Insiemi numerici

Alessio Del Vigna

4 settembre 2023

Indice

1 I numeri naturali

L'insieme dei *numeri naturali* è

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

Essenzialmente i numeri naturali nascono per contare. Per spiegare meglio cosa questo significhi, utilizziamo un passo dal bellissimo libro [1]:

> Creati dalla mente umana per contare gli oggetti di vari insiemi, i numeri non hanno alcun riferimento alle caratteristiche individuali degli oggetti contati. Il numero sei è un'astrazione di tutti gli effettivi insiemi contenenti sei oggetti; esso non dipende da nessuna delle qualità specifiche di tali oggetti né dai simboli usati. Soltanto in uno studio intellttualmente piuttosto evoluto diventa chiaro il carattere astratto dell'idea di numero. Per i bambini i numeri rimangono sempre collegati a oggetti tangibili, come dita o granelli, e i linguaggi primitivi danno al numero un senso concreto, attribuendo nomi diversi ai numeri che rappresentano oggetti di tipo diverso.

Il processo di astrazione del concetto di cardinalità non è per nulla banale e ha impiegato molto tempo per realizzarsi. Basti pensare che perfino oggi ci sono popolazioni che usano diversi modi di contare a seconda del tipo di oggetto che stanno contando.

1.1 Gli assiomi di Peano

Nella seconda metà dell'Ottocento, grazie al lavoro del matematico Peano, i numeri naturali ottengono la loro formalizzazione matematica. In particolare, Peano propone una definizione assiomatica di $\mathbb{N}$ nel suo trattato *Arithmetices principia, nova methodo exposita* del 1889. Gli assiomi sono i seguenti:

(A1) 0 è un numero naturale;

(A2) il successore di ogni numero naturale è un numero naturale;

(A3) 0 non è il successore di alcun numero naturale;

(A4) numeri naturali diversi hanno successori diversi;

(A5) se un insieme di numeri naturali contiene lo 0 ed il successore di ogni suo elemento, allora esso coincide con l'insieme dei numeri naturali.

Quelli appena enunciati sono conosciuti come *assiomi di Peano* e definiscono in modo unico la struttura dell'insieme $\mathbb{N}$ dei numeri naturali, fatto che non proveremo. Ci limitiamo quindi a commentare gli assiomi vedendo intuitivamente cosa implicano riguardo alla struttura dell'insieme $\mathbb{N}$.

Il primo assioma (A1) afferma che lo 0 è uno degli elementi dell'insieme $\mathbb{N}$, che risulta quindi non vuoto. Il secondo assioma (A2) ci dice che se partiamo da un numero naturale e ne facciamo il successore otteniamo ancora un numero naturale. Scriviamo $s(n)$ per indicare il successore del numero naturale n. L'assioma (A3) afferma che 0 è un numero naturale

che non ha predecessore. Consideriamo $s(0)$, il successore di 0: cosa possiamo dire di questo numero naturale? Per l'assioma (A3) il successore di 0 non può essere 0, e dunque è un nuovo numero naturale, che viene indicato con 1. Continuiamo: cosa possiamo dire del successore di 1? Per l'assioma (A3) il successore di 1 non può essere lo 0 e per l'assioma (A4) il successore di 1 non può essere 1 in quanto, altrimenti, avremmo due numeri naturali distinti con stesso successore. Il successore di 1 deve quindi essere un nuovo numero naturale, che si indica con il simbolo 2. Questo ragionamento può essere ripetuto per mostrare che, continuando ad applicare il successore, si ottengono sempre nuovi numeri naturali; questi sono

$$0,\ s(0) = 1,\ s(s(0)) = 2,\ s(s(s(0))) = 3,\ \ldots$$

Tutti questi numeri naturali sono "la discendenza" dello 0 ottenuta applicando il successore. A cosa serve dunque l'assioma (A5)? Senza entrare troppo nei dettagli, con questo assioma si riesce a mostrare che, oltre ai numeri naturali che si ottengono come discendenza dello 0, non vi sono altri numeri naturali. L'assioma (A5) è di fondamentale importanza e prende il nome di *principio di induzione*. Uno degli impieghi di questo assioma è una tecnica dimostrativa, la dimostrazione per induzione, che vedremo più avanti.

1.2 Addizione e moltiplicazione

Definizione 1.1. Siano n e m numeri naturali. La *somma* tra n e m è il numero naturale che si ottiene da n applicando m volte il successore. L'operazione che, dati i due numeri n e m, restituisce la loro somma si chiama *addizione*.

Teorema 1.2 (proprietà dell'addizione)**.** *Valgono le seguenti proprietà:*

(i) $\forall n, m \in \mathbb{N}\ \ n + m = m + n$ *(proprietà commutativa dell'addizione);*

(ii) $\forall n, m, r \in \mathbb{N}\ \ n + (m + r) = (n + m) + r$ *(proprietà associativa dell'addizione);*

(iii) $\forall n \in \mathbb{N}\ \ n + 0 = n$ *(il numero* 0 *è l'elemento neutro dell'addizione).*

Dimostrazione. La (i) e la (ii) richiedono l'uso dell'induzione, per cui ne omettiamo la dimostrazione.

(iii) Segue direttamente dalla definizione di somma. Infatti, dato $n \in \mathbb{N}$, fare $n + 0$ significa applicare zero volte il successore ad n, che dà come risultato n stesso. □

Definizione 1.3. Siano n e m numeri naturali. Il *prodotto* tra n e m è il numero naturale che si ottiene sommando n con se stesso m volte, ossia

$$n \cdot m = \underbrace{n + n + \cdots + n}_{m \text{ volte}}.$$

L'operazione che, dati i due numeri n e m, restituisce il loro prodotto si chiama *moltiplicazione*. Quando non vi sono ambiguità non scriviamo il simbolo della moltiplicazione, ossia scriviamo nm invece di $n \cdot m$.

Teorema 1.4 (proprietà della moltiplicazione)**.** *Valgono le seguenti proprietà:*

(i) $\forall n, m \in \mathbb{N} \quad n \cdot m = m \cdot n$ *(proprietà commutativa della moltiplicazione);*

(ii) $\forall n, m, r \in \mathbb{N} \quad n \cdot (m \cdot r) = (n \cdot m) \cdot r$ *(proprietà associativa della moltiplicazione);*

(iii) $\forall n \in \mathbb{N} \quad n \cdot 1 = n$ *(il numero* 1 *è l'elemento neutro della moltiplicazione).*

(iv) $\forall n \in \mathbb{N} \quad n \cdot 0 = 0$.

Dimostrazione. La (i) e la (ii) richiedono l'induzione, per cui ne omettiamo la dimostrazione.

(iii) Dalla definizione di moltiplicazione, fare $n \cdot 1$ significa sommare n con se stesso una volta, il ché ha come risultato n.

(iv) Ancora dalla definizione di moltiplicazione, fare $n \cdot 0$ significa sommare n con se stesso zero volte, il ché dà una somma vuota, che è nulla. □

Teorema 1.5 (proprietà distributiva)**.** *Per ogni* $n, m, r \in \mathbb{N}$ *vale*

$$n \cdot (m + r) = n \cdot m + n \cdot r.$$

Dimostrazione. Dimostriamo questa proprietà in due modi, il primo sfruttando la definizione di moltiplicazione, il secondo in maniera grafica.

