CAPITOLO

1

I numeri naturali

Contare è il primo gesto matematico: lo facciamo da bambini con le dita, ma dietro quel gesto c'è una struttura che non smette di sorprendere.

OBIETTIVI

1. Descrivere l'insieme $\mathbb{N}$, rappresentarlo su una semiretta e confrontare i suoi elementi.
2. Eseguire le quattro operazioni e la divisione con resto, conoscendo il ruolo dello zero.
3. Usare le proprietà delle operazioni e delle potenze per calcolare in modo rapido e corretto.
4. Riconoscere multipli, divisori e numeri primi; scomporre un numero in fattori primi.
5. Calcolare MCD e mcm, anche con l'algoritmo di Euclide, e usarli per risolvere problemi.
6. Passare dalla base dieci alla base due e viceversa, e distinguere un sistema posizionale da uno additivo.

INDICE DEL CAPITOLO

1.1 L'insieme dei numeri naturali 2
1.2 Le quattro operazioni 3
1.3 Le proprietà delle operazioni 5
1.4 Le potenze e le espressioni 7
1.5 Divisibilità, numeri primi, MCD e mcm 9
1.6 I sistemi di numerazione 15

Matematica 1 · Parte I · I numeri · versione 1.0
Capitolo 1: I numeri naturali · pagine 25–46 del volume completo · estratto per lo studio

Quanti studenti ci sono nella tua classe? Quanti messaggi hai ricevuto oggi? Quante pagine ha questo libro? A tutte queste domande si risponde con un numero «da contare»: 0, 1, 2, 3, e così via. Sono i numeri che impariamo per primi, tanto familiari che sembra non ci sia più niente da scoprire. In realtà i numeri naturali nascondono domande che hanno impegnato i matematici per più di duemila anni: quanti sono i numeri primi? Esiste un modo veloce per trovare il massimo comune divisore di due numeri enormi? Perché il computer «pensa» con due sole cifre?

In questo capitolo riprendiamo quello che sai dalla scuola media, ma con uno sguardo nuovo. Non ci basterà saper fare i calcoli: vorremo capire *perché* le regole funzionano, quali proprietà le giustificano, quando un'operazione si può eseguire e quando no. È il passaggio dall'aritmetica come insieme di procedure alla matematica come ragionamento: lo stesso passaggio che ti accompagnerà per tutto il liceo.

1.1 L'insieme dei numeri naturali

1.1.1 Che cosa sono i numeri naturali

I **numeri naturali** sono i numeri 0, 1, 2, 3, 4, …: quelli che servono a contare gli oggetti di una collezione finita, compresa la collezione vuota, che ha zero oggetti. Il loro insieme si indica con il simbolo $\mathbb{N}$:

$$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$$

I puntini indicano che l'elenco non finisce mai. In questo libro, come nella maggior parte dei testi italiani, lo zero è considerato un numero naturale. Quando vogliamo escluderlo scriviamo $\mathbb{N}^*$ oppure $\mathbb{N} \setminus \{0\}$, cioè «$\mathbb{N}$ privato dello zero». Per dire che un numero appartiene a $\mathbb{N}$ usiamo il simbolo $\in$: scriviamo $7 \in \mathbb{N}$ («7 appartiene a $\mathbb{N}$») e invece $\frac{1}{2} \notin \mathbb{N}$ («un mezzo non appartiene a $\mathbb{N}$»).

1.1.2 Successivo, precedente e ordine

Ogni numero naturale n ha un **successivo**, che è $n + 1$. Ogni numero naturale diverso da 0 ha anche un precedente, che è $n - 1$; lo zero invece non ha precedente in $\mathbb{N}$. Due numeri come 6 e 7, uno successivo dell'altro, si dicono consecutivi.

Questa costruzione «un passo alla volta» suggerisce di rappresentare i naturali su una **semiretta orientata**: si fissa un punto di partenza, l'origine, a cui si associa lo 0; si sceglie un verso (di solito verso destra) e un'unità di misura, cioè un segmento che si riporta più volte. A ogni

numero corrisponde così un punto (Figura 1.1). Non tutti i punti della semiretta corrispondono però a numeri naturali: quelli tra 6 e 7, per esempio, restano «scoperti».

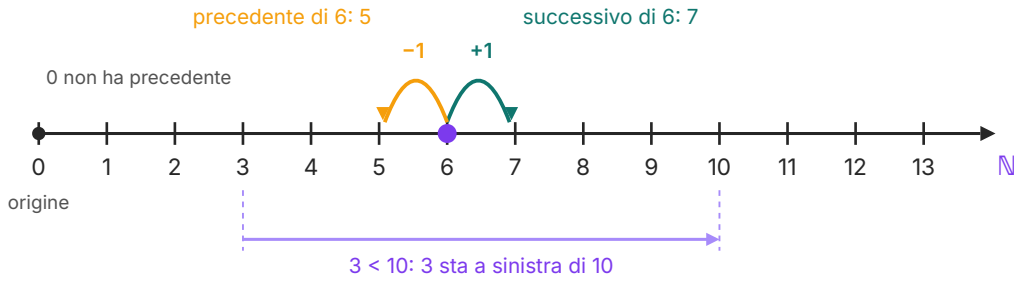


Figura 1.1 La semiretta dei numeri naturali. Ogni numero ha un successivo (+1); ogni numero tranne 0 ha un precedente (−1). Il numero minore sta sempre a sinistra del maggiore.

Dati due numeri naturali diversi, uno dei due è sempre minore dell'altro: diciamo che $\mathbb{N}$ è un insieme **totalmente ordinato**. Per confrontare i numeri usiamo i simboli

$$< \text{(minore)}, > \text{(maggiore)}, \leq \text{(minore o uguale)}, \geq \text{(maggiore o uguale)}.$$

Così $3 < 10$, $10 > 3$, e anche $5 \leq 5$ è vero, perché «minore o uguale» è soddisfatto quando i due numeri sono uguali. Sulla semiretta, $a < b$ significa che il punto di a sta a sinistra del punto di b.

Dalla figura si leggono tre caratteristiche importanti di $\mathbb{N}$.

- $\mathbb{N}$ **ha un minimo**, lo 0: nessun naturale è minore di 0.
- $\mathbb{N}$ **non ha un massimo**: qualunque numero tu scelga, il suo successivo è più grande. Per questo $\mathbb{N}$ è un insieme infinito.
- $\mathbb{N}$ **è discreto**: tra due numeri consecutivi non c'è nessun altro numero naturale. Diciamo che $\mathbb{N}$ è un insieme **discreto**. Nel capitolo 3 incontrerai i numeri razionali, che si comportano in modo opposto.

1.2 Le quattro operazioni

1.2.1 Addizione e moltiplicazione

Un'operazione associa a due numeri, presi in un certo ordine, un terzo numero detto *risultato*. Nell'addizione $8 + 5 = 13$ i numeri 8 e 5 si chiamano *addendi* e 13 è la *somma*. Nella moltiplicazione $8 \cdot 5 = 40$ i numeri 8 e 5 sono i *fattori* e 40 è il *prodotto*. La moltiplicazione è un'addizione ripetuta: $8 \cdot 5 = 8 + 8 + 8 + 8 + 8$.

Sommando o moltiplicando due numeri naturali si ottiene sempre un numero naturale. Si dice che addizione e moltiplicazione sono **operazioni interne** a $\mathbb{N}$: non «fanno uscire» dall'insieme.

1.2.2 Sottrazione e divisione

Nella sottrazione $13 - 5 = 8$ il primo numero è il *minuendo*, il secondo il *sottraendo*, il risultato la *differenza*. La sottrazione è l'operazione inversa dell'addizione: $13 - 5 = 8$ perché $8 + 5 = 13$. Ma che cosa succede con $5 - 13$? Non esiste alcun numero naturale che, sommato a 13, dia 5. La sottrazione $a - b$ si può eseguire in $\mathbb{N}$ solo se $a \geq b$: dunque la sottrazione **non** è un'operazione interna a $\mathbb{N}$.

Allo stesso modo la divisione esatta $40 : 5 = 8$ è l'inversa della moltiplicazione: $40 : 5 = 8$ perché $8 \cdot 5 = 40$. Qui 40 è il *dividendo*, 5 il *divisore*, 8 il *quoziente*. E $7 : 2$? Nessun naturale moltiplicato per 2 dà 7: anche la divisione esatta non è interna a $\mathbb{N}$. Per allargare le possibilità di calcolo serviranno nuovi numeri: gli interi relativi (capitolo 2) per la sottrazione, i razionali (capitolo 3) per la divisione.

1.2.3 La divisione con resto

Quando la divisione esatta non è possibile, possiamo comunque chiederci quante volte il divisore «sta» nel dividendo e che cosa avanza. Se dividiamo 17 caramelle tra 5 amici, ciascuno ne riceve 3 e ne avanzano 2 (Figura 1.2).

