

I NUMERI NATURALI

ARITMETICA

Operazioni, potenze, divisibilità,
numeri primi, MCD e mcm

si comincia da zero e non si finisce mai



Prof. A. Perna

IllogicoMatematico

Indice

1	Cosa serve prima di partire	3
2	L'insieme $\mathbb{N}$	3
3	Le quattro operazioni e l'ordine in cui si fanno	4
4	Le proprietà: come si calcola a mente	6
5	Le potenze	7
6	La divisione con resto	9
7	Multipli, divisori e criteri di divisibilità	10
8	Numeri primi e scomposizione	12
9	MCD e mcm	14
10	Spartire o ritrovarsi: MCD o mcm nei problemi	15
11	Contare i divisori	16

1 Cosa serve prima di partire

Questo è il primo argomento: non c'è niente, prima, che si debba avere già studiato al superiore. Servono tre cose imparate alle medie, e se qualcuna è arrugginita si ripassa qui, adesso.

Cosa devi già sapere

- **Le quattro operazioni in colonna.** Saper fare $347 + 268$, $802 - 356$, $47 \cdot 26$ e $952 : 8$ senza calcolatrice. Se la moltiplicazione in colonna è incerta, vale la pena rifarne cinque adesso: tutto il capitolo la usa.
- **Leggere e scrivere i numeri grandi.** 47 308 si legge «quarantasettemilatrecentotto». Il puntino separa le migliaia e non è una virgola.
- **La divisione come «sta dentro quante volte».** $20 : 4 = 5$ perché il 4 sta dentro il 20 cinque volte. Questa lettura serve al paragrafo sulla divisione con resto più della regola della divisione in colonna.

Una parola sul perché questo capitolo esiste, dato che «i numeri» sembrano la cosa più ovvia del mondo. Perché in fondo al capitolo ci sono la scomposizione in fattori primi, il MCD e il mcm: tre strumenti che tornano fra due mesi con le frazioni, fra un anno con le frazioni algebriche, e che chi non ha capito qui si porta dietro come un debito.

2 L'insieme $\mathbb{N}$

I numeri che servono per *contare* formano l'insieme dei **numeri naturali**, che si indica con $\mathbb{N}$.

Formula 2.1: L'insieme dei numeri naturali:

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

Lo **zero è dentro**. Quando serve escluderlo si scrive $\mathbb{N}^* = \{1, 2, 3, \dots\}$, e si dice.

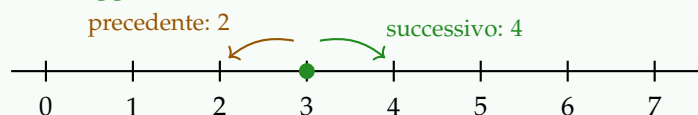
Tre fatti che sembrano banali e che invece si usano per tutto il capitolo.

Formula 2.2: Le tre proprietà di $\mathbb{N}$:

- **Ha un primo elemento**, lo zero, e non ha ultimo elemento: dopo ogni numero ce n'è un altro. $\mathbb{N}$ è **infinito**.
- **È ordinato**: dati due naturali diversi, uno è minore dell'altro. Si scrive $3 < 7$, oppure $7 > 3$.
- **È discreto**: fra 3 e 4 non c'è nessun naturale. Ogni numero n diverso da zero ha un

precedente $n - 1$ e un successivo $n + 1$.

Esempio Svolto 2.1: Leggere la retta dei numeri:



Perché è utile. Sulla retta, «più grande» significa «più a destra». Tutte le volte che un esercizio chiede di ordinare dei numeri, la retta è il modo di non sbagliare.

Lo zero è un numero naturale?

Dipende dal libro, e non è una questione di verità: è una convenzione. Molti testi italiani lo includono, alcuni testi stranieri no. In queste pagine **lo zero è dentro**, e quando una formula richiede di escluderlo lo si scrive a chiare lettere. Se il tuo libro usa l'altra convenzione non cambia niente di sostanziale: cambia dove si mette l'asterisco.

3 Le quattro operazioni e l'ordine in cui si fanno

Un'**espressione** è una sequenza di operazioni da eseguire. Il risultato è uno solo, ma solo se tutti eseguono le operazioni *nello stesso ordine*: per questo l'ordine è una regola e non un gusto personale.