Seguendo la definizione di moltiplicazione si ha

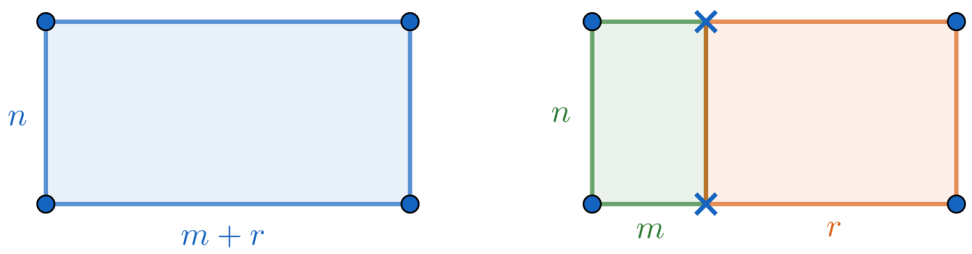
$$n \cdot (m + r) = \underbrace{n + \cdots + n}_{m + r \text{ volte}}.$$

La somma che compare a secondo membro ha $m + r$ addendi, per cui può essere spezzata in una somma con m addendi seguita da una somma con r addendi, cioè

$$n \cdot (m + r) = \underbrace{n + \cdots + n}_{m + r \text{ volte}} = \underbrace{n + \cdots + n}_{m \text{ volte}} + \underbrace{n + \cdots + n}_{r \text{ volte}}.$$

Di nuovo usando la definizione di moltiplicazione si osserva che l'ultima espressione a cui siamo pervenuti è proprio $n \cdot m + n \cdot r$, e abbiamo concluso.

Quella che proponiamo adesso è un esempio di *proof without words* (che significa *dimostrazione senza parole*).



□

Teorema 1.6 (legge di annullamento del prodotto)**.** *Siano n e m numeri naturali. Si ha $nm = 0$ se e solo se $n = 0 \vee m = 0$.*

Dimostrazione. ($\Leftarrow$) Se $n = 0$ o $m = 0$ allora $nm = 0$ per il Teorema 1.4-(iv).

($\Rightarrow$) È più conveniente considerare la contronominale, espressa dalla seguente implicazione: se $n \neq 0 \wedge m \neq 0$ allora $nm \neq 0$. Dato che per definizione

$$nm = \underbrace{n + n + \cdots + n}_{m \text{ volte}}.$$

se $n \neq 0$ e il numero di addendi è $m \neq 0$ segue che $nm \neq 0$. □

1.3 Ordinamento

Stiamo per definire quando un numero naturale è minore di un altro. L'idea che sta dietro alla definizione è che un numero è minore di un altro quando si può ottenere il secondo dal primo sommandoci una quantità non nulla.

Definizione 1.7. Siano $n, m \in \mathbb{N}$. Diciamo che n è *minore* di m, e scriviamo $n < m$, se esiste $k \neq 0$ tale che $n + k = m$. Quando $n < m$ si dice anche che m è *maggiore* di n e si può scrivere $m > n$.

Esempio 1.8. Si ha che $3 < 8$ perché $3 + 5 = 8$ (in questo caso $k = 5$). Vale che $10 > 6$ perché $6 + 4 = 10$ (in questo caso $k = 4$).

Definizione 1.9. Siano $n, m \in \mathbb{N}$. Diciamo che n è *minore o uguale a* m, e scriviamo $n \leq m$, se $n < m \vee n = m$, ossia se esiste $k \in \mathbb{N}$ tale che $n + k = m$. Quando $n \leq m$ si dice anche che m è *maggiore o uguale a* n e si può scrivere $m \geq n$.

Lemma 1.10. *Valgono le proprietà seguenti.*

(i) $\forall n \in \mathbb{N} \quad n < n + 1$;

(ii) $\forall n \in \mathbb{N} \quad 0 \leq n$.

(iii) *L'insieme* $\mathbb{N}$ *è* totalmente ordinato*, ossia comunque presi n e m numeri naturali si ha $n < m$ o $n > m$ o $n = m$.*

Dimostrazione. (i) Segue immediatamente dalla definizione di "$<$" con $k = 1$.

(ii) Fissato $n \in \mathbb{N}$, la tesi segue direttamente dalla definizione di "$\leq$" con $k = n$.

La (iii) richiederebbe l'induzione, per cui ne omettiamo la dimostrazione. □

[Rappresentazione su retta]

Definizione 1.11. Sia X un sottoinsieme di $\mathbb{N}$. Diciamo che un certo elemento $m \in X$ è il *minimo* di X se

$$\forall x \in X \quad m \leq x.$$

Analogamente diciamo che un certo elemento $M \in X$ è il *massimo* di X se

$$\forall x \in X \quad M \geq x.$$

Per indicare il minimo e il massimo di un insieme X si scrive rispettivamente $\min X$ e $\max X$.

Osserviamo che il fatto che abbiamo definito cosa sono l'elemento minimo e l'elemento massimo di un sottoinsieme di $\mathbb{N}$ non significa che questi esistano sempre, come i seguenti esempi mostrano.

Esempio 1.12. Vediamo alcuni esempi di determinazione dell'elemento minimo e massimo di un sottoinsieme.

(i) Consideriamo $X = \{n \in \mathbb{N} : 4 \leq n \leq 6\} = \{4, 5, 6\}$. È di immediata verifica che il minimo di X è 4 e il massimo di X è 6.

(ii) Consideriamo $X = \mathbb{N}$. Il minimo di $\mathbb{N}$ è il numero 0, come mostra il Lemma 1.10-(ii). Il massimo di $\mathbb{N}$, invece, non esiste, e per provarlo si procede per assurdo. Se $\mathbb{N}$ avesse un massimo, chiamiamolo M, allora tutti gli elementi di $\mathbb{N}$ sarebbero $\leq M$. Dunque anche $M + 1$ sarebbe $\leq M$, e questo è assurdo.

(iii) Sia $\mathcal{P}$ l'insieme dei numeri pari e $\mathcal{D}$ l'insieme dei numeri dispari. È immediato mostrare che

$$\min \mathcal{P} = 0 \quad \text{e} \quad \min \mathcal{D} = 1,$$

mentre né $\mathcal{P}$ né $\mathcal{D}$ hanno massimo.

(iv) Sia $\mathfrak{P}$ l'insieme dei numeri primi. Il minimo di $\mathfrak{P}$ è 2. Il massimo di $\mathfrak{P}$ non esiste perché $\mathfrak{P}$ è un insieme infinito, ma questo fatto non è per nulla ovvio (Teorema 1.42).

Negli esempi precedenti non abbiamo mai incontrato un caso di sottoinsieme di $\mathbb{N}$ senza elemento minimo: in effetti ciò è sempre vero ed è il contenuto del primo punto del prossimo risultato, di cui omettiamo la dimostrazione perché richiederebbe l'uso dell'induzione.