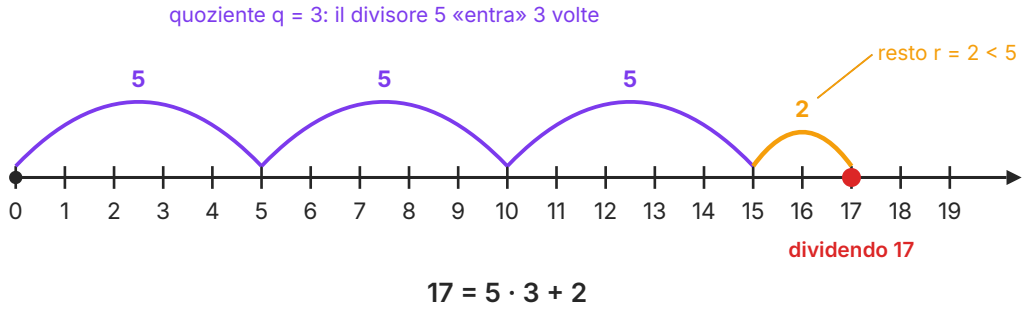


Figura 1.2 La divisione con resto $17 : 5$. A partire da 0 si fanno salti di 5 finché si resta entro 17: i salti sono 3 (il quoziente) e ciò che manca per arrivare a 17 è 2 (il resto).

IN SINTESI

Divisione con resto

Dati due numeri naturali a e b, con $b \neq 0$, esistono e sono unici due numeri naturali q (il quoziente) e r (il resto) tali che

$$a = b \cdot q + r \text{ con } 0 \leq r < b.$$

La divisione è esatta quando $r = 0$.

La condizione $r < b$ è essenziale: anche $17 = 5 \cdot 2 + 7$ è un'uguaglianza vera, ma 7 non è il resto, perché con 7 caramelle avanzate se ne può dare ancora una a ciascuno. Osserva anche che il resto può essere 0, e che se $a < b$ il quoziente è 0 e il resto è a stesso: 3 : 8 dà quoziente 0 e resto 3, perché $3 = 8 \cdot 0 + 3$.

1.2.4 Il ruolo dello zero

Lo zero ha un comportamento speciale in tutte le operazioni. Nell'addizione non cambia nulla: $a + 0 = a$. Nella moltiplicazione «annulla» tutto: $a \cdot 0 = 0$. E nella divisione?

- **$0 : a = 0$** se $a \neq 0$, perché $0 \cdot a = 0$.
- ***a* : 0 è impossibile** se $a \neq 0$. Per esempio 6 : 0 dovrebbe essere un numero che, moltiplicato per 0, dà 6; ma qualunque numero moltiplicato per 0 dà 0. Non esiste alcun risultato: la divisione si dice **impossibile**.
- **0 : 0 è indeterminata**. Il risultato dovrebbe essere un numero che, moltiplicato per 0, dà 0: ma questo è vero per *tutti* i numeri. Non c'è un unico risultato, e la divisione si dice **indeterminata**.

Attenzione: scrivere «6 : 0 = 0» oppure «6 : 0 = 6» è sbagliato. In entrambi i casi, impossibile o indeterminata, la divisione per zero non ha significato: il divisore deve sempre essere diverso da 0.

1.3 Le proprietà delle operazioni

Le proprietà delle operazioni non sono regole da imparare a memoria fini a sé stesse: sono gli strumenti che permettono di calcolare in modo più veloce e, più avanti, di trasformare le espressioni con le lettere. Le enunciamo con le lettere a, b, c, che stanno per numeri naturali qualsiasi.

1.3.1 Proprietà commutativa, associativa e distributiva

La **proprietà commutativa** dice che, in un'addizione o in una moltiplicazione, cambiando l'ordine dei termini il risultato non cambia: $a + b = b + a$ e $a \cdot b = b \cdot a$. La **proprietà associativa** dice che si possono raggruppare i termini come si vuole: $(a + b) + c = a + (b + c)$, e lo stesso per il prodotto. Grazie a queste due proprietà possiamo scrivere $2 + 7 + 8$ senza parentesi e sommare per primi i termini «comodi»: $2 + 8 = 10$, poi $10 + 7 = 17$.

Sottrazione e divisione **non** godono di queste proprietà: $9 - 4 \neq 4 - 9$ (anzi, il secondo non si può nemmeno calcolare in $\mathbb{N}$), e $(24 : 6) : 2 = 2$ mentre $24 : (6 : 2) = 8$.

La **proprietà distributiva** lega due operazioni diverse. La moltiplicazione è distributiva rispetto all'addizione e alla sottrazione:

$$a \cdot (b + c) = a \cdot b + a \cdot ca \cdot (b - c) = a \cdot b - a \cdot c$$

Per esempio $7 \cdot 12 = 7 \cdot (10 + 2) = 70 + 14 = 84$. La divisione è distributiva rispetto all'addizione e alla sottrazione **solo a destra**, cioè quando la somma è il dividendo (e le divisioni sono tutte esatte):

$$(a + b) : c = a : c + b : c \text{ ad esempio } (40 + 12) : 4 = 10 + 3 = 13.$$

A sinistra invece non funziona: $60 : (10 + 2) = 60 : 12 = 5$, mentre $60 : 10 + 60 : 2 = 6 + 30 = 36$.

1.3.2 Proprietà invariantiva, elementi neutri e assorbenti

La **proprietà invariantiva** della sottrazione dice che la differenza non cambia se si aggiunge o si toglie lo stesso numero a entrambi i termini: $83 - 29 = 84 - 30 = 54$. Quella della divisione dice che il quoziente (di una divisione esatta) non cambia se si moltiplicano o si dividono dividendo e divisore per lo stesso numero diverso da zero: $1400 : 25 = 5600 : 100 = 56$.

Un **elemento neutro** è un numero che, in un'operazione, lascia invariato l'altro termine: 0 è neutro per l'addizione ($a + 0 = a$), 1 è neutro per la moltiplicazione ($a \cdot 1 = a$). Lo 0 è invece l'**elemento assorbente** della moltiplicazione: $a \cdot 0 = 0$. Ne segue la legge di annullamento del prodotto: un prodotto è zero se e solo se almeno uno dei fattori è zero. La ritroverai, molto utile, quando risolverai le equazioni.

Tabella 1.1 Le proprietà delle operazioni in $\mathbb{N}$ (✓ = vale; – = non vale).

Proprietà	Addizione	Sottrazione	Moltiplicazione	Divisione
Interna a $\mathbb{N}$	✓	–	✓	–
Commutativa	✓	–	✓	–
Associativa	✓	–	✓	–
Distributiva	–	–	✓ rispetto a + e –	✓ solo a destra, rispetto a + e –
Invariantiva	–	✓ (± stesso numero)	–	✓ (· o : stesso numero ≠ 0)
Elemento neutro	0	0 solo a destra ($a - 0 = a$)	1	1 solo a destra ($a : 1 = a$)
Elemento assorbente	–	–	0	–

ESEMPIO SVOLTO

Calcolo mentale con le proprietà

Calcola a mente: a) $25 \cdot 17 \cdot 4$; b) $99 \cdot 36$; c) $1800 : 45$.

a) Per la proprietà commutativa e associativa, $25 \cdot 17 \cdot 4 = (25 \cdot 4) \cdot 17 = 100 \cdot 17 = 1700$.

b) Scriviamo $99 = 100 - 1$ e usiamo la proprietà distributiva: $99 \cdot 36 = 100 \cdot 36 - 1 \cdot 36 = 3600 - 36 = 3564$.

c) Per la proprietà invariantiva moltiplichiamo dividendo e divisore per 2: $1800 : 45 = 3600 : 90 = 360 : 9 = 40$ (nell'ultimo passaggio abbiamo diviso entrambi per 10).

1.4 Le potenze e le espressioni

1.4.1 Che cos'è una potenza

Come la moltiplicazione abbrevia un'addizione ripetuta, così la potenza abbrevia una moltiplicazione ripetuta. Se a e n sono numeri naturali e $n \geq 2$, la **potenza** a^n è il prodotto di n fattori uguali ad a:

$$a^n = a \cdot a \cdot \ldots \cdot a \ (n \text{ fattori}) \quad \text{per esempio } 2^5 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32.$$

Il numero a si chiama **base**, il numero n esponente. Si legge «a elevato alla n»; a^2 si legge anche «a al quadrato» e a^3 «a al cubo». La definizione si completa con due casi particolari, scelti in modo che le proprietà che vedremo restino sempre valide:

- $a^1 = a$ per ogni a;
- $a^0 = 1$ per ogni $a \neq 0$;
- 0^0 **non è definita**: è un'espressione priva di significato.

Perché $a^0 = 1$? Pensa al quoziente $2^5 : 2^5$, che vale $32 : 32 = 1$. Se vogliamo che valga la regola «quoziente di potenze di uguale base: si sottraggono gli esponenti», deve essere anche $2^5 : 2^5 = 2^{5-5} = 2^0$. Quindi $2^0 = 1$. Con base 0 questo ragionamento non funziona, perché $0^5 : 0^5 = 0 : 0$, che è indeterminata.

