotenti si dice anche che hanno la stessa *cardinalità*, o la stessa *potenza*. Per indicare che  $A$  e  $B$  sono equipotenti si scrive  $|A| = |B|$ .

Piú in generale, si dice che la cardinalità di  $A$  é *minore o uguale* di quella di  $B$ , e si scrive  $|A| \leq |B|$ , se esiste una funzione iniettiva di  $A$  in  $B$ . Se, poi, é  $|A| \leq |B|$  e non esiste una funzione iniettiva di  $B$  in  $A$  si dice che la cardinalità di  $A$  é *minore* di quella di  $B$  e si scrive  $|A| < |B|$ .  $\diamond$

**ESERCIZIO 1.5.2** Siano  $A, B, C$  insiemi. Provare che:

- $|A| = |A|$ ;
- $|A| = |B|, |B| = |C| \Rightarrow |A| = |C|$ ;
- $|A| \leq |B|, |B| \leq |C| \Rightarrow |A| \leq |C|$ .

<sup>7</sup>Si tenga presente che se esiste una funzione biunivoca  $f$  tra  $A$  e  $B$ , ne esiste anche una fra  $B$  e  $A$ : l'inversa di  $f$ .

**DEFINIZIONE 1.5.3** Un insieme non vuoto  $A$  si dice *finito* se esiste un intero positivo  $n$  tale che  $A$  è equipotente a  $[1, n]$ ; in questo caso l'intero  $n$  si chiama *cardinalità* di  $A$  e coincide con la nozione di *numero di elementi* di  $A$ . La cardinalità di un insieme finito si chiama anche *ordine* dell'insieme. Per definizione si assume anche che l'insieme vuoto sia finito con cardinalità zero. Un insieme che non sia finito si dice *infinito*.  $\diamond$

**ESERCIZIO 1.5.4** Siano  $A, B$  due insiemi finiti. Provare che:

- $|A \cup B| = |A| + |B| - |A \cap B|$  (principio di inclusione-esclusione);
- $|A \times B| = |A| \times |B|$ .

**ESERCIZIO 1.5.5** Sia  $A$  un insieme finito e  $f$  una funzione di  $A$  in  $A$ . Provare le seguenti equivalenze:

$$f \text{ iniettiva} \Leftrightarrow f \text{ suriettiva} \Leftrightarrow f \text{ biunivoca.}$$

Riportiamo, senza dimostrazioni, alcuni risultati fondamentali sulle cardinalità.

**PROPOSIZIONE 1.5.6** Un insieme è infinito se, e solo se, è equipotente ad un suo sottoinsieme proprio.

**PROPOSIZIONE 1.5.7** Se  $A$  e  $B$  sono insiemi, risulta:

- $|A| \leq |B|$  o  $|B| \leq |A|$  (teorema di Hartogs);
- $|A| \leq |B|$  e  $|B| \leq |A| \Rightarrow |A| = |B|$  (teorema di Bernstein);
- $A$  infinito e  $|A| \leq |B| \Rightarrow B$  infinito;
- $A$  infinito  $\Rightarrow |A \times A| = |A|$ ;
- $|A| < |P(A)|$  (teorema di Cantor);

Figura 1.2: F. Bernstein (1878-1956)

**ESEMPIO 1.5.8** L'insieme  $N = \{1, 2, \dots, n, \dots\}$  degli interi positivi é infinito. Tale insieme, infatti, contiene il sottoinsieme dei numeri pari  $2N = \{2n : n \in N\}$  e la funzione

$$n \in N \rightarrow 2n \in 2N$$

é evidentemente biunivoca. Ne segue che é infinito ogni insieme che contenga  $N$ ; in particolare sono infiniti  $N_0, Z, Q, R, C$ . Un altro sottoinsieme di  $N$  equipotente ad  $N$  é, per esempio, l'insieme  $\{n^2 : n \in N\}$  dei quadrati degli elementi di  $N$ .  $\diamond$

Figura 1.3: G. Cantor (1845-1918)

**ESERCIZIO 1.5.9** *Provare che  $A[x]$ , con  $A = N, N_0, Z, Q, R, C$  é un insieme infinito.*

**DEFINIZIONE 1.5.10** Un insieme equipotente ad  $N$  si dice *numerabile*, o che ha la *potenza del numerabile*.  $\diamond$

**ESEMPIO 1.5.11** Sia  $A = \{a_1, a_2, \dots, a_k\}$  un insieme finito non vuoto con  $k$  elementi. La funzione  $f : A \cup N \rightarrow N$  definita da

$$f(a_i) = i \text{ e } f(n) = k + n, \quad i = 1, 2, \dots, k, \quad n \in N$$

é biunivoca e, quindi,  $A \cup N$  é numerabile.  $\diamond$

**PROPOSIZIONE 1.5.12** *Risultano numerabili: l'insieme  $Z$  degli interi relativi, l'insieme  $Q$  dei numeri razionali e tutti i sottoinsiemi infiniti di un insieme numerabile.*

**PROPOSIZIONE 1.5.13** *L'insieme  $R$  dei numeri reali é equipotente all'insieme  $P(N)$  delle parti di  $N$  e, quindi,  $N$  ha cardinalitá minore di quella di  $R$ . In particolare,  $R$  non é numerabile.*

**DEFINIZIONE 1.5.14** Un insieme equipotente ad  $R$ , e quindi a  $P(N)$ , si dice *continuo*, o che ha la *potenza del continuo*.  $\diamond$

**ESERCIZIO 1.5.15** *Provare che l'insieme  $C$  dei numeri complessi ha la potenza del continuo.*

## 1.6 Coefficienti binomiali

Ricordiamo che il *fattoriale* di un intero non negativo  $n$ , che si denota con  $n!$ , é definito per induzione dalle seguenti posizioni:

$$0! := 1 \text{ e } n! := (n-1)!n = 1 \cdot 2 \cdots (n-1) \cdot n, \text{ per ogni } n > 0.$$

Figura 1.4: I.Newton (1643-1727)

**ESERCIZIO 1.6.1** Siano  $n$  un intero positivo e  $A, B$  due insiemi finiti d'ordine  $n$ . Provare che il numero delle funzioni biunivoche di  $A$  su  $B$  é  $n!$ .

**ESERCIZIO 1.6.2** Siano  $n, h$  interi positivi e  $A, B$  due insiemi finiti d'ordine rispettivamente  $h$  e  $n$ . Provare che il numero delle funzioni di  $A$  in  $B$  é  $n^h$ . Provare inoltre che, nel caso  $n \geq h$ , il numero delle funzioni iniettive di  $A$  in  $B$  é

$$n(n-1)(n-2) \cdots (n-h+1).$$

Questo numero si chiama *fattoriale decrescente di  $n$  di indice  $h$*  e si denota con  $(n)_h$ .