Formula 3.1: L'ordine delle operazioni:

1. Le **parentesi**, dalla più interna alla più esterna: prima le tonde (), poi le quadre [], poi le graffe { }.
2. Le **potenze**.
3. **Moltiplicazioni e divisioni**, nell'ordine in cui compaiono, **da sinistra a destra**.
4. **Addizioni e sottrazioni**, nell'ordine in cui compaiono, **da sinistra a destra**.

Il punto che si sbaglia non è il primo: è il «da sinistra a destra». Moltiplicazione e divisione stanno sullo *stesso* piano, e così addizione e sottrazione. Non esiste nessuna regola che dica «prima tutte le moltiplicazioni e poi tutte le divisioni».

La catena delle sottrazioni

Quanto fa $8 - 3 + 2$?

Chi fa prima l'addizione ottiene $8 - 5 = 3$. **Sbagliato**. Addizione e sottrazione hanno la

stessa priorità, quindi si va da sinistra:

$$8 - 3 + 2 = 5 + 2 = 7$$

Lo stesso vale per le divisioni: $24 : 4 : 2$ fa $6 : 2 = 3$, non $24 : 2 = 12$.

Esempio Svolto 3.1: Espressione con parentesi annidate:

Calcoliamo $\{ [(12 - 5) \cdot 3 + 4] : 5 \}^2$.

1. La tonda, che è la più interna.

$$(12 - 5) = 7 \longrightarrow \{ [7 \cdot 3 + 4] : 5 \}^2$$

2. Dentro la quadra: prima il prodotto, poi la somma.

$$7 \cdot 3 = 21, \quad 21 + 4 = 25 \longrightarrow \{ 25 : 5 \}^2$$

3. La graffa.

$$25 : 5 = 5 \longrightarrow 5^2$$

4. La potenza, per ultima.

$$5^2 = 25$$

5. **Controllo.** Un modo per accorgersi di un errore grosso: l'ultima operazione è un quadrato, quindi il risultato deve essere un quadrato perfetto. 25 lo è. Se fosse venuto 24, c'era da rifare i conti.

Metodo 3.1: Come si scrive un'espressione senza perdersi:

1. Riscrivo l'espressione su una riga nuova a ogni passaggio, **copiando tutto il resto**. La maggior parte degli errori è un pezzo perso per strada, non un conto sbagliato.
2. A ogni riga eseguo **una sola** operazione per gruppo.
3. Se un passaggio richiede più di due numeri, lo spezzo.
4. Il conto laterale si scrive a margine: $7 \cdot 3 = 21$.

Le operazioni «impossibili» in $\mathbb{N}$

In $\mathbb{N}$ addizione e moltiplicazione si possono sempre fare: il risultato è ancora un naturale. Sottrazione e divisione no. $3 - 8$ non ha risposta fra i naturali, e nemmeno $7 : 2$. Non è un difetto: è il motivo per cui più avanti si costruiscono i numeri interi (per la sottrazione) e i razionali (per la divisione). Ogni insieme nuovo nasce da un'operazione che nel vecchio non si poteva fare.

4 Le proprietà: come si calcola a mente

Le proprietà delle operazioni sembrano tre regole da imparare a memoria. Sono invece l'unico modo per fare a mente conti che sembrano da calcolatrice: servono a **cambiare la forma** del conto in una più comoda.

Formula 4.1: Le proprietà da conoscere:

- **Commutativa** (somma e prodotto): l'ordine non conta.

$$a + b = b + a \quad a \cdot b = b \cdot a$$

- **Associativa** (somma e prodotto): si può raggruppare come si vuole.

$$(a + b) + c = a + (b + c) \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

- **Distributiva** del prodotto rispetto a somma e differenza:

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

- **Invariantiva** della sottrazione: aggiungendo lo stesso numero a entrambi i termini, la differenza non cambia.

$$a - b = (a + k) - (b + k)$$

- **Invariantiva** della divisione: moltiplicando o dividendo entrambi i termini per lo stesso numero (non zero), il quoziente non cambia.

$$a : b = (a \cdot k) : (b \cdot k)$$

Sottrazione e divisione **non** sono commutative né associative: $8 - 3 \neq 3 - 8$.

