# APPUNTI DI ARITMETICA

a cura di Paolo Francini

(versione 2.0, marzo 2010)

Per *aritmetica*, o *teoria dei numeri*, si intende lo studio dei numeri interi. Sebbene si tratti forse degli oggetti più familiari della matematica, essi offrono un gran numero di problemi difficili da risolvere e da affrontare con metodi sistematici, tanto è vero che numerosi problemi dell'aritmetica, alcuni dei quali molto famosi, sono tuttora aperti. Cercheremo di dimostrare alcuni fatti di rilievo, dai quali scaturiranno idee per affrontare -e talvolta risolvere- almeno alcuni problemi fondamentali. Così facendo, ritroveremo concetti e risultati già familiari, ma non sempre meditati con la dovuta attenzione.
Gran parte delle questioni e delle proposizioni qui descritte sono già contenute negli Elementi di Euclide, in particolare nei libri VII, VIII e IX. Il nostro lavoro potrebbe anche essere pensato come una presentazione in linguaggio attuale di quel materiale, al quale di tanto in tanto faremo qualche rimando. Una difficoltà nella lettura della parte aritmetica degli Elementi è data, rispetto alle nostre abitudini, dal fatto che l'idea di numero ($\alpha\rho\iota\vartheta\mu o\varsigma$) in Euclide è legata all'idea di molteplicità, al punto da non comprendere neppure l'unità ($\mu o\nu\alpha\varsigma$): i numeri iniziano da 2. Ciò costringe spesso a distinzioni, duplicazioni degli enunciati, o formulazioni che possono apparirci talvolta tortuose. Inoltre non si fa uso di simbolismo: l'esposizione è interamente verbale, con il solo ausilio delle figure che spesso accompagnano le dimostrazioni (rappresentando i numeri sotto forma di segmenti). Tutto ciò può rendere faticosa la lettura di Euclide. La sua eleganza resta in ogni caso cristallina.

Nelle note che seguono, il simbolo $\mathbb{Z}$ indicherà l'insieme dei numeri interi, compresi quelli negativi:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}.$$

Il simbolo $\mathbb{N}$ indicherà invece l'insieme dei numeri naturali, vale a dire gli interi non-negativi:

$$\mathbb{N} = \{0, 1, 2, 3, ...\}.$$

# 1 Divisibilità.

**Definizione 1.1** Dati $a, b \in \mathbb{Z}$ si dice che $b$ è *multiplo di* $a$ (in simboli: $a|b$) se esiste $k \in \mathbb{Z}$ tale che $a \cdot k = b$.

Si dice anche che $b$ *è divisibile per* $a$, o che $a$ *è divisore di* $b$, o che $a$ *divide* $b$. La relazione di divisibilità è cruciale in ogni aspetto della teoria dei numeri. Euclide usa l'espressione "misurare" ($\kappa\alpha\tau\alpha\mu\varepsilon\tau\rho\varepsilon\iota\nu$): $a$ *misura* $b$ significa appunto $a|b$.

**Esempio 1.1** Per esempio, si ha:

- $3|15$;
- $3 \not| 10$;
- $3|3$;
- $(-24)|0$;
- $0 \not| 4$;
- $1|(-18)$;
- $0|0$.

**Esercizio 1.1** Dimostrare la validità di tutte le relazioni elencate dell'esempio 1.1.

**Teorema 1.1** *Per ogni* $a, b, c, d \in \mathbb{Z}$ *si ha:*

- $a|a$ [riflessività]*;*
- $a|0$*;*
- $1|a$*;*
- *se* $a|b$ *e* $b|c$*, allora* $a|c$*;* [transitività (Elementi, libro VII, prop. 5)]
- *se* $a|b$ *o* $a|c$*, allora* $a|bc$*;*
- *se* $a|b$ *e* $a|c$*, allora* $a|b+c$ *e* $a|b-c$*;*
- *se* $a|b$ *e* $a'|b'$*, allora* $aa'|bb'$ *(in particolare: se* $a|b$ *allora* $ka|kb$ *e* $a^k|b^k$*, per ogni* $k$ *intero positivo);*
- *se* $k \neq 0$ *e* $ka|kb$*, allora* $a|b$.

**Esercizio 1.2** Fare un esempio per ciascuna delle proprietà elencate nel teorema 1.1.

**Esercizio 1.3** Dimostrare il teorema 1.1.

**Esercizio 1.4** È vero che, se $a|bc$, allora $a|b$ oppure $a|c$?

**Esercizio 1.5** E' possibile che si abbia $a|b$ e anche $b|a$? In quali casi?

**Esercizio 1.6** Per $a, b \in \mathbb{N}$, è vero che da $a|b$ segue $a \leqslant b$? Sotto quali ipotesi è valida l'implicazione?

**Esercizio 1.7** Per quali interi $n$ si ha $n+2|5n+24$?

Svolgimento. Osserviamo intanto che, comunque sia scelto l'intero $n$, il divisore $n+2$ e il dividendo $5n+24$ sono sempre numeri interi.
Teniamo conto che $n+2|k(n+2)$ per ogni intero $k$. Dunque, se $n$ è tale che $n+2|5n+24$, allora $n+2|5n+24+k(n+2)$, qualunque sia l'intero $k$ (vedi teorema 1.1).
Ci piacerebbe scegliere $k$ in modo che il dividendo $5n+24+k(n+2)$ si riduca ad una costante. A quel punto, si tratterebbe solo di passare in rassegna i divisori di tale costante.
Ponendo $k=-5$, il dividendo risulta appunto $5n+24-5(n+2)=14$. Pertanto se $n$ è tale che $n+2|5n+24$, allora $n+2|5n+24-5(n+2)$, ossia $n+2|14$. I divisori di 14 sono $\pm 1$, $\pm 2$, $\pm 7$, $\pm 14$. Quindi occorre che $n+2$ sia uno dei numeri $\pm 1$, $\pm 2$, $\pm 7$, $\pm 14$. Dunque $n$ deve essere uno dei numeri $-3, -1$, $-4, 0$, $-9, 5$, $-16, 12$.
Si tratta infine di verificare se tutti questi numeri forniscono soluzioni valide: quello che abbiamo scoperto finora è che, se $n$ è una soluzione, allora deve essere uno dei valori trovati: abbiamo, per così dire, ristretto il cerchio. Ma si vede facilmente che tutti i numeri trovati forniscono soluzioni valide.
Ricapitolando: i numeri interi tali che $n+2|5n+24$ sono precisamente $-3$, $-1$, $-4$, $0$, $-9$, $5$, $-16$, $12$. □

È bene riflettere con attenzione sull'esempio offerto dall'esercizio 1.7. Per quanto semplice, l'applicazione di quel metodo già ci permette di risolvere una certa quantità di equazioni diofantee [1]. Facciamo qualche altro esempio.

**Esercizio 1.8** Per quali interi $n$ si ha $2n-3|6n+11$?

**Esercizio 1.9** Per quali interi $n$ si ha $3n-2|5n+8$?

Svolgimento. Come nell'esercizio 1.7, l'idea sarebbe di aggiungere al dividendo $5n+8$ un multiplo del divisore $3n-2$, in maniera da ottenere una costante. In questo caso, però, 5 non è multiplo di 3, quindi non si riesce ad eliminare $5n$ esattamente allo stesso modo. Tuttavia possiamo osservare che, se $3n-2|5n+8$, allora $3n-2|h(5n+8)$, qualunque sia l'intero $h$. Quindi, se $3n-2|5n+8$, allora $3n-2|h(5n+8)+k(3n-2)$ per ogni coppia di interi $h, k$. Scegliendo $h=3$ e $k=-5$ si ricava allora che $3n-2|34$. Esaminando tutti i divisori di 34, come fatto nell'esercizio 1.7, si trovano quindi le possibili soluzioni intere e si procede poi a verifica. □

**Esercizio 1.10** Per quali interi $n$ si ha $3n-5|7n+9$?

[1] Per *equazione diofantea* s'intende un'equazione della quale si cercano le soluzioni intere.

**Esercizio 1.11** Per quali interi $n$ si ha $6n-4|5n+6$?

**Esercizio 1.12** Risolvere l'equazione diofantea $mn-5m-n=7$.

Svolgimento. Ecco un metodo. Mettiamo in evidenza $m$ e riscriviamo l'equazione: $m(n-5)=n+7$. Risolvere questa equazione (con $m$ e $n$ interi) equivale a trovare quali sono gli interi $n$ tali che $n-5|n+7$. A questo punto si procede come visto negli esempi precedenti, con l'accortezza che in questo caso occorre determinare anche i valori di $m$ in corrispondenza a quelli trovati per $n$. □

**Esercizio 1.13** Risolvere l'equazione diofantea $3ab+5b=11+2a$.

**Esercizio 1.14** Risolvere l'equazione diofantea $6a^2+b+7=3ab$.

Svolgimento. Conviene mettere in evidenza $b$ e scrivere l'equazione nella forma $b(3a-1)=6a^2+7$, ossia $3a-1|6a^2+7$. Anche in questo caso si deve avere $3a-1|6a^2+7+k(3a-1)$, comunque sia scelto $k$. Possiamo quindi scegliere $k=-2a$, che deve sicuramente essere intero se $a$ è intero. Da qui: $3a-1|2a+7$ e segue, come visto prima, $3a-1|3(2a+7)-2(3a-1)$, ossia $3a-1|23$. A questo punto è possibile esaminare i vari casi e poi procedere a verifica di quanto trovato. □

**Esercizio 1.15** Risolvere l'equazione diofantea $5a^2+7b+9=8ab$.

**Definizione 1.2** Dato $n\in\mathbb{N}$, il simbolo $\mathsf{div}(n)$ indicherà l'insieme dei numeri naturali che dividono $n$ (i divisori di $n$). Ossia:

$$\mathsf{div}(n)=\{a|\, a\in\mathbb{N}\wedge a|n\}.$$

Inoltre, indicheremo con $\mathsf{mult}(n)$ l'insieme dei numeri naturali divisibili per $n$ (i multipli di $n$). Ossia:

$$\mathsf{mult}(n)=\{a|\, a\in\mathbb{N}\wedge n|a\}.$$

**Esercizio 1.16** Determinare gli insiemi $\mathsf{div}(1)$, $\mathsf{div}(7)$, $\mathsf{div}(12)$, $\mathsf{div}(32)$, $\mathsf{mult}(1)$.

**Teorema 1.2** *Per ogni $n\in\mathbb{N}$ si ha che:*

- $1\in \mathit{div}(n)$ *e* $n\in \mathit{div}(n)$*;*
- $0\in \mathit{mult}(n)$ *e* $n\in \mathit{mult}(n)$.

**Teorema 1.3** *Per ogni $n\neq 0$, $\mathit{div}(n)$ è un insieme finito e $\mathit{mult}(n)$ è infinito.*

**Esercizio 1.17** Mostrare che $\mathsf{div}(0)=\mathbb{N}$ e $\mathsf{mult}(0)=\{0\}$, $\mathsf{div}(1)=\{1\}$ e $\mathsf{mult}(1)=\mathbb{N}$.

**Esercizio 1.18** Dimostrare i teoremi 1.2 e 1.3.

**Esercizio 1.19** Stabilire la validità o meno di ciascuna delle seguenti affermazioni:

- se $a \in \mathsf{div}(b)$ e $a \in \mathsf{div}(c)$, allora $a \in \mathsf{div}(b+c)$;
- se $a \in \mathsf{div}(b)$, allora $a \in \mathsf{div}(kb)$, per ogni $k \in \mathbb{N}$;
- se $a \in \mathsf{div}(n)$, allora anche $n/a \in \mathsf{div}(n)$;
- se $a \in \mathsf{mult}(n)$, allora $ka \in \mathsf{mult}(n)$, per ogni $k \in \mathbb{N}$;
- se $a \in \mathsf{mult}(b)$ e $b \in \mathsf{mult}(c)$, allora $a \in \mathsf{mult}(c)$;
- se $a \in \mathsf{mult}(n)$ e $b \in \mathsf{mult}(n)$, allora $a+b \in \mathsf{mult}(n)$ e $b-a \in \mathsf{mult}(n)$.

**Esercizio 1.20** *Dimostrare che, per ogni $a, b \in \mathbb{N}$:*

- *se $\mathit{div}(a) = \mathit{div}(b)$, allora $a = b$;*
- *se $\mathit{mult}(a) = \mathit{mult}(b)$, allora $a = b$.*

**Definizione 1.3** Per $n > 0$, si indica con $\mathsf{d}(n)$ la cardinalità di $\mathsf{div}(n)$, ossia il numero di divisori positivi di $n$.

Naturalmente, tra i divisori e tra i multipli di un intero, vi sarebbero anche dei numeri negativi, vale a dire gli opposti dei divisori e dei multipli positivi. Per una questione di comodità, riserviamo però i simboli $\mathsf{div}(n)$ e $\mathsf{mult}(n)$ per indicare i soli divisori e multipli naturali. In ogni caso, quando ci servirà considerare anche divisori o multipli negativi, non sarà un grave problema. Per esempio, sarà chiaro che il numero totale dei divisori di $n$ è $2\mathsf{d}(n)$.

**Esercizio 1.21** Determinare tutti i valori di $\mathsf{d}(n)$, per $n$ che varia da 1 a 20.

**Esercizio 1.22** Confutare o confermare queste proposizioni:

- $\mathsf{d}(n) \leqslant n$ per ogni intero positivo $n$;
- $\mathsf{d}(a \cdot b) = \mathsf{d}(a) \cdot \mathsf{d}(b)$ per ogni coppia di interi positivi $a, b$;
- se $a \leqslant b$, allora $\mathsf{d}(a) \leqslant \mathsf{d}(b)$;
- se $a|b$, allora $\mathsf{d}(a) \leqslant \mathsf{d}(b)$.

**Esercizio 1.23** Per quali $n$ si ha $\mathsf{d}(n) = n$?

**Esercizio 1.24** Dimostrare che $\mathsf{d}(n)$ è dispari se $n$ è un quadrato e $\mathsf{d}(n)$ è pari se $n$ non è un quadrato.

Suggerimento. Osservare che, se $k$ è un divisore di $n$, lo è anche $n/k$. □

**Teorema 1.4** *Siano $m, n \in \mathbb{N}$ con $m|n$. Allora:*

- *$\mathit{div}(m) \subseteq \mathit{div}(n)$;*
- *$\mathit{mult}(m) \supseteq \mathit{mult}(n)$.*

**Esercizio 1.25** Dimostrare il teorema 1.4.

## 2 La divisione con resto.

La relazione $a|b$ significa che, se si sottrae ripetutamente il numero $a$ a partire da $b$, a un certo punto si ottiene 0.

Possiamo considerare la medesima successione

$$b,\ b-a,\ b-2a,\ b-3a,\ ...,\ b-ka,\ ...$$

per una coppia qualsiasi di numeri naturali $a, b$.

Se $a = 0$, non ci si allontana mai da $b$ (caso poco interessante). Supponiamo dunque $a > 0$. La successione, essendo decrescente, non può andare avanti all'infinito rimanendo nei naturali (non può durare più di $a$ passi). L'ultimo numero naturale trovato si dice *resto* della divisione di $b$ per $a$. Indicandolo con la lettera $r$, per come esso è ricavato, si avrà $r < a$ (altrimenti...) e $a|b-r$.

Facciamo un esempio. Se $a = 7$ e $b = 31$, si ha la sequenza $31, 24, 17, 10, 3$: il resto della divisione di 31 per 7 è 3. Per quanto sopra, possiamo scrivere $31 = 7+7+7+7+3 = 7 \cdot 4 + 3$.

In generale, si conclude quanto segue:

**Teorema 2.1** *[Divisione con resto.] Dati $a, b \in \mathbb{N}$, con $a \neq 0$, esiste una coppia di numeri naturali $q, r$, con $r < a$, tali che $b = a \cdot q + r$. Tale coppia $q, r$ è inoltre unica.*

L'unicità segue subito dal fatto che $r = b - a \cdot q \in \{b,\ b-a,\ b-2a,\ b-3a,\ ...,\ b-k \cdot a,\ ...\} \cap \mathbb{N}$. In tale insieme non può esserci più di un elemento minore di $a$, ossia il suo elemento minimo $m$: già per quello immediatamente maggiore $m+a$ si avrebbe $m+a \geqslant a$. Perciò c'è un solo resto possibile $r$ e, siccome $a \cdot q = b-r$, anche $q$ è unico: è pari a $(b-r) : a$ il quoziente della divisione di $b-r$ per $a \neq 0$.

**Esercizio 2.1** Dimostrare che, nella divisione per un intero positivo $n$ dei numeri naturali $a$ e $b$, si ottengono resti uguali se e solo se $n|a-b$.

**Esercizio 2.2** Dati $a, b \in \mathbb{N}$, sia $n$ un intero positivo. Indichiamo con $\tilde{a}$ e $\tilde{b}$ i resti ottenuti nella divisione di $a$ e di $b$ per $n$. Valgono i fatti seguenti:

- sono uguali i resti nella divisione per $n$ di $a+b$ e di $\tilde{a}+\tilde{b}$;
- sono uguali i resti nella divisione per $n$ di $a \cdot b$ e di $\tilde{a} \cdot \tilde{b}$.

**Esercizio 2.3** Dati dei numeri interi $a$ e $b$, dimostrare che, se nella divisione per un intero positivo $n$ sia di $a$ che di $b$ si ottiene il resto 1, allora anche nella divisione di $a \cdot b$ per $n$ si ottiene il resto 1.

**Esercizio 2.4** Dimostrare che:

- il resto nella divisione per $4$ di un quadrato è $0$ o $1$.
- se un numero dispari $d$ è somma di due quadrati, allora $d = 4n+1$ per qualche $n \in \mathbb{N}$.

**Esercizio 2.5** Dimostrare che il resto nella divisione per $3$ di un quadrato non può essere $2$.

**Esercizio 2.6** Quali tra queste possono essere le cifre finali nella scrittura di un quadrato?

- $2$;
- $3$;
- $7$;
- $8$;
- $66$;
- $35$;
- $51$;
- $99$.

Possiamo interpretare la divisione con resto anche dal punto di vista delle frazioni. Se la divisione di $m$ per $n$ dà resto $r$, con $m = n \cdot q + r$, allora $\frac{m}{n} = q + \frac{r}{n}$: la frazione $\frac{m}{n}$ è così decomposta nella somma dell'intero $q$ e della frazione propria $\frac{r}{n}$ (dato che $r < n$).

La divisione con resto permette anche di cercare lo sviluppo decimale di $\frac{m}{n}$, dopo avere trovato la sua parte intera $q$. Infatti si può scrivere:

$$\frac{m}{n} = q + \frac{r}{n} = q + \frac{1}{10} \cdot \left(\frac{10r}{n}\right),$$

che corrisponde, nell'algoritmo della divisione, all'azione di aggiungere una cifra decimale 0 in coda al dividendo. Eseguendo la divisione con resto di $10r$ per $n$, scriviamo la frazione $\frac{10r}{n}$ come $\frac{10r}{n} = q_1 + \frac{r_1}{n}$, cosicché

$$\frac{m}{n} = q + \frac{1}{10} \cdot \left(q_1 + \frac{r_1}{n}\right) = q + \frac{q_1}{10} + \frac{1}{10} \cdot \left(\frac{r_1}{n}\right).$$

Il numero $q_1$ è la prima cifra dello sviluppo decimale di $\frac{m}{n}$. Si noti che $0 \leqslant q_1 < 10$, ossia $q_1$ è in effetti una singola cifra decimale: infatti da $r < n$ segue che $10 \cdot n > 10r$.

A questo punto, se $r_1 = 0$ abbiamo terminato, ossia $\frac{m}{n} = q + \frac{q_1}{10}$ (il numero $\frac{m}{n}$ può essere scritto con lo sviluppo finito della forma "$q, q_1$", dove $q$ è la parte intera e $q_1$ una cifra decimale).
Se invece $r_1 > 0$, possiamo proseguire come si è appena fatto:

$$\frac{m}{n} = q + \frac{q_1}{10} + \frac{1}{10} \cdot \left(\frac{r_1}{n}\right) = q + \frac{q_1}{10} + \frac{1}{100} \cdot \left(\frac{10r_1}{n}\right),$$

eseguando ancora la divisione con resto di $10r_1$ per $n$: si avrà $\frac{10r_1}{n} = q_2 + \frac{r_2}{n}$, con $r_2 < n$, e dunque

$$\frac{m}{n} = q + \frac{q_1}{10} + \frac{1}{100} \cdot \left(\frac{10r_1}{n}\right) = q + \frac{q_1}{10} + \frac{1}{100} \cdot \left(q_2 + \frac{r_2}{n}\right) = q + \frac{q_1}{10} + \frac{q_2}{100} + \frac{1}{100} \cdot \left(\frac{r_2}{n}\right).$$

L'intero $q_2 < 10$ è la seconda cifra dello sviluppo decimale di $\frac{m}{n}$.
Scrivendo $\frac{1}{100} \cdot \frac{r_2}{n} = \frac{1}{1000} \cdot \frac{10r_2}{n}$, si può proseguire ancora come sopra e trovare le ulteriori cifre dello sviluppo.
Fino a quando si va avanti? Proviamo con qualche esempio.

