Capitolo 10

Divisibilità MCD e mcm

WEB (Materiali vari)

“

Studia questo capitolo con l’AI: quiz, esercizi e altro

Ripassa con le flashcard

Esercizi auto-generati

Sorgente di questo capitolo

Schede, test e video di matematika.it

Esercizi del prof. De Capoa

Si dice che un numero misura un altro numero quando il primo, contato un numero di volte, lo riproduce esattamente.”

— Euclide, *Elementi*, libro VII, def. 3 (III sec. a.C.)

CC BY-NC-SA 4.0 · a cura di Giovanni Nicco

10.1. Introduzione motivazionale

quiz e materiali con l'AI

Quando dividiamo 12 per 3 otteniamo un risultato intero, 4, senza "avanzi". Quando invece dividiamo 14 per 3, qualcosa avanza: il quoziente è 4, ma rimane un resto di 2. La distinzione fra divisioni "esatte" e divisioni "con resto" è il punto di partenza dell'*aritmetica modulare* e di tutta la teoria dei numeri.

In questo capitolo studiamo a fondo questa distinzione. Introdurremo la relazione di *divisibilità* fra numeri interi, alcuni *criteri* pratici per decidere rapidamente se un numero è divisibile per un altro (per 2, 3, 5, 9, 11, ecc.), il *massimo comune divisore* (MCD) e il *minimo comune multiplo* (mcm) di due o più numeri, e infine l'*algoritmo di Euclide* per calcolare l'MCD in modo veloce anche per numeri grandi.

Queste nozioni saranno la chiave per ridurre le frazioni ai minimi termini (capitolo 12), per semplificare scomposizioni e raccoglimenti (capitolo 19), e per discutere la *fattorizzazione unica* dei numeri naturali (capitolo 11).

10.2. Divisori e multipli

quiz e materiali con l'AI
flashcard del paragrafo

Definizione 10.1 — Divisibilità

Siano $a, b \in \mathbb{Z}$ con $b \neq 0$. Si dice che b **divide** a (oppure: a **è multiplo** di b) se esiste un intero $k \in \mathbb{Z}$ tale che $a = b \cdot k$. Si scrive

$$b \mid a \quad (\text{“}b \text{ divide } a\text{”}).$$

Se invece nessun k realizza l'uguaglianza, si scrive $b \nmid a$.

Esempio 10.1

$3 \mid 12$ perché $12 = 3 \cdot 4$; $3 \nmid 14$ perché non esiste $k \in \mathbb{Z}$ con $14 = 3k$. Inoltre $(-3) \mid 12$ (con $k = -4$) e $5 \mid 0$ (con $k = 0$): **ogni intero non nullo divide** 0.

Nota — Convenzioni

- Per ogni $a \in \mathbb{Z}$, $1 \mid a$ e $-1 \mid a$.
- Per ogni $a \in \mathbb{Z} \setminus \{0\}$, $a \mid a$ e $a \mid -a$.
- Il caso $b = 0$ è escluso: "divisione per zero" non è definita. Equivalentemente, $0 \nmid a$ per ogni a.

Teorema 10.1 — Proprietà elementari della divisibilità

Per ogni $a, b, c \in \mathbb{Z}$:

- se $a \mid b$ e $b \mid c$, allora $a \mid c$ *(transitiva)*;

- se $a \mid b$ e $a \mid c$, allora $a \mid (b+c)$ e $a \mid (b-c)$;
- se $a \mid b$, allora $a \mid b \cdot c$ per ogni $c \in \mathbb{Z}$;
- se $a \mid b$ e $b \neq 0$, allora $|a| \leq |b|$.

Dimostrazione (idea). Tutte si verificano sostituendo le definizioni. Ad esempio, se $a \mid b$ (cioè $b = ak$) e $a \mid c$ (cioè $c = ah$), allora $b + c = a(k + h)$, dunque $a \mid b + c$.

Definizione 10.2 — Divisori e multipli di un numero

Per $n \in \mathbb{N}^*$, l'insieme dei **divisori** (positivi) di n è

$$D(n) = \{\, d \in \mathbb{N}^* \mid d \mid n \,\}.$$

L'insieme dei **multipli** (positivi) di n è

$$M(n) = \{\, k \cdot n \mid k \in \mathbb{N}^* \,\}.$$

$D(n)$ è *finito* ($D(12) = \{1, 2, 3, 4, 6, 12\}$); $M(n)$ è *infinito* ($M(3) = \{3, 6, 9, 12, \ldots\}$).