Esempio Svolto 4.1: Tre conti che sembrano difficili e non lo sono:

1. $25 \cdot 36$ con l'associativa.

Il 25 diventa comodo se incontra un 4, perché $25 \cdot 4 = 100$. Allora spezzo il 36:

$$25 \cdot 36 = 25 \cdot (4 \cdot 9) = (25 \cdot 4) \cdot 9 = 100 \cdot 9 = \mathbf{900}$$

2. $99 \cdot 47$ con la distributiva.

Moltiplicare per 99 è scomodo, per 100 è immediato. Allora scrivo $99 = 100 - 1$:

$$99 \cdot 47 = (100 - 1) \cdot 47 = 4700 - 47 = \mathbf{4653}$$

3. $1\,003 - 998$ con l'invariantiva.

Aggiungo 2 a entrambi i termini, così il secondo diventa tondo:

$$1003 - 998 = 1005 - 1000 = 5$$

4. Controllo. In $99 \cdot 47$ il risultato deve finire per 3, perché $9 \cdot 7 = 63$. Torna.

La distributiva non si applica alla somma

La distributiva vale quando **un prodotto** incontra una somma:

$$(5 + 3) \cdot 2 = 5 \cdot 2 + 3 \cdot 2 = 16 \quad \text{giusto}$$

Ma non esiste niente di simile per la somma da sola:

$$5 + (3 \cdot 2) \neq (5 + 3) \cdot (5 + 2)$$

A sinistra fa 11, a destra 80. Nel dubbio si calcola il valore nei due modi e si vede che non torna: un controesempio numerico smonta qualunque «regola» inventata.

Il trucco dei numeri vicini a 100

$98 \cdot 97 = 98 \cdot (100 - 3) = 9800 - 294 = 9506$. Provalo con $97 \cdot 96$ e con $101 \cdot 103$: tre secondi a testa, senza carta. Non è un gioco di prestigio, è la distributiva.

5 Le potenze

Scrivere $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ è scomodo. La potenza è un'abbreviazione, e come tutte le abbreviazioni utili ha le sue regole.

Formula 5.1: Definizione di potenza:

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

a si chiama **base**, n **esponente**. Si legge « a alla n ».

$$a^1 = a \quad a^0 = 1 \quad (\text{con } a \neq 0) \quad 1^n = 1$$

La scrittura 0^0 **non ha significato**.

Formula 5.2: Le cinque proprietà delle potenze:

Operazione	Regola	Esempio
Prodotto, stessa base	$a^m \cdot a^n = a^{m+n}$	$3^2 \cdot 3^4 = 3^6$
Quoziente, stessa base	$a^m : a^n = a^{m-n}$	$3^5 : 3^2 = 3^3$
Potenza di potenza	$(a^m)^n = a^{m \cdot n}$	$(3^2)^4 = 3^8$
Prodotto, stesso esponente	$a^n \cdot b^n = (a \cdot b)^n$	$2^3 \cdot 5^3 = 10^3$
Quoziente, stesso esponente	$a^n : b^n = (a : b)^n$	$8^2 : 4^2 = 2^2$

Nelle prime tre **la base non cambia**; nelle ultime due **l'esponente non cambia**. Non esiste nessuna regola per $a^m + a^n$: la somma di potenze non si semplifica.

Esempio Svolto 5.1: Le proprietà in fila:**1. Prodotto e quoziente insieme.**

$$\frac{2^7 \cdot 2^3}{2^8} = \frac{2^{10}}{2^8} = 2^{10-8} = 2^2 = 4$$

2. Potenza di potenza, con attenzione.

$$(5^2)^3 = 5^{2 \cdot 3} = 5^6$$

e non 5^8 : gli esponenti si *moltiplicano*, non si elevano.

3. Stesso esponente, basi diverse.

$$4^3 \cdot 25^3 = (4 \cdot 25)^3 = 100^3 = 1\,000\,000$$

Calcolare $64 \cdot 15\,625$ a mano avrebbe richiesto molto più tempo, con lo stesso risultato.