Teorema 1.13. *L'ordinamento su* $\mathbb{N}$ *gode delle seguenti proprietà.*

(i) *L'insieme* $\mathbb{N}$ *è* ben ordinato*, ossia ogni sottoinsieme non vuoto di* $\mathbb{N}$ *ha il minimo.*

(ii) *Un sottoinsieme non vuoto di* $\mathbb{N}$ *ha il massimo se e solo se è finito.*

1.4 Divisibilità

Definizione 1.14. Dati due numeri naturali n e d, diciamo che d è un *divisore* di n (o che n è un *multiplo* di d) se esiste un intero k tale che $n = dk$. In tal caso scriviamo $d \mid n$, che si legge "d divide n".

Esempio 1.15. Abbiamo che $6 \mid 30$ perché $30 = 6 \cdot 5$ ($k = 5$ in questo caso). Per scrivere invece che 6 non è un divisore di 20 si può scrivere $6 \nmid 20$; ciò significa che non c'è nessun numero che moltiplicato per 6 dia come risultato 20.

Alcune delle principali proprietà di questa relazione sono contenute nella proposizione seguente.

Proposizione 1.16. *La relazione di divisibilità gode delle proprietà seguenti.*

(i) *Per ogni* $n \in \mathbb{N}$ *si ha* $1 \mid n$ *e* $n \mid n$.

(ii) *Per ogni* $n \in \mathbb{N}$ *si ha* $n \mid 0$.

(iii) *Se* $n \neq 0$ *e* $d \mid n$ *allora* $d \leq n$.

Dimostrazione. (i) Sia n un numero naturale. Dato che $1 \cdot n = n$ si ha che $1 \mid n$ e $n \mid n$.

(ii) Sia n un numero naturale. Dato che $n \cdot 0 = 0$ si ha che $n \mid 0$.

(iii) Sia n un numero naturale diverso da 0. Siccome $d \mid n$ si ha che $dk = n$ per qualche k diverso da 0 (perché lo è n). Ciò significa che

$$n = \underbrace{d + \cdots + d}_{k \text{ volte}} = d + \underbrace{d + \cdots + d}_{k-1 \text{ volte}}$$

e dunque si ha che $d \leq n$. □

Esprimiamo a parole il contenuto del precedente risultato. Il punto (i) afferma che ogni numero naturale ha come divisori 1 e se stesso, mentre il punto (ii) afferma che 0 è multiplo di qualsiasi altro numero. Infine il punto (iii) afferma che i divisori di un numero positivo non possono eccedere il numero stesso.

1.5 Sottrazione e divisione

A partire da addizione e moltiplicazione si possono definire le loro "operazioni inverse", la sottrazione e la divisione. Esse però non saranno definite per tutte le coppie di numeri naturali e dunque non possono essere considerate delle vere e proprie operazioni su $\mathbb{N}$.

Definizione 1.17. Siano $n, m \in \mathbb{N}$. La *differenza* tra n e m, che si indica con $n - m$, è quel numero naturale che sommato ad m dà n. L'operazione che, dati i due numeri n e m, restituisce la loro differenza si chiama *sottrazione*.

Esempio 1.18. Si ha che $19 - 6 = 13$ perché $6 + 13 = 19$, ossia 13 è quel numero che sommato a 6 dà 19. Invece $7 - 10$ non è definito, in quanto non esiste alcun numero naturale che sommato a 10 dia 7.

Come mostrano i precedenti esempi la differenza di due numeri naturali non esiste sempre. Possiamo riformulare la definizione di differenza dicendo che $n - m$ esiste se e solo se esiste un numero naturale d tale che $m + d = n$. Ma ciò equivale a dire che $n \geq m$ (si veda la Definizione 1.9). Pertanto abbiamo mostrato che $n - m$ esiste se e solo se $n \geq m$.

Definizione 1.19. Siano $n, m \in \mathbb{N}$ non entrambi nulli. Il *rapporto* tra n e m, che si indica con $n : m$, è quel numero naturale che moltiplicato per m dà n. L'operazione che, dati i due numeri n e m, restituisce il loro rapporto si chiama *divisione*.

Esempio 1.20. Si ha che $15 : 3 = 5$ perché $3 \cdot 5 = 15$, ossia 5 è quel numero che moltiplicato per 3 dà 15. Invece $4 : 3$ non è definito, in quanto non esiste alcun numero naturale che moltiplicato a 3 dia 4.

Come per la sottrazione, anche il rapporto tra due numeri naturali non esiste sempre. Se riformuliamo la definizione di rapporto abbiamo che $n : m$ esiste se e solo se esiste un numero naturale d tale che $m \cdot d = n$. Ma ciò equivale a dire che $m \mid n$ (si veda la Definizione 1.14). Pertanto abbiamo mostrato che $n : m$ esiste se e solo se $m \mid n$, ossia se e solo se n è multiplo di m.

1.6 Potenze e loro proprietà

Definizione 1.21. Siano a e n due numeri naturali non entrambi nulli. Definiamo la *potenza* a^n come

$$a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ volte}}.$$

Il numero a si chiama *base* della potenza, mentre n è detto *esponente* della potenza.

Esempio 1.22. La potenza di un numero è definita come moltiplicazione ripetuta di quel numero. Si ha ad esempio $2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$.

Proposizione 1.23. *Valgono le seguenti due proprietà.*

(i) $\forall n \neq 0 \quad 0^n = 0$.

(ii) $\forall a \neq 0 \quad a^0 = 1$.

Dimostrazione. (i) La potenza 0^n è la moltiplicazione di 0 con se stesso n volte, che è 0.

(ii) Dato $a \neq 0$ la potenza a^0 è un prodotto vuoto, che pertanto deve coincidere con l'elemento neutro della moltiplicazione, ossia 1. □

Osservazione 1.24. La definizione di potenza esclude il caso in cui sia a sia n sono nulli. In altre parole, la scrittura 0^0 non è definita, ossia non le si attribuisce un significato.

Teorema 1.25 (proprietà delle potenze)**.** *Per le basi e gli esponenti per cui le potenze scritte di seguito esistono, valgono le seguenti proprietà.*

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

(ii) $a^n : a^m = a^{n-m}$ *se* $n \geq m$.

(iii) $(a \cdot b)^n = a^n \cdot b^n$.

(iv) $(a : b)^n = a^n : b^n$ *se* $b \mid a$.

(v) $(a^n)^m = a^{nm}$.

Dimostrazione. (i) Sfruttiamo la definizione di potenza:

$$a^n \cdot a^m = \underbrace{a \cdot \ldots \cdot a}_{n \text{ volte}} \cdot \underbrace{a \cdot \ldots \cdot a}_{m \text{ volte}} = \underbrace{a \cdot \ldots \cdot a}_{n+m \text{ volte}} = a^{n+m}.$$

(ii) Si deve provare che a^{n-m} è il risultato della divisione tra a^n e a^m, pertanto basta provare che il prodotto tra a^{n-m} e a^m è a^n. Infatti si ha

$$a^{n-m} \cdot a^m = a^{n-m+m} = a^n,$$

dove nel primo passaggio abbiamo usato la proprietà dimostrata al punto (i).