**Esempio 2.1**

$$\begin{aligned}
\tfrac{101}{8} &= 12 + \tfrac{5}{8} \\
&= 12 + \tfrac{1}{10} \cdot \left(\tfrac{50}{8}\right) = 12 + \tfrac{1}{10} \cdot \left(6 + \tfrac{2}{8}\right) = 12 + \tfrac{6}{10} + \tfrac{1}{10} \cdot \left(\tfrac{2}{8}\right) \\
&= 12 + \tfrac{6}{10} + \tfrac{1}{100} \cdot \left(\tfrac{20}{8}\right) = 12 + \tfrac{6}{10} + \tfrac{1}{100} \cdot \left(2 + \tfrac{4}{8}\right) = 12 + \tfrac{6}{10} + \tfrac{2}{100} + \tfrac{1}{100} \cdot \left(\tfrac{4}{8}\right) \\
&= 12 + \tfrac{6}{10} + \tfrac{2}{100} + \tfrac{1}{1000} \cdot \left(\tfrac{40}{8}\right) = 12 + \tfrac{6}{10} + \tfrac{2}{100} + \tfrac{5}{1000} \\
&= 12,625.
\end{aligned}$$

**Esempio 2.2**

$$\begin{aligned}
\tfrac{74}{11} &= 6 + \tfrac{8}{11} \\
&= 6 + \tfrac{1}{10} \cdot \left(\tfrac{80}{11}\right) = 6 + \tfrac{1}{10} \cdot \left(7 + \tfrac{3}{11}\right) = 6 + \tfrac{7}{10} + \tfrac{1}{10} \cdot \left(\tfrac{3}{11}\right) \\
&= 6 + \tfrac{7}{10} + \tfrac{1}{100} \cdot \left(\tfrac{30}{11}\right) = 6 + \tfrac{7}{10} + \tfrac{1}{100} \cdot \left(2 + \tfrac{8}{11}\right) = 6 + \tfrac{7}{10} + \tfrac{2}{100} + \tfrac{1}{100} \cdot \left(\tfrac{8}{11}\right) \\
&= 6 + \tfrac{7}{10} + \tfrac{2}{100} + \tfrac{1}{1000} \cdot \left(\tfrac{80}{11}\right) = 6 + \tfrac{7}{10} + \tfrac{2}{100} + \tfrac{1}{1000} \cdot \left(7 + \tfrac{3}{11}\right) = ... \\
&= 6,727...
\end{aligned}$$

È chiaro che, da qui in avanti si alterneranno una cifra 7 e una cifra 2: si usa la notazione $6, \overline{72}$.

In generale, due sono le possibilità:

- o ad un certo punto si trova un resto nullo, in tal caso il processo si arresta e la frazione $\frac{m}{n}$ viene scritta sotto forma di decimale con un numero finito di cifre;
- oppure potrebbe non aversi mai un resto nullo e quindi il processo non avrebbe termine.

In quest'ultimo caso, tuttavia, non sarebbe possibile avere tutti i resti $r_1, r_2, ..., r_k, ...$ sempre differenti: infatti il divisore è sempre lo stesso numero $n$ ed i possibili resti sono solo un numero finito ($n-1$, nel caso non si trovi mai 0). Pertanto, si dovrà prima o poi trovare un resto uguale ad uno già trovato in precedenza, per esempio $q_s = q_t$. Siccome $q_{s+1}$ e $q_{t+1}$ dipendono poi solo da $q_s$ e $q_t$, si avrà anche $q_{s+1} = q_{t+1}$. Dal momento in cui un resto si ripete, anche i successivi si ripeteranno nello stesso ordine all'infinito. Si ottiene perciò una situazione ciclica e si dice che lo sviluppo decimale è *periodico*.

Questo ragionamento dimostra il seguente teorema.

**Teorema 2.2** *Lo sviluppo decimale di una frazione o è finito o è infinito periodico.*

È pertanto escluso che lo sviluppo decimale di una frazione possa essere infinito e non periodico: le cifre non possono evitare di dover ripetere per sempre una qualche sequenza.

Un'importante osservazione a proposito è che l'eventualità di dare luogo a uno sviluppo finito oppure infinito periodico non deriva da carateri intrinseci delle frazioni, ma dipende dalla base del sistema di numerazione.

**Esempio 2.3** Nell'abituale sistema decimale, si ha $\frac{1}{2} = 0,5$, mentre in base 7 si avrebbe:

$$\begin{aligned}
\tfrac{1}{2} &= 0 + \tfrac{1}{2} \\
&= 0 + \tfrac{1}{10} \cdot \left(\tfrac{10}{2}\right) = 0 + \tfrac{1}{10} \cdot \left(3 + \tfrac{1}{2}\right) = 0 + \tfrac{3}{10} + \tfrac{1}{10} \cdot \tfrac{1}{2} \\
&= 0 + \tfrac{3}{10} + \tfrac{1}{100} \cdot \left(\tfrac{10}{2}\right) = 0 + \tfrac{3}{10} + \tfrac{1}{100} \cdot \left(3 + \tfrac{1}{2}\right) = 0 + \tfrac{3}{10} + \tfrac{3}{100} + \tfrac{1}{100} \cdot \tfrac{1}{2} = ... \\
&= 0,33... = 0,\overline{3}.
\end{aligned}$$

Una medesima frazione può quindi dare luogo, in una base, ad uno sviluppo finito e, in un'altra base, ad uno sviluppo infinito periodico.

**Esercizio 2.7** Dimostrare che una frazione $\frac{m}{n}$, ridotta ai minimi termini, dà luogo ad uno sviluppo decimale finito se e solo se nessun numero primo diverso da 2 e da 5 divide $n$.

**Esercizio 2.8** Come andrebbe riformulato il contenuto dell'esercizio se si utilizzasse una diversa base di numerazione $b > 1$?

**Esercizio 2.9** Da quante cifre al massimo può essere formato il periodo dello sviluppo decimale di una frazione $\frac{m}{n}$?

**Esercizio 2.10** Determinare gli sviluppi decimali delle frazioni $\frac{9}{20}$, $\frac{53}{16}$, $\frac{12}{7}$, $\frac{4}{13}$.

**Esercizio 2.11** Dimostrare che il numero $0,10110111011110111110...$ è irrazionale.

**Esercizio 2.12** Dimostrare che il numero $0,12345678910111213141516171819202 1...$ è irrazionale.

# 3 L'algoritmo euclideo.

In questa sezione ci interessiamo dei divisori e dei multipli che due numeri naturali possono avere in comune. Vale a dire, consideriamo l'insieme

$$\mathsf{div}(a) \cap \mathsf{div}(b)$$

(i divisori in comune ai due interi $a$ e $b$) e l'insieme

$$\mathsf{mult}(a) \cap \mathsf{mult}(b)$$

(i multipli in comune ai due interi $a$ e $b$). Si tratta, essenzialmente, del contenuto del libro VII degli Elementi.
Iniziamo con qualche esempio.

**Esercizio 3.1** Determinare gli insiemi:

- $\mathsf{div}(12) \cap \mathsf{div}(30)$ e $\mathsf{mult}(12) \cap \mathsf{mult}(30)$;
- $\mathsf{div}(6) \cap \mathsf{div}(24)$ e $\mathsf{mult}(6) \cap \mathsf{mult}(24)$;
- $\mathsf{div}(21) \cap \mathsf{div}(10)$ e $\mathsf{mult}(21) \cap \mathsf{mult}(10)$;
- $\mathsf{div}(1) \cap \mathsf{div}(6)$ e $\mathsf{mult}(1) \cap \mathsf{mult}(6)$;
- $\mathsf{div}(0) \cap \mathsf{div}(9)$ e $\mathsf{mult}(0) \cap \mathsf{mult}(9)$.

**Teorema 3.1** *Per ogni $m, n \in \mathbb{N}$ si ha:*

- $1 \in \mathit{div}(m) \cap \mathit{div}(n)$ *e* $0 \in \mathit{mult}(m) \cap \mathit{mult}(n)$*;*
- *se* $m|n$*, allora* $\mathit{div}(m) \cap \mathit{div}(n) = \mathit{div}(m)$ *e* $\mathit{mult}(m) \cap \mathit{mult}(n) = \mathit{mult}(n)$*;*
- $\mathit{div}(1) \cap \mathit{div}(n) = \{1\}$ *e* $\mathit{mult}(1) \cap \mathit{mult}(n) = \mathit{mult}(n)$*;*
- $\mathit{div}(0) \cap \mathit{div}(n) = \mathit{div}(n)$ *e* $\mathit{mult}(0) \cap \mathit{mult}(n) = \{0\}$.

**Esercizio 3.2** Dimostrare il teorema 3.1.

**Esercizio 3.3** Dimostrare che, per ogni $a, b \in \mathbb{N}$:

- $\mathsf{div}(a) \cap \mathsf{div}(b)$ è finito, a meno che non sia $a = 0$ e $b = 0$;
- $\mathsf{mult}(a) \cap \mathsf{mult}(b)$ è infinito, a meno che non sia $a = 0$ o $b = 0$.

**Esercizio 3.4** Dimostrare che, dati i numeri naturali $a \geqslant b$, si ha $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a-b) \cap \mathsf{div}(x) = \mathsf{div}(a+b) \cap \mathsf{div}(x)$, dove $x$ è uno qualsiasi dei numeri $a$, $b$.

**Definizione 3.1** I numeri naturali $m$ e $n$ sono detti *coprimi* -o *relativamente primi*, o anche *primi tra loro*- se $\mathsf{div}(m) \cap \mathsf{div}(n) = \{1\}$ (cioè se 1 è il solo intero positivo che li divide entrambi).

**Esercizio 3.5** Quali numeri naturali sono coprimi con 0? E con 1?

**Esercizio 3.6** Dimostrare che due numeri naturali consecutivi sono sempre coprimi.

**Esercizio 3.7** Dimostrare che, estraendo 46 numeri da un sacchetto della tombola, se ne troveranno sicuramente due coprimi.

Veniamo adesso al principale risultato di questa sezione. Già dagli esempi precedenti sarà chiaro che i divisori e i multipli in comune tra due numeri naturali formano degli insiemi particolari. Più precisamente, si può osservare che i divisori in comune a due numeri sono, a loro volta, tutti e soli i divisori di un certo numero, così come i multipli in comune a due numeri sono tutti e soli i multipli di un certo numero. Euclide dimostra questi fatti nelle proposizioni

**Teorema 3.2** *Data una coppia di numeri naturali $a$ e $b$, esistono dei numeri naturali $D$ e $m$ tali che:*

- $\mathit{div}(a) \cap \mathit{div}(b) = \mathit{div}(D)$;
- $\mathit{mult}(a) \cap \mathit{mult}(b) = \mathit{mult}(m)$.

Dimostrazione. Iniziamo da $\mathsf{div}(a) \cap \mathsf{div}(b)$. Procediamo per induzione sul massimo tra $a$ e $b$, che denotiamo con $\mathsf{max}(a,b)$.

- Se $\mathsf{max}(a,b) = 0$, allora $a = b = 0$ e si ha $\mathsf{div}(0) \cap \mathsf{div}(0) = \mathsf{div}(0) = \mathbb{N}$.
- Sia ora $\mathsf{max}(a,b) = n > 0$ e assumiamo che, per tutte le coppie di interi $a', b'$ tali che $\mathsf{max}(a',b') < n$ si abbia $\mathsf{div}(a') \cap \mathsf{div}(b') = \mathsf{div}(D)$ per qualche numero $D$. Se si avesse $a = b$, la tesi sarebbe subito verificata: in tal caso sarebbe ovviamente $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a) \cap \mathsf{div}(a) = \mathsf{div}(a)$. Supponiamo dunque di avere $a \neq b$: per esempio $a > b$ (e quindi $n = a$). Ancora, se fosse $b = 0$, si avrebbe $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a) \cap \mathsf{div}(0) = \mathsf{div}(a)$ (vedi anche il teorema 3.1. Supponiamo dunque che sia $a > b > 0$ e consideriamo $\mathsf{div}(a-b) \cap \mathsf{div}(b)$. Intanto, si è appena visto nell'esercizio 3.4 che $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a-b) \cap \mathsf{div}(b)$. Inoltre, si vede subito che $\mathsf{max}(a-b, b) < n$: infatti si ha $b < a = n$ e $a - b < a = n$ dato che $b > 0$. Per l'ipotesi induttiva, esiste pertanto un numero naturale $D$ tale che $\mathsf{div}(a-b) \cap \mathsf{div}(b) = \mathsf{div}(D)$. Ma, visto che $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a-b) \cap \mathsf{div}(b)$, si ha la conclusione.

Per quanto riguarda $\mathsf{mult}(a) \cap \mathsf{mult}(b)$, osserviamo intanto che, se $a = 0$ oppure $b = 0$, allora $\mathsf{mult}(a) \cap \mathsf{mult}(b) = \{0\} = \mathsf{mult}(0)$, come già visto nel teorema 3.1: la tesi è verificata. Sopponiamo dunque $a > 0$ e $b > 0$. Osserviamo intanto che senz'altro esiste un multiplo positivo comune: infatti $ab \in \mathsf{mult}(a) \cap \mathsf{mult}(b)$. Sia ora $m$ il più piccolo elemento positivo presente in $\mathsf{mult}(a) \cap \mathsf{mult}(b)$. Si vede che $\mathsf{mult}(a) \cap \mathsf{mult}(b) = \mathsf{mult}(m)$. Infatti:

- Ogni multiplo di $m$, che è multiplo di $a$ e di $b$, sarà a sua volta multiplo di $a$ e di $b$ (vedi anche il teorema 1.1): quindi ogni elemento di $\mathsf{mult}(m)$ è anche contenuto in $\mathsf{mult}(a) \cap \mathsf{mult}(b)$.
- Sia, viceversa, $k$ un qualsiasi multiplo positivo di $a$ e di $b$: si tratta di mostrare che $k$ è multiplo di $m$. Sia $r$ il resto di $k$ nella divisione per $m$. Essendo $m$ e $k$ entrambi multipli di $a$ e di $b$, anche $r$ lo sarà, per quanto già visto nel teorema 1.1, o anche nell'esercizio 1.20: il resto $r$ si ottiene infatti da $k$ sottraendo $m$ un certo numero di volte. Ma dato che $r < m$, deve essere $r = 0$, dato che è $m$ il più piccolo divisore positivo comune ad $a$ e $b$. Ciò significa appunto che $m|k$. □

È inoltre immediato notare che i numeri $D$ e $m$ appena trovati sono *unici*, nel senso che non ce ne sono altri con le medesime proprietà.

**Esercizio 3.8** Dimostrare l'unicità dei numeri $D$ e $m$ la cui esistenza è provata nel teorema 3.2.

**Definizione 3.2** [MCD] Si dice *massimo comune divisore* dei numeri naturali $a$ e $b$, indicato con la scrittura $\mathsf{MCD}(a, b)$, o talvolta anche soltanto $(a, b)$, il numero naturale $D$ tale che $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(D)$.

**Definizione 3.3** [mcm] Si dice *minimo comune multiplo* dei numeri naturali $a$ e $b$, indicato con la scrittura $\mathsf{mcm}(a, b)$, il numero naturale $m$ tale che $\mathsf{mult}(a) \cap \mathsf{mult}(b) = \mathsf{mult}(m)$.

Si noti che l'uso dell'articolo determinativo *il* in queste definizioni è giustificato da quanto dimostrato nel teorema 3.2 e nell'esercizio 3.8 (esistenza e unicità). È chiaro, dalle definizioni 3.1 e 3.2, che il MCD di due numeri coprimi è 1.

**Esercizio 3.9** Dimostrare che, per ogni $a, b \in \mathbb{N}$, si ha:

- se $n|a$ e $n|b$, allora $n|\mathsf{MCD}(a, b)$;
- se $a|n$ e $b|n$, allora $\mathsf{mcm}(a, b)|n$.

Queste proprietà, che caratterizzano il MCD e il mcm di due numeri, sono già esplicitamente enunciate e dimostrate anche da Euclide, nel corollario alla proposizione 2 e nella proposizione 35 del libro VII.

Il MCD e il mcm sono dunque, rispettivamente, il *massimo* (dei divisori comuni) e il *minimo* (dei multipli comuni) *rispetto alla relazione di divisibilità*. Incidentalmente, per gli interi positivi, questa relazione è inclusa nell'ordinamento naturale, nel senso che $a|b \Rightarrow a \leqslant b$. Quindi, confondendo il significato degli aggettivi *massimo* e *minimo* (rispetto alla divisibilità) con i loro significati abituali (rispetto all'ordinamento naturale) non porta a conclusioni erronee. Tuttavia, è più corretto pensare le espressioni *massimo* e *minimo* in termini di divisibilità, per quanto la differenza sia sottile. La cosa diviene più visibile se consideriamo anche il numero 0: infatti, poiché $\mathsf{div}(0) \cap \mathsf{div}(0) = \mathsf{div}(0)$ in maniera ovvia, $\mathsf{MCD}(0,0) = 0$. Ma l'insieme dei divisori comuni è dato da $\mathsf{div}(0) \cap \mathsf{div}(0) = \mathbb{N}$: dove 0 è appunto il *massimo* elemento rispetto alla relazione di divisibilità (0 ѝmultiplo di ogni numero), mentre sarebbe il *minimo* rispetto all'ordinamento naturale.

Ma come si calcolano nella pratica il MCD e il mcm di due numeri? Vi sono diversi metodi, alcuni più "rudimentali", altri più "raffinati". Cominciamo dai primi, che possono essere farraginosi ma comunque del tutto validi. Per il MCD, basta fare l'elenco completo dei divisori dei due numeri, quindi prendere il più grande. Per il mcm, si possono elencare i multipli di uno dei due numeri, in ordine crescente, fermandosi appena se ne trova uno che è divibile anche per l'altro numero. Altri metodi sono più rapidi, soprattutto al crescere dei numeri in gioco: ne vedremo alcuni nel seguito.

**Esercizio 3.10** Con riferimento a quanto trovato nell'esercizio 3.1 e alle definzioni 3.2 3.3, indicare i risultati di queste operazioni:

- $\mathsf{MCD}(12, 30)$ e $\mathsf{mcm}(12, 30)$;
- $\mathsf{MCD}(6, 24)$ e $\mathsf{mcm}(6, 24)$;
- $\mathsf{MCD}(21, 10)$ e $\mathsf{mcm}(21, 10)$;
- $\mathsf{MCD}(1, 6)$ e $\mathsf{mcm}(1, 6)$;
- $\mathsf{MCD}(0, 9)$ e $\mathsf{mcm}(0, 9)$.

**Esercizio 3.11** Siano $a, b \in \mathbb{N}$ non entrambi nulli e sia $D = \mathsf{MCD}(a, b)$. Dimostrare che allora i numeri $a/D$ e $b/D$ sono coprimi.

**Esercizio 3.12** Siano $a, b \in \mathbb{N}$, con $b \neq 0$, e sia $D = \mathsf{MCD}(a, b)$. Dimostrare che allora la frazione $\frac{(a/D)}{(b/D)}$ è ridotta ai minimi termini.

**Esercizio 3.13** È vero o falso che, per ogni $a, b \in \mathbb{N}$, si ha $\mathsf{MCD}(a, b)|\mathsf{mcm}(a, b)$? E che $\mathsf{MCD}(a, b) \leqslant \mathsf{mcm}(a, b)$? E se abbiamo $a, b > 0$?

**Esercizio 3.14** Dimostrare che, se $a, b, c \in \mathbb{N}$ e $b|c$, allora si ha $\mathsf{MCD}(a,b)|\mathsf{MCD}(a,c)$ e $\mathsf{mcm}(a,b)|\mathsf{mcm}(a,c)$.

Le operazioni MCD e mcm possiedono diverse proprietà. Elenchiamo alcune delle principali.

**Teorema 3.3** [proprietà del MCD] *Per ogni $a, b, c \in \mathbb{N}$ si ha:*

- $MCD(a,b) = MCD(b,a)$; [prop. commutativa]
- $MCD(a,0) = a$; [0 elemento neutro]
- $MCD(a,1) = 1$; [1 elemento assorbente]
- $MCD(a, MCD(b,c)) = MCD(MCD(a,b), c)$; [prop. associativa]
- $MCD(ab, ac) = a \cdot MCD(b,c)$. [prop. distributiva rispetto al prodotto]

[proprietà del mcm] *Per ogni $a, b, c \in \mathbb{N}$ si ha:*

- $mcm(a,b) = mcm(b,a)$; [prop. commutativa]
- $mcm(b,1) = b$; [1 elemento neutro]
- $mcm(b,0) = 0$; [0 elemento assorbente]
- $mcm(a, mcm(b,c)) = mcm(mcm(a,b), c)$; [prop. associativa]
- $mcm(ab, ac) = a \cdot mcm(b,c)$. [prop. distributiva rispetto al prodotto]

Valendo la proprietà associativa, quando si considerano tre (o anche più) numeri, si usano in genere scritture quali $\mathsf{MCD}(a,b,c)$ invece che $\mathsf{MCD}(a, \mathsf{MCD}(b,c))$ o altre. Sarà chiaro che $\mathsf{MCD}(a,b,c)$ indica quel numero naturale $D$ tale che $\mathsf{div}(a) \cap \mathsf{div}(b) \cap \mathsf{div}(c) = \mathsf{div}(D)$.

**Esercizio 3.15** Dimostrare il teorema 3.3.

**Esercizio 3.16** Dimostrare che, dati i numeri naturali $a \geqslant b$, si ha $\mathsf{MCD}(a,b) = \mathsf{MCD}(a-b,x) = \mathsf{MCD}(a+b,x)$, dove $x$ è uno qualsiasi tra i numeri $a$ e $b$.

È possibile utilizzare questa proprietà per il calcolo del MCD, in maniera semplice e rapida. L'idea è di ridursi a coppie di interi sempre più piccoli, ossia di realizzare una successione decrescente: è l'idea centrale di tutta la trattazione euclidea dell'aritmetica. L'osservazione cruciale è la seguente.

**Teorema 3.4** *[Algoritmo euclideo.] Dati i numeri naturali $a \geqslant b$, si ha $MCD(a,b) = MCD(a-b,b)$.*

Dimostrazione. Il risultato è già stato provato negli esercizi 3.4 e 3.16, scegliendo $x = b$. In effetti, si vede subito che $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(a-b) \cap \mathsf{div}(b)$, da cui segue che $\mathsf{MCD}(a,b) = \mathsf{MCD}(a-b,b)$. □

Il teorema 6 indica un metodo di calcolo molto efficiente per il MCD di due numeri. Vediamo come.

**Esempio 3.1** Vogliamo trovare il valore di $\mathsf{MCD}(1782, 504)$, se possibile senza dover ricercare ed elencare tutti i divisori dei due numeri (che potrebbero essere molti). In base al teorema 6, vale questa catena di uguaglianze:

$$\begin{aligned}\mathsf{MCD}(1782, 504) &= \mathsf{MCD}(1278, 504) = \mathsf{MCD}(774, 504)\\ &= \mathsf{MCD}(504, 270)\\ &= \mathsf{MCD}(270, 234)\\ &= \mathsf{MCD}(234, 36) = \mathsf{MCD}(198, 36) = \mathsf{MCD}(162, 36) =\\ &= \mathsf{MCD}(126, 36) = \mathsf{MCD}(90, 36) = \mathsf{MCD}(54, 36)\\ &= \mathsf{MCD}(36, 18) = \mathsf{MCD}(18, 18)\\ &= \mathsf{MCD}(18, 0) = 18.\end{aligned}$$

Infatti, già si era notato nel teorema 3.3 che $\mathsf{MCD}(0, n) = n$ per ogni $n \in \mathbb{N}$.