Le potenze di 10 hanno un aspetto molto semplice: 10^n si scrive con un 1 seguito da n zeri ($10^3 = 1000$, $10^6 = 1\,000\,000$). Per questo sono alla base della notazione scientifica, che userai in fisica e in chimica.

1.4.2 Le proprietà delle potenze

IN SINTESI

Le cinque proprietà delle potenze

Per basi e esponenti naturali (con le basi diverse da 0 dove compaiono esponenti nulli o divisioni):

1. **Prodotto di potenze di uguale base:** $a^m \cdot a^n = a^{m+n}$ ($2^3 \cdot 2^4 = 2^7$)
2. **Quoziente di potenze di uguale base:** $a^m : a^n = a^{m-n}$, con $m \geq n$ ($5^8 : 5^6 = 5^2$)
3. **Potenza di una potenza:** $(a^m)^n = a^{m \cdot n}$ ($(3^2)^4 = 3^8$)
4. **Prodotto di potenze di uguale esponente:** $a^n \cdot b^n = (a \cdot b)^n$ ($4^3 \cdot 5^3 = 20^3$)
5. **Quoziente di potenze di uguale esponente:** $a^n : b^n = (a : b)^n$, se la divisione $a : b$ è esatta ($12^5 : 4^5 = 3^5$)

Ognuna di queste proprietà si giustifica contando i fattori. Per esempio $2^3 \cdot 2^4 = (2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2 \cdot 2)$: in tutto i fattori uguali a 2 sono $3 + 4 = 7$. E $(3^2)^4 = 3^2 \cdot 3^2 \cdot 3^2 \cdot 3^2$: quattro gruppi di due fattori, cioè $2 \cdot 4 = 8$ fattori. Nella quarta proprietà, $4^3 \cdot 5^3 = (4 \cdot 4 \cdot 4) \cdot (5 \cdot 5 \cdot 5)$, e riordinando i fattori (proprietà commutativa e associativa) si ottiene $(4 \cdot 5) \cdot (4 \cdot 5) \cdot (4 \cdot 5) = 20^3$.

ERRORE FREQUENTE

La potenza non si distribuisce su una somma. $(3 + 4)^2 = 7^2 = 49$, mentre $3^2 + 4^2 = 9 + 16 = 25$. In generale $(a + b)^n \neq a^n + b^n$: la quarta proprietà vale per il *prodotto*, non per la somma.

Potenza di potenza e «esponente potenza» sono cose diverse. $(2^3)^2 = 2^{3 \cdot 2} = 2^6 = 64$, mentre 2^{3^2} significa 2 elevato a $3^2 = 9$, cioè $2^9 = 512$.

Non si sommano potenze con le regole del prodotto: $2^3 + 2^4 = 8 + 16 = 24$, e non 2^7.

1.4.3 Le espressioni e l'ordine delle operazioni

Un'**espressione** aritmetica è una sequenza di numeri legati da segni di operazione ed eventualmente da parentesi. Per evitare ambiguità, tutti seguono le stesse convenzioni.

DA RICORDARE

L'ordine delle operazioni

1. Si eseguono prima le operazioni dentro le parentesi: prima le tonde ( ), poi le quadre [ ], infine le graffe { }.

2. All'interno di ciascuna parentesi (e alla fine fuori da tutte) si calcolano prima le **potenze**, poi **moltiplicazioni e divisioni** nell'ordine in cui compaiono da sinistra a destra, infine **addizioni e sottrazioni**, anch'esse da sinistra a destra.

L'ordine conta davvero: $2 + 3 \cdot 4$ vale $2 + 12 = 14$, non $5 \cdot 4 = 20$. E $24 : 4 \cdot 2$ vale $6 \cdot 2 = 12$ (si procede da sinistra a destra), non $24 : 8 = 3$.

ESEMPIO SVOLTO

Un'espressione con le potenze

Calcola $\{[(2^4 \cdot 2^2) : 2^3 + 3 \cdot 4] : 5 + 3^2\} : 13$.

Tonde: $2^4 \cdot 2^2 = 2^6$ (prima proprietà).

Quadre: $2^6 : 2^3 = 2^3 = 8$ (seconda proprietà); poi $3 \cdot 4 = 12$; quindi $8 + 12 = 20$.

Graffe: $20 : 5 = 4$; $3^2 = 9$; $4 + 9 = 13$.

Infine $13 : 13 = \mathbf{1}$.

1.5 Divisibilità, numeri primi, MCD e mcm

1.5.1 Multipli e divisori

Se la divisione $a : b$ è esatta, cioè se esiste un naturale k tale che $a = b \cdot k$, diciamo che a è un **multiplo** di b, e che b è un **divisore** di a (o che b divide a, o che a è divisibile per b). Per esempio $42 = 6 \cdot 7$: 42 è multiplo di 6 e di 7, che sono suoi divisori.

I multipli di un numero sono infiniti: i multipli di 6 sono 0, 6, 12, 18, 24, … Lo 0 è multiplo di ogni numero, perché $0 = b \cdot 0$. I divisori di un numero diverso da 0, invece, sono in numero finito: i divisori di 42 sono 1, 2, 3, 6, 7, 14, 21, 42. Ogni numero è divisibile per 1 e per sé stesso.

1.5.2 I criteri di divisibilità

Per sapere se un numero è divisibile per un altro non sempre serve eseguire la divisione: per alcuni divisori basta guardare le cifre. La Tabella 1.2 riassume i **criteri di divisibilità** più usati.

Tabella 1.2 Criteri di divisibilità, con un esempio per ciascuno.

Per	Un numero è divisibile se…	Esempio
2	l'ultima cifra è pari (0, 2, 4, 6, 8)	3578: ultima cifra 8
3	la somma delle cifre è divisibile per 3	4125: 4 + 1 + 2 + 5 = 12
4	le ultime due cifre formano un numero divisibile per 4 (oppure sono 00)	7316: 16 = 4 · 4
5	l'ultima cifra è 0 o 5	2035
9	la somma delle cifre è divisibile per 9	5841: 5 + 8 + 4 + 1 = 18
10	l'ultima cifra è 0	6490
11	la differenza tra la somma delle cifre di posto dispari e quella delle cifre di posto pari (contando da destra) è 0 o un multiplo di 11	8371: posti dispari 1 + 3 = 4, posti pari 7 + 8 = 15; 15 − 4 = 11
25	le ultime due cifre sono 00, 25, 50 o 75	3475

Perché funziona, per esempio, il criterio del 4? Un numero come 7316 si può scrivere come 7300 + 16 = 73 · 100 + 16. Poiché 100 = 4 · 25 è multiplo di 4, anche 73 · 100 lo è; quindi 7316 è divisibile per 4 se e solo se lo è 16. Lo stesso ragionamento, con 100 = 25 · 4, giustifica il criterio del 25. Per il 3 e il 9 si sfrutta il fatto che 10, 100, 1000, … superano di 1 un multiplo di 9 (9, 99, 999, …): togliendo questi multipli resta proprio la somma delle cifre.

1.5.3 Numeri primi e numeri composti

Un numero naturale maggiore di 1 si dice **numero primo** se ha esattamente due divisori: 1 e sé stesso. Si dice **numero composto** se ha più di due divisori. Così 2, 3, 5, 7, 11, 13 sono primi; 4, 6, 8, 9, 10, 12 sono composti. Il numero 2 è l'unico primo pari. I numeri 0 e 1 sono casi a parte: **1 non è né primo né composto** (ha un solo divisore), e nemmeno 0 è primo, perché è divisibile per tutti i numeri diversi da zero.

Un metodo semplice per trovare tutti i primi fino a un certo numero è il **crivello di Eratostene**, dal nome del matematico greco Eratostene di Cirene (III secolo a.C.). Si scrivono i numeri da 2 a 100; si cerchia il 2 e si cancellano tutti i suoi multipli successivi; il primo numero non cancellato, il 3, è primo: lo si cerchia e si cancellano i suoi multipli; poi si fa lo stesso con 5 e con 7. A questo punto ci si può fermare: ogni numero composto fino a 100 ha un fattore primo

minore o uguale a 10, perché due fattori entrambi maggiori di 10 darebbero un prodotto maggiore di 100. I numeri rimasti sono tutti primi: fino a 100 sono 25 (Figura 1.3).