**DEFINIZIONE 1.6.3** Siano  $S$  un insieme finito d'ordine  $n$  e  $h$  un intero non negativo. Il numero dei sottoinsiemi di  $S$  d'ordine  $h$  si denota con

$$\binom{n}{h}$$

e si chiama *coefficiente binomiale*. ◇

**ESERCIZIO 1.6.4** Provare che, per ogni intero non negativo  $n$ , risulta

$$\binom{n}{0} = 1; \quad \binom{n}{1} = n; \quad \binom{n}{n} = 1; \quad \binom{n}{h} = 0, \quad h > n;$$

e

$$\binom{n}{h} = \frac{n!}{h!(n-h)!} = \frac{n(n-1) \cdots (n-h+1)}{h!}, \quad 0 \leq h \leq n.$$

Figura 1.5: B.Pascal (1500-1557)

**ESERCIZIO 1.6.5** *Provare che, per ogni intero non negativo  $n$  e per ogni intero  $h$  tale che  $0 \leq h \leq n$ , risulta*

$$\binom{n}{h} = \binom{n}{n-h}$$

e

$$\binom{n+1}{h} = \binom{n}{h} + \binom{n}{h-1}.$$

**ESERCIZIO 1.6.6** *Provare che, per ogni intero non negativo  $n$  e per ogni  $a, b \in A$ ,  $A = Z, Q, R, C$ , risulta*

$$(a+b)^n = \sum_{h=0}^n \binom{n}{h} a^{n-h} b^h \quad (\text{formula di Newton del binomio}).$$

**ESERCIZIO 1.6.7** *Provare per induzione che, se un insieme finito  $S$  ha ordine  $n$ , allora l'insieme  $P(S)$  delle parti di  $S$  é finito ed ha ordine  $2^n$ . Dedurne che*

$$\sum_{h=0}^n \binom{n}{h} = 2^n.$$

La seconda relazione dell'esercizio 1.6.5 mostra che, se si considera la tabella infinita  $T$  avente come riga  $(n+1)$ -esima

$$\binom{n}{0} \quad \binom{n}{1} \quad \cdots \quad \binom{n}{n-1} \quad \binom{n}{n},$$

allora ogni elemento di  $T$  non appartenente alla prima colonna e alla prima riga é somma dell'elemento scritto immediatamente sopra<sup>8</sup> e di quello a sinistra di quest'ultimo. La tabella  $T$

<sup>8</sup>Quando sopra un elemento non troviamo alcun numero sottintendiamo che ci sia scritto zero.



**DEFINIZIONE 1.7.3** Siano  $n, k$  interi con  $n > 0$  e  $k \geq 0$ . Il numero delle partizioni di un insieme finito d'ordine  $n$  in esattamente  $k$  blocchi si denota con  $S(n, k)$  e si chiama *numero di Stirling di secondo tipo (di indici  $n$  e  $k$ )*.  $\diamond$

**PROPOSIZIONE 1.7.4** I numeri di Stirling  $S(n, k)$  verificano la relazione di ricorrenza

$$S(n, k) = S(n - 1, k - 1) + kS(n - 1, k), \quad 2 \leq k \leq n - 1, \quad (1.2)$$

con le condizioni

$$S(n, 1) = S(n, n) = 1; \quad S(n, k) = 0, \quad k > n. \quad (1.3)$$

**DIMOSTRAZIONE.** Sia  $S$  un insieme finito d'ordine  $n$ . E' chiaro che l'unica partizione  $\pi$  di  $S$  con un solo blocco é  $\pi = \{S\}$  e l'unica con  $n$  blocchi é quella formata dai singleton degli elementi<sup>9</sup> di  $S$ . Questo prova che  $S(n, 1) = S(n, n) = 1$ . Inoltre, poiché il numero di blocchi di una partizione di  $S$  non supera  $n$ , abbiamo  $S(n, k) = 0$  per ogni  $k > n$ .

Supponiamo dunque  $n - 1 \geq k \geq 2$  e, detto  $a$  un elemento di  $S$ , poniamo  $X = S \setminus \{a\}$ . Allora una partizione di  $S$  in  $k$  blocchi si ottiene in uno, e uno soltanto, dei seguenti modi:

- aggiungendo il blocco formato dal singleton di  $a$  ad una partizione in  $k - 1$  blocchi di  $X$ ,
- aggiungendo l'elemento  $a$  ad uno dei blocchi di una partizione in  $k$  blocchi di  $X$ .

Poiché la prima operazione può essere fatta in un solo modo e la seconda in  $k$  modi distinti, resta provata la nostra relazione di ricorrenza.  $\diamond$

**OSSERVAZIONE 1.7.5** Prescindendo dal loro significato combinatorio, i numeri di Stirling possono definirsi per ricorrenza mediante le condizioni iniziali (1.3) e la formula di ricorrenza (1.2).  $\diamond$

La relazione (1.2) mostra che, se si considera la tabella infinita  $\Sigma$  (*triangolo di Stirling*) avente come riga  $n$ -esima

$$S(n, 1) \quad S(n, 2) \quad \cdots \quad S(n - 1, n) \quad S(n, n),$$

allora ogni elemento di  $\Sigma$  non appartenente alla prima colonna e alla prima riga e appartenente alla  $k$ -esima colonna é somma di  $k$  volte l'elemento scritto immediatamente sopra<sup>10</sup> e di quello che si trova a sinistra di quest'ultimo. Le prime sette righe di tale tabella sono date da

1						
1	1					
1	3	1				
1	7	6	1			
1	15	25	10	1		
1	31	90	65	15	1	
1	63	301	350	140	21	1

<sup>9</sup>Il *singleton* di un elemento  $a \in S$  é il sottoinsieme  $\{a\}$  di  $S$ .

<sup>10</sup>Quando sopra un elemento non troviamo alcun numero sottointendiamo che ci sia scritto zero.

Figura 1.7: E.T.Bell (1883-1960)

**ESERCIZIO 1.7.6** *Provare che, per ogni intero  $n > 1$ , risulta*

$$S(n, 2) = 2^{n-1} - 1, \quad S(n, n-1) = \binom{n}{2}$$

e

$$S(n, k) = \sum_{m=0}^{n-1} \binom{n-1}{m} S(m, k-1).$$

**DEFINIZIONE 1.7.7** Sia  $n$  un intero positivo. Il numero di tutte le partizioni di un insieme finito d'ordine  $n$  si denota con  $B(n)$  e si chiama *numero di Bell*.  $\diamond$

**ESERCIZIO 1.7.8** *Provare che, per ogni intero positivo  $n$ , risulta*

$$B(n) = \sum_{k=1}^n S(n, k).$$

## 1.8 Numeri di Fibonacci e rapporto aureo

**DEFINIZIONE 1.8.1** Si chiamano *numeri di Fibonacci*, e si denotano con  $F_n$ , gli interi della successione  $\{F_n, n \geq 0\}$  (detta *di Fibonacci*) definiti dalla relazione di ricorrenza

$$F_n = F_{n-1} + F_{n-2}$$

e dalle condizioni iniziali

$$F_0 = 0, \quad F_1 = 1.$$

$\diamond$

I primi dodici elementi della successione di Fibonacci sono:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89.$$

**PROPOSIZIONE 1.8.2 (identità di Cassini)** Per ogni intero positivo  $n$ , risulta

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

**DIMOSTRAZIONE.** Essendo l'asserto vero per  $n = 1$ , possiamo procedere per induzione su  $n$  e, a tale scopo, supponiamo  $n > 1$  e l'asserto vero per  $n - 1$ . Abbiamo dunque

$$F_n F_{n-2} - F_{n-1}^2 = (-1)^{n-1}, \quad F_{n-2} = F_n - F_{n-1}$$

e sostituendo nella prima uguaglianza il valore di  $F_{n-2}$ , otteniamo

$$F_n(F_n - F_{n-1}) - F_{n-1}^2 = (-1)^{n-1},$$

da cui

$$F_n^2 - F_{n-1}(F_n + F_{n-1}) = (-1)^{n-1}.$$

Se nell'ultima relazione poniamo  $F_n + F_{n-1} = F_{n+1}$ , abbiamo l'uguaglianza

$$F_n^2 - F_{n+1}F_{n-1} = (-1)^{n-1}$$

che, moltiplicata per  $-1$ , dá

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n,$$

come volevamo dimostrare. ◇

Figura 1.8: G.D.Cassini(1625-1712)

Usando l'identità di Cassini é possibile trovare una formula esplicita (*forma chiusa*) per il numero Fibonacci  $F_n$ . Vale infatti il seguente teorema, di cui omettiamo la dimostrazione.