Osservando la successione riportata nell'esempio 3.1, ci si rende conto che è possibile ridurre il numero di passi. In effetti, le sottrazioni ripetute a partire da una coppia -per esempio, $(234, 36)$- conducono fino a trovare il resto della divisione del maggiore rispetto al minore (in questo caso 18). Si può dunque abbreviare il procedimento, radunando le varie sottrazioni dove il minore rimane lo stesso nel calcolo del resto di una divisione. L'esempio precedente verrebbe così riscritto:

$$\begin{aligned}&\mathsf{MCD}(1782, 504) = \mathsf{MCD}(504, 270) = \mathsf{MCD}(270, 234) =\\ = \;&\mathsf{MCD}(234, 36) = \mathsf{MCD}(36, 18) = \mathsf{MCD}(18, 0) = 18.\end{aligned}$$

In generale, a partire da una coppia $(a_1, a_2)$ con $a_1 \geqslant a_2$, si può procedere in questo modo:

- se $a_2 = 0$, allora $\mathsf{MCD}(a_1, a_2) = a_1$;
- se $a_2 > 0$, allora $\mathsf{MCD}(a_1, a_2) = \mathsf{MCD}(a_2, a_3)$ (dove $a_3$ indica il resto nella divisione di $a_1$ per $a_2$).

Risulta dunque $a_3 < a_2$ e si può andare avanti nello stesso modo (se $a_3 = 0$ abbiamo finito, altrimenti si considera la coppia $(a_3, a_4)$, dove $a_4$ è il resto nella divisione di $a_2$ per $a_3$, che sarà a sua volta minore di $a_3$, e così via). Si ottiene dunque una successione di numeri naturali $a_1 \geqslant a_2 > a_3 > ... > a_n > ...$ che va avanti fino a che si trovano termini $a_n > 0$. Ma questa successione decrescente di numeri naturali non può proseguire per più di $a_1$ passi. All'ultimo passo si dovrà avere $a_k = 0$ e quindi $\mathsf{MCD}(a_1, a_2) = a_{k-1}$. Questa procedura è detta algoritmo euclideo: essa è infatti descritta nelle proposizioni 1 e 2 del VII libro degli elementi. Possiamo immaginarla come una sorta di discesa a *gradini* verso il MCD: partiamo con $(a_1, a_2)$, poi scendiamo a $(a_2, a_3)$, $(a_3, a_4)$, e così via, fino a trovare $(M, 0)$ che ci indica $MCD(a_1, a_2)$.

**Esercizio 3.17** Trovare $\mathsf{MCD}(294, 273)$, $\mathsf{MCD}(28152, 90)$, $\mathsf{MCD}(3185, 4459)$.

**Esercizio 3.18** Quanto vale MCD$(13, 130000014)$? E MCD$(21, 21000035)$?

Per due numeri reali positivi $x_1 \geqslant x_2$, esiste $k \in \mathbb{N}$ tale che $x_2 \cdot k > x_1$: è il cosiddetto *postulato di Archimede*[2], l'algoritmo euclideo può ossere applicato a numeri positivi qualsiasi, anche non interi. Partendo da una coppia $x_1 \geqslant x_2$ di numeri reali positivi, possiamo scrivere (in maniera unica):

$x_1 = q_1 \cdot x_2 + x_3$ (dove $q_1 \in \mathbb{N}$ e $x_3 \in \mathbb{R}$ con $0 \leqslant x_3 < x_2$)
$x_2 = q_2 \cdot x_3 + x_4$ (dove $q_2 \in \mathbb{N}$ e $x_4 \in \mathbb{R}$ con $0 \leqslant x_4 < x_3$)
...
$x_n = q_n \cdot x_{n+1} + x_{n+2}$ (dove $q_n \in \mathbb{N}$ e $x_{n+2} \in \mathbb{R}$ con $0 \leqslant x_{n+2} < x_{n+1}$).

Cosa può accadere andando avanti con questa successione $x_1 \geqslant x_2 > x_3 > ... > x_n > ...$? Trattandosi di numeri reali, questa successione decrescente potrebbe anche continuare all'infinito mantenendosi su valori positivi. Le cose stanno in maniera piuttosto semplice. La questione viene trattata anche da Euclide nella parte iniziale del libro X degli Elementi.

**Teorema 3.5** *A partire dai numeri reali positivi $x_1 \geqslant x_2$, sia $x_1 \geqslant x_2 > x_3 > ... > x_n > ...$ la sequenza dei resti successivi ottenuti con l'algoritmo euclideo. Nella sequenza si trova prima o poi un termine $x_k = 0$ se e solo se il rapporto $x_1/x_2$ è razionale.*

Dimostrazione. Supponiamo di avere

$x_1 = q_1 \cdot x_2 + x_3$ (dove $q_1 \in \mathbb{N}$ e $x_3 \in \mathbb{R}$ con $0 < x_3 < x_2$)
$x_2 = q_2 \cdot x_3 + x_4$ (dove $q_2 \in \mathbb{N}$ e $x_4 \in \mathbb{R}$ con $0 < x_4 < x_3$)
...
$x_{n-1} = q_{n-1} \cdot x_n + x_{n+1}$ (dove $q_{n-1} \in \mathbb{N}$ e $x_{n+1} \in \mathbb{R}$ con $0 < x_{n+1} < x_n$)
$x_n = q_n \cdot x_{n+1}$ (dove $q_n \in \mathbb{N}$).

Allora, procedendo a ritroso con delle sostituzioni successive (prima $x_n$, poi $x_{n-1}$, e così via, fino a $x_2$ e $x_1$) si riesce ad esprimere ciascun $x_i$ come multiplo intero di $x_{n+1}$. In particolare si avrà $x_1 = x_{n+1} \cdot m$ e $x_2 = x_{n+1} \cdot n$, dove $m$ e $n$ sono interi positivi, dunque $x_1/x_2 = m/n$.
Viceversa, se $x_1/x_2 = m/n$, vale a dire $x_1/m = x_2/n$, si ponga $z = x_1/m = x_2/n$. Allora $x_1/z$ e $x_2/z$ sono interi. Si possono ripercorrere i passi dell'algoritmo euclideo dividendo ciascun membro per $z$. Per esempio, la relazione $x_1 = q_1 \cdot x_2 + x_3$ (con $q_1 \in \mathbb{N}$ e $0 \leqslant x_3 < x_2$) diviene $(x_1/z) = q_1 \cdot (x_2/z) + (x_3/z)$ (con $q_1 \in \mathbb{N}$ e $0 \leqslant (x_3/z) < (x_2/z)$). Ora $(x_1/z)$ e $(x_2/z)$ sono interi, pertanto lo è anche $(x_3/z) = (x_1/z) - q_1 \cdot (x_2/z)$. Andando avanti in questo modo, i numeri $(x_i/k)$ che compaiono sono tutti interi. La loro sequenza coincide con la sequenza dei resti successivi nell'algoritmo euclideo che si ottiene a partire dalla coppia di interi positivi $((x_1/z), (x_2/z))$. Ma già sappiamo che nella sequenza di resti ottenuti con l'algoritmo euclideo a partire da due interi positivi si arriva

[2] È così chiamato per via del fatto che esso viene enunciato da Archimede come 5° postulato nel trattato "La sfera e il cilindro". Questa la formulazione di Archimede: *date due lunghezze o aree o volumi diseguali, la maggiore supera la minore di una grandezza tale che, sommandosi a se stessa, sia in grado di superare qualunque assegnata grandezza che sia con esse confrontabile.*

prima o poi a 0. □

Per due numeri positivi $x_1$ e $x_2$, avere un rapporto razionale equivale a possedere un sottomultiplo comune $z$, inteso nel senso che, sommando ripetutamente tale $z$, si ottengono sia $x_1$ che $x_2$, ossia $x_1 = z \cdot m$ e $x_2 = z \cdot n$, con $m$ e $n$ interi positivi. Infatti, se $x_1/x_2 = m/n$, allora $x_1/m = x_2/n$ e, ponendo $z = x_1/m = x_2/n$, si ha appunto $x_1 = z \cdot m$ e $x_2 = z \cdot n$. Viceversa, se $x_1 = z \cdot m$ e $x_2 = z \cdot n$ con $m$ e $n$ interi positivi, allora $x_1/x_2 = m/n$. Per questa ragione, in tal caso si dice anche che i numeri $x_1$ e $x_2$ sono *commensurabili* (in caso contrario, sono detti *incommensurabili*): appunto perché il sommultiplo comune $z$ li "misura" entrambi (nel senso euclideo).
Ricapitoliamo. Applicando l'algoritmo euclideo a dei numeri reali $x_1 \geqslant x_2 > 0$, possono presentarsi due situazioni differenti:

- se $x_1$ e $x_2$ sono incommensurabili (ossia $(x_1/x_2) \notin \mathbb{Q}$), si genera una successione infinita e decrescente di resti reali e positivi;
- se $x_1$ e $x_2$ sono commensurabili (ossia $(x_1/x_2) \in \mathbb{Q}$), si genera una sequenza finita di resti si conclude con 0; l'ultimo termine positivo $x_h$, prima di trovare 0, è un sottomultiplo comune di $x_1$ e $x_2$, nel senso che $x_1/x_h$ e $x_2/x_h$ sono interi.

**Esercizio 3.19** Dimostrare che, se i numeri reali positivi $x_1$ e $x_2$ sono commensurabili, allora il sottomultiplo comune $D$ che si trova con l'algoritmo euclideo è multiplo di qualsiasi sottomultiplo comune a $x_1$ e $x_2$. Ossia: se $z > 0$ è tale che $x_1/z$ e $x_2/z$ sono interi, allora anche $D/z$ è intero.

In virtù di quanto affermato nell'esercizio 3.20, tale sottomultiplo $D$ viene si dice esso stesso *massimo comune divisore* di $x_1$ e $x_2$ e si indica ancora con la notazione $\mathsf{MCD}(x_1, x_2)$. Analogamente, per $x_1$ e $x_2$ commensurabili si può mostrare l'esistenza di un $\mathsf{mcm}(x_1, x_2)$: un multiplo comune che è sottomultiplo di qualasiasi altro multiplo comune a $x_1$ e $x_2$. Usando un sottomultiplo comune come unità di misura (ossia dividendo tutti i numeri in gioco per tale sottomultiplo), queste operazioni si riducono a calcoli puramente aritmetici, dove compaiono solo numeri interi.

**Esercizio 3.20** Verificare che:

- $\mathsf{MCD}(7\sqrt{3}, 10\sqrt{3}) = \sqrt{3}$ e $\mathsf{mcm}(7\sqrt{3}, 10\sqrt{3}) = 70\sqrt{3}$;
- $\mathsf{MCD}(\frac{4}{9}, \frac{8}{15}) = \frac{4}{45}$ e $\mathsf{mcm}(\frac{4}{9}, \frac{8}{15}) = \frac{8}{3}$.

Le operazioni di MCD e mcm, ora eseguite anche su coppie di numeri reali non interi, godono di proprietè analoghe a quelle già viste nel caso puramente aritmetico.

**Esercizio 3.21** Siano $x_1 \geqslant x_2$ numeri positivi commensurabili. Dimostrare che si ha:

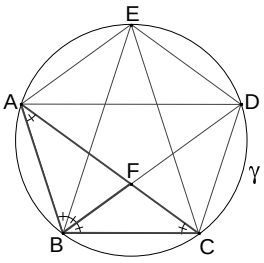
- $\mathrm{MCD}(x_1, x_2) > 0$;
- $\mathrm{MCD}(k \cdot x_1, k \cdot x_2) = k \cdot \mathrm{MCD}(x_1, x_2)$ per ogni $k$ reale positivo;
- $\mathrm{mcm}(k \cdot x_1, k \cdot x_2) = k \cdot \mathrm{mcm}(x_1, x_2)$ per ogni $k$ reale positivo;
- $\mathrm{MCD}(x_1, x_2) = \mathrm{MCD}(x_1 - x_2, x_i) = \mathrm{MCD}(x_1 + x_2, x_i)$, dove $x_i$ è uno qualsiasi tra i numeri $x_1$ e $x_2$.

È talvolta possibile servirsi di ciò anche nella geometria, ad esempio per provare l'incommensurabilità delle misure di due segmenti. Quello che segue è uno dei casi più celebri.

**Esempio 3.2** Il lato di un pentagono regolare e la sua diagonale sono incommensurabili. Per dimostrarlo, consideriamo un pentagono regolare $ABCDE$, inscritto nella circonferenza $\gamma$, nel quale tracciamo le 5 diagonali (tutte di eguale lunghezza). Sia $\alpha$ l'ampiezza di un angolo alla circonferenza che insiste su uno degli archi delimitati da vertici consecutivi del pentagono. Gli angoli interni del triangolo $ABC$ assommano a $5\alpha$, perciò $\alpha$ è $\frac{1}{5}$ di un angolo piatto ($36°$).

Ora supponiamo, per assurdo, che sia $\mathrm{MCD}(\overline{CA}, \overline{AB}) = \mathsf{H} > 0$. Osserviamo che:

- $AB = AF$, infatti $F\hat{A}B = \alpha$ e $A\hat{B}F = 2\alpha$, quindi $B\hat{F}A = 2\alpha = A\hat{B}F$ e $AB = AF$;
- i triangoli $ABC$ e $CFB$ sono simili, infatti $B\hat{C}A = F\hat{B}C = \alpha$, $C\hat{A}B = B\hat{C}F = \alpha$ e $A\hat{B}C = C\hat{F}B = 3\alpha$.




Valgono pertanto le seguenti uguaglianze:

$$\mathsf{H} = \mathrm{MCD}(\overline{CA}, \overline{AB}) = \mathrm{MCD}(\overline{CA} - \overline{BA}, \overline{AB}) = \mathrm{MCD}(\overline{CA} - \overline{FA}, \overline{AB}) = \mathrm{MCD}(\overline{CF}, \overline{BC}).$$

Per i due triangoli isosceli $ABC$ e $CFB$ ha quindi lo stesso valore $\mathsf{H} > 0$ il MCD tra la base e il lato obliquo. Ma questo non può accadere, essendo i due triangoli

simili e diseguali. Detto infatti $k = (\overline{CF}/\overline{AB}) < 1$ il rapporto di similitudine [3], si verrebbe ad avere:

$$\mathsf{H} = \mathsf{MCD}(\overline{BC}, \overline{CF} = \mathsf{MCD}(k \cdot \overline{CA}, k \cdot \overline{AB} = k \cdot \mathsf{MCD}(\overline{CA}, \overline{AB}) = k \cdot \mathsf{H},$$

impossibile per $k \neq 1$ e $H \neq 0$.

[3] È interessante calcolare il valore del rapporto di similitudine $k$, che è anche pari al rapporto tra il lato e la diagonale del pentagono. Si ha $k = CF/AB = BC/CA$, vale a dire $k = CF/FA = FA/CA$, dal momento che $AB = BC = FE$. Significa che $FA$ è medio proporzionale tra l'intera diagonale $CA$ e la parte rimanente $CF$. Per il suo valore numerico, basta osservare che l'uguaglianza precedente equivale a $(CA - FA)/FA = FA/CA$, ossia $(CA/FA) - (FA/FA) = FA/CA$, vale a dire $\frac{1}{k} - 1 = k$, che si può anche scrivere come $k^2 = 1 - k$. Di qui si ottiene $k = \frac{\sqrt{5}-1}{2}$, in genere chiamato *rapporto aureo*.

# 4 I numeri primi.

Il concetto di numero primo è tra i più antichi e più fondamentali di tutta la matematica. I numeri primi sono quei numeri che non possono essere scritti come prodotti di altri interi più piccoli. Traduciamo questa idea nella seguente definizione.

**Definizione 4.1** Un numero naturale $n > 1$ si dice *primo* se

$$\forall a, b \in \mathbb{N}\,(\, a \cdot b = n \Rightarrow ((a = 1 \wedge b = n) \vee (a = n \wedge b = 1))\,).$$

La definizione di numero primo può essere formulata in più modi, lievemente differenti nella forma, ma ovviamente equivalenti. Ne vediamo alcuni qui di seguito.

**Teorema 4.1** *Per un intero positivo $n$ le seguenti condizioni si equivalgono:*

- *$n$ è un numero primo;*
- *$n > 1$ e $\forall a, b \in \mathbb{N}\,(\, n = a \cdot b \Rightarrow (a = 1 \vee b = 1)\,)$;*
- *$n > 1$ e $\forall a, b \in \mathbb{N}\,(\, n = a \cdot b \Rightarrow (a = n \vee b = n)\,)$;*
- *$n > 1$ e $\forall m \in \mathbb{N}\,(\, m|n \Rightarrow (m = 1 \vee m = n)\,)$;*
- *$d(n) = 2$.*

Un numero maggiore di 1 che non sia primo è detto *composto*. Un numero composto $n$ si può dunque scrivere nella forma $n = a \cdot b$, con $1 < a < n$ e $1 < b < n$.

**Esercizio 4.1** Siano $p$ e $q$ numeri primi. È possibile che si abbia $p|q$? In quali casi?

**Esercizio 4.2** Siano $a, b \in \mathbb{N}$ con $a|b$. Dimostrare che, se $a$ è un numero composto, anche $b$ è composto.

**Esercizio 4.3** Sia $p$ un numero primo e sia $n \in \mathbb{N}$. Allora o $\mathrm{MCD}(p, n) = p$ (se $p|n$) oppure $\mathrm{MCD}(p, n) = 1$ (se $p \not| n$). [Elementi, libro VII, prop. 29]

Quanti sono i numeri primi? Può anche venire spontaneo pensare che ve ne siano infiniti. Ma la cosa non è affatto scontata. In linea di principio, potrebbe succedere che, da un certo momento in avanti, si trovino solo numeri composti, che sono tutti prodotti di numeri più piccoli. Non possiamo escluderlo in maniera immediata.

Per decidere la questione, serve dunque una dimostrazione. O una dimostrazione di infinità, oppure la dimostrazione che gli interi sopra un certo numero sono tutti prodotti di altri numeri più piccoli.

Per provare l'infinità, potremmo cercare di far vedere che, per ogni intero $n$, esiste un numero primo maggiore di $n$. Oppure, si potrebbe esibire, per ciascun numero primo $p$, il successivo numero primo, mostrando così che ce n'è sempre uno. Purtroppo non si riesce a trovare una regola immediata che permetta di stabilire quale sia il successivo di un numero primo. Scorrendo la sequenza dei numeri primi, ci si accorge che talvolta sono molto fitti e talvolta sono invece lontani. Si ha l'impressione che tendono a diradarsi andando avanti, ma ogni tanto tornano ad infittirsi. Un andamento irregolare, che sembra sfuggire ad una regola semplice. Vediamo come inizia la lista:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29,
31, 37, 43, 47, 53, 59, 61, 67, 71, 73,
79, 83, 89, 97, 101, 103, 107, 109, 113, 127,
131, 137, 139, 149, 151, 157, 163, 167, 173, 179,
181, 191, 193, 197, 199, 211, 223, 227, 229, 233,
239, 241, 251, 257, 263, 269, 271, 277, 281, 283,
293.

Fino a 50 ce ne sono 15, da 50 a 100 ce ne sono 10, da 100 a 150 ce ne sono 10 , da 150 a 200 ce ne sono 11, da 200 a 250 ce ne sono 7 e da 250 a 300 ce ne sono 8. Se andiamo avanti ne troviamo -così pare- via via più raramente.
In una situazione come questa, fino a che non si dimostra una delle due alternative, non siamo in grado di conlcudere nulla, neppure approssimativamente.

Potremmo anche chiederci: in un intervallo di 50 (o più) interi consecutivi, vi sarà sempre almeno un numero primo? La risposta non è del tutto evidente.

**Esercizio 4.4** Trovare 50 numeri interi consecutivi che non siano primi.

Esistono dunque intervalli anche lunghi (di lunghezza arbitraria) di interi privi di numeri primi. Tuttavia, possiamo dimostrare che i numeri primi sono infiniti.

**Teorema 4.2** *Esistono infiniti numeri primi.*

Dimostrazione. Seguiamo le orme di Euclide, che nella proposizione 20 del libro IX degli Elementi fornisce la prima dimostrazione pervenuta a noi di questo risultato. Il suo ragionamento è ancora oggi un modello di eleganza e semplicità. Egli non menziona esplicitamente l'infinità[4]: aggira l'ostacolo mostrando che, dato un qualsiasi insieme finito $\mathcal{P}$ di numeri primi, esiste almeno un numero primo fuori da $\mathcal{P}$. Ciò equivale, chiaramente, a dimostrare che i numeri primi

[4] Forse per la cautela dei greci verso il concetto di infinito.

sono infiniti.

Sia dunque, come detto, $\mathcal{P} = \{p_1, p_2, ..., p_n\}$ un qualsiasi insieme finito di numeri primi, e sia $K = p_1 \cdot p_2 \cdot ... \cdot p_n$ il loro prodotto [5]. Consideriamo adesso il numero $K + 1$. Quali elementi di $\mathcal{P}$ dividono $K + 1$? Dato che, per ogni elemento $p_h \in \mathcal{P}$, si ha $p_h|K$, se avessimo $p_h|K+1$, risulterebbe $p_h|(K+1)-K$ (teorema 1.1), ossia $p_h|1$: impossibile, l'unico divisore di 1 è 1, che non è primo.