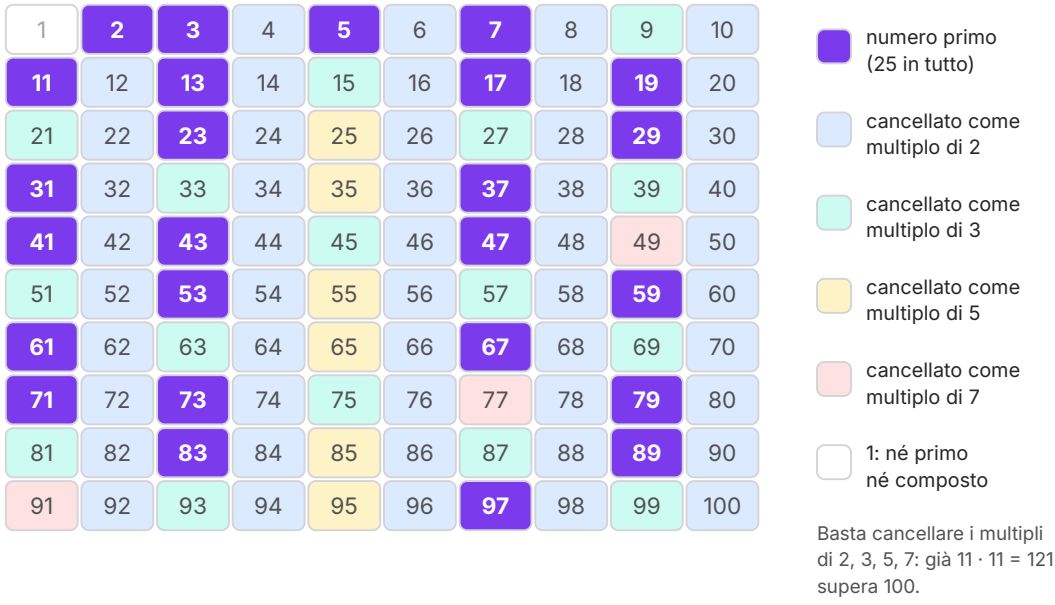


Figura 1.3 Il crivello di Eratostene da 1 a 100. Ogni numero composto è colorato secondo il più piccolo primo che lo divide, cioè secondo il passaggio in cui viene cancellato. Le caselle viola sono i 25 numeri primi minori di 100.

APPROFONDIMENTO

I numeri primi sono infiniti

Negli *Elementi*, l'opera scritta da Euclide ad Alessandria intorno al 300 a.C., si trova (nel libro IX) una delle dimostrazioni più celebri di tutta la matematica: i numeri primi sono più di qualunque quantità finita assegnata. L'idea, in linguaggio moderno, è questa. Supponiamo di avere un elenco finito di primi, per esempio 2, 3, 5. Costruiamo il numero $N = 2 \cdot 3 \cdot 5 + 1 = 31$. Diviso per 2, per 3 o per 5, N dà sempre resto 1: nessun primo dell'elenco lo divide. Allora o N stesso è primo, oppure ha un fattore primo che non è nell'elenco. In ogni caso l'elenco era incompleto. Poiché il ragionamento vale per qualunque elenco finito, i primi non possono finire.

Attenzione: N non è sempre primo. Con 2, 3, 5, 7, 11, 13 si ottiene $30\,031 = 59 \cdot 509$: un numero composto, ma i suoi fattori 59 e 509 sono primi nuovi, che non erano nell'elenco.

1.5.4 La scomposizione in fattori primi

I numeri primi sono i «mattoni» con cui si costruiscono, per moltiplicazione, tutti gli altri numeri. Questo fatto è così importante da avere un nome solenne.

È il **teorema fondamentale dell'aritmetica**: ogni numero naturale maggiore di 1 si può scrivere come prodotto di numeri primi, e questa scrittura è **unica**, a meno dell'ordine dei fattori.

Non dimostreremo il teorema, ma lo useremo spesso. Per ottenere la **scomposizione in fattori primi** (o fattorizzazione) di un numero si divide ripetutamente per i primi 2, 3, 5, 7, 11, ..., aiutandosi con i criteri di divisibilità, finché si arriva a 1. Si possono disporre i calcoli «ad albero» oppure in colonna (Figura 1.4). Alla fine i fattori uguali si raccolgono in potenze.

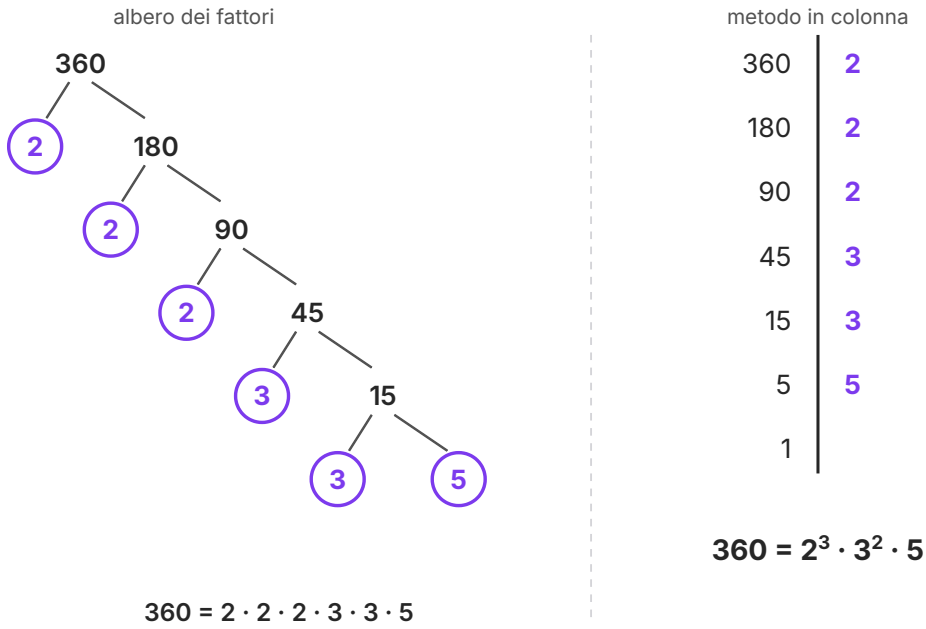


Figura 1.4 Due modi di scomporre 360 in fattori primi: l'albero dei fattori (a sinistra) e il metodo in colonna (a destra). I primi trovati sono cerchiati; in entrambi i casi si ottiene $360 = 2^3 \cdot 3^2 \cdot 5$.

L'unicità garantita dal teorema è preziosa: chiunque scomponga 360, partendo da qualunque divisione, troverà sempre tre fattori 2, due fattori 3 e un fattore 5. Dalla scomposizione si leggono subito i divisori di un numero: i divisori di 360 sono tutti e soli i prodotti $2^i \cdot 3^j \cdot 5^k$ con $i \le 3$, $j \le 2$, $k \le 1$.

1.5.5 Massimo comune divisore e minimo comune multiplo

Il **massimo comune divisore** di due o più numeri, indicato con MCD, è il più grande tra i loro divisori comuni. Il **minimo comune multiplo**, indicato con mcm, è il più piccolo tra i loro mul-

tipli comuni diversi da zero. Per esempio i divisori di 12 sono 1, 2, 3, 4, 6, 12 e quelli di 18 sono 1, 2, 3, 6, 9, 18: i divisori comuni sono 1, 2, 3, 6, quindi MCD(12, 18) = 6. I multipli di 12 sono 12, 24, 36, 48, … e quelli di 18 sono 18, 36, 54, …: il primo comune è 36, quindi mcm(12, 18) = 36.

Due numeri il cui MCD è 1 si dicono **primi tra loro** (o coprimi): per esempio 8 e 15, che non sono primi ma non hanno fattori in comune. Elencare divisori e multipli diventa presto scomodo; con la scomposizione in fattori primi il calcolo è rapido.

IN SINTESI

MCD e mcm con la scomposizione in fattori primi

MCD: prodotto dei soli fattori primi **comuni**, ciascuno preso una sola volta con l'esponente **minore**.

mcm: prodotto dei fattori primi **comuni e non comuni**, ciascuno preso una sola volta con l'esponente **maggiore**.

Per **due** numeri vale $\text{MCD}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$.

ESEMPIO SVOLTO

MCD e mcm di 120 e 252

Scomponiamo: $120 = 2^3 \cdot 3 \cdot 5$ e $252 = 2^2 \cdot 3^2 \cdot 7$.

MCD: i fattori comuni sono 2 e 3; con l'esponente minore: $2^2 \cdot 3 = 12$.

mcm: tutti i fattori, 2, 3, 5, 7, con l'esponente maggiore: $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 8 \cdot 9 \cdot 35 = 2520$.