(iii) Sfruttiamo nuovamente la definizione di potenza per scrivere

$$(a \cdot b)^n = \underbrace{(ab) \cdot \ldots \cdot (ab)}_{n \text{ volte}}$$

Grazie alla proprietà associativa e commutativa della moltiplicazione possiamo riscrivere il precedente prodotto come

$$\underbrace{(ab) \cdot \ldots \cdot (ab)}_{n \text{ volte}} = \underbrace{a \cdot \ldots \cdot a}_{n \text{ volte}} \cdot \underbrace{b \cdot \ldots \cdot b}_{n \text{ volte}} = a^n \cdot b^n.$$

(iv) Dobbiamo provare che $(a : b)^n$ è il risultato della divisione fra a^n e b^n, per cui basta dimostrare che il prodotto tra $(a : b)^n$ e b^n è a^n. Infatti si ha

$$(a : b)^n \cdot b^n = (a : b \cdot b)^n = a^n,$$

dove nel primo passaggio abbiamo usato la proprietà dimostrata al punto (iii).

(v) Sfruttiamo la definizione di potenza per due volte per scrivere

$$(a^n)^m = \underbrace{a^n \cdot \ldots \cdot a^n}_{m \text{ volte}} = \underbrace{\underbrace{a \cdot \ldots \cdot a}_{n \text{ volte}} \cdot \ldots \cdot \underbrace{a \cdot \ldots \cdot a}_{n \text{ volte}}}_{m \text{ volte}}.$$

Il prodotto che abbiamo scritto ha m blocchi costituiti ciascuno dalla moltiplicazione di n volte a con se stesso, pertanto il numero di fattori del prodotto è nm. Ciò comporta che l'ultimo prodotto scritto è proprio a^{nm}. □

Osserviamo che le proprietà delle potenze, in particolare quelle dalla (i) alla (iv), coinvolgono soltanto moltiplicazioni o divisioni fra potenze con stessa base o stesso esponente. Nessuna proprietà vale per somma o sottrazione di potenze, ed è facile convincersene esibendo dei controesempi.

1.7 La divisione euclidea

Come distribuiamo il più uniformemente possibile 80 quaderni a 25 bambini? Certo non potremo dare $80/25 = 3.2$ quaderni ad ogni bambino. Piuttosto potremmo dare 3 quaderni ad ognuno e ci avanzeranno 5 quaderni. Questo secondo modo risulta il più adatto: visto che i quaderni non si possono "spezzare", il problema era relativo ai numeri naturali, e pertanto la risposta deve esser data ancora in termini di numeri naturali. La divisione che abbiamo fatto è un esempio di *divisione con resto*.

Teorema 1.26 (teorema di divisione)**.** *Siano n e $m \neq 0$ due numeri naturali. Allora esistono e sono unici due interi q e r tali che $n = qm + r$ e $0 \leq r < m$.*

Dimostrazione. Consideriamo i multipli di m, ossia 0, m, $2m$, $3m$, ..., e vediamo dove può stare n rispetto a questa sequenza. Si danno due casi: o n è un multiplo di m (verde in Figura 1) oppure n si trova fra due multipli consecutivi di m (caso arancio in Figura 1).

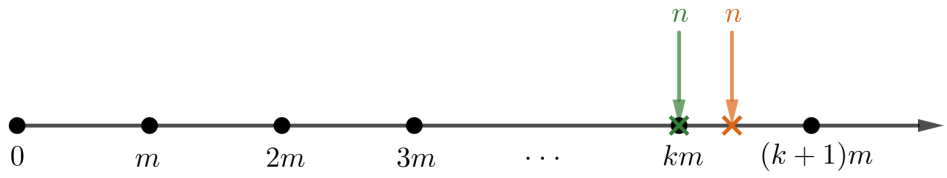


Figura 1. Figura a supporto della dimostrazione del Teorema 1.26. In verde il caso in cui n è multiplo di m, in arancio il caso in cui n è compreso fra due multipli consecutivi di m.

(i) Se n è un multiplo di n significa che $n = km$ per un qualche k numero naturale. Ma allora basta prendere $q = k$ e $r = 0$ e la tesi è provata.

(ii) Se n sta fra due multipli consecutivi di m significa che $km < n < (k+1)m$ per qualche k numero naturale. Affermiamo che basta prendere $q = k$ e $r = n - km$ e la tesi è provata. Infatti per costruzione abbiamo che $n = km + r = qm + r$. Inoltre $r = n - km > 0$ perché $n > km$ per ipotesi; e infine, ricordando che $n < (k + 1)m$ segue

$$r = n - km < (k + 1)m - km = km + m - km = m,$$

che è quanto volevamo.

Che q e r siano unici segue direttamente dalla costruzione che abbiamo fatto. □

La scrittura di n come $qm+r$ in modo unico data dal teorema precedente prende il nome di *divisione euclidea* tra n e m. I numeri q e r si dicono rispettivamente *quoziente* e *resto* della divisione.

1.8 Massimo comune divisore e minimo comune multiplo

Definizione 1.27. Siano n e m due interi non entrambi nulli. Il *massimo comun divisore* tra n e m è il massimo tra i divisori comuni ad n e m. Il massimo comun divisore tra n e m si indica con $\mathrm{MCD}(n, m)$, o con $\gcd(n, m)$[1], o con (n, m).

Esempio 1.28. Vediamo con un esempio come si costruisce il massimo comun divisore tra due interi seguendo la definizione. Calcoliamo $\mathrm{MCD}(30, 12)$. Consideriamo l'insieme dei divisori di 30 e l'insieme dei divisori di 12, rispettivamente

$$D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\} \quad \text{e} \quad D_{12} = \{1, 2, 3, 4, 6, 12\}.$$

I divisori comuni sono $D_{30} \cap D_{12} = \{1, 2, 3, 6\}$. Il massimo di questo insieme è 6, che è dunque il massimo divisore comune, ossia $\mathrm{MCD}(30, 12) = 6$.