**PROPOSIZIONE 1.8.3** Per ogni intero non negativo  $n$ , risulta

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right].$$

**OSSERVAZIONE 1.8.4** Il numero

$$\left(\frac{1 + \sqrt{5}}{2}\right),$$

che compare nella relazione precedente, prende il nome di *rapporto aureo* (nel rinascimento veniva chiamato *divina proportione*) e rappresenta il rapporto tra le lunghezze  $a, b$  di due segmenti per cui risulta

$$\frac{a}{b} = \frac{a+b}{a}.$$

Il Lettore ricorderá dalla geometria elementare che il rapporto aureo é esattamente il rapporto tra la misura di un qualsiasi segmento  $AB$  e quella della sua *sezione aurea* (cioé il segmento  $AC$  medio proporzionale tra  $AB$  e  $BC$ , che risulta di misura pari a  $\frac{1}{2}(-1 + \sqrt{5})\overline{AB}$ ).  $\diamond$

**ESERCIZIO 1.8.5** *Provare che nella figura 1.9, costruita a partire dal segmento  $AB$  di lunghezza  $a$  e dal suo punto medio  $M$ , la lunghezza  $b$  del segmento  $BC$  é tale che  $a/b$  sia il rapporto aureo.*

Figura 1.9: Sezione aurea

**OSSERVAZIONE 1.8.6** I numeri  $F_n$  prendono il nome dal matematico *Leonardo Pisano Fibonacci*, che li introdusse (probabilmente) per primo allo scopo di risolvere il seguente problema: *quante coppie di conigli nasceranno in un anno se a gennaio abbiamo una coppia appena nata che ogni mese dá alla luce una nuova coppia e ogni coppia é produttiva dopo due mesi dalla nascita?* Non dovrebbe essere difficile rendersi conto che dopo  $n$  mesi ci saranno esattamente  $F_{n+1}$  coppie. Sorprendentemente questi numeri intervengono in molti fenomeni naturali e numerose questioni statistiche.  $\diamond$

## 1.9 Esercizi

**1.9.1** Siano  $A, B, C$  insiemi. Provare le seguenti proprietá:

- $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ ;
- $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$ ;
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ ;
- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ .

Figura 1.10: L.Pisano Fibonacci (1170-1250)

**1.9.2** Siano  $A$  e  $B$  insiemi. Provare che risulta  $A \times B = B \times A$  se, e solo se,  $A = B$ .



## Capitolo 2

# Aritmetica in $\mathbb{Z}$

*La matematica é la "regina delle scienze" e la teoria dei numeri é la "regina della matematica".*  
Carl Friedrich Gauss

### 2.1 La divisione euclidea

**DEFINIZIONE 2.1.1** Dati due interi  $a$  e  $b$ , con  $b \neq 0$ , si dice che  $b$  divide  $a$  se esiste un intero  $q$  tale che  $a = bq$ . In questo caso si usa la notazione  $b \mid a$  e si dice anche che  $b$  é un *divisore* o *fattore* di  $a$ , ovvero che  $a$  é un *multiplo* di  $b$ , o ancora che  $a$  é *divisibile* per  $b$ .  $\diamond$

**OSSERVAZIONE 2.1.2** Si noti che, per definizione, 0 non divide alcun intero.  $\diamond$

**ESEMPIO 2.1.3** L'intero  $-3$  divide  $21$ , perché risulta  $21 = (-3)(-7)$ . Analogamente, abbiamo  $25 \mid 0$ , perché  $0 = 25 \cdot 0$ .  $\diamond$

Valgono le seguenti proprietà:

- Ogni intero non nullo é divisibile per se stesso (*proprietá riflessiva* della divisibilitá).
- 1 e  $-1$  sono gli unici divisori di 1,
- 0 é divisibile per ogni intero non nullo.
- $a \mid b$  e  $b \mid c \Rightarrow a \mid c$  (*proprietá transitiva* della divisibilitá).
- $a \mid b$  e  $b \mid a \Leftrightarrow a = \pm b$  (in questo caso  $a$  e  $b$  si dicono *associati*).
- Se  $c$  é un divisore di  $a$  e di  $b$ , allora  $c$  divide ogni intero del tipo  $ma + nb$ , ove  $m, n$  sono interi.

**OSSERVAZIONE 2.1.4** E' chiaro che ogni intero non nullo  $a$  é multiplo di 1,  $-1$ ,  $a$ ,  $-a$ . Per tale motivo 1,  $-1$ ,  $a$ ,  $-a$  si dicono *divisori banali* di  $a$ . Nel caso  $a \neq \pm 1$ , un divisore di  $a$  diverso da  $a$  e  $-a$  si dice *proprio*.  $\diamond$

**ESEMPIO 2.1.5** Gli interi 2, 3, 5, 7, 11 posseggono soltanto divisori banali. L'intero 15, oltre ai divisori banali, possiede quattro divisori non banali: 3,  $-3$ , 5 e  $-5$ .  $\diamond$

**ESERCIZIO 2.1.6** Due interi distinti hanno gli stessi divisori se, e solo se, sono associati.

**TEOREMA 2.1.7 (divisione euclidea)** Siano  $a, b$  interi con  $b > 0$ . Allora esiste un'unica coppia di interi  $(q, r)$  per cui risulta

$$a = bq + r \quad e \quad 0 \leq r < b. \quad (2.1)$$

**DIMOSTRAZIONE.** Cominciamo a provare la (2.1) nel caso  $a \geq 0$ , osservando che, se  $a < b$ , risulta  $(q, r) = (0, a)$ , cioè  $a = b \cdot 0 + a$ . Possiamo, quindi, supporre  $a \geq b$  e procedere per induzione su  $a$ . In queste ipotesi, essendo  $a > a - b \geq 0$ , possiamo scrivere  $a - b = bq_1 + r$ , con  $0 \leq r < b$ , da cui ricaviamo

$$a = (a - b) + b = (bq_1 + r) + b = b(q_1 + 1) + r,$$

cioè

$$a = bq + r,$$

avendo posto  $q = q_1 + 1$ .

Nel caso  $a < 0$ , risulta  $-a > 0$  e, per quanto già provato, esiste ed è unica la coppia  $(q_0, r_0)$  tale che

$$-a = bq_0 + r_0 \quad \text{con} \quad 0 \leq r_0 < b. \quad (2.2)$$

Se  $r_0 = 0$ , risulta  $a = b(-q_0)$  e la (2.1) si ottiene per  $(q, r) = (-q_0, 0)$ . Se  $r_0 > 0$ , dalla (2.2) ricaviamo

$$a = b(-q_0) - r_0 = b(-q_0 - 1) + (b - r_0)$$

e, osservato che  $0 < b - r_0 < b$ , la (2.1) si ottiene per  $(q, r) = (-q_0 - 1, b - r_0)$ .

Proviamo, ora, l'unicità della coppia  $(q, r)$ . A tale scopo, nell'ipotesi che valga la (2.1), sia  $(q', r')$  una coppia di interi per cui  $a = bq' + r'$  e  $0 \leq r' < b$  e supponiamo  $q' < q$ . Allora  $q - q' \geq 1$  e abbiamo

$$r' = a - bq' = (a - bq) + b(q - q') \geq r + b \Rightarrow r' \geq b,$$

il che è assurdo. Invertendo i ruoli di  $q$  e  $q'$  si vede che non può essere  $q < q'$ ; così abbiamo  $r = r'$  e  $q = q'$  e l'asserto è provato.  $\diamond$

**DEFINIZIONE 2.1.8** Gli interi  $q$  ed  $r$  di cui alla proposizione precedente si chiamano rispettivamente *quoziente* e *resto* della divisione di  $a$  per  $b$ .  $\diamond$

**ESEMPIO 2.1.9** Per  $a = -15$  e  $b = 2$ , risulta  $q = -8$  e  $r = 1$ .  $\diamond$

**OSSERVAZIONE 2.1.10** Notiamo che, nel corso della dimostrazione della proposizione precedente, il procedimento usato per trovare il quoziente e il resto della divisione tra  $a(> 0)$  e  $b(> 0)$  non è altro che l'usuale *algoritmo della divisione mediante sottrazioni successive*, noto al Lettore dalle scuole medie: *si sottrae ripetutamente  $b$  ad  $a$  fino ad ottenere un intero  $r$  non negativo e minore di  $b$  (il numero di sottrazioni è il quoziente  $q$  ed  $r$  il resto)*.  $\diamond$

Figura 2.1: Euclide (circa 365-300 A.C.)