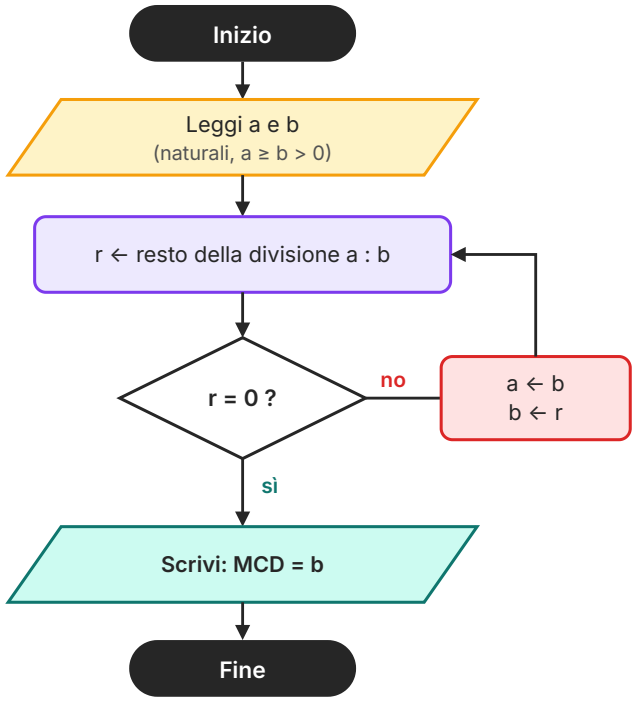
Controllo: $\text{MCD} \cdot \text{mcm} = 12 \cdot 2520 = 30\,240$ e $120 \cdot 252 = 30\,240$. ✓

Perché la relazione $\text{MCD} \cdot \text{mcm} = a \cdot b$ vale per due numeri? Per ciascun fattore primo, il MCD prende l'esponente minore e il mcm il maggiore; minore + maggiore è proprio la somma dei due esponenti, cioè l'esponente di quel primo nel prodotto $a \cdot b$. Con tre numeri il ragionamento si rompe, perché «minore + maggiore» trascura l'esponente intermedio: per 2, 4 e 8 si ha MCD = 2 e mcm = 8, ma $2 \cdot 8 = 16$ mentre $2 \cdot 4 \cdot 8 = 64$.

1.5.6 L'algoritmo di Euclide

Per numeri grandi anche la scomposizione diventa faticosa: prova a scomporre 30 031 a mano! Esiste però un metodo per trovare il MCD senza scomporre nulla, descritto già negli *Elementi* di Euclide (libro VII). Si basa su un'osservazione semplice: se $a = b \cdot q + r$, i divisori comuni di a e b sono esattamente i divisori comuni di b e r. Infatti un numero che divide a e b divide anche $r = a - b \cdot q$; e uno che divide b e r divide anche $a = b \cdot q + r$. Quindi $\text{MCD}(a, b) = \text{MCD}(b, r)$: si sostituisce la coppia di partenza con una coppia di numeri più piccoli, e si ripete finché il resto è 0. L'ultimo divisore usato è il MCD.

Questa procedura è un esempio di **algoritmo**: una sequenza finita di istruzioni precise che, eseguite in ordine, risolvono un problema in un numero finito di passi. Gli algoritmi si possono descrivere con un diagramma di flusso, in cui ogni forma ha un significato: gli ovali indicano inizio e fine, i parallelogrammi l'ingresso e l'uscita dei dati, i rettangoli le istruzioni, i rombi le domande a cui si risponde sì o no (Figura 1.5).



Esempio: MCD(252, 198)

a	*b*	*r*
252	198	54
198	54	36
54	36	18
36	**18**	0

$252 = 198 \cdot 1 + 54$

$198 = 54 \cdot 3 + 36$

$54 = 36 \cdot 1 + 18$

$36 = 18 \cdot 2 + 0$

MCD(252, 198) = 18

Figura 1.5 Diagramma di flusso dell'algoritmo di Euclide e sua esecuzione per MCD(252, 198). La freccia «a ← b» significa «a prende il valore di b». Il ciclo si ripete finché il resto non diventa 0.

Nell'esempio della figura le coppie successive sono (252, 198), (198, 54), (54, 36), (36, 18), e l'ultimo divisore è 18. Controllo con la scomposizione: $252 = 2^2 \cdot 3^2 \cdot 7$ e $198 = 2 \cdot 3^2 \cdot 11$, quindi MCD = $2 \cdot 3^2 = 18$. Ricavato il MCD, il mcm segue dalla relazione per due numeri: mcm = 252 · 198 : 18 = 2772.

L'algoritmo di Euclide è il primo di una lunga serie: anche la conversione in base due che vedremo tra poco, e perfino il crivello di Eratostene, sono algoritmi. Nel capitolo 17 studieremo gli algoritmi in sé: come si descrivono, come si controlla che funzionino e come un computer li esegue.

1.5.7 Problemi con MCD e mcm

Come capire, in un problema, se serve il MCD o il mcm? Una buona regola pratica: si cerca il **MCD** quando bisogna *dividere* quantità diverse in parti uguali, le più grandi possibili (piastrelle, confezioni, gruppi); si cerca il **mcm** quando eventi che si ripetono con periodi diversi devono *coincidere* di nuovo (autobus, turni, ingranaggi).

ESEMPIO SVOLTO

Due problemi tipici

Le piastrelle. Un pavimento rettangolare misura 270 cm per 420 cm. Vogliamo coprirlo con piastrelle quadrate tutte uguali, senza tagliarle, con il lato (in centimetri interi) più grande possibile. Il lato deve dividere sia 270 sia 420, ed essere il massimo possibile: è MCD(270, 420). Da $270 = 2 \cdot 3^3 \cdot 5$ e $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ si ottiene $\text{MCD} = 2 \cdot 3 \cdot 5 = 30$. Servono $(270 : 30) \cdot (420 : 30) = 9 \cdot 14 = 126$ piastrelle di lato 30 cm.

Gli autobus. Dal capolinea partono la linea 4 ogni 15 minuti e la linea 9 ogni 25 minuti. Se alle 8:00 partono insieme, quando ripartiranno di nuovo insieme? Le partenze comuni avvengono dopo un numero di minuti che è multiplo sia di 15 sia di 25; la prima è mcm(15, 25). Da $15 = 3 \cdot 5$ e $25 = 5^2$ si ha $\text{mcm} = 3 \cdot 5^2 = 75$ minuti: la prossima partenza comune è alle 9:15.

1.6 I sistemi di numerazione

1.6.1 La notazione posizionale in base dieci

Un numero e il modo in cui lo scriviamo non sono la stessa cosa: «dodici», 12, XII e 1100_2 sono quattro scritture diverse dello stesso numero. Il modo di scrivere i numeri che usiamo ogni giorno è un **sistema di numerazione posizionale** in base dieci: usa dieci cifre (0, 1, ..., 9), e il valore di ogni cifra dipende dalla *posizione* che occupa. Nel numero 3507 la cifra 3 vale 3 migliaia, la cifra 5 vale 5 centinaia; nella posizione delle decine c'è 0, che segnala che le decine mancano:

$$3507 = 3 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10^1 + 7 \cdot 10^0.$$

Questa è la forma polinomiale del numero. L'idea decisiva è lo zero come cifra «segnaposto»: senza di esso non si distinguerebbe 357 da 3507.

Non tutti i sistemi di numerazione sono posizionali. Nei numeri romani (I = 1, V = 5, X = 10, L = 50, C = 100, D = 500, M = 1000) un simbolo vale sempre lo stesso, dovunque si trovi: il sistema è additivo, e XVII = 10 + 5 + 1 + 1 = 17 (con la sola convenzione che un simbolo minore scritto prima di uno maggiore si sottrae, come in IV = 4). Senza lo zero e senza il valore di posizione, i calcoli scritti erano lentissimi: prova a moltiplicare XXXVII per XIV senza tradurli!

APPROFONDIMENTO

Le cifre «arabe» vengono dall'India

Il sistema posizionale decimale con lo zero si sviluppò in India nei primi secoli del Medioevo e giunse in Europa attraverso i matematici del mondo arabo: per questo parliamo di cifre *indo-arabe*. Un ruolo decisivo nella sua diffusione in Europa lo ebbe il pisano Leonardo Fibonacci, che nel 1202 completò il *Liber abaci*, un trattato che insegnava a calcolare con le nuove cifre e ne mostrava i vantaggi nei commerci. Prima, in Europa, si usavano soprattutto i numeri romani, scomodi per i calcoli scritti.

1.6.2 Il sistema binario

Nulla obbliga a usare dieci cifre. Nel **sistema binario**, o in base due, le cifre sono solo 0 e 1 e ogni posizione vale il doppio della precedente: 1, 2, 4, 8, 16, 32, … cioè le potenze di 2. Per indicare la base si scrive un piccolo indice: 1101_2 significa

$$1101_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 0 + 1 = 13.$$

Questo è anche il metodo per passare **dalla base 2 alla base 10**: si scrive il numero in forma polinomiale e si calcola. Per il passaggio inverso, **dalla base 10 alla base 2**, si usa il metodo delle divisioni successive: si divide il numero per 2, poi si divide per 2 il quoziente ottenuto, e così via finché il quoziente è 0; i resti, letti dall'ultimo al primo, sono le cifre binarie (Figura 1.6).