4. Controllo. Nel punto 1: $2^7 = 128$, $2^3 = 8$, $2^8 = 256$, e $\frac{128 \cdot 8}{256} = \frac{1024}{256} = 4$. Torna.

Le tre confusioni sulle potenze

- $2^3 \cdot 2^4 = 2^7$, **non** 4^7 . La base resta. Per convincersi: $2^3 \cdot 2^4$ è $(2 \cdot 2 \cdot 2) \cdot (2 \cdot 2 \cdot 2 \cdot 2)$, sette fattori uguali a 2.
- $2^3 + 2^4$ **non** è 2^7 . Vale $8 + 16 = 24$, e $2^7 = 128$. Le somme di potenze si calcolano, non si semplificano.
- $0^5 = 0$, non 1. La regola $a^0 = 1$ riguarda l'*esponente zero*, non la base.

La scacchiera e i chicchi di grano

Una vecchia storia racconta di un inventore degli scacchi che chiese come premio un chicco di grano sulla prima casella, due sulla seconda, quattro sulla terza, e così via raddoppiando fino alla sessantaquattresima.

Il totale è $2^{64} - 1$, cioè più di diciotto miliardi di miliardi di chicchi: molte volte la produzione mondiale annuale di grano. Il re accettò perché «sono solo chicchi». Le potenze crescono in un modo che l'intuizione non prevede: è anche per questo che valgono un paragrafo.

6 La divisione con resto

In $\mathbb{N}$ la divisione spesso «non viene»: $17 : 5$ non dà un numero naturale. Ma non è vero che non si possa dire niente. Si può dire *quante volte ci sta e quanto avanza*.

Formula 6.1: Divisione con resto: Dati D (dividendo) e d (divisore, con $d \neq 0$), esistono e sono **unici** due naturali q (quoziente) e r (resto) tali che

$$D = d \cdot q + r \quad \text{con} \quad 0 \leq r < d$$

La condizione $r < d$ è quella che rende la scrittura unica: se il resto fosse grande come il divisore, il divisore ci starebbe un'altra volta. Se $r = 0$ la divisione è **esatta** e si dice che d divide D .

Esempio Svolto 6.1: $247 : 15$, con la verifica:

1. Quante volte il 15 sta nel 247?

$15 \cdot 10 = 150$, $15 \cdot 16 = 240$, $15 \cdot 17 = 255$: troppo. Quindi $q = 16$.

2. Quanto avanza?

$$r = 247 - 240 = 7$$

3. Controllo della condizione sul resto.

Serve $0 \leq r < 15$: il resto è 7, va bene. Se fosse venuto 18, l'errore era nel quoziente.

4. Verifica con la formula.

$$d \cdot q + r = 15 \cdot 16 + 7 = 240 + 7 = \mathbf{247} = D$$

Questa verifica costa dieci secondi e trova quasi tutti gli errori: da fare sempre.

Dividere per zero

$5 : 0$ non fa zero, non fa infinito, non fa cinque: **non esiste**. Il motivo si vede dalla formula: cercheremmo un q con $5 = 0 \cdot q + r$, cioè $5 = r$, ma serve anche $r < d = 0$, e non esiste un resto minore di zero.

Attenzione al caso contrario, che invece è legittimo: $0 : 5 = 0$, e va benissimo.

7 Multipli, divisori e criteri di divisibilità

Formula 7.1: Multipli e divisori: Se la divisione $b : a$ è esatta, si dice che

- b è un **multiplo** di a ;
- a è un **divisore** di b , e si scrive $a \mid b$ (si legge « a divide b »).

Sono due modi di dire la stessa cosa, guardata da capi opposti: $3 \mid 12$, e 12 è multiplo di 3. I multipli di un numero sono **infiniti**; i divisori sono **finiti**. Ogni numero n ha almeno i divisori 1 e n .

I **criteri di divisibilità** dicono se una divisione sarà esatta senza farla. Sono la cosa più utile del capitolo per il calcolo veloce e per semplificare le frazioni.