**DEFINIZIONE 2.1.11** La funzione  $| \cdot | : a \in \mathbb{Z} \rightarrow |a| \in \mathbb{N}_o$  definita da

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$$

si chiama *valore assoluto*. L'intero  $|a|$  si chiama *valore assoluto di  $a$* . ◇

Il teorema che segue é una semplice generalizzazione del precedente.

**TEOREMA 2.1.12 (divisione euclidea in  $\mathbb{Z}$ )** Siano  $a, b$  interi con  $b \neq 0$ . Allora esiste un'unica coppia di interi  $(q, r)$  per cui risulta  $a = bq + r$  e  $0 \leq r < |b|$ .

**COROLLARIO 2.1.13** Siano  $a, b$  due interi con  $b \neq 0$ . Allora  $b$  divide  $a$  se, e solo se, é zero il resto della divisione di  $a$  per  $b$ .

## 2.2 Sistemi di numerazione

Sia  $a \geq 2$  un fissato intero e consideriamo un arbitrario intero  $n > 0$ . Applicando ripetutamente la divisione euclidea, possiamo scrivere in un unico modo:

$$\begin{aligned} n &= aq_0 + r_0, \\ q_0 &= aq_1 + r_1, \\ q_1 &= aq_2 + r_2, \\ &\dots \\ q_{m-2} &= aq_{m-1} + r_{m-1}, \\ q_{m-1} &= aq_m + r_m, \quad q_m = 0, \end{aligned} \tag{2.3}$$

ove gli  $r_j$  sono interi non negativi minori di  $a$ .

**OSSERVAZIONE 2.2.1** Eliminando i quozienti  $q_j$  dalle precedenti relazioni (2.3), otteniamo

$$n = aq_0 + r_0 = a(aq_1 + r_1) + r_0 =$$

$$\begin{aligned}
&= a^2 q_1 + r_1 a + r_0 = a^2(aq_2 + r_2) + r_1 a + r_0 = \dots \\
&= r_m a^m + r_{m-1} a^{m-1} + \dots + r_2 a^2 + r_1 a + r_0.
\end{aligned}$$

e la funzione

$$\nu_a : n \rightarrow (r_m, r_{m-1}, \dots, r_1, r_0)$$

tra  $N$  e le successioni finite e non nulle di interi non negativi minori di  $a$  é biunivoca.  $\diamond$

**DEFINIZIONE 2.2.2** Sia

$$n = r_m a^m + r_{m-1} a^{m-1} + \dots + r_2 a^2 + r_1 a + r_0, \quad \text{con } 0 \leq r_j < a. \quad (2.4)$$

La scrittura

$$(r_m r_{m-1} \dots r_2 r_1 r_0)_a$$

prende il nome di *rappresentazione in base  $a$  dell'intero  $n$* . Quando la base  $a$  della rappresentazione dell'intero  $n$  é chiara dal contesto, si usa scrivere

$$r_m r_{m-1} \dots r_2 r_1 r_0,$$

invece di  $(r_m r_{m-1} \dots r_2 r_1 r_0)_a$ .  $\diamond$

**OSSERVAZIONE 2.2.3** La definizione precedente, naturalmente, presuppone che si sia fissato un insieme di  $a$  simboli, detti *cifre*, per rappresentare tutti gli interi maggiori o uguali a zero e minori di  $a$ . A volte, specialmente in teoria dell'informazione, per le cifre si usa il termine inglese *digit*. Nel caso  $a = 2$  le cifre vengono chiamate anche *bit*.  $\diamond$

**DEFINIZIONE 2.2.4** La funzione che ad ogni intero positivo associa la successione delle cifre che lo rappresentano in base  $a$  si chiama *sistema di numerazione in base  $a$* .  $\diamond$

Figura 2.2: Codex Vigilanus (976 D.C.)

**OSSERVAZIONE 2.2.5** Di solito in un sistema di numerazione lo zero si denota con 0 e l'unit  con 1. I sistemi di numerazione pi  in uso sono i seguenti:

- Il sistema in base *dieci* o *decimale*, le cui cifre sono nell'ordine: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
- Il sistema in base *due* o *binario*, le cui cifre sono nell'ordine: 0, 1.
- Il sistema in base *otto* le cui cifre sono nell'ordine: 0, 1, 2, 3, 4, 5, 6, 7.
- Il sistema in base *sedici* o *esagesimale*, le cui cifre da zero a nove sono quelle decimali e le rimanenti sono: A:=dieci, B:=undici, C:=dodici, D:=tredici, E:=quattordici, F:=quindici.

I sistemi di numerazione che abbiamo introdotto si chiamano *posizionali*: il valore da attribuire ad una cifra che compare nella rappresentazione di un numero non dipende solo dalla cifra ma anche dalla sua posizione. Le origini del sistema di numerazione decimale non sono del tutto chiare;   molto probabile che fu ideato dagli indiani, forse nel VI secolo D.C., e successivamente trasmesso agli arabi. Tra coloro che maggiormente contribuirono a diffondere in Europa questo sistema di numerazione attorno al XIII secolo vi fu Leonardo Pisano Fibonacci (1170-1250), che con il suo "*Liber Abaci*" (1228) present  il sistema posizionale e le conseguenti regole di calcolo, evidenziando i notevoli vantaggi del nuovo metodo.

Il pi  antico testo europeo contenente le cifre decimali, tranne lo zero, risale al 976 D.C. e si trova nel "*Codex Vigilanus*" (vedi fig. 2.2).  

**ESEMPIO 2.2.6**  $(109)_{dieci} = (1101101)_{due} = (6D)_{sedici}$ .  

**ESEMPIO 2.2.7**  $a = (10)_a$ , per ogni intero  $a > 1$ .  

## 2.3 Massimo comune divisore e algoritmo di Euclide

Assegnati due interi  $a$  e  $b$ , un loro *divisore comune*   un intero  $c$  che divide sia  $a$  che  $b$ .

**ESEMPIO 2.3.1** I divisori comuni di 12 e 18 sono:  $\pm 1, \pm 2, \pm 3, \pm 6$ .  

**DEFINIZIONE 2.3.2** Un intero  $d$  si dice *massimo comune divisore* di due assegnati interi  $a$  e  $b$  se  $d$    un divisore comune di  $a$  e  $b$  e se ogni divisore comune di  $a$  e  $b$    anche un divisore di  $d$ .  

**OSSERVAZIONE 2.3.3** Se  $a$  e  $b$  hanno un massimo comune divisore  $d$ , allora ne hanno esattamente due:  $d$  e  $-d$ .  

**ESEMPIO 2.3.4** I massimi comuni divisori di 12 e 18 sono 6 e  $-6$ .  

**OSSERVAZIONE 2.3.5** Un massimo comune divisore di  $a$  e  $b$    anche un massimo comune divisore di  $a$  e  $-b$ .  

**OSSERVAZIONE 2.3.6** Sia  $a = bq + r$ . Allora un intero  $d$    massimo comune divisore di  $a$  e  $b$  se, e solo se,  $d$    massimo comune divisore di  $b$  ed  $r$ .  