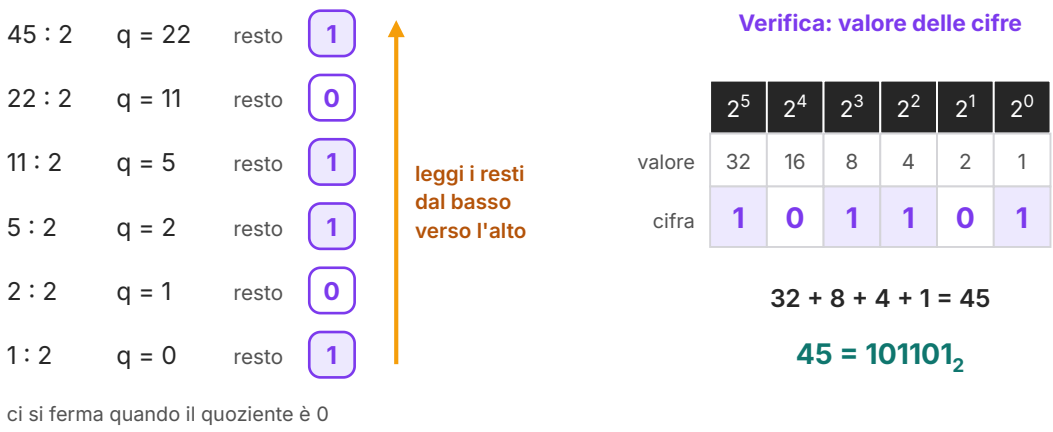


Figura 1.6 Conversione di 45 in base 2 con il metodo delle divisioni successive. I resti, letti dal basso verso l'alto, danno 101101_2; la tabella a destra verifica il risultato sommando le potenze di 2 corrispondenti alle cifre 1.

COLLEGAMENTI

Bit, byte e colori esadecimali

I circuiti di un computer distinguono bene due stati, come «passa corrente» e «non passa corrente»: per questo i dati sono codificati in binario. Una cifra binaria si chiama bit (da *binary digit*); otto bit formano un *byte*. Con 8 bit si scrivono $2^8 = 256$ numeri diversi, da 0 a 255. Le lunghe file di 0 e 1 sono scomode da leggere, e gli informatici usano spesso la **base sedici** (esadecimale), con le cifre 0–9 e le lettere A, B, C, D, E, F per i valori da 10 a 15. Nelle pagine web un colore si scrive con tre coppie di cifre esadecimali, che indicano quanto rosso, verde e blu mescolare: ciascuna coppia va da 00 (zero) a FF = $15 \cdot 16 + 15 = 255$.

Con questi strumenti, operazioni, proprietà, potenze, divisibilità, numerazione, abbiamo costruito il primo «piano» dell'edificio dei numeri. Nel prossimo capitolo lo allargheremo con i numeri negativi, per rendere sempre possibile la sottrazione.

SINTESI

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ è totalmente ordinato, discreto, ha minimo 0 e non ha massimo; ogni numero ha un successivo, ogni numero tranne 0 un precedente.
- Addizione e moltiplicazione sono interne a $\mathbb{N}$; sottrazione e divisione esatta no.
- Divisione con resto: $a = b \cdot q + r$ con $0 \le r < b$ ($b \neq 0$).
- $a : 0$ è impossibile se $a \neq 0$; $0 : 0$ è indeterminata.
- Proprietà commutativa e associativa per + e ·; distributiva di · rispetto a + e −; la divisione è distributiva solo a destra; invariantiva per − e :.
- 0 è neutro per l'addizione e assorbente per la moltiplicazione; 1 è neutro per la moltiplicazione.
- $a^1 = a$; $a^0 = 1$ se $a \neq 0$; 0^0 non è definita. Le cinque proprietà valgono per prodotti e quozienti, mai per somme.
- Nelle espressioni: parentesi tonde, quadre, graffe; poi potenze, moltiplicazioni e divisioni, addizioni e sottrazioni.
- Un primo ha esattamente due divisori; 1 non è né primo né composto; i primi sono infiniti (Euclide).
- Ogni naturale maggiore di 1 si scompone in modo unico in fattori primi.
- MCD: fattori comuni con l'esponente minore; mcm: comuni e non comuni con l'esponente maggiore; per due numeri MCD · mcm = $a \cdot b$. L'algoritmo di Euclide trova il MCD con divisioni successive.
- Nei sistemi posizionali il valore di una cifra dipende dalla posizione; in base 2 le posizioni valgono 1, 2, 4, 8, ...

ESERCIZI

Comprendere

1. ● Quale affermazione sull'insieme $\mathbb{N}$ è vera?
   A. $\mathbb{N}$ ha un massimo.
   B. Ogni numero naturale ha un precedente in $\mathbb{N}$.
   C. Tra due numeri naturali consecutivi non ci sono altri numeri naturali.
   D. Lo 0 non appartiene a $\mathbb{N}$.

2. ● Nella divisione con resto $47 : 6$ il quoziente e il resto sono:
   A. $q = 7, r = 5$
   B. $q = 6, r = 11$
   C. $q = 8, r = 1$
   D. $q = 7, r = 4$

3. ● L'operazione $0 : 0$ è:
   A. uguale a 0
   B. uguale a 1
   C. impossibile
   D. indeterminata

4. ● $(2^3)^2$ è uguale a:
   A. 2^5
   B. 2^6
   C. 2^9
   D. 4^5

5. ●● Quale di questi numeri è divisibile per 11?
   A. 1234
   B. 5172
   C. 9361
   D. 4545

6. ●● Il numero binario 11010_2 in base dieci vale:
   A. 13
   B. 52
   C. 24
   D. 26

7. ● Vero o falso? Correggi le affermazioni false.
a) 1 è un numero primo. b) La sottrazione è un'operazione interna a $\mathbb{N}$. c) 0 è multiplo di ogni numero naturale. d) Se un numero è divisibile per 9, allora è divisibile per 3. e) Per tre numeri qualsiasi MCD · mcm è uguale al prodotto dei tre numeri.

8. ● Vero o falso? Correggi le affermazioni false.
a) $a^0 = 1$ per ogni $a \in \mathbb{N}$. b) $(3 + 4)^2 = 3^2 + 4^2$. c) $2^5 \cdot 5^5 = 10^5$. d) $(12 + 18) : 6 = 12 : 6 + 18 : 6$. e) $6 : (2 + 1) = 6 : 2 + 6 : 1$.

9. ● Completa.
a) Nella sottrazione $a - b = c$, a si chiama _____ , b _____ , c _____ . b) Nella divisione con resto $a = b \cdot q + r$ deve essere $0 \leq r <$ _____ . c) Due numeri sono primi tra loro se il loro MCD è _____ . d) Un sistema di numerazione è posizionale se il valore di una cifra dipende _____ .

Calcolare

10. ● Calcola a mente, indicando la proprietà che usi: a) $25 \cdot 37 \cdot 4$; b) $99 \cdot 23$; c) $46 + 27 + 54$; d) $1400 : 25$; e) $83 - 29$.

11. ● Esegui la divisione con resto e scrivi l'uguaglianza $a = b \cdot q + r$: a) 125 : 9; b) 300 : 17; c) 1000 : 37; d) 8 : 15.

12. ● Applica le proprietà delle potenze e scrivi il risultato come un'unica potenza: a) $3^4 \cdot 3^5$; b) $7^{12} : 7^4$; c) $(5^2)^3$; d) $6^7 : 2^7$; e) $4^3 \cdot 25^3$ (come potenza di 10); f) $(2^3 \cdot 2^4)^2 : 2^{10}$.

13. ● Calcola: a) $2^0 + 0^2 + 1^5$; b) $10^4 - 10^3$; c) 2^{3^2} e $(2^3)^2$; d) $5^3 - 5^2$.

14. ● Calcola il valore dell'espressione $[(3^2 + 4 \cdot 2) \cdot 2 - 6^2 : 4] : 5$.

15. ●● Calcola il valore dell'espressione $\{[(2^5 : 2^3 + 1)^2 - 5 \cdot 3] \cdot 2 + 2^4\} : 6$.

16. ●● Calcola il valore dell'espressione $[(6^3 : 6) : 3^2 + 5^0]^2 : 5 - 2$.

17. ● Stabilisci, usando i criteri, per quali tra 2, 3, 4, 5, 9, 10, 11, 25 è divisibile il numero 7920.

18. ● Scomponi in fattori primi: a) 84; b) 252; c) 1125; d) 2310; e) 4096.

19. ●● Calcola MCD e mcm con la scomposizione in fattori primi: a) 36 e 60; b) 84, 126 e 210; c) 35 e 48.

20. ●● Calcola il MCD con l'algoritmo di Euclide, scrivendo tutte le divisioni: a) MCD(1071, 462); b) MCD(377, 233).

21. ●● Converti: a) 37 in base 2; b) 100 in base 2; c) 1011011_2 in base 10; d) $2A_{16}$ in base 10; e) 255 in base 16.

Dimostrare e argomentare

22. ●● Spiega perché $7 : 0$ è impossibile, mentre $0 : 0$ è indeterminata. Che cosa hanno in comune i due casi?

23. ●● Trova l'errore: «$2^3 \cdot 3^2 = 6^5$, perché si moltiplicano le basi e si sommano gli esponenti». Calcola poi il valore corretto.

24. ●● Dimostra che la somma di tre numeri naturali consecutivi è sempre un multiplo di 3. (Suggerimento: chiama n il più piccolo dei tre.)

25. ●● Spiega perché per stabilire se un numero è divisibile per 4 basta guardare le sue ultime due cifre.

26. ●●● Mostra con un esempio che la relazione MCD · mcm = prodotto dei numeri può essere falsa per tre numeri, e spiega perché invece è sempre vera per due.