Esempio 1.29. Consideriamo il caso in cui dobbiamo calcolare il massimo comun divisore tra un numero non nullo e 0. Calcoliamo ad esempio $\mathrm{MCD}(25, 0)$. Dato che ogni numero naturale è divisore di 0 (si ricordi la Proposizione 1.16-(ii)), i divisori comuni fra 25 e 0 sono proprio i divisori di 25, per cui il loro massimo è 25. Più in generale, se $n \neq 0$ si ha che

$$\mathrm{MCD}(n, 0) = n.$$

Proposizione 1.30. *Siano n e m due interi non entrambi nulli. Il massimo comun divisore tra n e m esiste.*

Dimostrazione. Sia D_n l'insieme dei divisori di n e sia D_m l'insieme dei divisori di m. L'insieme dei divisori comuni ad n e m è l'intersezione $D_n \cap D_m$. Dalla Proposizione 1.16-(iii) segue che gli elementi di D_n devono essere $\leq n$, e dunque che D_n è un insieme finito. Analogamente si ha anche che D_m è finito. Dunque la loro intersezione $D_n \cap D_m$ è un insieme finito e pertanto grazie al Teorema 1.13-(ii) ha un massimo. Tale massimo è proprio il massimo comune divisore. □

Adesso ci occupiamo del problema di determinare il massimo comun divisore tra due numeri. In teoria, un metodo possibile è quello di determinare tutti i divisori positivi di entrambi i numeri, per poi determinare il più grande tra quelli comuni, come abbiamo visto nel precedente esempio. Ciò è sconsigliabile nella pratica, in quanto il calcolo dei divisori di un numero è in generale molto laborioso. Un secondo metodo passa attraverso la fattorizzazione dei due numeri in fattori primi (come vedremo nella Sezione 1.9). Questo secondo metodo risulta efficiente solo se la fattorizzazione in primi dei due numeri è già nota in qualche modo. In generale, infatti, anche il problema di fattorizzare in primi un numero è molto difficile[2]. Abbandonate per ora questa due strade, esiste un metodo molto efficiente per il

[1] La sigla "gcd" sta per l'espressione inglese *greatest common divisor*.

[2] Anzi, è proprio su questa difficoltà che si basa uno dei metodi di crittografia più efficienti usato in questi anni, il metodo RSA. Per dare un'idea della scala di grandezza a cui si riferisce il nostro discorso, il metodo RSA si basa sul fatto che attualmente non sia possibile fattorizzare in "tempo utile" un numero di 600 cifre che è il prodotto di due primi.

calcolo del massimo comun divisore, che non prevede né fattorizzazioni in primi né calcolo di divisori, ma semplicemente l'esecuzione ripetuta di divisioni euclidee. Il metodo è noto come *algoritmo di Euclide*. Questo metodo si fonda su questo lemma.

Lemma 1.31. *Siano n, m, q e r quattro numeri naturali, con n e m non entrambi nulli e con q e r non entrambi nulli. Se $n = qm + r$ allora*

$$\mathrm{MCD}(n, m) = \mathrm{MCD}(m, r).$$

Dimostrazione. Sia $D_n \cap D_m$ l'insieme dei divisori comuni a n e m, e sia $D_m \cap D_r$ l'insieme dei divisori comuni a m e r. Sia d un divisore di n e di m, e mostriamo che d è anche un divisore di r. Poiché $n = dk$ e $m = dh$ per qualche k e qualche h naturali, segue

$$r = n - qm = dk - q \cdot dh = d(k - qh),$$

da cui segue che d è divisore di r. Ciò mostra che $D_n \cap D_m$ è un sottoinsieme di $D_m \cap D_r$, poiché ogni elemento del primo insieme è anche elemento del secondo. In modo del tutto analogo si prova che $D_m \cap D_r$ è un sottoinsieme di $D_n \cap D_m$. Ma allora

$$D_n \cap D_m = D_m \cap D_r,$$

ossia l'insieme dei divisori comuni a n e m coincide con l'insieme dei divisori comuni a m e r. Di conseguenza coincideranno i massimi di questi due insiemi, che sono rispettivamente $\mathrm{MCD}(n, m)$ e $\mathrm{MCD}(m, r)$. □

Vediamo come usare il lemma precedente per il calcolo del massimo comun divisore. Partiamo da due numeri naturali n e m, non entrambi nulli, e supponiamo che $n \geq m$. La divisione euclidea tra n e m dà due numeri naturali q e r tali che

$$n = qm + r \quad \text{e} \quad 0 \leq r < m.$$

La prima della due proprietà è proprio l'ipotesi della Lemma 1.31, da cui segue che

$$\mathrm{MCD}(n, m) = \mathrm{MCD}(m, r).$$

Che vantaggio abbiamo ottenuto? Il secondo massimo comun divisore è quello tra m, che era il più piccolo tra n e m, ed r, che è minore di m (e quindi di n) per la proprietà del resto della divisione euclidea. Dunque il secondo massimo comun divisore è più semplice da calcolare rispetto al primo. Il secondo vantaggio è che abbiamo di fronte il calcolo di un nuovo massimo comun divisore, quindi possiamo ripetere il procedimento e semplificare ulteriormente il calcolo, come mostra il prossimo esempio.

Esempio 1.32. Supponiamo di dover calcolare il massimo comun divisore fra $n = 132$ e $m = 72$. La divisione euclidea fra n e m dà come quoziente 1 e come resto 60, ossia

$$132 = 1 \cdot 72 + 60.$$

Questa relazione è proprio l'ipotesi del Lemma 1.31. Ripercorrendo la dimostrazione del lemma, da questa relazione segue che l'insieme dei divisori comuni a 132 e 72 coincide con l'insieme dei divisori comuni a 72 e 60, e dunque che

$$\mathrm{MCD}(132, 72) = \mathrm{MCD}(72, 60).$$

A questo punto si può procedere in modo analogo con la divisione euclidea fra 72 e 60, e così via. La sequenza di divisioni successive è la seguente:

$$\begin{array}{r|l} 132 & 72 \\ \hline 60 & 1 \end{array} \qquad \begin{array}{r|l} 72 & 60 \\ \hline 12 & 1 \end{array} \qquad \begin{array}{r|l} 60 & 12 \\ \hline 0 & 5 \end{array}$$

All'ultima ci possiamo fermare perché abbiamo ottenuto come resto 0. L'applicazione ripetuta del Lemma 1.31 dà

$$\mathrm{MCD}(132, 72) = \mathrm{MCD}(72, 60) = \mathrm{MCD}(60, 12) = \mathrm{MCD}(12, 0) = 12,$$

e ci ha permesso di calcolare il massimo comun divisore di 132 e 72.

Osservazione 1.33. Nel precedente esempio è accaduto che, eseguendo divisioni euclidee successive, siamo arrivati ad una divisione con resto 0. In quel caso abbiamo concluso perché il calcolo del massimo comun divisore è immediato. Chi ci garantisce che ciò accada sempre? Guardiamo i resti delle divisioni euclidee. Questi resti formano una sequenza di numeri naturali strettamente decrescente (ossia in cui ciascun resto è minore del precedente) e dunque ad un certo punto si deve ottenere come resto 0. Infatti, se così non fosse, l'insieme dei resti sarebbe un insieme di numeri naturali senza minimo, il ché contraddice il fatto che $\mathbb{N}$ è un insieme ben ordinato.

Definizione 1.34. Siano n e m due interi non nulli. Il *minimo comune multiplo* tra n e m è il minimo tra i multipli comuni ad n e m, eccetto lo 0. Il minimo comune multiplo tra n e m si indica con $\mathrm{mcm}(n, m)$, o con $\mathrm{lcm}(n, m)$[3], o con $[n, m]$.

Esempio 1.35. Vediamo come si determina il minimo comune multiplo tra due numeri seguendo la definizione appena data. Calcoliamo $\mathrm{mcm}(30, 12)$. L'insieme dei multipli di 30 e l'insieme dei multipli di 12 sono rispettivamente

$$M_{30} = \{0,\, 30,\, 60,\, 90,\, \ldots\} \quad \text{e} \quad M_{12} = \{0,\, 12,\, 24,\, 36,\, 48,\, 60,\, 78,\, \ldots\}\,.$$

L'insieme dei multipli comuni è $M_{30} \cap M_{12} = \{0,\, 60,\, 120,\, 180,\, \ldots\}$. Il minimo di questo insieme eccettuato è 60, ossia $\mathrm{mcm}(30, 12) = 60$.