Formula 7.2: I criteri da sapere: Un numero è divisibile per

	se	esempio
2	l'ultima cifra è pari (0, 2, 4, 6, 8)	134 6
3	la somma delle cifre è divisibile per 3	432 $\rightarrow 4 + 3 + 2 = 9$
4	le ultime <i>due</i> cifre formano un multiplo di 4	13 16 $\rightarrow 16$
5	l'ultima cifra è 0 oppure 5	27 35
8	le ultime <i>tre</i> cifre formano un multiplo di 8	5 128 $\rightarrow 128$
9	la somma delle cifre è divisibile per 9	432 $\rightarrow 9$
10	l'ultima cifra è 0	45 70
11	la differenza fra la somma delle cifre di posto dispari e quella di posto pari è 0 o multiplo di 11	490 6

Esempio Svolto 7.1: Perché funziona il criterio del 3:

Non è magia, ed è una delle poche dimostrazioni alla portata di tutti al primo anno. Prendiamo 432 e spezziamolo:

$$432 = 4 \cdot 100 + 3 \cdot 10 + 2$$

Ora il passaggio furbo: $100 = 99 + 1$ e $10 = 9 + 1$.

$$432 = 4 \cdot (99 + 1) + 3 \cdot (9 + 1) + 2 = \underbrace{4 \cdot 99 + 3 \cdot 9}_{\text{divisibile per 3}} + \underbrace{(4 + 3 + 2)}_{\text{somma delle cifre}}$$

Il primo gruppo è divisibile per 3 sempre, perché 99 e 9 lo sono. Quindi tutto il numero è divisibile per 3 **se e solo se** lo è la somma delle cifre. Qui $4 + 3 + 2 = 9$, divisibile per 3 e anche per 9: infatti $432 : 3 = 144$ e $432 : 9 = 48$.

Lo stesso ragionamento, con 9 al posto di 3, dimostra il criterio del 9: anche 99 e 9 sono multipli di 9.

Esempio Svolto 7.2: Il criterio dell'11 su 4906:

Si sommano le cifre di posto dispari e quelle di posto pari, contando **da destra**:

$$\text{posti dispari: } 6 + 9 = 15 \quad \text{posti pari: } 0 + 4 = 4$$

$$15 - 4 = \mathbf{11}$$

È un multiplo di 11, quindi $11 \mid 4906$. Verifica: $4906 : 11 = 446$.

Il criterio del 4 non è quello del 2 applicato due volte

1346 è divisibile per 2 (finisce per 6) ma **non** per 4: le ultime due cifre sono 46, e 46 non è multiplo di 4. Infatti $1346 : 4$ dà quoziente 336 e resto 2.

Regola pratica: per il 2 si guarda *una* cifra, per il 4 *due*, per l'8 *tre*. Il numero di cifre da guardare cresce con la potenza di 2.

Il criterio del 7, che nessuno insegna

Esiste e si fa a mente: si toglie l'ultima cifra, si raddoppia, e si sottrae da quel che resta. Se il risultato è divisibile per 7, lo era anche il numero di partenza.

Su 203: togliamo il 3, resta 20; il doppio di 3 è 6; $20 - 6 = 14 = 7 \cdot 2$. Quindi $7 \mid 203$, e infatti $203 = 7 \cdot 29$.

Su 1001: resta 100, il doppio dell'ultima cifra è 2, $100 - 2 = 98 = 7 \cdot 14$. Sì. E $1001 = 7 \cdot 11 \cdot 13$: una scomposizione che vale la pena ricordare.

8 Numeri primi e scomposizione

Formula 8.1: Numeri primi e composti: Un naturale maggiore di 1 è

- **primo** se ha *esattamente due* divisori, 1 e se stesso;
- **composto** se ne ha più di due.

1 non è primo (ha un solo divisore) e non è composto: sta a parte. **2 è primo**, ed è l'unico primo pari.

«1 è primo» e «2 non è primo»

Sono i due errori più diffusi, e sono opposti.

1 non è primo perché la definizione chiede due divisori distinti, e l'1 ne ha uno solo. Non è una cattiveria dei matematici: se l'1 fosse primo, la scomposizione di 12 potrebbe essere $2^2 \cdot 3$, oppure $1 \cdot 2^2 \cdot 3$, oppure $1^{99} \cdot 2^2 \cdot 3$, e il teorema del prossimo riquadro — quello che garantisce che la scomposizione è *unica* — sarebbe falso.