**TEOREMA 2.3.7 (algoritmo di Euclide)** Se  $a, b$  sono interi non nulli, allora esiste un massimo comune divisore di  $a$  e  $b$ .

**DIMOSTRAZIONE.** In forza dell'osservazione 2.3.5 non é restrittivo supporre che  $a$  e  $b$  siano positivi. Costruiamo la seguente successione di divisioni, fino ad ottenere un resto uguale a zero:

$$\begin{aligned}
 a &= bq_1 + r_1 && \text{con } 0 \leq r_1 < b, \\
 b &= r_1q_2 + r_2 && \text{con } 0 \leq r_2 < r_1, \\
 r_1 &= r_2q_3 + r_3 && \text{con } 0 \leq r_3 < r_2, \\
 r_2 &= r_3q_3 + r_4 && \text{con } 0 \leq r_{k-2} < r_{k-3}, \\
 &\dots && \\
 r_{k-4} &= r_{k-3}q_{k-2} + r_{k-2} && \text{con } 0 \leq r_4 < r_3, \\
 r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} && \text{con } 0 \leq r_{k-1} < r_{k-2}, \\
 r_{k-2} &= r_{k-1}q_k + r_k && \text{con } r_k = 0.
 \end{aligned} \tag{2.5}$$

Allora, in forza dell'osservazione 2.3.6, abbiamo che  $r_{k-1}$  é un massimo comune divisore di  $a$  e  $b$ .  $\diamond$

**OSSERVAZIONE 2.3.8** Si noti che il procedimento riportato nella (2.5) é un vero e proprio algoritmo (detto anche *delle divisioni successive*) per il calcolo di un massimo comune divisore di  $a$  e  $b$ : *il massimo comune divisore cercato é l'ultimo resto non nullo nella successione di divisioni (2.5)*. Tale algoritmo é stato descritto per la prima volta duemilatrecento anni fa da *Euclide* nei suoi "Elementi" e, ancora oggi, é il piú efficiente che si conosca.  $\diamond$

**ESEMPIO 2.3.9** Vediamo come lavora l'algoritmo (2.5) nel caso  $a = 306$  e  $b = 135$ :

$$\begin{aligned}
 306 &= 135 \cdot 2 + 36 && \text{con } 0 \leq 36 < 135, \\
 135 &= 36 \cdot 3 + 27 && \text{con } 0 \leq 27 < 36, \\
 36 &= 27 \cdot 1 + 9 && \text{con } 0 \leq 9 < 27, \\
 27 &= 9 \cdot 3 + 0.
 \end{aligned}$$

L'ultimo resto non nullo é 9, che quindi é un massimo comune divisore di 306 e 135.  $\diamond$

**TEOREMA 2.3.10 (identità di Bézout)** *Siano  $a, b$  interi non nulli e  $d$  un loro massimo comune divisore. Allora  $d$  si puó scrivere come combinazione lineare di  $a$  e  $b$  a coefficienti in  $Z$ , esistono cioè due interi  $m, n$  tali che*

$$d = ma + nb. \tag{2.6}$$

**DIMOSTRAZIONE.** Partendo dalla prima delle uguaglianze (2.5) e andando verso le successive, abbiamo

$$\begin{aligned}
 r_1 &= a - bq_1, \\
 r_2 &= b - r_1q_2 = (-q_2)a + (1 + q_1q_2)b \\
 r_3 &= r_1 - r_2q_3 = (1 + q_2q_3)a + [-q_1 - (1 + q_1q_2)q_3]b
 \end{aligned}$$

e, cosí continuando, abbiamo che ogni  $r_j$  é combinazione lineare a coefficienti in  $Z$  di  $a$  e  $b$ . In particolare questa proprietá sará vera per  $r_{k-1}$  e, essendo  $d = \pm r_{k-1}$ , l'asserto é completamente provato.  $\diamond$

**ESEMPIO 2.3.11** Applichiamo il procedimento del teorema precedente all'esempio 2.3.9, ove  $a = 306$ ,  $b = 135$  e  $d = 9$ . Abbiamo:

$$36 = 306 - 2 \cdot 135,$$

$$27 = 135 - 3 \cdot 36 = 135 - 3(306 - 2 \cdot 135) = -3 \cdot 306 + 7 \cdot 135,$$

$$9 = 36 - 27 = (306 - 2 \cdot 135) + (-3 \cdot 306 + 7 \cdot 135) = 4 \cdot 306 - 9 \cdot 135.$$

Gli interi cercati sono, dunque,  $m = 4$  e  $n = -9$ .  $\diamond$

**ESERCIZIO 2.3.12** *Provare che due interi non nulli  $a, b$  hanno un unico massimo comune divisore positivo (che si denota con  $MCD(a, b)$  o con  $(a, b)$ ).*

**ESERCIZIO 2.3.13** *Sia  $d = \pm MCD(a, b)$  e supponiamo  $a = da_1$  e  $b = db_1$ . Provare che risulta  $MCD(a_1, b_1) = 1$  (in questo caso  $a_1$  e  $b_1$  si dicono primi tra loro o coprimi).*

**ESERCIZIO 2.3.14** *Provare che due interi  $a, b$  sono coprimi se, e solo se, esistono  $m, n \in \mathbb{Z}$  tali che  $ma + nb = 1$ .*

**ESERCIZIO 2.3.15** *Siano  $a$  e  $b$  coprimi e  $a$  divida  $bc$ . Provare che  $a$  divide  $c$ .*

**PROPOSIZIONE 2.3.16** *Provare che, se  $a, b, c$  sono interi con  $a, b \neq 0$ , l'equazione*

$$ax + by = c \tag{2.7}$$

*ha soluzioni intere se, e solo se,  $c$  é un multiplo di un massimo comune divisore  $d$  di  $a$  e  $b$ .*

**DIMOSTRAZIONE.** Se  $(\bar{x}, \bar{y})$  é una soluzione intera della (2.7),  $d$  divide  $a\bar{x} + b\bar{y} = c$ , perché  $d$  divide sia  $a$  che  $b$ . Viceversa, se  $c = kd$ , con  $k \in \mathbb{Z}$ , e  $d = ma + nb$  (cfr.(2.6)), risulta

$$c = kd = k(ma + nb) = a(km) + b(kn)$$

e  $(\bar{x}, \bar{y}) = (km, kn)$  é una soluzione intera della (2.7).  $\diamond$

**PROPOSIZIONE 2.3.17** *Nell'ipotesi che l'equazione (2.7) abbia una soluzione intera  $(h, k)$ , sia  $d$  un massimo comune divisore di  $a$  e  $b$  e sia  $a = da_1$ ,  $b = db_1$ . Allora le soluzioni intere della (2.7) sono tutte e sole quelle del tipo*

$$(h + nb_1, k - na_1), \quad n \in \mathbb{Z}. \tag{2.8}$$

**DIMOSTRAZIONE.** É immediato verificare che una coppia del tipo (2.8) é una soluzione intera della (2.7). Supponiamo, dunque, che  $(\bar{x}, \bar{y})$  sia una soluzione intera della (2.7) e osserviamo che, in queste ipotesi, si ha:

$$a(\bar{x} - h) = b(k - \bar{y}) \Rightarrow a_1(\bar{x} - h) = b_1(k - \bar{y})$$

e, poiché  $a_1$  e  $b_1$  sono coprimi, abbiamo che  $a_1$  divide  $k - \bar{y}$  e  $b_1$  divide  $\bar{x} - h$ . Ne segue che esiste un intero  $n$  per cui  $(\bar{x}, \bar{y}) = (h + nb_1, k - na_1)$  e l'asserto é completamente provato.  $\diamond$

**DEFINIZIONE 2.3.18** Un intero  $m$  si dice *minimo comune multiplo* di due assegnati interi non nulli  $a$  e  $b$  se  $a$  e  $b$  dividono  $m$  e se ogni multiplo di  $a$  e  $b$  é anche un multiplo di  $m$ .  $\diamond$

**ESERCIZIO 2.3.19** *Sia  $d = MCD(a, b)$  e  $ab = dm$ . Provare che  $m$  é un minimo comune multiplo di  $a, b$ .*

**ESERCIZIO 2.3.20** Se  $a$  e  $b$  sono coprimi, provare che  $ab$  é un minimo comune multiplo di  $a$  e  $b$ .

**ESERCIZIO 2.3.21** Provare che due interi non nulli  $a, b$  hanno esattamente due minimi comuni multipli, che sono l'uno l'opposto dell'altro (l'unico minimo comune multiplo positivo di  $a, b$  si denota con  $\text{mcm}(a, b)$ ).