Proposizione 1.36. *Siano n e m due interi non nulli. Il minimo comune multiplo tra n e m esiste.*

[3]La sigla "lcm" sta per l'espressione inglese *least common multiple*.

Dimostrazione. Sia M_n l'insieme dei multipli di n e sia M_m l'insieme dei multipli di m. L'insieme dei multipli comuni ad n e m è l'intersezione $M_n \cap M_m$. Poiché 0 è multiplo di qualsiasi numero, questa intersezione ha anche 0 come elemento, pertanto consideriamo l'insieme $(M_n \cap M_m) \setminus \{0\}$ dei multipli comuni eccetto lo 0. Questo insieme è certamente non vuoto perché il prodotto nm è un multiplo di n e anche di m, e dunque grazie al Teorema 1.13-(i) ha un minimo. Tale minimo è il minimo comune multiplo tra n e m. □

Teorema 1.37. *Siano n e m due numeri naturali non nulli. Allora*

$$\mathrm{MCD}(n, m) \cdot \mathrm{mcm}(n, m) = nm.$$

Dimostrazione. **[Completare]** □

Esempio 1.38. Usiamo il legame tra massimo comune divisore e minimo comune multiplo dato dal precedente teorema per calcolare nuovamente $\mathrm{mcm}(30, 12)$. Con l'algoritmo di Euclide si trova subito che $\mathrm{MCD}(30, 12) = 6$, e ciò comporta

$$\mathrm{mcm}(30, 12) = \frac{30 \cdot 12}{\mathrm{MCD}(30, 12)} = \frac{30 \cdot 12}{6} = 60.$$

1.9 Numeri primi e teorema fondamentale dell'aritmetica

I numeri primi hanno da sempre affascinato i matematici. Il grande matematico Gauss (1777-1855) sintetizzò il suo giudizio sulla teoria dei numeri in questo celebre aforisma: "La matematica è la regina delle scienze e la teoria dei numeri è la regina della matematica". I numeri naturali sono stati studiati sin dall'antichità e la dimostrazione che i numeri primi sono infiniti risale addirittura a Euclide. Ciononostante numerose congetture che riguardano i numeri primi non sono state ancora dimostrate, come vedremo in questa sezione.

Definizione 1.39. Un numero naturale $p \geq 2$ è *primo* se ha come unici divisori solo 1 e p. Un numero ≥ 2 che non è primo si dice *composto*.

Denoteremo con $\mathfrak{P}$ l'insieme dei numeri primi. Non è difficile stendere una lista dei primi numeri primi:

$$2, 3, 5, 7, 11, 13, 17, \ldots$$

dove abbiamo usato i puntini perché l'insieme dei numeri primi è infinito, come proveremo poco più avanti. Si osservi che 1 non è un numero primo. Così per curiosità riportiamo uno dei più grandi numeri primi scoperti sinora[4], ossia

$$2^{82589933} - 1,$$

che consta di quasi 25 milioni di cifre!

[4]La scoperta risale al dicembre 2018, come si può verificare consultando il sito `https://www.mersenne.org/primes/`.

Osservazione 1.40. Osserviamo che 2 è l'unico numero primo pari. Infatti se p è un numero primo > 2 allora non può essere pari altrimenti avrebbe anche 2 fra i suoi divisori.

Come mai i numeri primi sono di così grande interesse? Uno dei motivi è senz'altro il seguente teorema, che mostra che i primi sono i "mattoni" con cui si possono costruire gli altri numeri naturali.

Teorema 1.41 (fondamentale dell'aritmetica)**.** *Ogni numero naturale ≥ 2 può essere espresso in modo unico (a meno dell'ordine dei fattori) come prodotto di potenze di primi distinti.*

La rappresentazione fornita dal teorema fondamentale dell'aritmetica prende il nome di *fattorizzazione*. Degli esempi di fattorizzazioni sono

$$18 = 2 \cdot 3^2, \quad 105 = 3 \cdot 5 \cdot 7, \quad 504 = 2^3 \cdot 3^2 \cdot 7, \quad 2021 = 43 \cdot 47.$$

Siamo finalmente pronti per provare che l'insieme $\mathfrak{P}$ dei numeri primi è infinito. Quella che segue è probabilmente la capostipite (a livello storico e di rilevanza) delle dimostrazioni per assurdo, nonché un indiscusso colpo di genio di Euclide.

Teorema 1.42 (Euclide)**.** *L'insieme $\mathfrak{P}$ è infinito.*

Dimostrazione. Supponiamo per assurdo che i numeri primi siano finiti, siano essi $p_1, \ldots, p_k$, ordinati in ordine crescente. Consideriamo il numero

$$M = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1.$$

Dato che M è più grande di 1, M deve avere un qualche fattore primo per il teorema fondamentale dell'aritmetica. Osserviamo però che tale fattore primo non può essere nessuno dei primi $p_1, \ldots, p_k$ poiché per costruzione M ha resto 1 nella divisione con ciascuno di questi. Abbiamo ottenuto una contraddizione, dunque l'assunzione che $\mathfrak{P}$ sia finito non può essere vera. □

1.10 Amenità sui numeri primi

1.10.1 Il crivello di Eratostene

Vediamo adesso un metodo per determinare tutti i numeri primi che non superano un dato numero n, il *crivello di Eratostene*. Si scrivono tutti i numeri naturali da 2 fino a n e poi si cancellano tutti i multipli del primo numero, ossia 2, escluso lui stesso. Si prende poi il primo numero non cancellato e si ripete l'operazione con i numeri che seguono, proseguendo fino a che non si applica l'operazione all'ultimo numero non cancellato. I numeri che restano, per costruzione, sono i numeri primi minori o uguali a n. La Figura 2 mostra l'applicazione del crivello per determinare i numeri primi che non superano 100.

Lemma 1.43. *Se $n \geq 2$ è un numero composto allora ha un fattore primo $\leq \sqrt{n}$.*

	2	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Figura 2. Applicazione del crivello di Eratostene per determinare i numeri primi ≤ 100 (in grassetto).

Dimostrazione. Se n è composto allora $n = ab$, dove a e b sono numeri naturali > 1. Affermiamo che almeno uno tra a e b deve essere $\leq \sqrt{n}$: infatti, se così non fosse, allora avremmo $n = ab > \sqrt{n}\sqrt{n} = n$, assurdo. Supponiamo ad esempio che $a \leq \sqrt{n}$. Dato che $a > 1$ per ipotesti, il teorema fondamentale dell'aritmetica comporta che a deve avere un fattore primo, che deve dunque essere $\leq \sqrt{n}$. Tale fattore primo di a è anche un fattore primo di n. □

Il precedente lemma comporta che il crivello di Eratostene riesce ad individuare tutti i primi $\leq n$ quando si è esplorato l'elenco di numeri fino a $\sqrt{n}$. Nell'esempio presentato in Figura 2 volevamo determinare i primi ≤ 100 e in effetti si può verificare che, una volta cancellati tutti i multipli di 7 (che è l'ultimo primo che non supera $\sqrt{100} = 10$), non sono rimasti altri numeri composti.