Teorema 10.2 — Divisione euclidea in $\mathbb{Z}$

Per ogni $a \in \mathbb{Z}$ e ogni $b \in \mathbb{N}^*$, esistono e sono unici $q, r \in \mathbb{Z}$ tali che

$$a = b \cdot q + r, \qquad 0 \leq r < b.$$

Il numero q si dice **quoziente** e r **resto** della divisione di a per b.

Dimostrazione (idea). L'idea è di sottrarre b ripetutamente da a (o sommarlo, se $a < 0$) finché si rientra nell'intervallo $[0, b-1]$: il numero di sottrazioni è q, ciò che resta è r. L'unicità si dimostra per assurdo supponendo due rappresentazioni e sottraendole.

Esempio 10.2

Dividendo $a = 47$ per $b = 5$: $47 = 5 \cdot 9 + 2$, quoziente $q = 9$, resto $r = 2$. La condizione $0 \leq 2 < 5$ è verificata.
Dividendo $a = -47$ per $b = 5$: $-47 = 5 \cdot (-10) + 3$, quoziente $q = -10$, resto $r = 3$. *Non* si scrive $-47 = 5 \cdot (-9) - 2$ perché si vuole il resto positivo.

Nota — Divisibilità in termini di resto

$b \mid a$ se e solo se la divisione euclidea di a per b ha resto $r = 0$. È la definizione operativa usata in tutti i criteri di divisibilità che seguono.

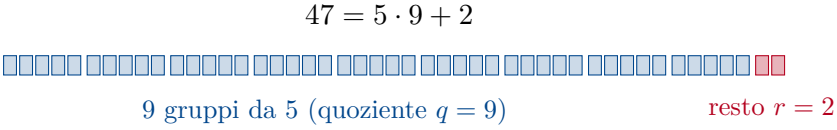


Figura 10.1: Visualizzazione geometrica della divisione euclidea: i 47 quadretti si raggruppano in 9 gruppi da 5 (quoziente, in blu) più 2 quadretti che "avanzano" (resto, in rosso). In simboli: $47 = 5 \cdot 9 + 2$.

10.3. Criteri di divisibilità

quiz e materiali con l'AI
flashcard del paragrafo

Per molti divisori piccoli esistono *criteri*: regole rapide che permettono di stabilire la divisibilità senza eseguire la divisione completa.

Teorema 10.3 — Criteri di divisibilità

Sia n un numero naturale.

- *Per* 2: $2 \mid n$ se e solo se l'ultima cifra di n è pari (cioè $0, 2, 4, 6, 8$).
- *Per* 5: $5 \mid n$ se e solo se l'ultima cifra di n è 0 o 5.
- *Per* 10: $10 \mid n$ se e solo se l'ultima cifra di n è 0.
- *Per* 3: $3 \mid n$ se e solo se la somma delle cifre di n è divisibile per 3.
- *Per* 9: $9 \mid n$ se e solo se la somma delle cifre di n è divisibile per 9.
- *Per* 4: $4 \mid n$ se e solo se il numero formato dalle ultime due cifre di n è divisibile per 4.
- *Per* 25: $25 \mid n$ se e solo se le ultime due cifre di n sono 00, 25, 50 o 75.
- *Per* 11: $11 \mid n$ se e solo se la differenza fra la somma delle cifre di posto dispari e la somma delle cifre di posto pari (partendo da destra) è divisibile per 11 (incluso 0).

Dimostrazione (criterio del 3). Sia $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. Poiché $10 \equiv 1 \pmod 3$, ogni $10^i \equiv 1 \pmod 3$. Allora

$$n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 3,$$

cioè n e la somma delle sue cifre danno lo stesso resto nella divisione per 3. In particolare $3 \mid n$ se e solo se 3 divide la somma delle cifre. La dimostrazione del criterio del 9 è identica (anche $10 \equiv 1 \pmod 9$).

Esempio 10.3 — Applicazione dei criteri

Stabilire i divisori di $n = 37\,845$ tra $\{2, 3, 4, 5, 9, 10, 11\}$.
Soluzione.