Nessuno dei numeri primi presenti in $\mathcal{P}$ divide quindi $K + 1$. Ma anche $K + 1$ dovrà essere disibile per almeno un numero primo $p'$: ne segue che tale $p'$ è fuori da $\mathcal{P}$. Dunque $\mathcal{P}$ non contiene tutti i numeri primi. Abbiamo dimostrato che un qualsiasi insieme finito non può contenere tutti quanti i numeri primi, che pertanto debbono essere infiniti. □

In realtà, se osserviamo con attenzione la dimostrazione del teorema 4.2, vediamo che un piccolo buco rimane ancora: abbiamo dato per scontato che $K + 1$ debba essere divisibile per qualche numero primo. Questo appare del tutto accettabile: o il numero $K + 1$ è primo esso stesso, o sarà multiplo di un numero primo più piccolo. Ma va dimostrato. È la proposizione 31 del libro VII degli Elementi.

**Teorema 4.3** *Per ogni intero $a > 1$ esiste un numero primo $p$ che divide $a$.*

Dimostrazione. Anche in questo caso, seguiremo il ragionamento di Euclide. Consideriamo l'intero $a$. Ci sono due possibilità:

- $a$ è primo: in tal caso $a$ stesso è il numero primo che divide $a$, e la tesi è verificata;
- $a$ è composto: in tal caso $a = a_1 \cdot b_1$, dove $a_1$ e $b_1$ sono interi tali che $1 < a_1 < a$ e $1 < b_1 < a$.

Nella seconda di queste ipotesi, consideriamo l'intero $a_1$. Anche per $a_1$ ci sono due possibilità:

- $a_1$ è primo: in tal caso, dato che $a_1|a$, la tesi è verificata;
- $a_1$ è composto: in tal caso $a_1 = a_2 \cdot b_2$, dove $a_2$ e $b_2$ sono interi tali che $1 < a_2 < a_1$ e $1 < b_2 < a_1$.

Ancora, nella seconda di queste ipotesi, consideriamo l'intero $a_2$. Anche per $a_2$ ci sono due possibilità:

- $a_2$ è primo: in tal caso, dato che $a_2|a_1$ e $a_1|a$, si ha $a_2|a$ (1.1) e la tesi è verificata;
- $a_2$ è composto: in tal caso $a_2 = a_3 \cdot b_3$, dove $a_3$ e $b_3$ sono interi tali che $1 < a_3 < a_2$ e $1 < b_3 < a_2$.

[5] Essendo in numero finito, possiamo moltiplicarli tutti quanti.

Fino a che non incontriamo un numero primo, possiamo così proseguire costruendo una successione decrescente $a, a_1, a_2, a_3, ...$ di interi maggiori di 1, tutti divisori di $a$ e tra loro differenti. Ma un intero positivo $a$ possiede solo un numero finito di divisori ($\mathsf{d}(a) \leqslant a$: vedi anche l'esercizio 1.23). Non è pertanto possibile che si vada avanti all'infinito: entro $a$ passi si trova dunque un numero primo $a_n$, il quale divide $a$. □

Come si vede, la conclusione è piuttosto delicata e chiama in causa in qualche modo l'infinito, sotto forma di una successione di numeri che *potrebbe* andare avanti per sempre.
Euclide conclude la dimostrazione con queste frasi: "E così, continuando questa ricerca, si otterrà un numero primo che divide $a$. Se non si trovasse, allora vi sarebbe una successione infinita di divisori di $a$, ciascuno minore del precedente, il che è impossibile nei numeri (naturali).". Si basa dunque sul fatto che *non esistono successioni infinite e sempre decrescenti di numeri naturali*, o che *ogni sottoinsieme (non vuoto) dei numeri naturali contiene un elemento minimo*. Esso viene assunto da Euclide in via implicita: non compare tra i postulati, né tra i teoremi provati fino a quel momento. Ci sono vari altri casi del genere negli Elementi. In seguito questo argomento sarà anche detto della *discesa infinita*, equivalente a quello che viene oggi indicato come *principio di induzione*.

**Esercizio 4.5** Dimostrare che due numeri naturali sono coprimi se e solo se nessun numero primo li divide entrambi.

Stabilita l'infinità dei numeri primi, possono nascere molte altre domande. Per esempio: si riuscirà a trovare una formula che esprima tutti i numeri primi, o almeno che ci dica quanti sono i primi in un dato intervallo? Per esempio: quanti saranno i numeri primi con ultima cifra uguale a 1, 2, 3, 4, 5, 6, 7, 8, 9, 0? Quanti i primi $p$ tali che $2p + 1$ è ancora primo? O quelli tali che $p - 1$ è un quadrato? Non sembrano questioni semplici. È legittimo aspettarsi che i numeri primi aventi certe proprietà debbano essere in diversi casi infiniti: ma, se si prova ad imitare la dimostrazione euclidea dell'infinità, ci si rende conto di come sia difficile adattarla ad altre questioni. Un caso dove, con qualche accortezza, si riesce ad imitare la dimostrazione euclidea è il seguente.

**Esercizio 4.6** Dimostrare che sono sono infiniti i numeri primi del tipo $4n + 3$, per $n \in \mathbb{N}$.

Il risultato dell'esercizio 4.6 può essere ulteriormente esteso, ma con grande fatica e servendosi di ben altri metodi (e comunque in maniera piuttosto contenuta [6], mentre la gran parte dei problemi restano tuttora aperti).

[6] Più precisamente, si riesce a dimostrare che, dati $a$ e $b$ coprimi, esistono infiniti numeri primi della forma $a \cdot n + b$, con $n \in \mathbb{N}$.

Intanto vediamo come trovare tutti i numeri primi fino a un dato numero: per esempio fino a 40. Prima elenchiamo tutti gli interi da 2 a 100:

$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, ...$

Ora selezioniamo il primo numero della lista e cancelliamo tutti i suoi multipli:

$②, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, 27, \cancel{28}, 29, \cancel{30}, ...$

Di nuovo, selezioniamo il primo numero superstite e non ancora cerchiato e cancelliamo tutti i suoi multipli:

$②, ③, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, 25, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, ...$

Di nuovo, selezioniamo il primo numero superstite e non ancora cerchiato e cancelliamo tutti i suoi multipli:

$②, ③, \cancel{4}, ⑤, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, ...$

E così via, fino a che non restano solo numeri cerchiati, che sono i numeri primi nell'intervallo considerato. Questo procedimento è conosciuto come *setaccio di Eratostene*.

**Esercizio 4.7** Spiegare perché i numeri che rimangono cerchiati con il setaccio di Eratostene sono tutti e soli i numeri primi compresi nell'intervallo.

**Esercizio 4.8** Dimostrare che, se $n$ è un numero composto, allora esiste un numero primo $p$ tale che $p|n$ e $p \leqslant \sqrt{n}$.

Quest'ultimo fatto è spesso utile per mostrare che un certo numero è primo. Ad esempio: dato che 163 non è divisibile per 2, per 3, per 5, per 7, per 11, e dato che $13^2 > 163$, si conclude che 163 è un numero primo.

# 5 La fattorizzazione unica.

Ogni intero maggiore di 1 è prodotto di numeri primi. Infatti un numero composto $n$ si potrà scrivere come prodotto di due interi maggiori di 1. Di questi fattori, quelli composti saranno a loro volta prodotto di due numeri maggiori di 1, e così via, fino ad esprimere $n$ come prodotto di fattori primi. Il processo termina perché le varie scomposizioni danno luogo a successioni decrescenti di numeri naturali. Vediamo un esempio.

**Esempio 5.1** Si ha: $168 = 6 \cdot 28 = (2 \cdot 3) \cdot (7 \cdot 4) = 2 \cdot 3 \cdot 7 \cdot 2 \cdot 2$, che sono tutti fattori primi. Ma si poteva procedere anche diversamente, per esempio: $168 = 2 \cdot 84 = 2 \cdot (2 \cdot 42) = 2 \cdot 2 \cdot (2 \cdot 21) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7$.

Come si è visto, ci sono in genere più vie per scomporre un intero in fattori primi: ma andando avanti fino ad avere solo fattori primi, allora in tutte le scomposizioni di un numero $n$ si ottengono sempre i medesimi fattori (a meno ovviamente dell'ordine). Si parla, in questo senso, di *fattorizzazione unica* degli interi. Questo fatto può essere formulato dicendo che le possibili scomposizioni in fattori primi di ogni intero $n > 1$ danno luogo ad uno stesso *multiinsieme*[7] di fattori primi, dipendente solo da $n$. Nel caso dell'esempio 5.1, si trovano rispettivamente i multiinsiemi di fattori primi $[2, 3, 7, 2, 2]$ e $[2, 2, 2, 3, 7]$, che coincidono.

Per dimostrare in via generale la proprietà di fattorizzazione unica degli interi, ci si basa sull'idea che un fattore primo presente in una scomposizione non può svanire se si segue una differente scomposizione: dovrà in ogni caso ritrovarsi in qualcuno dei fattori. Questo fatto -che è il contenuto della proposizione 30 del libro VII degli Elementi- può essere così formulato.

**Teorema 5.1** *Sia $p$ un numero primo e siano $m, n \in \mathbb{N}$. Se $p|m \cdot n$, allora $p|m$ oppure $p|n$.*

La dimostrazione di questo teorema cruciale richiede un po' di lavoro ed è rinviata alla sezione 6. Per il momento ci limitiamo ad assumerlo in quanto segue.

**Esempio 5.2** Si ha $5 \cdot 14 = 70$ e $7|70$. Ne segue che o $7|5$ o $7|14$: infatti $7|14$.

**Esempio 5.3** Si ha $4 \cdot 15 = 60$ e $6|60$. Tuttavia $6 \not| 4$ e $6 \not| 15$: infatti 6 non è primo.

**Esercizio 5.1** Dimostrare che, se $p$ è un numero composto, allora esistono numeri naturali $m$ e $n$ tali che $p|m \cdot n$ senza che si abbia né $p|m$ né $p|n$.

**Esercizio 5.2** Dimostrare che: [Elementi, Libro VII, prop. 23, 24, 25, 26]

[7] Per *multiinsieme* si intende una collezione che può contenere anche più copie di un medesimo elemento. Nel seguito, indicheremo i multiinsiemi con delle parentesi quadre che ne racchiudono gli elementi: $[a, b, c, ...]$.

- se $a$ e $b$ sono coprimi e $c|b$, allora $a$ e $c$ sono coprimi;
- se $a$ e $n$, così come $b$ e $n$, sono coprimi, allora anche $a \cdot b$ e $n$ sono coprimi;
- se $a$ e $b$ sono coprimi, allora lo sono anche $a^2$ e $b$, come anche $a^2$ e $b^2$;
- se $a$ e $n$ e anche $b$ e $m$ sono coprimi, allora $a \cdot b$ e $n \cdot m$ sono coprimi.

**Esercizio 5.3** Dimostrare che, se $a$ e $b$ sono coprimi, allora $a + b$ è coprimo con $a$ e con $b$, e viceversa. [Elementi, Libro VII, prop. 28]

**Esercizio 5.4** Dimostrare la seguente generalizzazione del teorema 5.1: se $p$ è un numero primo e $p|a_1 \cdot a_2 \cdot ... \cdot a_n$, allora esiste un $a_k$ tale che $p|a_k$.

**Esercizio 5.5** Ricavare dal teorema 5.1 il cosiddetto *principio di annullamento del prodotto* per i numeri interi: per ogni $a, b \in \mathbb{Z}$, se $a \cdot b = 0$, allora $a = 0$ oppure $b = 0$.

Svolgimento. Preso un qualsiasi numero primo $p$, si ha $p|0$: quindi, per il teorema 5.1, $p|a$ oppure $p|b$. Dato che i numeri primi sono infiniti (teorema 4.2), deve accadere che o infiniti di essi dividono $a$ o infiniti di essi dividono $b$. Ma l'unico numero intero con infiniti divisori è 0 (vedi anche il teorema 1.3), quindi $a = 0$ o $b = 0$. □

**Esercizio 5.6** Dimostrare la seguente generalizzazione dell'esercizio 5.5: se $a_1 \cdot a_2 \cdot ... \cdot a_n = 0$, allora esiste un $a_k$ tale che $a_k = 0$.

Procediamo adesso con il risultato principale.

**Teorema 5.2** *[Fattorizzazione unica.] Sia $n > 1$ un numero intero. Supponiamo che*

- $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_h$ *(dove $p_1, p_2, ..., p_h$ sono numeri primi);*
- $n = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_h$ *(dove $q_1, q_2, ..., q_k$ sono numeri primi).*

*Allora* $[p_1, p_2, p_3, ..., p_s] = [q_1, q_2, q_3, ..., q_t]$ [8].

L'enunciato significa che, scomponendo in fattori primi un intero $n > 1$, si ottengono in ogni caso gli stessi numeri primi lo stesso numero di volte.

Dimostrazione. Dato che

$$p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_t$$

e inoltre $p_1|p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_s$, si ha $p_1|q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_t$. Quindi, per il teorema 5.1 (più precisamente per quanto visto nell'esercizio 5.6), deve esistere un $q_i$ tale

[8] Come già detto, i simboli $[p_1, p_2, p_3, ..., p_s]$ e $[q_1, q_2, q_3, ..., q_t]$ indicano i *multiinsiemi* formati dai fattori primi delle due scomposizioni.

che $p_1|q_i$. Ma poiché $p_1$ e $q_i$ sono numeri primi, deve essere $p_1 = q_i$ (vedi anche l'esercizio 4.1). Cancelliamo allora questo numero da ambo i lati e riscriviamo l'uguaglianza:

$$p_2 \cdot p_3 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot \cancel{q_i} \cdot ... \cdot q_t.$$

Passiamo ora a $p_2$: per le stesse ragioni di prima, anche $p_2$ deve essere presente tra i fattori del prodotto $q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot \cancel{q_i} \cdot ... \cdot q_t$. Esiste dunque $j \neq i$ tale che $p_2 = q_j$. Provvediamo a cancellare tale fattore da ambo i lati, ottenendo l'uguaglianza:

$$p_3 \cdot ... \cdot p_s = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot \cancel{q_i} \cdot ... \cdot \cancel{q_j} ... \cdot q_t.$$

Andando avanti così per $s$ passi, a sinistra sarà rimasto 1: quindi anche a destra dovrà rimanere 1. Ciò significa che anche a destra debbono esserci all'inizio precisamente $s$ fattori primi e si è anche visto che, a meno dell'ordine, essi debbono essere uguali a quelli di sinistra. □

Abbiamo così stabilito che ogni intero $n > 1$ può essere scritto in modo unico -a meno dell'ordine dei fattori- nella forma

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s},$$

dove i $p_i$ sono numeri primi distinti e gli $a_i$ sono interi positivi.

**Teorema 5.3** Siano $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$ e $b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_s^{b_s}$, dove i $p_i$ sono numeri primi distinti e gli esponenti $a_i, b_i$ sono numeri naturali. Allora, $a|b$ se e solo se $a_i \leqslant b_i$ per ogni $i$.

**Esercizio 5.7** Dimostrare il teorema 5.3.

**Esercizio 5.8** Sia $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$ la scomposizione in fattori primi dell'intero positivo $n$.

- Dimostrare che $n$ è un quadrato se e solo se tutti gli esponenti $a_i$ soni pari.
- Dimostrare, in generale, che $n$ è una potenza $k$-esima se e solo se tutti gli esponenti $a_i$ sono divisibili per $k$.

**Esercizio 5.9** Il numero $6^6 \cdot 14^4 \cdot 21^{10}$ è un quadrato? È un cubo? Una quarta potenza?

Ritroviamo finalmente il familiare procedimento di calcolo di MCD e mcm basato sulla scomposizione in fattori. Facciamo notare che, se due interi sono espressi sotto forma di prodotti di potenze di vari numeri primi, possiamo sempre scriverli usando, per i due interi, potenze con le stesse basi: basta aggiungere, dove occorre, alcune potenze ad esponente nullo. Per esempio $24 = 2^3 \cdot 3$ e $50 = 2 \cdot 5^2$, li possiamo riscrevere così: $24 = 2^3 \cdot 3^1 \cdot 5^0$, $50 = 2^1 \cdot 3^0 \cdot 5^2$. Questa osservazione ci permette di enunciare in maniera semplice il prossimo -classico- risultato.

**Teorema 5.4** Siano $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$ e $b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_s^{b_s}$, dove i $p_i$ sono numeri primi distinti e gli esponenti $a_i, b_i$ sono numeri naturali. Allora si ha:

- $\mathsf{MCD}(a,b) = p_1^{\mathsf{min}(a_1,b_1)} \cdot p_2^{\mathsf{min}(a_2,b_2)} \cdot ... \cdot p_s^{\mathsf{min}(a_s,b_s)}$;
- $\mathsf{mcm}(a,b) = p_1^{\mathsf{max}(a_1,b_1)} \cdot p_2^{\mathsf{max}(a_2,b_2)} \cdot ... \cdot p_s^{\mathsf{max}(a_s,b_s)}$.

Dimostrazione. Sia $D = p_1^{\mathsf{min}(a_1,b_1)} \cdot p_2^{\mathsf{min}(a_2,b_2)} \cdot ... \cdot p_s^{\mathsf{min}(a_s,b_s)}$. È chiaro che $D|a$ e $D|b$, ossia $D \in \mathsf{div}(a) \cap \mathsf{div}(b)$, dato che gli esponenti dei fattori primi di $D$ sono, per costruzione, non maggiori dei corrispettivi in $a$ e $b$ (vedi teorema 5.3). Inoltre, ciascun divisore comune di $a$ e $b$ deve, su ciascun primo $p_i$, avere un esponente che non superi nessuno degli $a_i$ e $b_i$: quindi non supera neppure $\mathsf{min}(a_i, b_i)$, qualunque sia $i$ (sempre per il teorema 5.3). In conclusione $\mathsf{div}(a) \cap \mathsf{div}(b) = \mathsf{div}(D)$, ossia $D = \mathsf{MCD}(a,b)$. In maniera del tutto simile si ragiona per il $\mathsf{mcm}(a,b)$. □

**Esercizio 5.10** Determinare $\mathsf{MCD}(12^4 \cdot 15^2 \cdot 50^7, 12^6 \cdot 15 \cdot 50^4)$.

**Esercizio 5.11** Quanto vale $\mathsf{MCD}(11, 210000011)$? E $\mathsf{MCD}(55, 55000021)$?

**Esercizio 5.12** Dimostrare che, per ogni $a, b \in \mathbb{Z}$, si ha $a^2|b^2$ se e solo se $a|b$. In generale $a^k|b^k$ se e solo se $a|b$ (per $k$ intero positivo). [Elementi, libro VIII, prop. 14, 15, 16, 17.]

**Esercizio 5.13** Dimostrare che, per ogni $a, b \in \mathbb{N}$, si ha:

- $\mathsf{MCD}(a^2, b^2) = (\mathsf{MCD}(a,b))^2$ e $\mathsf{mcm}(a^2, b^2) = (\mathsf{mcm}(a,b))^2$;
- in generale, $\mathsf{MCD}(a^k, b^k) = (\mathsf{MCD}(a,b))^k$ e $\mathsf{mcm}(a^k, b^k) = (\mathsf{mcm}(a,b))^k$ per ogni intero positivo $k$.

**Esercizio 5.14** Quanto vale $\mathsf{MCD}(11, 210000011)$? E $\mathsf{MCD}(55, 55000021)$?

**Teorema 5.5** *Per ogni $a, b \in \mathbb{N}$, si ha $\mathsf{MCD}(a,b) \cdot \mathsf{mcm}(a,b) = a \cdot b$.*

Dimostrazione. I casi in cui uno degli interi $a$, $b$ sia 0 oppure 1 vanno visti a parte, ma sono immediati (...). Se sono entrambi maggiori di 1, possiamo scomporli in fattori primi e quindi calcolare i loro MCD e mcm così come si è fatto nel 5.4, servendosi di uno stesso insieme di fattori primi per $a$ e $b$ (eventualmente si aggiungono potenze del tipo $p^0$, dove occorre). Ora si osserva che, per ogni potenza $p_i^{a_i}$ e $p_i^{b_i}$, uno dei due fattori (il minore) viene compreso nel calcolo del $\mathsf{MCD}(a,b)$ e l'altro (il maggiore) viene poi compreso nel calcolo del $\mathsf{mcm}(a,b)$: questo proprio per quanto visto nel teorema 5.4. Pertanto, nel prodotto $\mathsf{MCD}(a,b) \cdot \mathsf{mcm}(a,b)$ si ritrovano precisamente tutti i fattori primi di $a$ e di $b$: esso vale quindi come $a \cdot b$. □

Quanto visto nel teorema 5.5 permette di calcolare anche il mcm, come il MCD, tramite l'algoritmo euclideo: una volta trovato $\mathsf{MCD}(a,b)$, si ha infatti

$\mathsf{mcm}(a,b) = \frac{a \cdot b}{\mathsf{MCD}(a,b)}$. Specialmente per numeri grandi, è un metodo di calcolo di norma più veloce sia del procedimento ingenuo (la ricerca manuale dei multipli successivi) sia della scomposizione in fattori primi.

**Esercizio 5.15** Dimostrare che, se $a, b \in \mathbb{N}$ sono coprimi, allora $\mathsf{mcm}(a,b) = a \cdot b$.

**Esercizio 5.16** Dimostrare le seguenti leggi distributive:

- per ogni $a, b, c \in \mathbb{N}$ si ha $\mathsf{MCD}(a, \mathsf{mcm}(b,c)) = \mathsf{mcm}(\mathsf{MCD}(a,b), \mathsf{MCD}(a,c))$;
- per ogni $a, b, c \in \mathbb{N}$ si ha $\mathsf{mcm}(a, \mathsf{MCD}(b,c)) = \mathsf{MCD}(\mathsf{mcm}(a,b), \mathsf{mcm}(a,c))$.

**Esercizio 5.17** Siano $a, b \in \mathbb{N}$ coprimi. Dimostrare $a \cdot b$ è un quadrato (o una $k$-esima potenza) se e solo se $a$ e $b$ sono entrambi dei quadrati (o delle $k$-esime potenze).

**Esercizio 5.18** Dati $a, b, n \in \mathbb{N}$, dimostrare che, se $n | a \cdot b$ e inoltre $a$ e $n$ sono coprimi, allora $n | b$.

**Esercizio 5.19** Dimostrare che, dato $K \in \mathbb{N}$, se due interi positivi $a$ e $b$ sono coprimi, allora i resti ottenuti dividendo per $b$ i numeri $K + a$, $K + 2a$, $K + 3a$, ..., fino a $K + ba$, sono tutti diversi (e costituiscono l'intero insieme $\{0, 1, ..., b-1\}$).