**ESERCIZIO 2.3.22** Estendere le definizioni di minimo comune multiplo e di massimo comune divisore al caso di piú di due interi.

## 2.4 Il teorema fondamentale dell'aritmetica

*I cosiddetti pitagorici avendo cominciato ad occuparsi di ricerche matematiche ed essendo grandemente progrediti in esse, furono condotti da questi loro studi ad assumere come principi di tutte le cose esistenti quelli di cui fanno uso le scienze matematiche. E poiché i primi che qui s'incontrano sono, per natura, i numeri, sembró loro di ravvisare in questi, molte piú analogie con ciò che esiste e avviene nel mondo, di quante se ne possono trovare nel fuoco, nella terra e nell'acqua [...]. Avendo poi riconosciuto che le proprietà e le relazioni delle armonie musicali corrispondono a rapporti numerici, e che in altri fenomeni naturali si riscontrano analoghe corrispondenze coi numeri furono tanto piú indotti ad ammettere che i numeri siano gli elementi di tutte le cose esistenti e che tutto il cielo sia proporzione ed armonia.*

*Aristotele (Metaphysica, I, 5)*

In questo paragrafo faremo vedere che ogni intero diverso da zero si può scrivere, in modo essenzialmente unico, come prodotto di numeri speciali, i *numeri primi*, che fra poco definiremo.

**DEFINIZIONE 2.4.1** Un elemento  $u \in Z$  si dice *invertibile* se esiste un intero  $u'$  tale che  $uu' = 1$ . ◇

**ESERCIZIO 2.4.2** Provare che gli unici elementi invertibili di  $Z$  sono  $1$  e  $-1$ .

**DEFINIZIONE 2.4.3** Un elemento  $a \in Z$  si dice *irriducibile* se é diverso da  $0, 1, -1$  e i suoi unici divisori sono quelli banali, cioè  $1, -1, a, -a$ . ◇

**ESERCIZIO 2.4.4** Provare che un intero  $a$ , diverso da  $0, 1, -1$ , é irriducibile se, ogni qualvolta  $a$  si scrive come prodotto  $a = bc$  con  $b, c \in Z$ , allora uno tra  $b$  e  $c$  é invertibile; cioè  $b = \pm 1$  e  $c = \pm a$ , oppure  $b = \pm a$  e  $c = \pm 1$ .

**DEFINIZIONE 2.4.5** Un elemento  $p \in Z$  si dice *primo* se é diverso da  $0, 1, -1$  e se ogni qualvolta divide un prodotto  $ab$ , con  $a, b \in Z$ , allora divide uno almeno dei fattori. ◇

**ESERCIZIO 2.4.6** Provare che un intero  $a$  é irriducibile (risp. primo) se, e solo se,  $-a$  é irriducibile (risp. primo).

**PROPOSIZIONE 2.4.7** *Un numero intero é primo se, e soltanto se, é irriducibile.*

**DIMOSTRAZIONE.** Sia  $p$  un primo e supponiamo  $p = ab$ . Poiché  $p|ab$ , abbiamo che  $p|a$  o  $p|b$ , cioè  $a = ph$  o  $b = pk$ , con  $h, k \in \mathbb{Z}$ . Ne segue che  $p = phb$  o  $p = pak$ , cioè  $hb = 1$  o  $ak = 1$  e quindi uno tra  $a$  e  $b$  é invertibile. Abbiamo cosí che  $p$  é irriducibile.

Sia ora  $p$  un irriducibile e supponiamo  $p|ab$ . Posto  $ph = ab$ , supponiamo per esempio che  $p$  non divida  $a$ . In queste ipotesi é  $MCD(a, p) = 1$  ed esistono due interi  $m, n$  tali che  $ma + np = 1$ . Allora risulta  $mab + npb = b$  e, dividendo  $p$  il primo membro di questa uguaglianza, deve dividere  $b$ . Abbiamo cosí che  $p$  é primo.  $\diamond$

**ESERCIZIO 2.4.8** *Sia  $p$  un primo che divide il prodotto  $a_1 a_2 \cdots a_k$ . Allora  $p$  divide almeno uno dei fattori  $a_1, a_2, \dots, a_k$ .*

L'importanza dei numeri primi in aritmetica risiede nella validità del seguente teorema.

**TEOREMA 2.4.9 (teorema fondamentale dell'aritmetica)** *Ogni intero  $n \geq 2$  può essere fattorizzato nella forma  $n = p_1 p_2 \cdots p_k$ , ove  $p_1, p_2, \dots, p_k$  sono primi positivi (non necessariamente distinti) e tale fattorizzazione é unica, a meno dell'ordine dei fattori.*

**DIMOSTRAZIONE.** Riportiamo una dimostrazione che fa uso del principio di buon ordinamento.

- Sia  $X$  l'insieme degli interi  $n \geq 2$  che non ammettono una fattorizzazione in primi positivi. Se assumiamo  $X \neq \emptyset$ , possiamo considerare il minimo  $m$  di  $X$ .

- L'intero  $m$  non é primo (altrimenti  $m \notin X$ ) e quindi é  $m = ab$ , con  $1 < a, b < m$ . Ne segue che  $a, b \notin X$ .

- Gli interi  $a, b$ , sono fattorizzabili in primi positivi e da ciò segue che  $m$  é fattorizzabile in primi; un assurdo.

- Sia  $Y$  l'insieme degli interi  $n \geq 2$  che ammettono fattorizzazioni distinte in primi, a meno dell'ordine dei fattori. Se  $Y \neq \emptyset$ , possiamo considerare il minimo  $m$  di  $Y$  e due sue diverse fattorizzazioni del tipo desiderato  $m = p_1 p_2 \cdots p_k$  e  $m = p'_1 p'_2 \cdots p'_l$ .

- $p_1 | m = p'_1 p'_2 \cdots p'_l \Rightarrow p_1$  divide almeno uno dei  $p'_j$ .