2 è primo: i suoi divisori sono 1 e 2, esattamente due. Essere pari non c'entra niente con l'essere primo.

Per trovare i primi c'è un metodo di duemiladuecento anni fa che funziona ancora: si scrivono i numeri e si cancellano i multipli.

Esempio Svolto 8.1: Il crivello di Eratostene fino a 60:

Si cancellano i multipli di 2, poi di 3, poi di 5, poi di 7. Chi sopravvive è primo (in verde). L'1 sta fuori dal gioco.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Fin dove bisogna cancellare? Fino al primo il cui quadrato supera 60. Siccome $7^2 = 49 \leq 60$ e $11^2 = 121 > 60$, si cancella fino al 7 e si smette. Il motivo: se un numero minore di 60 avesse un divisore maggiore di $\sqrt{60} \approx 7,7$, il divisore complementare sarebbe minore, e l'avremmo già trovato prima.

I primi fino a 60 sono 17. Vale la pena sapere a memoria almeno i primi otto: 2, 3, 5, 7, 11, 13, 17, 19.

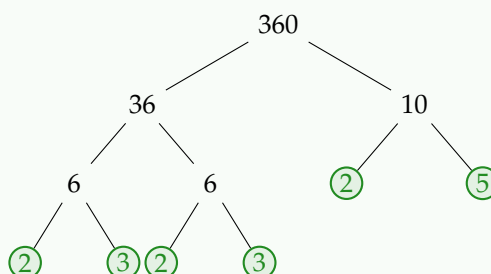
Formula 8.2: Teorema fondamentale dell'aritmetica: Ogni naturale maggiore di 1 si scrive come prodotto di numeri primi, e questa scrittura è **unica** a meno dell'ordine dei fattori.

$$360 = 2^3 \cdot 3^2 \cdot 5$$

È l'impronta digitale del numero: nessun altro naturale ha questa scomposizione, e 360 non ne ha altre.

Esempio Svolto 8.2: Scomporre 360, in due modi:

1. Con l'albero. Si spezza il numero in due fattori qualsiasi e si continua finché in fondo restano solo primi. Il punto notevole: *da qualunque coppia si parta, in fondo si trovano gli stessi primi.*



In fondo ci sono 2, 3, 2, 3, 2, 5: tre volte il 2, due volte il 3, una volta il 5.

$$360 = 2^3 \cdot 3^2 \cdot 5$$

2. In colonna, il metodo da usare negli esercizi perché non fa sbagliare. Si divide per i primi in ordine, finché si arriva a 1:

360	2
180	2
90	2
45	3
15	3
5	5
1	

Si leggono i primi nella colonna di destra: $2^3 \cdot 3^2 \cdot 5$.

3. Controllo. $8 \cdot 9 \cdot 5 = 72 \cdot 5 = 360$.

Metodo 8.1: Scomporre un numero senza impazzire:

1. Divido per 2 finché viene (criterio: finisce per cifra pari).
2. Passo al 3 (criterio: somma delle cifre), poi 5, 7, 11, 13.
3. Mi fermo quando il quoziente diventa 1.

4. Se arrivo a un primo il cui **quadrato supera** il numero rimasto e nessun primo ha funzionato, il numero rimasto è primo: si scrive e si chiude.

Quanti sono i numeri primi? Infiniti, e si dimostra

Euclide lo dimostrò così, e l'idea sta in tre righe.

Supponiamo per assurdo che i primi siano finiti: $p_1, p_2, \dots, p_n$, tutti quanti. Costruiamo il numero

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

Dividendo N per uno qualsiasi dei nostri primi si ottiene sempre resto 1, quindi N non è divisibile per nessuno di loro. Ma allora N è primo (e non era nella lista), oppure ha un divisore primo che non era nella lista. In entrambi i casi la lista non conteneva tutti i primi: contraddizione.

Quindi i primi non finiscono mai. È una dimostrazione di oltre duemila anni e non è mai stata superata in eleganza.