La scomposizione in fattori primi ci permette anche di determinare il numero $\mathsf{d}(a)$ dei divisori di un intero positivo $a$ per via *combinatoria*, cioè senza elencarli esplicitamente tutti. Infatti, una volta scritto $a$ nella forma $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$, in conseguenza del teorema 5.3 i divisori di $a$ sono tutti e soli i numeri del tipo $b = p_1^{b_1} \cdot p_2^{b_2} \cdot ... \cdot p_s^{b_s}$, dove $0 \leqslant b_i \leqslant a_i$ per ogni $i$. Per ottenere un divisore, si tratta quindi di scegliere $0 \leqslant b_1 \leqslant a_1$, $0 \leqslant b_2 \leqslant a_2$, ..., $0 \leqslant b_s \leqslant a_s$: ci sono $a_1 + 1$ possibilità per la scelta di $b_1$, $a_2 + 1$ possibilità per la scelta di $b_2$, e così via fino a $b_s$ per il quale vi sono $a_s + 1$ scelte possibili (per esempio, prendendo ciascun $b_i = 0$, si ottiene il divisore 1). Inoltre ognuna di queste $s$ scelte è decisiva, nel senso che, cambiandone anche solo una, si ottiene un diverso divisore (sempre per via della fattorizzazione unica). Possiamo pertanto riepilogare la nostra discussione nella forma che segue.

**Teorema 5.6** *Sia $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$, dove i $p_i$ sono numeri primi distinti. Allora, $\mathsf{d}(a) = (a_1 + 1) \cdot (a_2 + 1) \cdot ... \cdot (a_s + 1)$.*

**Esercizio 5.20** Quanti divisori positivi ha il numero 90000? E 900000? E $6^3 \cdot 8^5 \cdot 63 \cdot 70^8$?

**Esercizio 5.21** Dimostrare nuovamente che, per un intero positivo $n$, $\mathsf{d}(n)$ è dispari se e solo se $n$ è un quadrato.

**Esercizio 5.22** Qual è il prodotto di tutti i divisori positivi di 90000? E di 900000? E di $6^3 \cdot 8^5 \cdot 63 \cdot 70^8$?

**Esercizio 5.23** Dati gli interi positivi $m$ e $n$, con $m|n$, sia $[m;n]$ l'insieme dei loro divisori intermedi, vale a dire:

$$[m;n] = \{h|\, h \in \mathbb{N} \wedge h \in \mathsf{mult}(m) \cap \mathsf{div}(n)\}.$$

Allora $\mathsf{card}([m;n]) = \mathsf{d}(n/m)$.

**Esercizio 5.24** Siano $a$ e $b$ interi positivi. Dimostrare che:

- $\mathsf{d}(a \cdot b) \leqslant \mathsf{d}(a) \cdot \mathsf{d}(b)$;
- se $a$ e $b$ sono coprimi, allora $\mathsf{d}(a \cdot b) = \mathsf{d}(a) \cdot \mathsf{d}(b)$.

**Esercizio 5.25** Esistono interi positivi $n$ con $\mathsf{d}(n) = 11$? Quanti ce ne sono?

**Esercizio 5.26** Dimostrare che, per ogni intero $k > 1$, esistono infiniti interi positivi tali $n$ che $\mathsf{d}(n) = k$.

**Esercizio 5.27** Dimostrare che esistono infiniti interi positivi $n$ tali che $\mathsf{d}(n)|n$.

**Esercizio 5.28**
- Esistono interi positivi che sono multipli di $7$ e possiedono precisamente 7 divisori? Se sì, quali?
- Esistono interi positivi che sono multipli di $21$ e possiedono precisamente 21 divisori? Se sì, quali?
- Esistono interi positivi che sono multipli di $42$ e possiedono precisamente 42 divisori? Se sì, quali?
- Esistono interi positivi che sono multipli di $49$ e possiedono precisamente 49 divisori? Se sì, quali?

**Esercizio 5.29** Il numero $2010!$ termina con molti zeri. Quanti?

**Esercizio 5.30** Su un tavolo c'è una fila di 108 carte da gioco, tutte a faccia in sù.
Decidiamo di voltare tutte le carte che occupano una posizione pari ($2^a$, $4^a$, ...).
Poi voltiamo le carte in una posizione multipla di $3$ ($3^a$, $6^a$, ...).
Poi voltiamo le carte in una posizione multipla di $4$ ($4^a$, $8^a$, ...).
E così via, fino a che non si voltano le carte in posizione multipla di $108$ (solo la $108^a$).
In tutto questo, non si cambia mai di posto nessuna carta.
Alla fine, quante carte mostreranno la faccia e quante il dorso?

# 6 Equazioni diofantee di $1^\circ$ grado.

In questa sezione ci proponiamo diversi obiettivi. Intanto abbiamo lasciato in sospeso la dimostrazione di un fatto chiave: se un numero primo divide un prodotto, allora divide almeno uno dei fattori. Questa proprietà si è rivelata essere alla base della teoria della fattorizzazione unica vista nella sezione 5: vorremmo quindi porre rimedio al più presto alla lacuna. Ci giungeremo dopo alcune tappe, studiando le equazioni diofantee di 1○ grado.

Per iniziare, puntiamo l'attenzione su un problema classico: quali numeri si possono ottenere eseguendo somme o sottrazioni tra alcuni numeri assegnati? Prendiamo questo preblema.

**Esercizio 6.1** Avendo a disposizione una fontana e due brocche, rispettivamente da 8 e da 5 litri, si riesce a raccogliere precisamente 1 litro d'acqua? Come si può fare?

Possiamo procedere così. Riempiamo la brocca da 8. Con quell'acqua riempiamo la brocca da 5: restano 3 litri nella prima brocca. Gettiamo via i 5 litri della brocca ora piena, e spostiamo i 3 litri ottenuti nella brocca da 5. Riempiamo nuovamente la brocca da 8. Ora travasiamo parte di questi 8 litri nella brocca da 5, dove sono già presenti 3 litri, fino a riempirla. Resteranno quindi 6 litri nella brocca da 8. Gettiamo via i 5 litri della broca che ora è piena. Versiamo quindi nell'altra brocca parte dei 6 litri d'acqua presenti nella brocca da 8, fino a riempire i 5 litri. A questo punto nella brocca da 8 rimane 1 litro d'acqua.

Possiamo rappresentare la sequenza dei travasi con queste operazioni:

$$8-5, \quad 8-(5-(8-5)), \quad (8-(5-(8-5)))-5 = 8\cdot 2 + 5\cdot(-3) = 1.$$

Così facendo, abbiamo dunque anche trovato una soluzione dell'equazione diofantea [9] $8x + 5y = 1$.
E se le brocche fossero state da 6 e 9 litri? Si sarebbe riusciti a raccogliere 1 litro d'acqua con una serie di riempimenti e di travasi?
In questo caso, le capacità delle brocche in litri sono entrambe multiple di 3. Le operazioni permesse danno luogo a somme e differenze di tali capacità. Ma la somma o la differenza di multipli di 3 è sempre un multiplo di 3 (vedi anche il teorema 1.1 o l'esercizio 1.20): non si potrà mai ottenere 1, che non è multiplo di 3. Per la stessa ragione, l'equazione diofantea $6x + 9y = 1$ non ha soluzione.

Ci proponiamo di studiare le equazioni diofantee della forma $ax + by = h$, le quali sono dette *lineari*. Chiedersi se un'equazione del genere ha soluzioni equivale a domandarsi se l'intero $h$ possa essere ottento con somme o differenze degli

[9] Come già detto nella sezione 1, per equazione *diofantea* si intende un'equazione della quale interessano solo le soluzioni in $\mathbb{Z}$. Una delle questioni principali al riguardo è l'esistenza o meno di soluzioni: questione in genere non banale.

interi $a$ e $b$. Naturalmente, potremmo anche considerare equazioni diofantee lineari con un diverso numero di incognite. Ma si vede subito che il caso con 1 incognita è immediato e non richiede esami particolari. Mentre il caso di 3 o più incognite diviene chiaro una volta compreso il comportamento delle equazioni diofantee lineari in 2 incognite.

Data un'equazione equazione $ax + by = h$, piuttosto che affrontarla singolarmente, può convenire in un primo momento ignorare il valore di $h$, cercando di caratterizzare l'insieme di tutti gli interi della forma $ax + by$, dove $x, y \in \mathbb{Z}$, vale a dire i numeri ottenibili come somme e differenze di $a$ e $b$. Fatto ciò, per stabilire se l'equazione ha soluzione, basterà controllare se $h$ rientra o meno in tale insieme. Ci torna comodo quindi dare la definizione che segue.

**Definizione 6.1** Dati i numeri interi $a_1$, $a_2$, ..., $a_n$, si dice *ideale generato* da essi l'insieme degli interi che si possono ottenere sommando e sottraendo, anche più volte, i numeri $a_i$. Indicheremo tale insieme con la notazione $\big(a_1, a_2, ..., a_n\big)$. Vale a dire:

$$\big(a_1, a_2, ..., a_n\big) = \{a_1x_1 + a_2x_2 + ... + a_nx_n |\ \ x_1, x_2, ..., x_n \in \mathbb{Z}\}.$$

**Esempio 6.1** L'ideale generato da un singolo numero altro non è che l'insieme dei multipli in $\mathbb{Z}$ di quel numero.

**Teorema 6.1** *Qualunque siano $a, b \in \mathbb{Z}$, si ha:*

- *se $u, v \in \big(a, b\big)$, allora anche $u + v \in \big(a, b\big)$;*
- *se $v \in \big(a, b\big)$ e $k \in \mathbb{Z}$, allora anche $kv \in \big(a, b\big)$ (in particolare, $-v \in \big(a, b\big)$).*

**Esercizio 6.2** Dimostrare il teorema 6.2

**Esercizio 6.3** Dati $a, b \in \mathbb{Z}$, dimostrare che:

- $\big(a\big) \cup \big(b\big) \subseteq \big(a, b\big)$;
- se $k|a$ e $k|b$, allora $\big(a, b\big) \subseteq \big(k\big)$;
- se $a|a'$ e $b|b'$, allora $\big(a', b'\big) \subseteq \big(a, b\big)$;
- se $a|b$, allora $\big(a, b\big) = \big(a\big)$;
- $\big(1, a\big) = \mathbb{Z}$.

**Esercizio 6.4**

- In quali casi $\big(a\big) = \big(b\big)$?
- In quali casi $\big(a\big) \cup \big(b\big) = \big(a, b\big)$?

**Esercizio 6.5** Dimostrare che, dati $a, b \in \mathbb{N}$ con $b \neq 0$, detto $r$ il resto della divisione di $a$ per $b$, si ha $r \in \big(a, b\big)$.

**Esercizio 6.6** Dimostrare che, per ogni coppia $a, b \in \mathbb{Z}$, $\big(a, b\big) = \big(|a|, |b|\big)$.

Somme e differenze di multipli di un numero $n$ sono ancora multipli di $n$: perciò, se $n|a$ e $n|b$, allora $n|ax + by$ per ogni $x, y \in \mathbb{Z}$. Ciò significa che $\big(a, b\big) \subseteq \big(n\big)$ (e dunque, se $n \not| h$, l'equazione $ax + by = h$ non può avere soluzioni intere). Di qui si ricava il fatto che segue.

**Teorema 6.2** *Dati $a, b \in \mathbb{Z}$, si ha $\big(a, b\big) \subseteq \big(D\big)$, dove $D = MCD(a, b)$* [10].

Rimane solo da determinare di *quale* parte dell'ideale generato da $D$ si tratti.

**Esercizio 6.7** Siano $a, b \in \mathbb{Z}$ e sia $D = \mathsf{MCD}(a, b)$. Dimostrare che, se $D \in \big(a, b\big)$, allora $\big(a, b\big) = \big(D\big)$.

Nell'esempio iniziale, in cui $\mathsf{MCD}(8, 5) = 1$, si era visto che $1 \in \big(8, 5\big)$: in questo caso, $\big(8, 5\big) = \big(1\big) = \mathbb{Z}$. Se non fosse per i limiti di capienza delle brocche, potremmo raccogliere tutte le quantità intere di litri.
Vediamo qualche altro esempio.

**Esercizio 6.8** Verificare che $\big(18, 7\big) = \big(1\big) = \mathbb{Z}$, $\big(15, 21\big) = \big(3\big)$, $\big(15, 77\big) = \big(1\big) = \mathbb{Z}$, $\big(48, 28\big) = \big(4\big) = \mathbb{Z}$, $\big(91, 75\big) = \big(1\big) = \mathbb{Z}$.

In tutti gli esempi considerati, l'ideale generato da due interi coincide con l'ideale generato dal loro MCD. Ed è proprio questo ciò che accade in generale.

**Teorema 6.3** *Dati $a, b \in \mathbb{Z}$, si ha $\big(a, b\big) = \big(D\big)$, dove $D = MCD(a, b)$.*

Dimostrazione. Per quanto detto sopra (vedi l'esercizio 6.7), si tratta solo di provare che $M \in \big(a, b\big)$. Ma questo fatto è garantito dall'algoritmo euclideo descritto nella sezione 3 (per esempio il teorema ): il $\mathsf{MCD}(a, b)$, si può ricavare da una sequenza di addizioni o sottrazioni a partire dai numeri $a, b$ (che possiamo anche assumere non negativi, in virtù di quanto visto nell'esercizio ). Essendo cos` ottenuti, i numeri che si trovano a ciascun passo appartengono ancora all'ideale generato da $a$ e $b$ (vedi anche l'esercizio 6.5). Pertanto anche $M \in \big(a, b\big)$.□

Il teorema 6.3 viene spesso enunciato formulato nella forma seguente.

**Teorema 6.4** *[Teorema di Bézout.] Per ogni coppia $a, b \in \mathbb{Z}$, esiste una coppia $(x, y)$, con $x, y \in \mathbb{Z}$, tale che $ax + by = D$, dove $D = MCD(a, b)$. In particolare, se $a$ e $b$ sono coprimi, esistono degli interi $x$ e $y$ tali che $ax + by = 1$.*

L'algoritmo euclideo delle ripetute divisioni con resto ci offre anche una via per trovare una coppia $(x, y)$ siffatta, evitando di dover procedere per tentativi.

[10] Gli interi $a$ e $b$ potrebbero anche essere negativi, mentre finora abbiamo definito MCD e mcm solo per i naturali. Conveniamo di porre $\mathsf{MCD}(a, b) = \mathsf{MCD}(|a|, |b|)$ e $\mathsf{mcm}(a, b) = \mathsf{mcm}(|a|, |b|)$. Per esempio, $\mathsf{MCD}(-8, 12) = \mathsf{MCD}(8, 12) = 4$.

**Esempio 6.2** Facciamo un esempio pratico, prendendo $a = 2550$ e $b = 1001$. Si ha:

$$\begin{array}{lll}
2550 = 1001 \cdot 2 + 548, & (\text{ossia} & \underline{548} = \underline{2550} - \underline{1001} \cdot 2), \\
1001 = 548 \cdot 1 + 453, & (\text{ossia} & \underline{453} = \underline{1001} - \underline{548} \cdot 1), \\
548 = 453 \cdot 1 + 95, & (\text{ossia} & \underline{95} = \underline{548} - \underline{453} \cdot 1), \\
453 = 95 \cdot 4 + 73, & (\text{ossia} & \underline{73} = \underline{453} - \underline{95} \cdot 4), \\
95 = 73 \cdot 1 + 22, & (\text{ossia} & \underline{22} = \underline{95} - \underline{73} \cdot 1), \\
73 = 22 \cdot 3 + 7, & (\text{ossia} & \underline{7} = \underline{73} - \underline{22} \cdot 3), \\
22 = 7 \cdot 3 + 1, & (\text{ossia} & \underline{1} = \underline{22} - \underline{7} \cdot 3).
\end{array}$$

Si è così trovato il resto 1, che è dunque il $\mathsf{MCD}(2550, 1001)$. Risalendo a ritroso, possiamo scrivere le uguaglianze:

$$\begin{array}{ll}
\underline{1} = \underline{22} - \underline{7} \cdot 3 & = \underline{22} - (\underline{73} - \underline{22} \cdot 3) \cdot 3 \\
= \underline{73} \cdot (-3) + \underline{22} \cdot (10) & = \underline{73} \cdot (-3) + (\underline{95} - \underline{73} \cdot 1) \cdot (10) \\
= \underline{95} \cdot (10) + \underline{73} \cdot (-13) & = \underline{95} \cdot (10) + (\underline{453} - \underline{95} \cdot 4) \cdot (-13) \\
= \underline{453} \cdot (-13) + \underline{95} \cdot (62) & = \underline{453} \cdot (-13) + (\underline{548} - \underline{453} \cdot 1) \cdot (62) \\
= \underline{548} \cdot (62) + \underline{453} \cdot (-75) & = \underline{548} \cdot (62) + (\underline{1001} - \underline{548} \cdot 1) \cdot (-75) \\
= \underline{1001} \cdot (-75) + \underline{548} \cdot (137) & = \underline{1001} \cdot (-75) + (\underline{2550} - \underline{1001} \cdot 2) \cdot (137) \\
= \underline{2550} \cdot (137) + \underline{1001} \cdot (-349). &
\end{array}$$

Pertanto la coppia $(x, y) = (137, -349)$ soddisfa la relazione di Bézout $2550x + 1001y = 1$.

Come si può vedere, questo metodo è molto più veloce di una ricerca sistematica per tentativi (che pure si potrebbe fare). È chiaro che, una volta trovata una coppia $(x', y')$ per la quale si ottiene $D = \mathsf{MCD}(a, b)$, è immediato anche ottenere ogni suo multiplo $kM$: basta considerare la coppia $(kx', ky')$. Ad esempio, per trovare degli interi $x, y$ in modo che $2550x + 1001y = 8$, si potrà prendere $(x, y) = (8 \cdot 137, 8 \cdot (-349)) = (1096, -2792)$.

**Esercizio 6.9** Esistono coppie di interi $(x, y)$, tali che $2010x + 2059y = 1$? In caso affermativo trovarne una.

**Esercizio 6.10** Esistono coppie di interi $(x, y)$, tali che $1653x + 589y = 1$? In caso affermativo trovarne una.

**Esercizio 6.11** Esistono coppie di interi $(x, y)$, tali che $2009x + 3239y = 943$? In caso affermativo trovarne una.

**Esercizio 6.12** Esistono coppie di interi $(x, y)$, tali che $1711x + 851y = 527$? In caso affermativo trovarne una.

La discussione precedente si può anche riassumere con la proposizione qui di seguito.

**Teorema 6.5** *Dati $a, b, h \in \mathbb{Z}$, l'equazione $ax+by = h$ ha soluzioni intere $(x, y)$ se e solo se $D|h$, dove $D = \mathsf{MCD}(a, b)$.*

Arrivati a questo punto, è semplice generalizzare ad un numero qualsiasi di variabili i risultati che abbiamo appena visto per 2 variabili.

**Teorema 6.6** *Siano $a_1, a_2, ..., a_n \in \mathbb{Z}$ e sia $D = \mathsf{MCD}(a_1, a_2, ..., a_n)$. Valgono i seguenti fatti*[11]*:*

- $\big(a_1, a_2, ..., a_n\big) = \big(D\big)$*;*
- *esistono $x_1, x_2, ..., x_n \in \mathbb{Z}$, tali che $a_1x_1 + a_2x_2 + ... + a_nx_n = D$; in particolare, se $a_1, a_2, ..., a_n$ sono coprimi, esistono degli interi $x_1, x_2, ..., x_n$ tali che $a_1x_1 + a_2x_2 + ... + a_nx_n = 1$;*
- *l'equazione $a_1x_1 + a_2x_2 + ... + a_nx_n = h$ nelle incognite $x_1, x_2, ..., x_n$ ammette soluzioni intere se e solo se $D|h$.*

Questo risultato chiarisce in maniera completa la questione della risolubilità di qualsiasi equazione diofantea di $1^\circ$ grado.

**Esempio 6.3** Esistono terne di interi $(x, y, z)$ tali che $6x + 15y + 10z = 1$? Dal momento che $\mathrm{MCD}(6, 15, 10) = 1$, si ha $\big(6, 15, 10\big) = \big(1\big) = \mathbb{Z}$: dunque la risposta è affermativa. Proviamo a trovare una terna siffatta. Possiamo iniziare da $\big(6, 15\big) = \big(3\big)$. Esistono quindi $\tilde{x}, \tilde{y}$ tali che $6\tilde{x} + 15\tilde{y} = 3$: per esempio $\tilde{x} = -2$, $\tilde{y} = 1$. Ora guardiamo l'equazione $3t + 10z = 1$: qui si ha $\big(3, 10\big) = \big(1\big) = \mathbb{Z}$, perciò esistono interi $t, z$ che la soddisfano, per esempio $t = -3$ e $z = 1$. Rimettendo insieme i pezzi:

$$1 = 3\cdot(-3)+10\cdot(1) = (6\cdot(-2)+15\cdot(1))\cdot(-3)+10\cdot(1) = 6\cdot(6)+15\cdot(-3)+10\cdot(1).$$

Pertanto, la scelta di $(x, y, z) = (6, -3, 1)$ fornisce una soluzione all'equazione.

**Esercizio 6.13** Esistono terne di interi $x, y, z$, tali che $30x + 14y + 21z = 1$? In caso affermativo trovarne una.

Ora risulta finalmente agevole la dimostrazione di un fatto lungamente atteso. È la proposizione 30 del libro VII degli Elementi, sulla quale si basa tutta la teoria della fattorizzazione unica degli interi e che, a questo punto, risulta piuttosto semplice.