Problemi

27. ● Un pavimento rettangolare misura 360 cm per 504 cm. Si vuole coprirlo con piastrelle quadrate uguali, intere, con il lato (in centimetri interi) più grande possibile. Quanto misura il lato? Quante piastrelle servono?

28. ●● Da una piazza partono tre linee di autobus: la A ogni 12 minuti, la B ogni 18, la C ogni 30. Alle 7:00 partono tutte insieme. A che ora ripartiranno di nuovo tutte e tre insieme?

29. ● Per una gita, 156 studenti e 12 docenti devono viaggiare su pullman da 54 posti. Quanti pullman servono? Quante persone viaggiano sull'ultimo pullman, se gli altri sono completi?

30. ●● Hai 84 penne rosse e 120 penne blu e vuoi preparare il maggior numero possibile di confezioni uguali, ciascuna con lo stesso numero di penne rosse e lo stesso numero di penne blu, senza avanzi. Quante confezioni puoi preparare? Che cosa contiene ciascuna?

31. ●● (Informatica) Quanti numeri naturali diversi si possono scrivere con 8 bit? E con 10 bit? Qual è il numero più grande scrivibile con 10 bit?

32. ● Oggi è martedì. Che giorno della settimana sarà fra 100 giorni? (Suggerimento: usa la divisione con resto per 7.)

Con il computer

33. ●● *Euclide nel foglio di calcolo.* In un foglio di calcolo scrivi 2730 in A1 e 1430 in B1; in C1 scrivi =RESTO(A1;B1). Nella riga 2 scrivi =B1 in A2, =C1 in B2 e copia C1 in C2. Trascina la riga 2 verso il basso finché nella colonna C compare 0. a) Quali coppie compaiono nelle righe? b) Qual è il MCD(2730, 1430)? c) Verifica il risultato con la scomposizione in fattori primi.

34. ●● Usa lo stesso foglio per calcolare MCD(12345, 5432). Quante righe servono prima che compaia il resto 0? Che cosa puoi dire dei due numeri?

Verso la verifica

35. ●● Calcola il valore dell'espressione $\{[(3^4 : 3^2)^2 : 3^3 + 2 \cdot 5]^2 : 13 - 2^2\}$, usando dove possibile le proprietà delle potenze.

36. ●● Di due numeri si sa che il MCD è 6, il mcm è 72 e uno dei due è 18. Trova l'altro. È possibile che due numeri abbiano MCD = 5 e mcm = 72? Motiva la risposta.

37. ●●● Sfida. Trova il più piccolo numero naturale che, diviso per 2, per 3, per 4, per 5 e per 6, dà sempre resto 1, ed è divisibile per 7.

PER APPROFONDIRE

- [ENZ] Un romanzo in dodici «notti» in cui un ragazzo scopre, giocando, numeri primi, potenze e molto altro.
- [DUS] La storia dei numeri primi e delle domande ancora aperte su di essi, raccontata per un pubblico non specialista.
- [CR] Il primo capitolo tratta i numeri naturali, l'induzione e la teoria dei numeri primi a un livello più avanzato.
- [EUC] I libri VII e IX degli *Elementi*: l'algoritmo per il massimo comune divisore e l'infinità dei primi.

Glossario del capitolo

Algoritmo di Euclide
Metodo per calcolare il MCD di due numeri sostituendo la coppia (a, b) con (b, r), dove r è il resto di a : b, finché il resto è 0.

Crivello di Eratostene
Procedimento per trovare i numeri primi fino a un limite cancellando via via i multipli di ogni primo.

Divisione con resto
Dati a e b ≠ 0, la ricerca dei naturali unici q e r con a = b · q + r e 0 ≤ r < b.

Divisione impossibile
La divisione a : 0 con a ≠ 0: nessun numero può esserne il risultato.

Divisione indeterminata
La divisione 0 : 0: qualunque numero andrebbe bene come risultato, quindi non ce n'è uno solo.

Elemento assorbente
Numero che, in un'operazione, dà sempre sé stesso come risultato: 0 per la moltiplicazione.

Elemento neutro
Numero che in un'operazione lascia invariato l'altro termine: 0 per l'addizione, 1 per la moltiplicazione.

Insieme discreto
Insieme in cui tra due elementi consecutivi non ce ne sono altri, come $\mathbb{N}$ e $\mathbb{Z}$.

Massimo comune divisore (MCD)
Il più grande divisore comune a due o più numeri; si ottiene dai fattori primi comuni con l'esponente minore.

Minimo comune multiplo (mcm)
Il più piccolo multiplo comune, diverso da 0, di due o più numeri; si ottiene dai fattori primi comuni e non comuni con l'esponente maggiore.

Numeri naturali
I numeri 0, 1, 2, 3, … usati per contare; il loro insieme si indica con $\mathbb{N}$.

Numero composto
Numero naturale maggiore di 1 con più di due divisori.

Numero primo
Numero naturale maggiore di 1 che ha esattamente due divisori, 1 e sé stesso.

Operazione interna
Operazione che, applicata a elementi di un insieme, dà sempre un risultato nello stesso insieme: in $\mathbb{N}$ addizione e moltiplicazione, in $\mathbb{Z}$ anche la sottrazione.

Potenza
Prodotto di n fattori uguali alla base a, scritto a^n; $a^1 = a$, $a^0 = 1$ se $a \neq 0$, 0^0 non è definita.

Proprietà distributiva
a · (b + c) = a · b + a · c; per la divisione vale solo a destra: (a + b) : c = a : c + b : c.

Proprietà invariantiva
La differenza non cambia aggiungendo o togliendo lo stesso numero ai due termini; il quoziente non cambia moltiplicando o dividendo i due termini per lo stesso numero diverso da 0.

Sistema posizionale
Sistema di numerazione in cui il valore di una cifra dipende dalla posizione che occupa; in base 2 le posizioni valgono 1, 2, 4, 8, …

Successivo
Il numero naturale che segue immediatamente n, cioè n + 1.

Teorema fondamentale dell'aritmetica
Ogni naturale maggiore di 1 si scrive come prodotto di numeri primi in modo unico, a meno dell'ordine dei fattori.

Soluzioni

1. C. $\mathbb{N}$ non ha massimo, 0 non ha precedente e $0 \in \mathbb{N}$; tra due naturali consecutivi non ci sono altri naturali ($\mathbb{N}$ è discreto).

2. A. $47 = 6 \cdot 7 + 5$, con $0 \le 5 < 6$. (B e C hanno resto ≥ 6; con D l'uguaglianza $6 \cdot 7 + 4 = 46$ è falsa.)

3. D. Ogni numero moltiplicato per 0 dà 0: non c'è un unico risultato, quindi $0 : 0$ è indeterminata.

4. B. Potenza di potenza: $(2^3)^2 = 2^{3 \cdot 2} = 2^6 = 64$.

5. C. Per 9361: posti dispari $1 + 3 = 4$, posti pari $6 + 9 = 15$, differenza 11: divisibile ($9361 = 11 \cdot 851$). Per 1234 la differenza è 2, per 5172 è 9, per 4545 è 2.

6. D. $11010_2 = 16 + 8 + 0 + 2 + 0 = 26$.

7. a) F: 1 non è né primo né composto (ha un solo divisore). b) F: per esempio $3 - 5$ non ha risultato in $\mathbb{N}$. c) V: $0 = n \cdot 0$. d) V: $9 = 3 \cdot 3$, quindi ogni multiplo di 9 è multiplo di 3. e) F: vale solo per due numeri; per 2, 4, 8 si ha $\text{MCD} \cdot \text{mcm} = 2 \cdot 8 = 16 \neq 64$.

8. a) F: solo per $a \neq 0$; 0^0 non è definita. b) F: $7^2 = 49$, mentre $9 + 16 = 25$. c) V: $2^5 \cdot 5^5 = (2 \cdot 5)^5 = 10^5$. d) V: distributiva a destra, $30 : 6 = 5 = 2 + 3$. e) F: $6 : 3 = 2$, mentre $6 : 2 + 6 : 1 = 3 + 6 = 9$ (la divisione non è distributiva a sinistra).

9. a) minuendo, sottraendo, differenza. b) b (il divisore). c) 1. d) dalla posizione che occupa nella scrittura del numero.

10. a) $(25 \cdot 4) \cdot 37 = 100 \cdot 37 = 3700$ (commutativa e associativa). b) $(100 - 1) \cdot 23 = 2300 - 23 = 2277$ (distributiva). c) $(46 + 54) + 27 = 100 + 27 = 127$ (commutativa e associativa). d) $5600 : 100 = 56$ (invariantiva, $\cdot 4$). e) $84 - 30 = 54$ (invariantiva, $+1$).

11. a) $125 = 9 \cdot 13 + 8$. b) $300 = 17 \cdot 17 + 11$. c) $1000 = 37 \cdot 27 + 1$. d) $8 = 15 \cdot 0 + 8$.