1.10.2 La funzione dei divisori

Consideriamo un numero naturale $n \geq 2$ e un suo divisore $d \neq 1$. I fattori primi di d sono necessariamente un sottoinsieme dei fattori primi di n e, inoltre, per ogni primo p l'esponente di p nella fattorizzazione di d non può eccedere l'esponente di p nella fattorizzazione di n. Ad esempio se $n = 2016 = 2^5 \cdot 3^2 \cdot 7$ allora alcuni suoi divisori sono

$$2^4 \cdot 3^2, \quad 3, \quad 3^2 \cdot 7, \quad 2 \cdot 3 \cdot 7, \quad \dots$$

Questa semplice osservazione ha una conseguenza fondamentale. Indichiamo con $d(n)$ il numero di divisori di n, così per esempio $d(1) = 1$, $d(p) = 2$ per ogni primo p, $d(10) = 4$.

Teorema 1.44. *Sia $n \geq 2$ un numero naturale e sia $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ la sua fattorizzazione. Allora*

$$d(n) = (e_1 + 1) \cdot \ldots \cdot (e_k + 1).$$

Dimostrazione. Un divisore di n deve avere gli stessi fattori primi di n e l'esponente di ciascun fattore primo non può eccedere quello della fattorizzazione di n. In altre parole, ogni divisore di n ha la forma

$$p_1^{l_1} \cdot \ldots \cdot p_k^{l_k},$$

dove $0 \leq l_i \leq e_i$ per ogni $i = 1, \ldots, k$. Dato che quindi un divisore di n è univocamente determinato dalla scelta dei k esponenti $l_1, \ldots, l_k$ per contare il numero dei divisori di n è sufficiente contare il numero di scelte possibili per questi esponenti. Per l'esponente l_1 di p_1 ci sono $e_1 + 1$ scelte possibili, che sono i numeri da 0 a e_1, e così via per gli altri. A questo punto la tesi segue ricordando che il numero complessivo di scelte si ottiene moltiplicando il numero di possibilità per ogni scelta. □

Esempio 1.45. Vediamo un esempio per chiarire la precedente dimostrazione. Consideriamo $n = 6 =$ e la sua fattorizzazione $2^2 \cdot 3 \cdot 5$. Segue che 60 ha

$$(2 + 1) \cdot (1 + 1) \cdot (1 + 1) = 12$$

divisori, in quanto ogni divisore corrisponde a scegliere l'esponente di 2 nell'insieme $\{0, 1, 2\}$, l'esponente di 3 nell'insieme $\{0, 1\}$ e l'esponente di 5 nell'insieme $\{0, 1\}$.

1.11 Problemi non (ancora?) risolti

Il problema di come sono distribuiti in media i numeri primi è stato risolto in maniera soddisfacente grazie al *teorema dei numeri primi*, che qui non enunciamo perché richiede strumenti avanzati. Tuttavia altre questioni legate alla distribuzione dei primi, anche di semplice enunciazione, sono ancora oggi prive di risposta.

Iniziamo occupandoci della lunghezza degli intervalli fra due numeri primi consecutivi. Osserviamo preliminarmente un fatto ovvio: 2 e 3 sono gli unici due numeri primi che distano 1. La domanda immediatamente successiva riguarda i numeri primi che distano 2, che hanno un nome.

Definizione 1.46. Due primi che differiscono di 2 sono detti *primi gemelli*.

Ad esempio 3 e 5 sono due numeri primi gemelli, 5 e 7 anche, 101 e 103 anche. Viene dunque naturale chiedersi se sia possibile trovare infinite coppie di numeri primi gemelli. Si ritiene che la risposta sia affermativa, come enunciato di seguito nella *congettura dei primi gemelli*, tuttavia non c'è ad oggi una dimostrazione di questo fatto!

Congettura 1.47 (dei primi gemelli)**.** *Esistono infiniti primi p tali che $p + 2$ è primo.*

La prossima congettura che presentiamo è la *congettura di Goldbach*. Egli aveva osservato che ogni numero pari ≥ 4 si può scrivere come somma di due numeri primi. Ad esempio

$$8 = 3 + 5, \quad 20 = 7 + 13, \quad 48 = 29 + 19, \quad \text{e} \quad 100 = 3 + 97.$$

Goldbach aveva scritto di questa sua osservazione a Eulero (siamo nel 1742), chiedendo di dimostrarla o di trovare un controesempio. Ma Eulero non vi riuscì mai e ad oggi questo problema rimane ancora irrisolto.

Congettura 1.48 (di Goldbach)**.** *Ogni numero pari ≥ 4 si può scrivere come somma di due numeri primi.*

Uno dei risultati più forti attualmente disponibili, dimostrato da Ramaré nel 1995, è che ogni numero pari ≥ 4 si può scrivere come somma di al massimo 6 numeri primi.

Per concludere, una piccola riflessione sulla difficoltà di dimostrazione di queste congetture. I numeri primi hanno una definizione di tipo moltiplicativo, in quanto si parla di loro divisori; inoltre i numeri primi intervengono nella scomposizione dei numeri naturali come prodotto di fattori, come sappiamo dal teorema fondamentale dell'aritmetica. Le congetture anzi esposte, invece, sono di natura additiva ed è proprio questo che le rende intrinsecamente più difficoltose.

1.12 Oltre i numeri naturali

L'insieme $\mathbb{N}$ dei numeri naturali è un insieme dotato di due operazioni, l'addizione e la moltiplicazione, che godono di certe proprietà. Tuttavia alcuni problemi non hanno soluzione nei numeri naturali: ad esempio, non esiste alcun numero che sommato a 8 dia come risultato 3 o, in altre parole, la differenza $3 - 8$ non ha significato in $\mathbb{N}$.

Il metodo per sopperire a questi problemi consiste nell'allargare l'insieme numerico in maniera opportuna: si parla quindi di *estensione di un insieme numerico*. Informalmente, estendere un insieme numerico X significa passare ad un nuovo insieme numerico X', i cui elementi sono tali da risolvere tutti i problemi che erano risolubili in X, ma anche altri problemi che i numeri di X non sono in grado di risolvere. Più precisamente, un insieme numerico X' è un'*estensione* dell'insieme numerico X se valgono le seguenti due condizioni:

(E1) le operazioni di X' devono essere definite in modo da conservare tutte le proprietà valide nell'insieme X (*permanenza delle proprietà formali*);

(E2) l'insieme X' deve avere X come sottoinsieme e le operazioni dell'insieme X', quando ristrette agli elementi di X, agiscono come le operazioni di X (*principio di isomorfismo*).