**Teorema** 5.1 *Sia $p$ un numero primo e siano $m, n \in \mathbb{N}$. Se $p|m \cdot n$, allora $p|m$ oppure $p|n$.*

[11] In realtà sono fatti tutti equivalenti: si tratta di forme diverse in cui può essere presentata questa medesima proprietà

Dimostrazione. Supponiamo che $p|m \cdot n$ ma $p \not| n$. In tal caso $p$ e $n$ sono coprimi (vedi anche l'esercizio 4.3). Per il teorema di Bézout 6.4, esistono allora degli interi $x$ e $y$ tali che $px + ny = 1$. Se, in questa relazione, moltiplichiamo a sinistra e a destra per $m$, otteniamo:

$$mpx + mny = m.$$

Ma, per ipotesi, $p|mn$: quindi la somma $mpx + mny$ è divisibile per $p$, essendo entrambi gli addendi divisibili per $p$: pertanto $m$ è divisibile per $p$. Abbiamo provato che se il numero primo $p$ divide il prodotto di due interi, ma non divide uno dei fattori, allora deve dividere l'altro. Questo è proprio il significato della tesi. □

Ora che disponiamo di un criterio per stabilire se un'equazione diofantea ha o meno soluzione e sappiamo, nel caso vi siano soluzioni, come trovarne una per mezzo dell'algoritmo euclideo (vedi l'esempio 6.3). Possiamo domandarci, nel caso le soluzioni esistano, quante siano e come determinarle tutte. Indagheremo quindi l'intero insieme delle soluzioni di un'equazione diofantea $ax + by = h$ [12], dove $h$ è multiplo di $M = \mathsf{MCD}(a, b)$.
Prendiamo una coppia $(x', y')$ che sia soluzione dell'equazione diofantea $ax + by = h$.

- Se $(x'', y'')$ è anch'essa soluzione di $ax + by = h$, allora, sottraendo membro a membro, si ottiene una coppia $(x' - x'', y' - y'')$ che fornisce una soluzione dell'equazione omogenea $ax + by = 0$: infatti $a(x' - x'') + b(y' - y'') = (ax' + by') - (ax'' + by'') = h - h = 0$.
- D'altra parte, se $(\tilde{x}, \tilde{y})$ è una qualsiasi soluzione dell'equazione omogenea $ax + by = 0$, allora $(x' + \tilde{x}, y' + \tilde{y})$ è soluzione di $ax + by = h$: infatti $a(x' + \tilde{x}) + b(y' + \tilde{y}) = (ax' + by') + (a\tilde{x} + b\tilde{y}) = h + 0 = h$.

Abbiamo pertanto dimostrato il fatto seguente.

**Teorema 6.7** *Sia $(x', y')$ una soluzione intera dell'equazione $ax + by = h$, dove $a, b, h \in \mathbb{Z}$. Facendo variare $(\tilde{x}, \tilde{y})$ tra le soluzioni intere dell'equazione omogenea $ax + by = 0$, le coppie della forma $(x' + \tilde{x}, y' + \tilde{y})$ forniscono tutte e sole le soluzioni intere dell'equazione $ax + by = h$.*

Il risultato visto nel teorema 6.14 rimane immuatato anche per equazioni con più di 2 incognite. Resta dunque da descrivere l'insieme delle soluzioni di equazioni del tipo $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$. Vediamo alcune caratteristiche di tale insieme.

**Teorema 6.8** *Consideriamo l'equazione omogenea di $1^\circ$ grado $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$, con $a_1, a_2, ..., a_n \in \mathbb{Z}$.*

[12] Ci limiteremo solo al caso di due incognite, ma le cose non cambiano se anche le incognite sono di piu

- *La scelta* $(x'_1, x'_2, ..., x'_n) = (0, 0, ..., 0)$ *dà una soluzione dell'equazione assegnata.*
- *Se* $(x'_1, x'_2, ..., x'_n)$ *e* $(x''_1, x''_2, ..., x''_n)$ *sono soluzioni intere dell'equazione assegnata, allora anche* $(x'_1 + x''_1, x'_2 + x''_2, ..., x'_n + x''_n)$ *è una soluzione;*
- *Se* $(x'_1, x'_2, ..., x'_n)$ *è una soluzione intera dell'equazione assegnata e* $k \in \mathbb{Z}$*, allora anche* $(kx'_1, kx'_2, ..., kx'_n)$ *è una soluzione;*
- *Se* $(x'_1, x'_2, ..., x'_n)$ *è una soluzione intera dell'equazione assegnata e* $k|MCD(x'_1, x'_2, ..., x'_n)$ *(*$k \neq 0$*), allora anche* $(x'_1/k, x'_2/k, ..., x'_n/k)$ *è una soluzione.*

**Esercizio 6.14** Dimostrare il teorema .

**Esercizio 6.15** Dimostrare che, se un'equazione diofantea $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$ ha almeno una soluzione di interi non tutti nulli, allora ne ha infinite.

**Esercizio 6.16** Data un'equazione diofantea $a_1x_1 + a_2x_2 + ... + a_nx_n = 0$, dimostrare i fatti che seguono.

- L'equazione ha infinite soluzioni, tranne il caso $n = 1$ con $a_1 \neq 0$.
- Nel caso $n = 2$, assumendo $\mathrm{MCD}(a_1, a_2) = 1$, le soluzioni dell'equazione sono tutte e sole le coppie del tipo $(x_1, x_2) = (a_2k, -a_1k)$, al variare di $k \in \mathbb{Z}$.

Può infine essere interessante chiedersi, a partire da alcuni interi positivi, quali numeri siano ottenibili sommando, anche più volte, tali numeri (senza poter sottrarre).

**Esercizio 6.17** Disponendo di un gran numero di lingotti, dal peso di 25 e di 30 grammi, quali pesi è possibile totalizzare?

È chiaro che questa domanda equivale a chiedersi quali siano i vaolri di $h$ per i quali l'equazione $25x + 30y = h$ ha soluzioni $(x, y)$ di numeri naturali. È anche chiaro che, affinché un'equazione del tipo $ax + by = h$ abbia soluzioni naturali, è necessario che $h$ sia multiplo di $\mathrm{MCD}(a, b)$ (caso perticolare di quanto già visto nel teorema 6.2). Qualora ciò accada, possiamo sempre immaginare di aver diviso ambedue i lati dell'equazione per $\mathrm{MCD}(a, b)$, ottenendo così $a$ e $b$ coprimi.

**Esercizio 6.18** Dati gli interi positivi $a, b, h$, mostrare che l'equazione $ax+by = h$ possiede un numero finito di soluzioni di nmumeri naturali (eventualmente 0).

**Esercizio 6.19** Supponiamo che, nell'esercizio 6.17, sia possibile ottenere un certo peso totale $p$. Come fare per ottenere il peso $p$ con il minor numero possibile di lingotti?

**Esercizio 6.20** Dati $a, b \in \mathbb{N}$, sia $\big(a, b\big)^+ = \{ax + by | \, x, y \in \mathbb{N}\}$. Dimostrare che che:

- se $b = 0$, allora $\big(a, b\big)^+ = \mathsf{mult}(a)$;
- se $a$ e $b$ sono coprimi, allora per ogni intero $n \geqslant a \cdot b$ si ha $n \in \big(a, b\big)^+$.

**Esercizio 6.21** Dati $a, b \in \mathbb{N}$, sia $\big(a, b\big)^+ = \{am + bn | \, m, n \in \mathbb{N}\}$. Dimostrare che, se $a > 1$ e $b > 1$ sono coprimi, allora:

- $ab - a - b \notin \big(a, b\big)^+$;
- per ogni intero $n > ab - a - b$ si ha $n \in \big(a, b\big)^+$.

# 7 Altre equazioni diofantee.

In questa sezione ci occupiamo di studiare alcuni esempi importanti di equazioni diofantee di $2^\circ$ grado.

L'equazione $x^2 - y^2 = k$.

Questa equazione posisede alcuni caratteri esemplari, che la rendono interessante. Per risolverla, conviene servirsi del fatto che $x^2 - y^2 = (x + y)(x - y)$ e quindi cercare tra i fattori dell'intero $k$. In questo senso si tratta di equazioni esemplari: per quanto possibile, questo modo di procedere si tenta di applicarlo anche ad altri casi. Nell'equazione $x^2 - y^2 = k$, possiamo assumere che $k \in \mathbb{N}$ (eventualmente scambiando $x$ e $y$). Ci limiteremo a cercare le soluzioni con $x, y \in \mathbb{N}$ (per avere anche quelle con interi negativi, basterà considerare anche gli opposti dei valori trovati). Vediamo dunque alcuni esempi di equazioni del tipo $x^2 - y^2 = k$, per diversi valori di $k$.

**Esempio 7.1** Consideriamo l'equazione diofantea $x^2 - y^2 = 17$. Se la pensiamo nella forma $(x + y)(x - y) = 17$, dal momento che 17 è primo e che $x + y \geqslant x - y$ per $x, y \in \mathbb{N}$, si dovrà avere $\begin{cases} x + y = 17 \\ x - y = 1 \end{cases}$. Ne segue che $(x, y) = (9, 8)$ è l'unica soluzione in $\mathbb{N}$. Se cercassimo tutte le soluzioni in $\mathbb{Z}$, andrebbero annoverate anche le seguenti: $(x, y) = (-9, 8)$, $(x, y) = (9, -8)$, $(x, y) = (-9, -8)$.

**Esercizio 7.1** Dimostrare che, se $k$ ùn numero primo dispari, allora l'equazione diofantea $x^2 - y^2 = k$ ha un'unica soluzione in $\mathbb{N}$. Vale a dire che ogni numero primo dispari è esprimibile in un unico modo come differenza di quadrati.

**Esempio 7.2** Consideriamo l'equazione diofantea $x^2 - y^2 = 21$, ossia $(x + y)(x - y) = 21$. Dal momento che $21 = 7 \cdot 3$, possiamo cercare soluzioni che verificano $\begin{cases} x + y = 21 \\ x - y = 1 \end{cases}$, oppure soluzioni del tipo $\begin{cases} x + y = 7 \\ x - y = 3 \end{cases}$. Entrambi i sistemi hanno soluzione: ne segue che $(x, y) = (11, 10)$ oppure $(x, y) = (5, 2)$.

**Esempio 7.3** Determinare le soluzioni dell'equazione diofantea $x^2 - y^2 = 45$.

**Esercizio 7.2** Data l'equazione $x^2 - y^2 = k$, dove $k$ è un numero naturale dispari, dimostrare i fatti seguenti:

- ci sono soluzioni in $\mathbb{N}$;
- se $k$ non è primo, allora esiste più di una soluzione in $\mathbb{N}$.

**Esempio 7.4** Consideriamo adesso l'equazione diofantea $x^2 - y^2 = 14$, ossia $(x+y)(x-y) = 14$. Dal momento che $14 = 7 \cdot 2$ contiene 1 sola volta il fattore 2, solo uno tra i fattori $(x+y)$ e $(x-y)$ dovrebbe essere pari. Ma, per qualsiasi coppia di interi $x, y$, la somma $(x+y)$ e la differenza $(x-y)$ sono o entrambe pari o entrambe dispari. Infatti la loro somma risulta essere $(x+y)+(x-y) = 2x$, che è pari (mentre la somma di un pari e un dispari è un dispari). L'equazione è quindi priva di soluzioni intere.

**Esercizio 7.3** Mostrare che le equazioni del tipo $x^2 - y^2 = k$, con $k = 2n$ (dove $n$ è dispari), non hanno soluzioni intere.

**Esercizio 7.4** Determinare le soluzioni delle seguenti equazioni diofanteee:

- $x^2 - y^2 = 28$;
- $x^2 - y^2 = 56$.

**Esercizio 7.5** Dimostrare che le equazioni del tipo $x^2 - y^2 = k$, con $k = 4n$ ($n$ intero), possiedono soluzioni intere.

**Esercizio 7.6** Determinare le soluzioni delle seguenti equazioni diofanteee:

- $x^2 - 4y^2 = 13$;
- $9x^2 - y^2 = 32$.

In tutta evidenza, siamo stati agevolati dal fatto di poter facilmente scomporre i polinomi quali $x^2 - y^2$. Le cose sarebbero più difficili per equazioni come $2x^2 - y^2 = 1$ o anche $x^2 + 3y^2 = 27$.
Ricapitoliamo quanto appurato circa l'equazione $x^2 - y^2 = k$.

**Teorema 7.1** Dato l'intero positivo $k$, l'equazione $x^2 - y^2 = k$ ha soluzioni intere se e solo se $k$ è dispari oppure multiplo di $4$.

Possiamo anche stabilire quante siano le soluzioni dell'equazione, qualora ve ne siano.

**Esercizio 7.7** Dato l'intero positivo $k$, consideriamo l'equazione $x^2 - y^2 = k$.

- Per $k$ dispari, le soluzioni in $\mathbb{N}$ dell'equazione sono $\frac{\mathrm{d}(k)}{2}$ (se $k$ non è un quadrato), oppure $\frac{\mathrm{d}(k)+1}{2}$ (se $k$ è un quadrato).
- Per $k = 4h$, le soluzioni in $\mathbb{N}$ dell'equazione sono $\frac{\mathrm{d}(h)}{2}$ (se $h$ non è un quadrato), oppure $\frac{\mathrm{d}(h)+1}{2}$ (se $h$ è un quadrato).

L'equazione $x^2 = 2y^2$.

È un'equazione illustre: equivale a cercare, fatto salvo il caso $x = y = 0$, quali siano i numeri razionali di quadrato 2. È ben noto che non ve ne sono: ma si tratta di un risultato importante al punto di meritare un esame attento.
Iniziamo con una semplice osservazione: si tratta di un'equazione omogenea di 2° grado, vale a dire un'equazione algebrica dove ogni monomio è di 2° grado. È immdiato constatare il seguente fatto.

**Teorema 7.2** Data un'equazione diofantea omogenea in $n$ incognite $x_1$, $x_2$, ..., $x_n$, valgono questi fatti:

- essa ha sempre la soluzione banale $(x_1, x_2, ..., x_n) = (0, 0, ..., 0)$;
- se $(x'_1, x'_2, ..., x'_n)$ è una soluzione intera, anche $(kx'_1, kx'_2, ..., kx'_n)$ (dove $k \in \mathbb{Z}$) è una soluzione intera;
- 
- se $(x'_1, x'_2, ..., x'_n)$ è una soluzione intera e $k \neq 0$ divide tutti gli $x'_i$ $(1 \leqslant i \leqslant n)$, allora $(x'_1/k, x'_2/k, ..., x'_n/k)$ è ancora una soluzione intera;
- se $(x'_1, x'_2, ..., x'_n) \neq (0, 0, ..., 0)$ è una soluzione intera, allora $(x'_1/D, x'_2/D, ..., x'_n/D)$ (dove $D = \mathrm{MCD}(x'_1, x'_2, ..., x'_n)$) è una soluzione primitiva (ossia tale che $\mathrm{MCD}(x_1, x_2, ..., x_n) = 1$);
- se l'equazione ha una soluzione non banale, allora ne ha infinite.

**Esercizio 7.8** Dimostrare il teorema 7.2.

**Teorema 7.3** *Irrazionalità di* $\sqrt{2}$. *L'unica soluzione intera dell'equazione* $x^2 = 2y^2$ *è la coppia* $(x, y) = (0, 0)$.

Dimostrazione. Per assurdo. Supponiamo che esista una soluzione di interi $(\tilde{x}, \tilde{y}) \neq (0, 0)$: in tal caso dovrà aversi sia $\tilde{x} \neq 0$ che $y' \neq 0$. Essendo $\tilde{x}^2 = 2\tilde{y}^2$, abbiamo $\tilde{y}^2 | \tilde{x}^2$, da cui $\tilde{y} | \tilde{x}$ (vedi l'esercizio 5.12). Abbiamo perciò $\frac{\tilde{x}^2}{\tilde{y}^2} = 2$, che possiamo scrivere nella forma $(\tilde{x}/\tilde{y})^2 = 2$), ossia $n^2 = 2$ (dove $n = y/x$ è intero per quanto detto sopra). Ma 2 non è il quadrato di un numero intero. □

**Esercizio 7.9**
- Se $n$ non è un quadrato, l'equazione $x^2 = ny^2$ ha come unica soluzione la coppia $(0, 0)$.
- Se $n$ non è una potenza $k$-esima, l'equazione $x^k = ny^k$ ha come unica soluzione la coppia $(0, 0)$.

Queste proposizioni possono essere riformulate dicendo che $\sqrt{n} \notin \mathbb{Q}$ se $n$ non è un quadrato (più in generale, che $\sqrt[k]{n} \notin \mathbb{Q}$ se $n$ non è una $k$-esima potenza), ossia che $\sqrt{n} \in \mathbb{Q}$ se e solo se $\sqrt{n} \in \mathbb{N}$. In altre parole, i numeri del tipo $\sqrt{n}$, per $n \in \mathbb{N}$, o sono interi o sono irrazionali. Con l'aggiunta di siffatti elementi irrazionali, si ottengono a partire da $\mathbb{Q}$ più estesi insiemi numerici.

**Esercizio 7.10** Siano $a$ e $b$ numeri razionali e sia $c$ un numero irrazionale. Dimostrare che:

- $a+b$ e $ab$ sono razionali, come anche $a/b$ (se $b \neq 0$);
- $b+c$ è irrazionale, come anche $bc$ (se $b \neq 0$).

**Esercizio 7.11**
- Esistono coppie di numeri irrazionali positivi $c, d$, tali che sia $c+d$ sia $cd$ sono razionali?
- Esistono coppie di numeri irrazionali positivi $c, d$, tali che sia $c+d$ sia $c/d$ sono razionali?

**Esercizio 7.12** Dimostrare che $\sqrt{2}+\sqrt{3}$ è irrazionale.

**Esercizio 7.13** Dimostrare che, per ogni $n > 2$, le radici del polinomio $p(x) = x^2 - nx + 1$ sono numeri irrazionali positivi aventi somma e prodotto razionali.

## L'equazione $x^2 + y^2 = z^2$.

Anche questa è un'equazione nolto illustre. Esprime infatti la relazione pitagorica, che lega le misure dei cateti e dell'ipotenusa nei triangoli rettangoli. Vorremmo descrivere tutte le terne di interi positivi che soddisfano questa relazione, le cosiddette *terne pitagoriche*. Dato che anche la relazione pitagorica è omogenea, possiamo limitarci alle sole terne $(x, y, z)$ primitive, ossia quelle per cui $\mathsf{MCD}(x, y, z) = 1$. Le altre saranno date da qualsiasi multiplo di una terna primitiva.

**Esercizio 7.14** Sia $(x, y, z)$ una terna pitagorica, ossia una soluzione di interi positivi dell'equazione $x^2 + y^2 = z^2$.

- Dimostrare che, se la terna è primitiva, allora gli interi $x$ e $y$ sono uno pari e l'altro dispari, mentre $z$ è dispari;
- Dimostrare che, se la terna è primitiva, allora le coppie $x, y,\ y, z,\ z, x$ sono tutte e 3 coprime.
- Dimostrare che, se 2 degli interi $x$, $y$, $z$ sono coprimi, allora anche il terzo intero è coprimo con entrambi gli altri.

Enunciamo adesso la fisioniomia generale delle terne pitagoriche primitive. Questa descrizione si trova già negli Elementi, libro X, nel lemma 1 della proposizione 29, dove tuttavia non si dimostra che *tutte* le terne pitagoriche sono così generate.

**Teorema 7.4** *[Terne pitagoriche.] Sia $(x, y, z)$ una terna pitagorica primitiva (con $y$ pari). Allora esistono degli interi positivi $m, n$ tali che $(x, y, z) = (n^2 - m^2, 2mn, n^2 + m^2)$.* [13]

Dimostrazione. Notiamo che, essendo $y$ ed essendo $(x, y, z)$ una terna primitiva, $x$ e $z$ saranno dispari. Scriviamo la relazione pitagorica nella forma $x^2 = z^2 - y^2 = (z + y)(z - y)$. Osserviamo che $z + y$ e $z - y$ sono coprimi ed entrambi dispari. Infatti un eventuale numero primo $p$ che li divida entrambi, deve dividere sia la loro somma sia la loro differenza: ossia $p|2z$ e $p|2y$. Se $p|2z$, allora $p|2$ oppure $p|z$ (vedi teorema 5.1): ma $p \not| 2$ (visto che $z + y$ e $z - y$ sono dispari), perciò $p|z$. Allo stesso modo, da $p|2y$, segue che $p|y$. Pertanto, se $p|z+y$ e $p|z-y$, allora $p|z$ e $p|y$: in tal caso si avrebbe anche $p|x$ (vedi l'esercizio 7.14) e la terna non sarebbe primitiva. Segue che nessun numero primo divide $z + y$ e $z - y$, i quali sono dunque coprimi.
Nell'uguaglianza $x^2 = (z+y)(z-y)$ un quadrato è scritto come prodotto di due numeri coprimi: ne deriva che ciascuno di tali numeri (dispari) è a sua volta un quadrato (vedi l'esercizio 5.17). Sia $z + y = a^2$ e $z - y = b^2$ $(a > b)$, da cui $2z = a^2+b^2$ e $2y = a^2-b^2 = (a+b)(a-b)$. Si noti che $a+b$ e $a-b$ sono entrambi pari (somma e differenza di numeri dispari): poniamo $a + b = 2n$ e $a - b = 2m$ $(m < n)$, ossia $a = n + m$ e $b = n - m$. Quindi, $2y = (2m)(2n) = 4mn$ (cioè $y = 2mn$) e $2z = (n + m)^2 + (n - m)^2$ (cioè $z = n^2 + m^2$). Infine, $x^2 = z^2 - y^2 = (n^2 + m^2)^2 - (2mn)^2 = (n^2 - m^2)^2$ (cioè $x = n^2 - m^2$). □

**Teorema 7.5** *Siano $m < n$ interi positivi.*

- *$(n^2 - m^2, 2mn, n^2 + m^2)$ è una terna pitagorica.*
- *Se $m$ e $n$ sono coprimi e inoltre $m + n$ è dispari (ossia $m$ e $n$ sono uno pari e uno dispari), allora $(n^2 - m^2, 2mn, n^2 + m^2)$ è una terna pitagorica primitiva.*

**Esercizio 7.15** Dimostrare il teorema 7.5.

**Esercizio 7.16** Dimostrare che un triangolo rettangolo con lati interi ha area intera.

**Esercizio 7.17** Dimostrare che:

- se in una terna pitagorica ci sono due lati che differiscono di 1, allora la terna è primitiva;
- esistono infinite terne pitagoriche dove ci sono due lati che differiscono di 1.