12. a) 3^9. b) 7^8. c) 5^6. d) $(6 : 2)^7 = 3^7$. e) $(4 \cdot 25)^3 = 100^3 = (10^2)^3 = 10^6$. f) $(2^7)^2 : 2^{10} = 2^{14} : 2^{10} = 2^4$.

13. a) $1 + 0 + 1 = 2$. b) $10000 - 1000 = 9000$. c) $2^{3^2} = 2^9 = 512$; $(2^3)^2 = 2^6 = 64$. d) $125 - 25 = 100$.

14. $(9 + 8) \cdot 2 = 34$; $36 : 4 = 9$; $34 - 9 = 25$; $25 : 5 =$ **5**.

15. $2^5 : 2^3 = 2^2 = 4$; $(4 + 1)^2 = 25$; $25 - 15 = 10$; $10 \cdot 2 + 16 = 36$; $36 : 6 =$ **6**.

16. $6^3 : 6 = 6^2 = 36$; $36 : 9 = 4$; $4 + 1 = 5$; $5^2 = 25$; $25 : 5 - 2 =$ **3**.

17. Ultima cifra 0: divisibile per 2, 5, 10. Somma delle cifre $7 + 9 + 2 + 0 = 18$: divisibile per 3 e per 9. Ultime due cifre $20 = 4 \cdot 5$: divisibile per 4. Posti dispari $0 + 9 = 9$, posti pari $2 + 7 = 9$, differenza 0: divisibile per 11 ($7920 = 11 \cdot 720$). Ultime due cifre 20: non divisibile per 25. Quindi: 2, 3, 4, 5, 9, 10, 11.

18. a) $84 = 2^2 \cdot 3 \cdot 7$. b) $252 = 2^2 \cdot 3^2 \cdot 7$. c) $1125 = 3^2 \cdot 5^3$. d) $2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. e) $4096 = 2^{12}$.

19. a) $36 = 2^2 \cdot 3^2$, $60 = 2^2 \cdot 3 \cdot 5$: $\text{MCD} = 2^2 \cdot 3 = 12$, $\text{mcm} = 2^2 \cdot 3^2 \cdot 5 = 180$. b) $84 = 2^2 \cdot 3 \cdot 7$, $126 = 2 \cdot 3^2 \cdot 7$, $210 = 2 \cdot 3 \cdot 5 \cdot 7$: $\text{MCD} = 2 \cdot 3 \cdot 7 = 42$, $\text{mcm} = 2^2 \cdot 3^2 \cdot 5 \cdot 7 = 1260$. c) $35 = 5 \cdot 7$, $48 = 2^4 \cdot 3$: $\text{MCD} = 1$ (primi tra loro), $\text{mcm} = 35 \cdot 48 = 1680$.

20. a) $1071 = 462 \cdot 2 + 147$; $462 = 147 \cdot 3 + 21$; $147 = 21 \cdot 7 + 0$: $\text{MCD} = 21$. b) $377 = 233 \cdot 1 + 144$; $233 = 144 \cdot 1 + 89$; $144 = 89 \cdot 1 + 55$; $89 = 55 \cdot 1 + 34$; $55 = 34 \cdot 1 + 21$; $34 = 21 \cdot 1 + 13$; $21 = 13 \cdot 1 + 8$; $13 = 8 \cdot 1 + 5$; $8 = 5 \cdot 1 + 3$; $5 = 3 \cdot 1 + 2$; $3 = 2 \cdot 1 + 1$; $2 = 1 \cdot 2 + 0$: $\text{MCD} = 1$ (377 e 233 sono primi tra loro).

21. a) $37 = 100101_2$ $(32 + 4 + 1)$. b) $100 = 1100100_2$ $(64 + 32 + 4)$. c) $64 + 16 + 8 + 2 + 1 = 91$. d) $2 \cdot 16 + 10 = 42$. e) $255 = 15 \cdot 16 + 15 = \text{FF}_{16}$.

22. Traccia: $7 : 0$ dovrebbe essere un numero che moltiplicato per 0 dia 7, ma ogni numero moltiplicato per 0 dà 0: nessun risultato, divisione impossibile. $0 : 0$ dovrebbe essere un numero che moltiplicato per 0 dia 0: va bene qualunque numero, quindi non c'è un risultato unico, divisione indeterminata. In comune: in nessuno dei due casi la divisione dà un risultato ben definito, perciò il divisore deve essere sempre diverso da 0.

23. Le proprietà delle potenze valgono solo per potenze con la stessa base (si sommano gli esponenti) o con lo stesso esponente (si moltiplicano le basi), non per basi ed esponenti entrambi diversi. Valore corretto: $2^3 \cdot 3^2 = 8 \cdot 9 = 72$, mentre $6^5 = 7776$.

24. I tre numeri sono n, $n + 1$, $n + 2$. La somma è $n + n + 1 + n + 2 = 3 \cdot n + 3 = 3 \cdot (n + 1)$ per la proprietà distributiva: è un multiplo di 3 (il triplo del numero centrale). Es.: $7 + 8 + 9 = 24 = 3 \cdot 8$.

25. Ogni numero si scrive come (numero delle centinaia) · 100 + (numero formato dalle ultime due cifre). Poiché $100 = 4 \cdot 25$ è multiplo di 4, il primo addendo è sempre multiplo di 4; quindi il numero è divisibile per 4 se e solo se lo è il secondo addendo, cioè il numero formato dalle ultime due cifre.

26. Esempio: 2, 4, 8: MCD = 2, mcm = 8, MCD · mcm = 16, mentre $2 \cdot 4 \cdot 8 = 64$. Per due numeri, per ogni fattore primo il MCD prende l'esponente minore e il mcm il maggiore: la loro somma è la somma dei due esponenti, cioè l'esponente nel prodotto $a \cdot b$. Con tre numeri l'esponente intermedio non viene contato (qui per il primo 2: $1 + 3 = 4 \neq 1 + 2 + 3 = 6$).

27. Il lato è MCD(360, 504): $360 = 2^3 \cdot 3^2 \cdot 5$, $504 = 2^3 \cdot 3^2 \cdot 7$, MCD = 72 cm. Piastrelle: $(360 : 72) \cdot (504 : 72) = 5 \cdot 7 = 35$.

28. mcm(12, 18, 30): $12 = 2^2 \cdot 3$, $18 = 2 \cdot 3^2$, $30 = 2 \cdot 3 \cdot 5$; mcm $= 2^2 \cdot 3^2 \cdot 5 = 180$ minuti = 3 ore. Ripartono insieme alle 10:00.

29. Le persone sono $156 + 12 = 168 = 54 \cdot 3 + 6$. Servono 4 pullman; sull'ultimo viaggiano 6 persone.

30. Il numero di confezioni è MCD(84, 120) = 12 ($84 = 2^2 \cdot 3 \cdot 7$, $120 = 2^3 \cdot 3 \cdot 5$). Ogni confezione contiene $84 : 12 = 7$ penne rosse e $120 : 12 = 10$ penne blu.

31. Con 8 bit: $2^8 = 256$ numeri (da 0 a 255). Con 10 bit: $2^{10} = 1024$ numeri; il più grande è $1111111111_2 = 1024 - 1 = 1023$.

32. $100 = 7 \cdot 14 + 2$: dopo 14 settimane complete è di nuovo martedì, poi altri 2 giorni. Sarà giovedì.

33. a) (2730, 1430) con resto 1300; (1430, 1300) con resto 130; (1300, 130) con resto 0. b) MCD = 130. c) $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ e $1430 = 2 \cdot 5 \cdot 11 \cdot 13$, fattori comuni $2 \cdot 5 \cdot 13 = 130$.

34. Le righe sono (12345, 5432, 1481), (5432, 1481, 989), (1481, 989, 492), (989, 492, 5), (492, 5, 2), (5, 2, 1), (2, 1, 0): sette righe. L'ultimo divisore è 1, quindi MCD = 1: i due numeri sono primi tra loro.

35. $3^4 : 3^2 = 3^2$; $(3^2)^2 = 3^4$; $3^4 : 3^3 = 3$; $3 + 10 = 13$; $13^2 : 13 = 13$; $13 - 4 =$ **9**.

36. Per due numeri MCD · mcm $= a \cdot b$: $6 \cdot 72 = 18 \cdot b$, quindi $b = 432 : 18 = 24$ (controllo: MCD(18, 24) = 6, mcm(18, 24) = 72). MCD = 5 e mcm = 72 non è possibile: il MCD divide entrambi i numeri, che a loro volta dividono il mcm, quindi il MCD deve dividere il mcm; ma 5 non divide 72.

37. Se n dà resto 1 nella divisione per 2, 3, 4, 5, 6, allora $n - 1$ è multiplo comune di questi numeri, cioè multiplo di mcm(2, 3, 4, 5, 6) = 60. I candidati sono 61, 121, 181, 241, 301, … Dividendo per 7: $61 = 7 \cdot 8 + 5$, $121 = 7 \cdot 17 + 2$, $181 = 7 \cdot 25 + 6$, $241 = 7 \cdot 34 + 3$, $301 = 7 \cdot 43 + 0$. Il numero cercato è **301**.