Non é restrittivo supporre che  $p_1 | p'_1$  e da ciò segue  $p_1 = p'_1$ . Cosí abbiamo che l'intero  $\frac{m}{p_1} \geq 2$  é minore di  $m$  e possiede due distinte fattorizzazioni del tipo desiderato

$$\frac{m}{p_1} = p_2 p_3 \cdots p_k = p'_2 p'_3 \cdots p'_l,$$

un assurdo.  $\diamond$

**COROLLARIO 2.4.10** *Ogni intero  $n \geq 2$  può essere scritto nella forma*

$$n = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k},$$

*ove  $p_1, p_2, \dots, p_k$  sono primi positivi distinti e tale scrittura é unica, a meno dell'ordine dei fattori.*

**COROLLARIO 2.4.11** Siano  $a, b > 1$  due interi e

$$a = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}, \quad b = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

loro fattorizzazioni in primi distinti con  $h_i \geq 0$  e  $k_i \geq 0$ , per ogni  $i = 1, 2, \dots, s$ . Allora risulta

$$MCD(a, b) = p_1^{\min(h_1, k_1)} p_2^{\min(h_2, k_2)} \cdots p_s^{\min(h_s, k_s)}$$

e

$$mcm(a, b) = p_1^{\max(h_1, k_1)} p_2^{\max(h_2, k_2)} \cdots p_s^{\max(h_s, k_s)}.$$

**COROLLARIO 2.4.12** Sia  $m$  un intero tale che  $|m| \geq 2$ . Allora  $m$  possiede una fattorizzazione in primi. Inoltre, se

$$m = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

con  $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$  primi, allora si ha  $k = l$  ed esiste una permutazione  $\sigma$  di  $\{1, 2, \dots, k\}$  tale che  $p_j = \pm q_{\sigma(j)}$ , per ogni  $j = 1, 2, \dots, k$ .

**OSSERVAZIONE 2.4.13** E' da notare che se 1 e  $-1$  fossero considerati primi, il teorema fondamentale dell'aritmetica sarebbe falso.  $\diamond$

**OSSERVAZIONE 2.4.14** Il teorema fondamentale dell'aritmetica assicura che la conoscenza dell'insieme di tutti i numeri primi permette di costruire, mediante la moltiplicazione, tutti gli altri interi. E', inoltre, intuibile che le proprietà algebriche di un intero  $n$  dipendono dai primi che compaiono nella sua fattorizzazione in primi. Molti autori, usando un'allegoria estremamente calzante, paragonano ogni primo ad un *tipo di mattone* e gli interi alle *case* che possono costruirsi con questi mattoni. Purtroppo lo studio dei numeri primi, che é uno dei capitoli fondamentali della *teoria dei numeri*, presenta notevoli difficoltà e, ancora oggi, non si riesce a risolvere molti dei problemi ad essi relativi. E' questo uno dei motivi per cui l'aritmetica riveste un ruolo centrale nella crittografia moderna. L'efficienza di molti sistemi crittografici, infatti, dipende dalla possibilità di trovare facilmente numeri primi "molto grandi" e dalla difficoltà di decomporre in fattori primi gli interi "molto grandi".  $\diamond$

## 2.5 Alcune proprietà dei primi

*I matematici hanno finora tentato invano di scoprire qualche ordine nella successione dei numeri primi, e noi abbiamo ragione di credere che questo é un mistero nel quale la mente umana non penetrerà mai.*

*Leonhard Euler*

*(in G. Simmons, Calculus Gems, McGraw Hill Inc., 1992)*

Il teorema che segue stabilisce la non finitezza dell'insieme dei numeri primi. La sua dimostrazione, nota come "argomento di Euclide" e riportata negli "Elementi," pur nella sua semplicità, rimane per molti una delle piú belle ed eleganti di tutti i tempi.

**TEOREMA 2.5.1 (teorema di Euclide)** *L'insieme  $P$  dei numeri primi é infinito.*

**DIMOSTRAZIONE.** Si supponga che  $P = \{p_1, p_2, \dots, p_t\}$  sia finito e si ponga  $n = 1 + p_1 p_2 \cdots p_t$ . Poiché  $|n| \geq 2$ , esiste un primo  $p_i$  che divide  $n$ . Ne segue che  $p_i$  divide  $n - p_1 p_2 \cdots p_t = 1$ , un assurdo.  $\diamond$

**ESERCIZIO 2.5.2** Sia  $m$  un intero maggiore di 2. Provare che, se  $m$  non è divisibile per alcun intero  $n$  tale che  $2 \leq n \leq \sqrt{m}$ , allora  $m$  è primo.

**ESERCIZIO 2.5.3** Sia  $m$  un intero maggiore di 2. Provare che, se  $m$  non è divisibile per alcun primo positivo minore o uguale di  $\sqrt{m}$ , allora  $m$  è primo.

Figura 2.3: Eratostene (272 A.C. - 192 A.C.)

**ESERCIZIO 2.5.4** Sia  $m$  un intero maggiore di 2 e si consideri la successione  $Pr(m)$  di interi costruita con il seguente algoritmo (crivello di Eratostene):

1. scrivere la successione crescente degli interi da 2 ad  $m$ ;
2. cancellare dalla successione tutti gli interi maggiori di 2 che sono multipli di 2;
3. se nella nuova successione non vi sono interi maggiori di 2 e minori o uguali di  $\sqrt{m}$  terminare l'algoritmo (altrimenti andare al passo successivo);
4. detto  $p_1$  l'intero che compare dopo 2 nella nuova successione (chi è?), cancellare tutti gli interi maggiori di  $p_1$  che sono multipli di  $p_1$ ;
5. se nella nuova successione non vi sono interi maggiori di  $p_1$  e minori o uguali di  $\sqrt{m}$  terminare l'algoritmo (altrimenti andare al passo successivo);
6. detto  $p_2$  l'intero che compare dopo  $p_1$  nella nuova successione (chi è?), cancellare tutti gli interi maggiori di  $p_2$  che sono multipli di  $p_2$ ;
- .... continuare con la stessa regola fino a quando l'algoritmo termina ....

Provare che  $Pr(m)$  è la successione dei numeri primi che sono minori o uguali di  $m$ .

**OSSERVAZIONE 2.5.5** Uno dei problemi più interessanti che pone il teorema di Euclide è quello di studiare la distribuzione dei numeri primi nell'insieme dei numeri naturali; in altre parole, si tratta di trovare una formula per il numero  $\pi(m, n)$  dei primi  $p$  tali che  $m \leq p \leq n$ . La distribuzione molto irregolare dei primi su piccola scala non deve trarre in inganno: è possibile

provare che su grande scala questa distribuzione é abbastanza regolare. Per esempio, già nel diciottesimo secolo, ad opera di *Eulero*, si sapeva che era divergente la serie degli inversi dei numeri primi

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \dots = \sum_{n=1}^{\infty} \frac{1}{p_n}, \quad \text{con } p_n := n\text{-esimo primo positivo.}$$

Questo significa che le somme parziali

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots + \frac{1}{p_n}$$

crescono indefinitamente al crescere di  $n$ .

Osserviamo che la successione  $(\pi(n) = \pi(2, n))$  é crescente<sup>1</sup> e che il teorema di Euclide dice che

$$\lim_{n \rightarrow +\infty} \pi(n) = +\infty.$$

Un risultato interessante al riguardo é che la successione  $(\pi(n))$  tende asintoticamente all'infinito come la successione  $(n/\log n)$ , nel senso che

$$\lim_{n \rightarrow +\infty} \frac{\pi(n)}{n/\log n} = 1;$$

A tutt'oggi é aperto il problema del calcolo di una formula esplicita di  $\pi(m, n)$ . ◇

**ESERCIZIO 2.5.6** *Provare che, per ogni intero  $n > 1$ , la successione finita*

$$n! + 2, n! + 3, \dots, n! + n$$

*non contiene numeri primi. Dedurre che, per ogni intero positivo  $n$ , esistono due primi consecutivi<sup>2</sup>  $p, q$  tali che  $q - p \geq n$ .*

**ESERCIZIO 2.5.7** *Provare che, se  $n$  é un intero maggiore di 1 e  $p$  un primo positivo, allora non esiste alcun numero razionale  $y$  tale che  $y^n = p$ .*

**ESERCIZIO 2.5.8** *Provare che, se  $m, n$  sono interi positivi risulta*

$$2^{mn} - 1 = (2^m - 1)(2^{(n-1)m} + 2^{(n-2)m} + \dots + 2^n + 1).$$

*Dedurre che, se  $2^h - 1$  é un primo positivo, allora  $h$  é un primo. Trovare inoltre il piú piccolo primo positivo  $p$  tale che  $2^p - 1$  non é un primo.*

<sup>1</sup>Una successione  $(a_n)$  di interi si dice *crescente* se risulta  $a_n \leq a_{n+1}$ , per ogni  $n$ .