**Esercizio 7.18** Dimostrare che ogni intero maggiore di 2 figura come cateto in almeno una terna pitagorica.

[13] Le terne pitagoriche sono dunque date da tutti e soli i numeri della forma $(k \cdot (n^2 - m^2), k \cdot 2mn, k \cdot (n^2 + m^2))$, dove $k$ è un intero positivo.

**Esercizio 7.19** Dimostrare che:

- ogni quadrato maggiore di $1$ figura come cateto in almeno una terna pitagorica primitiva;
- ogni quadrato di un numero primo figura come cateto precisamente in una terna pitagorica primitiva.

**Esercizio 7.20** Dimostrare che in ogni terna pitagorica c'è un lato multiplo di $3$.

**Esercizio 7.21** Dimostrare che in ogni terna pitagorica c'è un lato multiplo di $3$.

**Esercizio 7.22** Dimostrare che ogni intero positivo può appartenere solo ad un numero finito di terne pitagoriche.

**Esercizio 7.23** Dimostrare che i numeri primi del tipo $4n + 3$, per $n \in \mathbb{N}$, non figurano come ipotenusa in nessuna terna pitagorica.

**Esercizio 7.24** Dimostrare che, in un triangolo rettangolo con lati interi, i raggi dei cerchi inscritti e dei tre cerchi ex-inscritti sono interi.

# 8 Postulati per l'aritmetica.

Abbiamo dimostrato un certo numero di proposizioni, che nell'insieme formano il nucleo dell'aritmetica di base. Tuttavia non abbiamo mai specificato le assunzioni iniziali. A partire da quali postulati ci stiamo muovendo?

Intanto, occorre sottolineare un punto fondamentale. In un certo senso, non è la teoria a *discendere* dai postulati, ma in qualche modo il contrario. La scelta dei postulati dovrà essere tale da poterne dedurre la trama di proposizioni viste nelle sezioni precedenti. Procediamo dunque dalla teoria ai postulati. In effetti, non accade mai che si stabiliscano dei postulati in maniera arbitraria, totalmente ignari delle loro conseguenze (da ricavarsi poi nel seguito). Accade semmai che, tenendo presente una teoria già sviluppata, ricca di connessioni al proprio interno o anche con altre teorie, si miri ad individuare un insieme di postulati e una sistemazione dei suoi primi elementi che permettano di ricostruirne logicamente i tratti salienti a partire da tali assunzioni. Così facendo, è poi vero che si porta avanti un'opera di chiarimento dei concetti e delle loro mutue relazioni che, a sua volta, può rafforzare la correttezza e la portata delle deduzioni.

Per queste ragioni questa sezione si trova alla fine e non all'inizio: ci sforziamo di vedere i postulati come traguardo, non solo come punto di partenza. Un traguardo che consiste appunto nell'individuare un'idonea base di partenza.

Curiosamente (ma forse non troppo), solo dagli ultimi decenni dell'ottocento si è avvertita l'esigenza di una chiara assiomatizzazione dell'aritmetica. In precedenza (anche in Euclide, che pure aveva introdotto assiomi e postulati per la geometria) le dimostrazioni aritmetiche finivano per poggiare su una serie di assunzioni implicite o intuitive, la cui verità doveva forse apparire non bisognosa di apposite assunzioni.

Com'è naturale, si possono individuare diverse maniere di assiomatizzare l'aritmetica [14]. In generale, quando si enunciano dei postulati per una teoria, si tende a ridurre il numero il più possibile. Si preferisce che i postulati assunti siano tra loro *indipendenti*: nel senso che nessuno di essi dovrebbe essere dimostrabile a partire dagli altri (essere, cioè, un teorema). Infatti, un postulato che fosse in realtà un teorema sarebbe superfluo in quanto postulato: anzi, la sua presenza tenderebbe a tenere nascosta la rete di deduzioni che lo ricollega agli altri. Ma proprio nella comprensione delle più varie reti deduttive consiste l'attività matematica. Per portare le cose all'estremo: se assumessimo l'*intera* teoria come postulato (magari dopo averne verificato le proposizioni in molti casi particolari), a quel punto non resterebbe più nulla da dimostrare. Quand'anche l'intera teoria si rivelasse in qualche senso "giusta", a quel punto non sarebbe più una teoria *matematica*: verrebbe per così dire svuotata. La matematica non consi-

[14] Sebbene, in un certo senso, nessuna di esse sia *del tutto* soddisfacente.

ste nel produrre affermazioni *giuste*: consiste semmai nel cercare di dimostrare delle affermazioni a partire da altre.

Ciò detto, non è di per sé indispensabile che i postulati assunti siano, tutti e sempre, mutuamente indipendenti. In certi casi può comunque essere comodo assumere un insieme di postulati lievemente ridondanti, senza che ne derivi alcun danno serio (per quanto sia sempre utile ed interessante mettere in luce l'eventuale dimostrabilità di uno dei postulati) [15] Ciò che davvero è capitale è che i postulati siano quantomeno coerenti, ossia che non diano luogo a contraddizioni.

Nel caso dell'aritmetica, le prime vere e proprie sistemazioni assiomatiche risalgono a Richard Dedekind e Giuseppe Peano (1889). Quest'ultimo fornì una lista di 5 postulati per i numeri naturali, a partire dai quali è possibile ricostruire tutti i numeri, definire le abituali operazioni e l'ordinamento, dmostrarne le usuali proprietà, fino a ricavare i fatti più familiari dell'aritmetica dei numeri naturali. A quel punto si possono *definire* i numeri interi relativi e, andando avanti, i numeri razionali e i reali.

In questa occasione preferiamo invece partire direttamente dai numeri interi relativi e dalle loro operazioni, assumendone le proprietà come postulati. Faremo un accenno agli assiomi di Peano in seguito.
Postulati per $\mathbb{Z}$. Nei numeri interi, ci sono degli elementi $0$ e $1$, e sono definite delle operazioni, dette *addizione* (indicata con $+$) e *moltiplicazione* (indicata con $\cdot$), ed una relazione di ordinamento (indicata con $<$), che soddisfano le seguenti proprietà:

- A.0 $0$ è elemento neutro per l'addizione [ossia: $n+0 = 0+n = n$, qualunque sia l'intero $n$];
- A.COM vale la legge commutativa per l'addizione [ossia: $m + n = n + m$, qualunque siano gli interi $m, n$];
- A.ASS vale la legge associativa per l'addizione [ossia: $(m + n) + p = m + (n + p)$, qualunque siano gli interi $m, n, p$];
- A.OPP per ogni intero $n$, esiste un elemento $(-n)$ (detto *opposto* di $n$) tale che $n + (-n) = (-n) + n = 0$;
- M.1 $1$ è elemento neutro per la moltiplicazione [ossia: $n \cdot 1 = 1 \cdot n = n$, qualunque sia l'intero $n$];
- M.COM vale la legge commutativa per la moltiplicazione [ossia, $m \cdot n = n \cdot m$, qualunque siano gli interi $m, n$];

[15] D'altra parte, dimostrare l'effettiva indipendenza di un dato insieme di postulati non è ovvio. In genere si tratta di far vedere che esistono dei sistemi di oggetti che rispettano determinati postulati ma non altri: cosa non sempre agevole.

- M.ASS vale la legge associativa per la moltiplicazione [ossia, $(m \cdot n) \cdot p = m \cdot (n \cdot p)$, qualunque siano gli interi $m, n, p$];
- DIST vale la legge distributiva [ossia, $(m+n) \cdot p = (m \cdot p) + (n \cdot p)$, qualunque siano gli interi $m, n, p$];
- O.01 si ha $0 < 1$ e non esistono interi $n$ con $0 < n < 1$;
- O.TRA vale la proprietà transitiva per l'ordinamento [ossia: se $m < n$ e $n < p$, allora $m < p$, qualunque siano gli interi $m, n, p$];
- O.TRI vale la legge di tricotomia per l'ordinamento [ossia: per $m, n$ interi, vale una ed una soltanto tra le alternative $m < n$, $m = n$, $n < m$];
- O.MON l'ordinamento gode della proprietà di monotonia reispetto all'addizione [ossia: per $m < n$, si ha $m + p < n + p$, qualunque siano gli interi $m, n, p$].

A questi postulati dovremmo anche aggiungere alcuni postulati che regolino l'uso del simbolo di uguaglianza ed i postulati di deduzione logica (che permettono di ricavare una proposizione a partire a partire da altre proposizioni). Non elenchiamo tutti questi postulati per il motivo che essi corrispondono alle regole di corretto ragionamento comunemente accettate e le assumiamo in maniera implicita.
Le assunzioni fatte bastano a ritrovare molti dei fatti più familiari sui numeri interi e le abituali regole di calcolo. Vediamo una breve rassegna.

**Teorema 8.1** [L'elemento 0 assorbe il prodotto.] *Per ogni intero $n$ si ha $n \cdot 0 = 0 \cdot n = 0$.*

Dimostrazione. Si ha infatti $n \cdot 0 = n \cdot ((1+1) \cdot 0)$, dal momento che $(1+1) \cdot 0 = 1 \cdot 0 + 1 \cdot 0$ (legge distributiva) e $1 \cdot 0 + 1 \cdot 0 = 0 + 0$ (1 è elemento neutro per $\cdot$) e $0 + 0 = 0$ (0 è elemento neutro per $+$).
Perciò $n \cdot 0 = n \cdot ((1+1) \cdot 0) = (n \cdot (1+1)) \cdot 0$ (legge associativa per $\cdot$) e quindi $n \cdot 0 = (n \cdot 1 + n \cdot 1) \cdot 0 = (n+n) \cdot 0 = n \cdot 0 + n \cdot 0$.
Dall'uguaglianza $n \cdot 0 = n \cdot 0 + n \cdot 0$, sommando ad ogni membro il numero $-(n \cdot 0)$ segue $-(n \cdot 0) + n \cdot 0 = -(n \cdot 0) + n \cdot 0 + n \cdot 0$, ossia $0 = n \cdot 0$. □

**Esercizio 8.1** Sistemare *tutti* i dettagli ed i passaggi della dimostrazione del teorema 8.1.

**Esercizio 8.2** [Concellazione della somma.] Dimostrare che, se $a + b = a + b'$, allora $b = b'$.

**Esercizio 8.3** [Unicità dell'opposto.] Dimostrare che, per ogni intero $n$, esiste un unico intero $n'$ tale che $n + n' = 0$.

**Esercizio 8.4** Dimostrare che, per ogni intero $n$, si ha $-(-n) = n$.

**Esercizio 8.5** Dimostrare che $-0 = 0$.

**Teorema 8.2** *Per ogni intero $n$ si ha $(-1) \cdot n = (-n)$.*

Dimostrazione. Intanto è importante comprendere con chiarezza che cosa c'è scritto: moltiplicando per $(-1)$ (l'opposto di 1) un qualsiasi intero, si ottiene l'opposto dell'intero. La tesi, visto l'esercizio 8.3, è dunque che $n + (-1) \cdot n = 0$. Questo è vero, infatti $n + (-1) \cdot n = 1 \cdot n + (-1) \cdot n = (1 + (-1)) \cdot n$. Ora, $1 + (-1) = 0$ per definizione e $0 \cdot n = 0$ per il teorema 8.1. □

**Esercizio 8.6** Dimostrare che $(-1) \cdot (-1) = 1$.

**Esercizio 8.7** Dimostrare che, per $m, n$ interi qualsiasi, si ha: $(-m) \cdot n = -(m \cdot n)$ e $(-m) \cdot (-n) = m \cdot n$.

**Esercizio 8.8** Dimostrare che, per ogni intero $n$, si ha $n < n + 1$.

**Esercizio 8.9** Dimostrare che, per ogni intero $n$, non ci sono interi compresi tra $n$ e $n + 1$.

Ciò equivale al fatto, ben familiare, che i numeri interi si succedono in maniera cosiddetta *discreta*: ogni intero $n$ ha un predecessore immediato $(n - 1)$ ed un successore immediato $(n + 1)$.

**Esercizio 8.10** Dimostrare che non esiste un massimo numero intero.

**Teorema 8.3** *Per ogni $m, n$, se $0 < m$ e $0 < n$, allora $0 < m + n$.*

Dimostrazione. Da $0 < n$ segue $m < m + n$ (uno dei postulati) e da $0 < m$ e $m < m + n$ segue $0 < m + n$ (postulato di transitività). □

Nel seguito chiameremo, come si fa di solito, *positivi* gli interi $n$ tali che $0 < n$ e *negativi* gli interi $n$ per i quali $n < 0$. Per esempio 1 è positivo per postulato. Indicheremo, al solito, con $\mathbb{N}$ l'insieme degli interi non negativi. Inoltre impiegheremo indistintamente le notazioni $a < b$ e $b > a$.

**Esercizio 8.11** Dimostrare che la somma di due numeri negativi è un numero negativo.

**Teorema 8.4** *L'insieme dei numeri naturali $\mathbb{N}$ è infinito.*

La dimostrazione dell'infinità di un insieme quando ancora non si dispone di una teoria compiuta dei numeri naturali è piuttosto delicata. La tentazione di servirsi intuitivamente di elencazioni del tipo $a_1, a_2, ...$ è sempre in agguato, ma occorre evitarla. Tuttavia, non è necessario avere già introdotto i numeri naturali per caratterizzare gli insiemi finiti e quelli infiniti (ciò richiede però

che si sia già in qualche modo sviluppata una sufficiente teoria degli insiemi...). Sono infatti infiniti tutti e soli quegli insiemi $X$ per i quali esiste una funzione iniettiva e non suriettiva $X \to X$. È sufficiente questa caratterizzazione per dimostrare i fatti di base riguardanti gli insiemi finiti ed infiniti: per esempio che l'unione di due insiemi finiti è un insieme finito o che un insieme contenente un insieme infinito è a sua volta infinito.

Dimostrazione del teorema 8.4. Consideriamo la funzione $\mathbb{N} \to \mathbb{N}$ definita da $f(n) = n + 1$. Essa è iniettiva (infatti da $n + 1 = n' + 1$ segue $n = n'$) e non suriettiva (infatti $f(n) \neq 0$ per tutti gli $n \in \mathbb{N}$). Pertanto l'insieme $\mathbb{N}$ è infinito.□

**Teorema 8.5** *Se $n$ è positivo, allora $(-n)$ è negativo, e viceversa.*

Dimostrazione. Se $n > 0$ allora sicuramente $(-n) \neq 0$ (vedi gli esercizi 8.3 e 8.5). Se fosse anche $(-n) > 0$, seguirebbe che $n + (-n) > 0$, ossia $0 > 0$ (assurdo). Per la legge di tricotomia, si conclude che $(-n) < 0$. Per il viceversa si ragiona allo stesso medo. □

Avendo stabilito per postulato la positività di 1, si ha dunque $(-1) < 0$.

**Esercizio 8.12** Siano $m < n$ degli interi positivi. Dimostrare che:

- $(-m) + n = n - m$ (che è positivo);
- $m + (-n) = -(n - m)$ (che è negativo);
- $(-m) + (-n) = -(m + n)$ (che è negativo).

Vorremmo almeno ritrovare le regole di calcolo più abituali: per esempio le regole dei segni nei prodotti. Per quanto riguarda le somme, ci siamo giè riusciti (vedi l'esercizio 8.12). Anche per i prodotti non sembra mancare molto (vedi il teorema 8.2 e gli esercizi 8.6 e 8.7). Ma, per come abbiamo presentato le cose, non è ancora del tutto chiarito che il prodotto di due numeri positivi sia positivo. Ovviamente, sarebbe lecito prendere questo fatto come postulato, ma può essere invece molto istruttivo cercare di dimostrarlo sulla base di quanto assunto finora.

**Esercizio 8.13** Assumendo che il prodotto di due numeri positivi sia sempre positivo, far vedere -senza impiegare il postulato O.01- che:

- che 1 è positivo;
- che $n^2 \geqslant 0$, qualunque sia l'intero $n$;
- che, se $a \cdot b = 0$, allora $a = 0$ oppure $b = 0$.

**Esercizio 8.14** Cercare di dimostrare dai postulati stabiliti per $\mathbb{Z}$ che il prodotto di due interi positivi è positivo.

In effetti, non è difficile far vedere che alcuni specifici prodotti di numeri positivi sono sono positivi. Per esempio: $2 \cdot 3 = 2 \cdot (1+1+1) = (2 \cdot 1) + (2 \cdot 1) + (2 \cdot 1)$ per la proprietà distributiva [sistemare i dettagli...]. Inoltre $2 \cdot 1 = 1 + 1 > 0$ (vedi il teorema 8.3). Pertanto $2 \cdot 3 > 0$ sempre per il teorema 8.3, essendo somma di numeri positivi.

Se si cerca di generalizzare questa dimostrazione ad un qualsiasi (imprecisato) prodotto $m \cdot n$, ci si trova però in difficoltà. Dovremmo immaginare, come in effetti si immagina normalmente, il prodotto $m \cdot n$ come " somma ripetuta" per $n$ volte dell'addendo $m$. Il problema è nel significato da attribuire all'espressione "$n$ volte": stiamo infatti cercando di scrivere un sistema di assiomi per i numeri interi, non possiamo quindi dare come già acquisita una *idea intuitiva* di numero intero!

Il ragionamento che ci piacerebbe poter fare, per dimostrare che il prodotto di due interi positivi $m, n$ è positivo, è grossomodo di questo tenore: $m \cdot n = m \cdot ((n-1)+1) = m \cdot (n-1) + m \cdot 1 = m \cdot (n-1) + m$. Ora, abbiamo tre casi:

- se $n - 1 = 0$, allora $m \cdot n = m$ che è per ipotesi positivo;
- se $n - 1 < 0$, in tal caso avremmo $n < 1$, ossia $n$ sarebbe un intero positivo minore di 1 [che non dovrebbero esistere, ma non abbiamo ancora dimostrato che non ce ne sono: forse anche questo va preso per postulato?];
- se invece $n-1 > 0$, se sapessimo che $m \cdot (n-1) > 0$, allora concluderemmo che anche $m \cdot n = m \cdot (n-1) + m$ è positivo (teorema 8.3).
- Pertanto, nel caso $n - 1 > 0$, immaginiamo di procedere come prima: $m \cdot (n-1) = m \cdot (n-2) + m$. Ancora, abbiamo tre casi possibili $n - 2 = 0$ (e allora tutto si sistema), $n-2 < 0$ (che vorremmo poter escludere, poiché significherebbe $1 < n < 2$), $n - 2 > 0$ (e allora...)...

L'idea sarebbe che, partendo da qualsiasi intero positivo $n$, a furia di sottrarre 1, prima o poi si dovrà trovare 0. Possiamo dimostrare questo a partire dai postulati che abbiamo elencato? Provarci può essere interessante [16]. Forse conviene assumere come postulato che il rpodotto di interi positivi sia positivo? È senz'altro una possibilità, da non scartare immediatamente.

Per adesso accantoniamo la questione, immaginando di averla in qualche maniera risolta (avendo cioè dimostrato o accettato cme assioma che il prodotto di due interi positivi è positivo).

**Esercizio 8.15** Assumiamo il fatto che il prodotto di due interi positivi sia positivo. Dimostrare che:

[16] Ma non ci sono possibilità di riuscita. Consideriamo ad esempio $\mathbb{Z}[i]$ (dove $\mathbb{Z}$ indica ciò che "abitualmente" si intende essere $\mathbb{Z}$), con la somma e il prodotto usuali e con l'ordinamento definito da $x + yi < x' + y'i$ se $y < y'$ oppure $y = y'$ e $x < x'$. Con queste definizioni si avrebbe $i > 0$ ma $i \cdot i = -1 < 0$. Si osservi che si avrebbe inoltre $n < i$ per ogni numero intero $n$ (nel senso "abituale") e che, sottraendo ripetutamente 1 da $i$, non si otterrà mai 0.

- se vale $a < b$ e $k$ è positivo, allora $ka < kb$;
- se $a, b$ sono interi positivi, allora $ab \geqslant a$ e $ab \geqslant b$;
- se $m, n$ sono interi positivi e $m|n$, allora $m \leqslant n$.

Ma neanche assumere per postulato la positività del prodotto di interi positivi basterebbe a chiudere la questione. Con un minimo di pazienza, riusciremmo a costruire ulteriori esempi di sistemi in grado di verificare tutte queste assunzioni, compresa quest'ultima, senza tuttavia corrispondere a ciò che in effetti intendiamo quando ci riferiamo ai "veri" numeri interi.

**Esempio 8.1** Consideriamo l'insieme $\mathbb{Z}[t]$ dei polinomi in una indeterminata $t$, a coefficienti nell'insieme $\mathbb{Z}$ dei "veri" numeri interi. Definiamo le operazioni nei modi usuali per i polinomi. Definiamo inoltre *positivo* un elemento $p(t) \in \mathbb{Z}[t]$ se il suo termine di grado massimo abbia coefficiente positivo (nel senso abituale), e definiamo $a(t) < b(t)$ se $a(t) - b(t)$ è un elemento *positivo*. È possibile verificare che:

- per l'insieme $Z[t]$, con queste operazioni e questo ordinamento, soddisfa tutti i postulati elencati per i numeri interi;
- se $a(t), b(t) \in \mathbb{Z}[t]$ sono *positivi*, anche $a(t) \cdot b(t)$ è *positivo*;
- non esistono in $\mathbb{Z}[t]$ elementi compresi tra 0 e 1.

**Esercizio 8.16** Dimostrare le affermazioni contenute nell'esempio 8.1.

Un esempio come 8.1 rende chiaro che, per catturare l'effettiva fisionomia dei numeri interi, manca qualcos'altro ancora. A ben guardare, cosa c'è di "aberrante", di veramente *inaccettabile*, che ha luogo nell'esempio 8.1? Accade che, procedendo a passi di 1 a partire da 0 non si giungerà mai (per esempio) all'elemento $t$. Come anche, partendo da $t$, non si giungerà mai a passi di 1 all'elemento $t^2$, e così via. Vi sono infinite parti per così dire "sconnesse". O anche, detto in altro modo, accade che ci siano elementi tra i quali sono compresi infiniti altri elementi (per esempio tra 0 e $t$). Ecco il punto cruciale: sommando ripetutamente il numero 1 si devono ottenere *tutti* gli interi positivi, senza che ne rimanga qualcuno inaccessibile. Questa proprietà è usualmente nota come *principio d'induzione* e può presentarsi in varie forme. A questo proposito, torna comodo dare alcune definizioni.