9 MCD e mcm

Formula 9.1: Massimo Comune Divisore e minimo comune multiplo: Dati due o più naturali non nulli:

- il **MCD** è il più grande fra i divisori comuni;
- il **mcm** è il più piccolo fra i multipli comuni diversi da zero.

Con le scomposizioni in fattori primi:

MCD primi **comuni**, con l'esponente **minore**

mcm primi **comuni e non comuni**, con l'esponente **maggiore**

Due numeri con $\text{MCD} = 1$ si dicono **primi fra loro** (o coprimi): per esempio 8 e 15, che non hanno fattori in comune pur non essendo primi.

Esempio Svolto 9.1: MCD e mcm di 360 e 84:

1. Le due scomposizioni.

$$360 = 2^3 \cdot 3^2 \cdot 5 \qquad 84 = 2^2 \cdot 3 \cdot 7$$

2. Il MCD: solo i primi comuni, esponente più piccolo.

Comuni: il 2 (esponenti 3 e 2, prendo 2) e il 3 (esponenti 2 e 1, prendo 1). Il 5 e il 7 non sono comuni, quindi restano fuori.

$$\text{MCD}(360, 84) = 2^2 \cdot 3 = \mathbf{12}$$

3. Il mcm: tutti i primi, esponente più grande.

$$\text{mcm}(360, 84) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 8 \cdot 9 \cdot 5 \cdot 7 = \mathbf{2520}$$

4. Controllo, con una proprietà che per due numeri vale sempre:

$$\text{MCD}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$$

Qui $12 \cdot 2520 = 30\,240$ e $360 \cdot 84 = 30\,240$. Torna. È il modo più rapido per accorgersi di aver sbagliato un esponente.

Il MCD non è «il numero più piccolo»

$\text{MCD}(360, 84)$ non è 84, e $\text{mcm}(360, 84)$ non è 360. Succede *solo* nel caso particolare in cui uno dei due divide l'altro: $\text{MCD}(6, 18) = 6$ e $\text{mcm}(6, 18) = 18$.

Controllo veloce: il MCD deve dividere entrambi i numeri, il mcm deve essere diviso da entrambi. Se non è così, è sbagliato.

Esempio Svolto 9.2: L'algoritmo di Euclide: il MCD senza scomporre:

Scomporre numeri grandi è lento. Euclide trovò una strada che usa solo divisioni con resto: si divide il maggiore per il minore, poi il divisore per il resto, e si continua. **L'ultimo resto non nullo è il MCD.**

Calcoliamo $\text{MCD}(1071, 462)$:

$$1071 = 2 \cdot 462 + 147$$

$$462 = 3 \cdot 147 + 21$$

$$147 = 7 \cdot 21 + 0$$

Il resto si annulla dopo il 21, quindi $\text{MCD}(1071, 462) = \mathbf{21}$.

Controllo. $1071 : 21 = 51$ e $462 : 21 = 22$: entrambe esatte. E $51 = 3 \cdot 17$, $22 = 2 \cdot 11$ non hanno più fattori in comune, quindi 21 era davvero il massimo.

10 Spartire o ritrovarsi: MCD o mcm nei problemi

Calcolare un MCD è meccanico. La difficoltà vera è un'altra: leggere un problema e capire quale dei due serve. Chi sbaglia, alla verifica, quasi mai sbaglia il conto: sbaglia la scelta.

Metodo 10.1: La domanda che scioglie il dubbio:

1. **Sto tagliando, spartendo, raggruppando** qualcosa che ho già? Le quantità di

partenza vengono *divise* in parti uguali? $\rightarrow$ **MCD**.

2. **Sto aspettando che due cose si ritrovino**, oppure cerco una quantità che contenga esattamente più gruppi diversi? Le quantità di partenza vengono *ripetute*? $\rightarrow$ **mcm**.

Prova del nove: il MCD è **più piccolo** o uguale ai numeri di partenza, il mcm è **più grande** o uguale. Se il problema parlava di spartire e la risposta è più grande dei dati, è stato usato quello sbagliato.