- L'ultima cifra è 5: $5 \mid n$, ma $2 \nmid n$ e $10 \nmid n$.
- Somma cifre: $3 + 7 + 8 + 4 + 5 = 27$; $3 \mid 27$ e $9 \mid 27$, dunque $3 \mid n$ e $9 \mid n$.

CC BY-NC-SA 4.0 · a cura di Giovanni Nicco

- Ultime due cifre: 45; $4 \nmid 45$, dunque $4 \nmid n$.
- Differenza "cifre alternate" (da destra): $(5+8+3)-(4+7) = 16-11 = 5$; $11 \nmid 5$, dunque $11 \nmid n$.

Divisori di n nell'insieme proposto: $\{3, 5, 9\}$.

10.4. MCD: definizione e calcolo

quiz e materiali con l'AI
flashcard del paragrafo

Definizione 10.3 — Massimo comune divisore

Dati $a, b \in \mathbb{N}^*$, il **massimo comune divisore** di a e b, indicato $\mathrm{MCD}(a,b)$ o (a,b), è il più grande naturale che divide sia a sia b:

$$\mathrm{MCD}(a,b) = \max(D(a) \cap D(b)).$$

Esempio 10.4

$D(12) = \{1,2,3,4,6,12\}$, $D(18) = \{1,2,3,6,9,18\}$. Divisori comuni: $\{1,2,3,6\}$. Il massimo è 6: $\mathrm{MCD}(12,18) = 6$.

Definizione 10.4 — Numeri coprimi

Due numeri $a, b \in \mathbb{N}^*$ si dicono **coprimi** (o *primi tra loro*) se $\mathrm{MCD}(a,b) = 1$.

Esempio 10.5

$\mathrm{MCD}(8,15) = 1$, dunque 8 e 15 sono coprimi. Lo sono anche 7 e 20, ma non 6 e 10 (che hanno MCD $= 2$).

Procedura — MCD per scomposizione in fattori primi

Per calcolare $\mathrm{MCD}(a,b)$:

1. Si scrive ciascuno dei due numeri come prodotto di fattori primi (capitolo 11).
2. Si prendono i fattori *comuni* ai due (cioè quelli che compaiono in entrambe le scomposizioni), *ciascuno con l'esponente più piccolo.*
3. Il prodotto di questi fattori (con i loro esponenti minimi) è $\mathrm{MCD}(a,b)$.

Esempio 10.6

Calcolare $\mathrm{MCD}(72,60)$.
Soluzione. $72 = 2^3 \cdot 3^2$, $60 = 2^2 \cdot 3 \cdot 5$. Fattori comuni: 2 e 3. Esponenti minimi: 2^2 e 3^1. Quindi

$$\mathrm{MCD}(72,60) = 2^2 \cdot 3 = 12.$$

CC BY-NC-SA 4.0 · a cura di Giovanni Nicco

10.5. mcm: definizione e calcolo

quiz e materiali con l'AI
flashcard del paragrafo

Definizione 10.5 — Minimo comune multiplo

Dati $a, b \in \mathbb{N}^*$, il **minimo comune multiplo** di a e b, indicato $\mathrm{mcm}(a,b)$ o $[a,b]$, è il più piccolo naturale non nullo che è multiplo sia di a sia di b:

$$\mathrm{mcm}(a,b) = \min\big(M(a) \cap M(b)\big).$$

Esempio 10.7

$M(4) = \{4, 8, 12, 16, 20, \dots\}$, $M(6) = \{6, 12, 18, 24, \dots\}$. Multipli comuni: $\{12, 24, 36, \dots\}$. Il minimo è 12: $\mathrm{mcm}(4,6) = 12$.

Procedura — mcm per scomposizione in fattori primi

Per calcolare $\mathrm{mcm}(a,b)$:

1. Si scrivono i due numeri come prodotto di fattori primi.
2. Si prendono *tutti* i fattori primi che compaiono in almeno una delle due scomposizioni, *ciascuno con l'esponente più grande.*
3. Il prodotto di questi fattori (con esponenti massimi) è $\mathrm{mcm}(a,b)$.