Nelle prossime sezioni vedremo le estensioni numeriche che hanno portato all'ampliamento dell'insieme dei numeri naturali $\mathbb{N}$ all'insieme dei numeri interi $\mathbb{Z}$, da quest'ultimo all'insieme dei numeri razionali $\mathbb{Q}$, e da questo all'insieme dei numeri reali $\mathbb{R}$.

2 I numeri interi

L'ampliamento dell'insieme dei numeri naturali a quello dei numeri interi deriva principalmente da due necessità. Dal punto di vista matematico i numeri interi servono per far sì che la sottrazione diventi sempre possibile. Da un punto di vista pratico, invece, ad un certo punto è servito trovare una scala numerica per misurare debiti e crediti, o temperature sopra e sotto lo zero. Attorno al 1500 i cosidetti maestri d'abaco introdussero i numeri negativi e dettero delle regole per poterli sommare, in risposta all'esigenza di dover sommare debiti e crediti. In realtà i numeri negativi non erano accettati, tant'è che venivano chiamati "numeri falsi". Per distinguerli dai numeri positivi venivano usate due scale numeriche: una scala blu per i numeri positivi, e quindi per i crediti, ed una rossa per i debiti (da cui prende vita l'espressione "avere il conto in rosso").

Tornando alla matematica, l'insieme dei *numeri interi* è l'insieme

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

dove, per ogni numero naturale n non nullo, la notazione $-n$ è abbreviazione della differenza $0 - n$. I due interi n e $-n$ sono detti *opposti*. Ad esempio, il numero -3 è l'opposto di 3 e denota il risultato della differenza $0 - 3$.

Definizione 2.1. Gli elementi dell'insieme $\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}$ sono detti *numeri positivi* e gli elementi dell'insieme $\mathbb{Z}^- = \{\ldots, -3, -2, -1\}$ sono detti *numeri negativi*.

Osserviamo che

$$\mathbb{Z} = \mathbb{Z}^- \cup \{0\} \cup \mathbb{Z}^+$$

e che gli insiemi di questa unione sono a due a due disgiunti. Dunque $\mathbb{Z}$ è partizionato in tre insiemi: i numeri positivi, i numeri negativi e lo 0.

Definizione 2.2. Due numeri interi si dicono *concordi* se sono entrambi positivi o entrambi negativi, e si dicono *discordi* se uno è positivo e l'altro è negativo.

Esempio 2.3. I numeri 2 e 9 sono concordi, così come i numeri -1 e -18. I numeri 5 e -8 sono discordi. I numeri 7 e -7 sono discordi, in particolare opposti.

Definizione 2.4. Sia n un numero intero. Il *valore assoluto* di n è

$$|n| = \begin{cases} n & \text{se } n \text{ è positivo o nullo} \\ -n & \text{se } n \text{ è negativo} \end{cases}.$$

Esempio 2.5. Il numero 5 è positivo e dunque $|5| = 5$. Il numero -2 è negativo e il suo opposto è 2, dunque $|-2| = 2$.

Dalla definizione segue che, dato un numero intero n, il suo valore assoluto $|n|$ è un numero positivo o nullo.

2.1 Le operazioni

Definiamo adesso addizione e moltiplicazione nell'insieme dei numeri interi. Ricordiamo dalla Sezione 1.12 che, affinché $\mathbb{Z}$ sia un'estensione di $\mathbb{N}$, devono accadere due fatti:

- l'addizione e la moltiplicazione in $\mathbb{Z}$ devono godere delle stesse proprietà di cui godevano le analoghe operazioni in $\mathbb{N}$ (si veda (E1)), ossia la proprietà commutativa e associativa per entrambe le operazioni, il fatto che 0 sia elemento neutro per l'addizione, che 1 sia elemento neutro per la moltiplicazione, e infine la proprietà distributiva dell'addizione rispetto alla moltiplicazione;
- le due operazioni, quando effettuate su due numeri naturali, devono dare lo stesso risultato che davano le "vecchie" addizione e moltiplicazione sugli stessi due numeri naturali (si veda (E2)).

Si può dimostrare che, assumendo questi vincoli, c'è un solo modo per definire addizione e moltiplicazione fra numeri interi, e che riassumiamo nelle prossime definizioni.

Definizione 2.6. Siano n e m due numeri interi. La *somma* tra n e m è indicata con $n+m$ e si determina così:

(i) se n e m sono concordi allora la loro somma è concorde ad n e m e ha per valore assoluto la somma dei valori assoluti di n e di m;

(ii) se n e m sono discordi e non opposti allora la loro somma è concorde con il numero che ha valore assoluto maggiore, e ha valore assoluto uguale alla differenza tra il maggiore e il minore dei valori assoluti dei due numeri;

(iii) se n e m sono opposti allora la loro somma è 0.

L'operazione così definita si chiama *addizione*.

Esempio 2.7. Vediamo alcuni esempi di somma di numeri interi.

(i) Si ha $2+7=9$ e $(-2)+(-7)=-9$, seguendo la regola (i). Osserviamo come, nel caso di due numeri positivi, l'addizione definita in $\mathbb{Z}$ diventi esattamente la "vecchia" addizione tra numeri naturali (come vuole (E2)).

(ii) Si ha $3+(-7)=-4$ e $(-6)+1=-5$, seguendo la regola (ii).

(iii) Si ha $(-3)+3=3+(-3)=0$, seguendo la regola (iii).

Definizione 2.8. Siano n e m due numeri interi. Il *prodotto* tra n e m è indicato con $n \cdot m$ e si determina così:

(i) se n e m sono concordi allora $n \cdot m$ è positivo e ha per valore assoluto il prodotto dei valori assoluti di n e di m;

(ii) se n e m sono discordi allora $n \cdot m$ è negativo e ha per valore assoluto il prodotto dei valori assoluti di n e di m.

L'operazione così definita si chiama *moltiplicazione*.

Esempio 2.9. Vediamo alcuni esempi di somma di numeri interi.

(i) $2 \cdot 7 = 14$ e $(-2) \cdot (-7) = 14$, seguendo la regola (i). Osserviamo come, nel caso di due numeri positivi, la moltiplicazione diventi esattamente la "vecchia" moltiplicazione tra numeri naturali (come vuole (E2)).

(ii) $3 \cdot (-7) = -21$ e $(-6) \cdot 1 = -6$, seguendo la regola (ii).

Si osservi come la regola dei segni segua direttamente dalla definizione di moltiplicazione che abbiamo dato. Dunque la regola dei segni è l'unica regola possibile affinché $\mathbb{Z}$ sia un'estensione di $\mathbb{N}$.

Lemma 2.10. *Per ogni numero intero n si ha $n \cdot 0 = 0$.*

Dimostrazione. Dalla definizione di addizione si ha $0 = 1 + (-1)$. Ciò comporta che

$$n \cdot 0 = n \cdot (1 + (-1)) = n \cdot 1 + n \cdot (-1) = n + (-n) = 0,$$

dove nel secondo passaggio abbiamo utilizzato il fatto che la moltiplicazione gode della proprietà distributiva rispetto all'addizione. □

Bibliografia

[1] R. Courant, H. Robbins, "Che cos'è la matematica? Introduzione elementare ai suoi concetti e metodi". Bollati Boringhieri, 2000