Esempio Svolto 10.1: Due problemi gemelli, con risposte opposte:

Problema A — le piastrelle. Una stanza è larga 360 cm e lunga 84 cm. La si vuole piastrellare con quadrati tutti uguali e interi, i più grandi possibile. Quanto misura il lato? *Ragionamento.* Il lato deve stare un numero intero di volte sia nel 360 sia nell'84: è un divisore comune. Lo vogliamo il più grande possibile: è il **MCD**.

$$\text{lato} = \text{MCD}(360, 84) = \mathbf{12} \text{ cm}$$

Quante piastrelle? $(360 : 12) \cdot (84 : 12) = 30 \cdot 7 = 210$.

Problema B — i due autobus. Dalla stessa fermata partono insieme due autobus: uno torna ogni 360 minuti, l'altro ogni 84 minuti. Dopo quanti minuti ripartono di nuovo insieme?

Ragionamento. L'istante cercato è un multiplo di 360 e anche di 84, e lo vogliamo il primo: è il **mcm**.

$$\text{attesa} = \text{mcm}(360, 84) = \mathbf{2520} \text{ minuti}$$

Cioè 42 ore.

Cosa cambia fra i due. Gli stessi due numeri, gli stessi calcoli di due pagine fa. Nel primo si *taglia* una quantità che c'è già (MCD, risultato piccolo); nel secondo si *aspetta* che due cicli si ripetano (mcm, risultato grande).

11 Contare i divisori

Quanti divisori ha 360? Elencarli tutti è lungo e ci si dimentica qualcuno. Dalla scomposizione si contano senza elencarli.

Formula 11.1: Numero dei divisori: Se $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k}$, il numero dei divisori di n è

$$(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

Si aggiunge 1 a ogni esponente perché ogni primo può comparire in un divisore con esponente $0, 1, \dots, a_i$: sono $a_i + 1$ possibilità.

Esempio Svolto 11.1: I divisori di 360:

Da $360 = 2^3 \cdot 3^2 \cdot 5^1$:

$$(3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = \mathbf{24} \text{ divisori}$$

Controllo, elencandoli davvero: 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360. Sono 24.

Perché è utile. Un numero con molti divisori si spartisce in molti modi: è il motivo per cui l'ora ha 60 minuti e il cerchio 360 gradi, e non 100. Con 60 si può dividere in 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 parti uguali; con 100 no.

I numeri perfetti

Sommiamo i divisori di 6, escluso il 6 stesso: $1 + 2 + 3 = 6$. Torna il numero di partenza. Con 28: $1 + 2 + 4 + 7 + 14 = 28$. Numeri così si chiamano **perfetti**.

Dopo 6 e 28 vengono 496 e 8128, poi si salta a 33 550 336: sono rarissimi. E non si sa se ne esistano di dispari — è un problema aperto da più di duemila anni, e nessuno sa rispondere. Vale la pena saperlo: in matematica le domande semplici non sono necessariamente quelle facili.

Contare in base 2, con i pesi della bilancia

Con quattro pesi da 1, 2, 4 e 8 grammi si pesa *qualunque* quantità intera da 1 a 15 grammi, e in un solo modo. Per 13: $8 + 4 + 1$, e il peso da 2 resta nel cassetto.

Scrivendo 1 quando il peso si usa e 0 quando no, 13 diventa 1101: è la scrittura in **base 2**, quella con cui contano i computer. Le potenze di 2 tornano perché ogni peso è il doppio del precedente. Con sette pesi si arriva a $2^7 - 1 = 127$.

Indice analitico

Algoritmo di Euclide, 14

Criteri di divisibilità, 10

Crivello di Eratostene, 12

Divisione con resto, 9

Divisione euclidea, 9

Divisore, 10

Espressioni, 4

Insieme $\mathbb{N}$, 3

MCD, 14

mcm, 14

Multiplo, 10

Numeri naturali, 3

Numeri primi fra loro, 14

Numero dei divisori, 16

Numero primo, 12

Ordine delle operazioni, 4

Potenza, 7

Potenze

proprietà, 7

Problemi con MCD e mcm, 15

Proprietà

associativa, 6

commutativa, 6

distributiva, 6

invariantiva, 6

Proprietà delle operazioni, 6

Scomposizione in fattori primi, 12

Teorema fondamentale dell'aritmetica, 12