<sup>2</sup>Due primi  $p, q$ , con  $p < q$ , si dicono *consecutivi* se  $q$  é il piú piccolo primo maggiore di  $p$ . Nel caso  $p = 2, q = 3$  o  $q = p + 2$ , i primi  $p, q$  si dicono *gemelli*. Non é noto se l'insieme delle coppie di primi gemelli é finito o infinito. Alcune coppie di primi gemelli sono:  $(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (10.006.427, 10.006.429)$ .

Figura 2.4: M.Mersenne (1588-1648)

**OSSERVAZIONE 2.5.9** I primi della forma  $m_p = 2^p - 1$  si chiamano *primi di Mersenne*, dal nome di uno dei matematici che li studiò. E' aperto il problema di stabilire se esistono o meno infiniti primi di Mersenne. Al momento (febbraio 2002) si conoscono solo trentanove primi di Mersenne (*cf.* 2.7.2), precisamente quelli corrispondenti ai seguenti valori di  $p$ : 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917. L'ultimo di questi é il piú grande numero primo conosciuto ed é stato scoperto il 14 novembre 2001 nell'ambito di un'organizzazione amatoriale di nome *GIMPS* (The Great Internet Mersenne Prime Search), che si occupa di trovare nuovi primi di Mersenne e può essere contattata via internet attraverso il seguente indirizzo: <http://www.mersenne.org>. Su questo sito web si trovano anche molte informazioni sui numeri di Mersenne e, piú in generale, sui numeri primi di forme particolari.  $\diamond$

Figura 2.5: P. de Fermat (1601-1665)

**ESERCIZIO 2.5.10** *Provare che, se  $2^h + 1$  é primo, allora  $h$  non può avere fattori dispari, cioè deve essere una potenza di 2.*

**OSSERVAZIONE 2.5.11** I numeri della successione  $f_n = (2^{2^n} + 1)$  si chiamano *numeri di Fermat*, dal nome del matematico che li introdusse. I cinque termini iniziali della successione sono

$$f_0 = 3, f_1 = 5, f_2 = 17, f_3 = 257, f_4 = 65537$$

e risultano primi; per questo motivo lo stesso Fermat congetturó che erano primi tutti i termini della successione. Fu *L.Euler* a provare la falsitá della congettura trovando che  $f_5 = 4294976297$  si decompone nel prodotto dei due primi 641 e 6700417. Il problema di stabilire se un numero di Fermat é primo (*primo di Fermat*) é molto difficile; ancora oggi  $f_0, f_1, f_2, f_3, f_4$  sono gli unici primi di Fermat noti e non si sa se i primi di Fermat sono in numero finito o infinito. E' noto, per esempio, che i numeri da  $f_6$  a  $f_{23}$  non sono primi e  $f_{24}$  é il piú piccolo numero di Fermat per cui non si sa se é primo (*cfr.2.7.3*).  $\diamond$

## 2.6 Esercizi

**2.6.1** Siano  $a, b, c, d$  interi non negativi. Provare le seguenti implicazioni:

$$a \leq b \leq c \Rightarrow c - b \leq c - a;$$

$$a \leq b \leq c \Rightarrow b - a \leq c - a;$$

$$a \leq b \leq c \leq d \Rightarrow c - b \leq d - a.$$

**2.6.2** Usando il principio di induzione, provare le seguenti identitá, per ogni intero positivo  $n$ .

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2},$$

$$1 + 3 + 5 + \dots + (2n-1) = n^2,$$

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

$$1^3 + 2^3 + 3^3 + \dots + n^3 = \left(\frac{n(n+1)}{2}\right)^2,$$

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3},$$

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

**2.6.3** Usando il principio di induzione, provare che  $2^n - 1 > n$ , per ogni intero  $n > 1$ .

**2.6.4** Provare che, per ogni intero  $a$  e per ogni intero positivo  $n$ , risulta

$$(a^n - 1) = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1).$$

**2.6.5** Provare che un intero della forma  $4^{2n} - 1$  é divisibile per 15, per ogni intero  $n \geq 1$ .

**2.6.6** Provare che risulta

$$(1 + a)^n > 1 + na,$$

per ogni intero  $n > 1$  e per ogni numero reale  $a$ , con  $a > -1$  e  $a \neq 0$ .

**2.6.7** Otto persone compongono il consiglio di amministrazione di una azienda e tra questi devono essere eletti un presidente, un segretario ed un tesoriere. Quante sono le soluzioni possibili?

**2.6.8** Definite per ricorrenza le seguenti successioni

$$a_1 = 1; \quad a_n = a_{n-1} + 3, \quad \text{per } n \geq 2;$$

$$b_1 = 1; \quad b_n = n^2 b_{n-1}, \quad \text{per } n \geq 2;$$

trovare una formula esplicita per  $a_n$  e  $b_n$ .

**2.6.9** Provare che, per ogni due interi  $a, b$ , risulta

$$|a + b| \leq |a| + |b| \quad \text{e} \quad |ab| = |a||b|.$$

**2.6.10** Scrivere nelle basi 3, 5, 8 il numero 358.

**2.6.11** Scrivere in base 10 i numeri  $(258)_{16}$ ,  $(45)_6$ ,  $(67)_8$ .

**2.6.12** Sia  $\alpha$  una delle nove cifre decimali diverse da zero. Per ogni intero positivo  $n$ , si denoti con  $k_\alpha(n)$  il numero degli interi positivi la cui notazione decimale contiene al più  $n$  cifre e, tra queste, la cifra  $\alpha$ . Provare che risulta  $k_\alpha(1) = 1$  e, per ogni  $n > 1$ ,

$$k_\alpha(n + 1) = 9k_\alpha(n) + 10^n.$$

**2.6.13** Siano  $a, b, c$  interi e si supponga che  $a, b$  sono divisori di  $c$ . Provare, mediante qualche esempio, che  $ab$  non é necessariamente un divisore di  $c$ . Provare che, se  $a, b$  sono coprimi, allora  $ab$  é un divisore di  $c$ .

**2.6.14** Calcolare  $MCD(18, 105)$  e  $MCD(205, 65)$ .

**2.6.15** Calcolare il  $MCD(a^2, b^3)$  sapendo che  $MCD(a, b) = 9$ .

**2.6.16** Calcolare il massimo comune divisore positivo  $d$  di 140 e 250 e determinare una coppia di interi  $(a, b)$  tale che  $d = 140a + 250b$ .

**2.6.17** Provare, usando l'algoritmo di Euclide, che 365 e 3752 sono coprimi.

**2.6.18** Provare che, per ogni intero  $n > 1$ , l'intero  $n^3 + 1$  non é primo.

**2.6.19** Trovare i numeri primi maggiori di 2 e minori di 100 usando il crivello di Eratostene.

**2.6.20** Provare che, se  $a, b$  sono interi positivi, risulta  $ab = MCD(a, b) \cdot mcm(a, b)$ .

**2.6.21** Provare che  $5n + 3$  e  $7n + 4$  sono coprimi per ogni intero non negativo  $n$ .

**2.6.22** Siano  $a, b$  interi positivi coprimi. Provare che esistono due interi  $d, e$  tali che

$$\frac{1}{ab} = \frac{d}{a} + \frac{e}{b}.$$