**Definizione 8.1** Sia $\mathsf{K} \subseteq \mathbb{N}$:

- K si dice *induttivo* se $k + 1 \in \mathsf{K}$ per ogni $k \in \mathsf{K}$;
- K si dice *induttivo in senso forte* se, per ogni numero naturale $n$, si ha $n \in \mathsf{K}$ qualora sia abbia $n' \in \mathsf{K}$ per tutti i numeri naturali $n' < n$.

**Teorema 8.6** *Assumendo i postulati già enunciati per $\mathbb{Z}$, le seguenti proposizioni risultano equivalenti:*

- ① [principio del minimo] *ogni sottoinsieme non vuoto di $\mathbb{N}$ possiede un elemento minimo;*
- ② [principio d'induzione] *se $\mathsf{A}$ è un sottoinsieme induttivo di $\mathbb{N}$ con $0 \in \mathsf{A}$, allora $\mathsf{A} = \mathbb{N}$;*
- ③ [induzione forte] *se $\mathsf{B} \subseteq \mathbb{N}$ è induttivo in senso forte, allora $\mathsf{B} = \mathbb{N}$;*
- ④ [discesa infinita] *per nessuna coppia di numeri naturali $a, b$ l'intervallo $(a, b)$ contiene infiniti elementi.*

Dimostrazione. Vediamo come è possibile concatenare queste proposizioni.

- ① $\Leftrightarrow$ ③
  Assumiamo ① e dimostriamo ③.
  Sia $\mathsf{B}$ un sottoinsieme di $\mathbb{N}$ tale che, se tutti i numeri naturali minori di $k$ appartengono a $\mathsf{B}$, anche $k \in \mathsf{B}$) (qualunque sia $k \in \mathbb{N}$). Supponiamo -per assurdo- che $\mathsf{B}$ non coincida con $\mathbb{N}$. Sia quindi $\tilde{\mathsf{B}}$ l'insieme (non vuoto) dei numeri naturali non contenuti in $\mathsf{B}$. Per ①, l'insieme $\tilde{\mathsf{B}}$ possiede un minimo $m$. Risulta $m > 0$ dal momento che necessariamente $0 \in \mathsf{B}$ (non essendoci alcun numero naturale minore di 0, è senz'altro vero che ogni numero naturale minore di 0 appartiene a $\mathsf{B}$: dunque 0 deve appartenere a $\mathsf{B}$). Ora, tutti i numeri naturali $m' < m$ appartengono a $\mathsf{B}$ (essendo $m$ il minimo numero naturale che non appartiene a $\mathsf{B}$). Ma allora, per la caratteristica di $\mathsf{B}$, anche $m \in \mathsf{B}$: contraddizione.

  Ora assumiamo ③ e dimostriamo ①.
  Sia $\mathsf{S}$ un sottoinsieme non vuoto di $\mathbb{N}$: vogliamo vedere che in $\mathsf{S}$ c'è un elemento minimo. Supponiamo -per assurdo- che non ci sia: vale a dire che, per ogni $s \in \mathsf{S}$, esista $s' \in \mathsf{S}$ con $s' < s$. Segue che $0 \notin \mathsf{S}$, non esistendo numeri naturali minori di 0 (il quale sarebbe perciò il minimo di $\mathsf{S}$). Sia dunque $\tilde{\mathsf{S}}$ il complementare di $\mathsf{S}$ in $\mathbb{N}$, ossia l'insieme dei numeri naturali non appartenenti a $\mathsf{S}$. Per quanto visto, $0 \in \tilde{\mathsf{S}}$. Sia adesso $k \in \mathbb{N}$, tale che, per ogni numero naturale $k' < k$, risulti $k' \in \tilde{\mathsf{S}}$. Allora anche $k \in \tilde{\mathsf{S}}$: altrimenti si avrebbe $k \in \mathsf{S}$ e $k$ sarebbe dunque il minimo elemento di $\mathsf{S}$ (dal momento che nessun numero naturale minore di $k$ sta in $\mathsf{S}$). L'insieme $\tilde{\mathsf{S}}$ ha perciò le proprietà previste nella condizione ③: quindi $\tilde{\mathsf{S}} = \mathbb{N}$ e $\mathsf{S} = \varnothing$: contraddizione. □

- ① $\Leftrightarrow$ ②
  Assumiamo ① e dimostriamo ②.
  Sia $\mathsf{A}$ un sottoinsieme induttivo di $\mathbb{N}$ contenente 0. Supponiamo -per assurdo- che sia $\mathsf{A} \neq \mathbb{N}$. In tal caso, indicato con $\tilde{\mathsf{A}}$ il complementare di $\mathsf{A}$ in $\mathbb{N}$, si ha $\tilde{\mathsf{A}} \neq \varnothing$. Per la proprietà ①, in $\tilde{\mathsf{A}}$ c'è un elemento minimo $m$.

Deve essere $m > 0$, dato che $0 \in \mathsf{A}$. Quindi $m-1 \in \mathbb{N}$ e inoltre $m-1 \in \mathsf{A}$, essendo $m$ il minimo elemento fuori da $\mathsf{A}$. Ma allora $(m-1)+1 \in \tilde{\mathsf{A}}$, poiché $\tilde{\mathsf{A}}$ è un insieme induttivo. Vale a dire $m \in \tilde{\mathsf{A}}$: contraddizione.

Ora assumiamo ② e dimostriamo ①.
Sia $\mathsf{X}$ un sottoinsieme non vuoto di $\mathbb{N}$ e sia $\mathsf{Y} = \{y | \exists x \in \mathsf{X} \,\text{con}\, y \geqslant x\}$, ossia l'insieme degli interi maggiori o uguali ad almeno un elemento di $\mathsf{X}$. Dato che $\mathsf{X} \subseteq \mathsf{Y}$, anche $\mathsf{Y}$ non è vuoto. Per come è costruito, se $y \in \mathsf{Y}$ anche tutti gli interi maggiori di $y$ appartengono a $\mathsf{Y}$; se $y' \notin \mathsf{Y}$ nessun intero minore di $y'$ appartiene a $\mathsf{Y}$. Vogliamo far vedere che $\mathsf{Y}$ ha un elemento minimo. Supponiamo -per assurdo- che $\mathsf{Y}$ non abbia elemento minimo: ossia che, per ogni $y \in \mathsf{Y}$, esista $y' \in \mathsf{Y}$ con $y' < y$. Segue che $0 \notin \mathsf{Y}$. Sia dunque $\tilde{\mathsf{Y}}$ l'insieme dei numeri naturali non appartenenti a $\mathsf{Y}$. Per quanto visto, $0 \in \tilde{\mathsf{Y}}$. Ora, per ogni $k \in \tilde{\mathsf{Y}}$, anche $k+1 \in \tilde{\mathsf{Y}}$. Infatti, se fosse $k+1 \notin \tilde{\mathsf{Y}}$ (cioè $k+1 \in \mathsf{Y}$), l'intero $k+1$ verrebbe ad essere il minimo elemento di $\mathsf{Y}$, dal momento che nessun elemento minore o uguale a $k$ può stare in $\mathsf{Y}$ e che, come si è visto sopra, non ci sono interi tra $k$ e $k+1$. Ne deriva che $k+1 \in \tilde{\mathsf{Y}}$, qualunque sia $k \in \tilde{\mathsf{Y}}$: ossia $\tilde{\mathsf{Y}}$ è un sottoinsieme induttivo di $\mathbb{N}$ contenente 0. In base a ②, $\tilde{\mathsf{Y}} = \mathbb{N}$ e quindi $\mathsf{Y} = \varnothing$, contro l'ipotesi fatta.
Concludiamo che $\mathsf{Y}$ possiede un elemento minimo $m$: tale $m$ sarà il minimo anche di $\mathsf{X}$ (giacché per ogni elemento $y \in \mathsf{Y}$ esiste un elemento $x \in \mathsf{X}$ con $x \leqslant y$, ma tale $x$ appartiene anche a $\mathsf{Y}$ visto che $\mathsf{X} \subseteq \mathsf{Y}$). □

- ① ⇒ ④
  Ora assumiamo ① e dimostriamo ④.
  Supponiamo -per assurdo- che l'intervallo di numeri naturali $(a, b)$contenga infiniti elementi. Allora anche l'intervallo $[0, b)$ contiene infiniti elementi. Sia $\mathsf{M}$ l'insieme di tutti quei numeri naturali $n$ tali che l'intervallo $[0, n)$ contiene infiniti elementi. Dato che $b \in \mathsf{M}$, l'insieme $\mathsf{M}$ non è vuoto. Per ①, in $\mathsf{M}$ c'è un elemento minimo $m$: perciò $[0, m)$ risulta infinito, mentre $[0, m-1)$ è finito. Ma, siccome $[0, m) = [0, m-1) \cup [m-1, m)$ e poiché $[m-1, m) = \{m-1\}$, questo significherebbe che anche $[0, m)$ dovrebbe essere finito (assurdo). □

- ④ ⇒ ②
  Ora assumiamo ④ e dimostriamo ②.
  Supponiamo -per assurdo- che non valga ②. Ciò significa che esiste un sottoinsieme induttivo $\mathsf{A}$ di $\mathbb{N}$ contenente 0 e non coincidente con $\mathbb{N}$: vale a dire che esiste un elemento $a \in \mathbb{N}$ tale che $a \notin \mathsf{A}$. Dobbiamo capire come potrebbe essere collocato l'elemento $a$ rispetto ad $\mathsf{A}$. Osserviamo prima di tutto che qualunque insieme induttivo è infinito (si può riadattare il ragionamento già impiegato per dimostrare il teorema 8.4). Si noti inoltre che, per quello che abbiamo provato sopra (① ⇒ ②), nell'insieme $\mathsf{A}$

vale il principio del minimo: ogni sottoinsieme non vuoto di A possiede un elemento minimo. Vorremmo mostrare che $a$ deve essere maggiore di ogni elemento di A. In caso contrario, supponendo che esista $n \in \mathsf{A}$ con $a \leqslant n$, si potrebbe considerare l'insieme (non vuoto) $\mathsf{M} = \{m \in \mathsf{A} |\, a \leqslant m\}$ degli elementi di A non minori di $a$. Detto $m'$ l'elemento minimo di M, si avrebbe $m' - 1 < a \leqslant m'$, dunque $a = m' \in \mathsf{A}$: contro l'ipotesi fatta. Pertanto $a$ è maggiore di qualsiasi elemento di A, vale a dire $\mathsf{A} \subseteq [0, a)$ e quindi $[0, a)$, contenendo un insieme infinito, è infinito (come anche l'intervallo $(0, a)$, che differisce da $[0, a)$ per un solo elemento). □

**Esercizio 8.17** Far vedere, per ciascuna delle condizioni equivalenti enunciate nel teorema 8.6, che l'insieme $\mathbb{Z}[t]$ non la rispetta.

**Esercizio 8.18** Mostrare che, assumendo il principio d'induzione nella forma ②, sarebbe possibile dimostrare che non vi sono interi compresi tra 0 e 1, senza assumerlo per postulato.

**Esercizio 8.19** Assumendo il principio d'induzione, dimostrare che:

- se A è un insieme di numeri interi contenente un intero $M$ e tale che $n+1 \in \mathsf{A}$ per ogni $n \in \mathsf{A}$, allora A contiene tutti gli interi maggiori o uguali a $M$;
- se B è un insieme di numeri interi contenente un intero $M$ e tale che $n-1 \in \mathsf{B}$ per ogni $n \in \mathsf{B}$, allora B contiene tutti gli interi minori o uguali a $M$.

Aggiungiamo dunque ai postlati il principio d'induzione, in una delle forme indicate nel teorema 8.6. L'enunciato ② è forse il più abituale e la sua assunzione permette tra l'altro, come appena visto, di eliminare una parte del postulato O.01.

Una volta ammesso anche il principio d'induzione tra i postulati, si ritrovano agevolmente i risultati più familiari dell'aritmetica. Il principio d'induzione afferma, in un certo senso, la *minimalità* di $\mathbb{N}$ rispetto alle sue proprietà. Esso taglia via ogni possibile coda successiva alla catena $1, 2, 3, ...$ e garantisce che tutti gli interi positivi siano raggiungibili a partire da 0 attraverso un "numero finito" di passi di lunghezza 1.

Questo postulato contiene tuttavia aspetti alquanto problematici. Esso finisce per chiamare in gioco la nozione di *insieme* (nella forma "qualunque sia il sottoinsieme A..."): una nozione di per sé esterna -e più generale- rispetto al sistema dei numeri interi che si vorrebbe descrivere. Vorremmo evitare che ciò accadesse. Preferiremmo per la teoria dei numeri un elenco di postulati del tutto autosufficienti, nei quali fossero menzionati solo gli oggetti descritti nella teoria (ossia i numeri interi), senza rimandi a nozioni o teorie preesistenti teorie. Questo obiettivo è stato a lungo perseguito nei primi decenni del '900,

fino alla scoperta (grazie ai risultati di Kurt Gödel) di ragioni profonde che impediscono di raggiungere un simile intento. Se ci vuole limitare ad enunciare postulati aritmetici in senso stretto, allora bisogna accontentarsi di versioni più deboli del principio d'induzione. Simili scelte generano versioni indebolite dell'aritmetica, che non corrispondono in pieno a quanto si vorrebbe comunemente intendere quando ci si riferisce ai numeri interi, dove non tutte le proposizioni aritmetiche vere sono effettivamente dimostrabili [17]. Da ciò consegue di dover scegliere tra un'assiomatizzazione non del tutto esauriente (che poi non basta a ricavare tutte le proposizioni vere) e il doversi poggiare su una nozione esterna e molto generale come quella di insieme (a sua volta bisognosa di una descrizione assiomatica). Le cose sembrano sfuggire dalle dita. Le assiomatizzazioni che possiamo realizzare sono *in buona sostanza* soddisfacenti, *ma non del tutto*.

Solo alcune parole di commento sulla scelta dei postulati. Anziché introdurre direttamente i numeri interi relativi (con operazioni e ordinamento), si sarebbe potuti partire dalla successione dei numeri naturali (appunto dotati di una funzione "successore"). Si tratta dei cosiddetti *assiomi di Peano*, il cui -assai frugale- contenuto merita di essere esaminato.

Assiomi di Peano per $\mathbb{N}$. Nei numeri naturali è contenuto un elemento $0$ ed è definita una funzione $s$ [18] tali che:

- $\boxed{\text{AP.1}}$ la funzione $\mathsf{s}$ è iniettiva [ossia: se $m \neq n$, allora $\mathsf{s}(m) \neq \mathsf{s}(n)$, qualunque siano i numeri naturali $m, n$];
- $\boxed{\text{AP.2}}$ $\mathsf{s}(n) \neq 0$, qualunque sia il numero naturale $n$;
- $\boxed{\text{AP.3}}$ ogni insieme induttivo [19] di numeri naturali contenente $0$ consiste di tutti i numeri naturali.

In buona sostanza, i primi due postulati garantiscono che, a partire da 0, con la funzione successore si generi una successione infinita che non torna mai su se stessa: $0$, $\mathsf{s}(0)$, $\mathsf{s}(\mathsf{s}(0))$, $\mathsf{s}(\mathsf{s}(\mathsf{s}(0)))$, ... Il postulato $\boxed{\text{AP.3}}$ garantisce che la successione così costruita esaurisce l'intero insieme dei numeri naturali, senza che vi siano parte sconnesse da questa. In questa rappresentazione il numero $n$ viene a essere rappresentato dall'elemento $\mathsf{s}(\mathsf{s}(...(0)...))$, dove l'operatore $\mathsf{s}$ figura appunto $n$ volte.

**Esercizio 8.20** Far vedere che i postulati $\boxed{\text{AP.1}}$, $\boxed{\text{AP.2}}$, $\boxed{\text{AP.3}}$ sono indipendenti: per ciascuno di essi, è possibile costruire un sistema di oggetti nel quale esso non vale mentre gli altri due valgono.

[17] È appunto questo il contenuto dei celebri teoremi di Gödel del 1931. Un esempio di un siffatto enunciato (vero ma non dimostrabile nelle teorie aritmetiche autosufficienti) fu poi costruito da Goodstein nel 1944.

[18] La funzione $\mathsf{s}$ va pensata come la funzione *successore*, vale a dire come $\mathsf{s}(n) = n + 1$. Ancora non abbiamo però a disposizione l'operazione di somma e neppure l'elemento 1: anzi, tali nozioni saranno *definite* proprio a partire da 0 e dalla funzione $\mathsf{s}$.

[19] Disponendo della funzione $\mathsf{s}$, si definisce *induttivo* un insieme $\mathsf{A}$ tale che $\mathsf{s}(a) \in \mathsf{A}$ per ogni $a \in \mathsf{A}$.

Con siffatti postulati, possiamo definire le principali nozioni che intervengono nella toeria dei numeri, comprese le operazioni aritmetiche e l'ordinamento. Per esempio:

- $1 := \mathsf{s}(0)$;
- $n + 0 := n$ e $n + \mathsf{s}(k) := \mathsf{s}(n + k)$;
- $n \cdot 0 := 0$ e $n \cdot \mathsf{s}(m) := (n \cdot m) + m$;
- $a < b$ se $\exists b' : \ a + \mathsf{s}(b') = b$.

Così facendo, è possibile *dimostrare* le varie proprietà delle operazioni e dell'ordinamento, che prima avevamo invece assunto come postulati. Vediamo alcuni esempi.

**Esercizio 8.21** Ammettendo gli assiomi di Peano e le definizioni sopra riportate, dimostrare che neinumeri naturali si ha:

- $1 > 0$;
- per ogni $m \neq 0$, esiste un $a$ tale che $m = \mathsf{s}(a)$;
- per ogni $n$ naturale si ha $n + 0 = 0 + n = n$;
- per ogni $n$ naturale si ha $n \cdot 0 = 0 \cdot n = 0$;
- per ogni $n$ naturale si ha $n + 1 = 1 + n = \mathsf{s}(n)$;
- per ogni $a, b$ si ha $a + \mathsf{s}(b) = \mathsf{s}(a) + b$;
- per ogni coppia $m, n$ si ha $m + n = n + m$;
- se $a + n = b + n$, allora $a = b$;
- per ogni $n$ si ha $0 \leqslant n$;
- non esistono numeri naturali $n$ tali che $0 < n < 1$;
- per ogni $a, b, c$, se $a < b$ e $b < c$ si ha $a < c$;
- se $a < b$, allora $a + n < b + n$;
- per ogni $a, b$ si ha $a < b$ oppure $a = b$ oppure $a > b$;
- per ogni $m$ si ha $m \cdot 1 = m$;
- se $m \neq 0$ e $n \neq 0$ si ha $m \cdot n \neq 0$;
- se $m \neq 0$ e $n \neq 0$ si ha $m \cdot n \geqslant m$ e $m \cdot n \geqslant$.

Siffate dimostrazioni vengono in genere condotte per induzione. Possono risultare a tratti anche tortuose e richiedere una certa perizia, sebbene le difficoltà siano più di organizzazione che reali. Si ritrovano così le varie proprietà delle operazioni e dell'ordinamento in $\mathbb{N}$.
A partire da $\mathbb{N}$, si costruisce poi esplicitamente l'insieme $\mathbb{Z}$. Con un minimo di pazienza si ricavano come teoremi i postulati a suo tempo enunciati a inizio per $\mathbb{Z}$. Questo approccio può essere più soddisfacente sul piano della costruzione logica, in quanto muove da assunzioni estremamente ridotte, che in sostanza si limitano a descrivere i numeri naturali come sequenza (un po' come quando si impara a contare). Anche in questo caso è però necessario un postulato d'induzione, che non è aggirabile. È una via lievemente più laboriosa, servono diverse manovre preliminari prima di avviare lo studio dell'aritmetica vera e propria. Se l'interesse è appunto l'aritmetica, può essere preferibile una presentazione più diretta e più algebrica di $\mathbb{Z}$, nella quale siano già incorporate le operazioni e l'ordinamento. La sostanza non cambia tuttavia di molto: cambia solo il modo scelto per introdurre i primi elementi.
Una parola infine sugli insiemi: giacché la nozione di insieme è chiamata in gioco più o meno inevitabilmente nei postulati dell'aritmetica, si può anche pensare di partire da una teoria generale degli insiemi e ricavare quindi al suo interno una teoria dei numeri naturali (che saranno individuati come particolari insiemi). Così facendo, non si incontrano particolari difficoltà nel definire singolarmente ciascun numero naturale. Ma per costruire il loro insieme complessivo, ossia per poter definire il concetto generale di numero naturale, ancora una volta finisce per essere necessario un apposito postulato, il quale affermi che gli oggetti così ottenuti (in un *numero finito* di passi) sono tutti e soli i numeri naturali: nella sostanza ci serve ancora un sostituto del principio d'induzione.

**Esercizio 8.22** Definiamo degli insiemi $\underline{0}$, $\underline{1}$, $\underline{2}$, ..., $\underline{n}$, ... , e così via, che possiamo immaginare in corrispondenza a ciascun numero naturale nel modo seguente: $\underline{0} := \varnothing$ e $\underline{k+1} := \underline{k} \cup \{\underline{k}\}$. La caratteristica di un insieme X di *avere cardinalità* $n$ si traduce nell'esistenza di una corrispondenza biunivoca tra X e l'insieme $\underline{n}$.

- Costruire gli insiemi $\underline{1}$, $\underline{2}$, $\underline{3}$, $\underline{4}$.
- Far vedere che la cardinalità di $\underline{n}$ è $n$.
- Far vedere che, se $\underline{m} \in \underline{n}$, allora $\underline{m} \subset \underline{n}$.
- A quale relazione tra insiemi corrisponde la relazione numerica $m < n$?
- Come si potrebbe definire l'operazione di addizione $m + n$ in termini insiemistici (vale a dire tra gli insiemi $\underline{m}$ e $\underline{n}$, in modo che la cardinalità di $\underline{m} + \underline{n}$ sia in effetti pari a $m + n$)?