Esempio 10.8

Calcolare $\mathrm{mcm}(72, 60)$.
Soluzione. $72 = 2^3 \cdot 3^2$, $60 = 2^2 \cdot 3 \cdot 5$. Fattori che compaiono almeno in una: 2, 3, 5. Esponenti massimi: 2^3, 3^2, 5^1. Quindi

$$\mathrm{mcm}(72,60) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

Teorema 10.4 — Relazione fra MCD e mcm

Per ogni $a, b \in \mathbb{N}^*$:

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

Dimostrazione (idea). Per ogni primo p che compare nelle due scomposizioni, sia α il suo esponente in a e β quello in b. L'esponente di p in $\mathrm{MCD}(a,b)$ è $\min(\alpha,\beta)$, quello in $\mathrm{mcm}(a,b)$ è $\max(\alpha,\beta)$. La loro somma è $\alpha + \beta$, che è proprio l'esponente di p in $a \cdot b$.

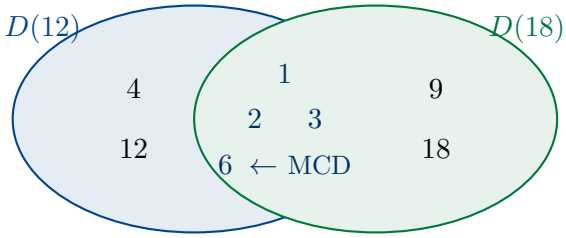
$$\mathrm{mcm}(a,b) = \frac{a \cdot b}{\mathrm{MCD}(a,b)}.$$

Questa identità è utilissima: una volta calcolato MCD, mcm si ottiene senza ricalcolare le scomposizioni.

CC BY-NC-SA 4.0 · a cura di Giovanni Nicco

Esempio 10.9 — Conferma

Con $a = 72$, $b = 60$: $\text{MCD} \cdot \text{mcm} = 12 \cdot 360 = 4320$, e $a \cdot b = 72 \cdot 60 = 4320$. ✓



divisori comuni: $\{1, 2, 3, 6\}$, $\max = 6 = \text{MCD}(12, 18)$

Figura 10.2: Lettura insiemistica del massimo comune divisore: nell'intersezione $D(12) \cap D(18)$ ci sono i divisori comuni dei due numeri; il *massimo* di questi è $\text{MCD}(12, 18) = 6$. Specularmente, $\text{mcm}(12, 18)$ è il *minimo* dell'intersezione di $M(12)$ e $M(18)$.

10.6. Algoritmo di Euclide

quiz e materiali con l'AI
flashcard del paragrafo

Per numeri grandi, scomporre in fattori primi può essere lungo. Esiste un metodo molto più rapido per calcolare l'MCD, noto fin dall'antichità: l'*algoritmo di Euclide*. Si basa su una sola osservazione, di una semplicità sorprendente.

Teorema 10.5 — Lemma di Euclide

Per ogni $a, b \in \mathbb{N}^*$ con $a \geq b$, se r è il resto della divisione di a per b, allora

$$\text{MCD}(a, b) = \text{MCD}(b, r).$$

In particolare, se $r = 0$, allora $\text{MCD}(a, b) = b$.

Dimostrazione (idea). Scriviamo $a = bq + r$. Un divisore comune di a e b deve dividere anche $r = a - bq$ (proprietà della divisibilità); viceversa, un divisore comune di b e r divide anche $a = bq + r$. Quindi $D(a) \cap D(b) = D(b) \cap D(r)$, e in particolare i massimi coincidono.

Procedura — Algoritmo di Euclide

Per calcolare $\text{MCD}(a, b)$ con $a \geq b > 0$:

1. Si esegue la divisione $a : b$, ottenendo quoziente q e resto r.
2. Se $r = 0$, l'MCD è b, e ci si ferma.
3. Altrimenti si pone $a \leftarrow b$, $b \leftarrow r$ e si ripete dal punto 1.

L'algoritmo termina in un numero finito di passi perché i resti formano una successione strettamente decrescente di numeri naturali.

CC BY-NC-SA 4.0 · a cura di Giovanni Nicco

Esempio 10.10 — Algoritmo di Euclide passo-passo

Calcolare $\mathrm{MCD}(252, 198)$.

Soluzione. Divisioni successive:

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 + 0 \end{aligned}$$

L'ultimo resto non nullo è 18. Quindi $\mathrm{MCD}(252, 198) = 18$.

Nota — Confronto con la scomposizione

Con la scomposizione: $252 = 2^2 \cdot 3^2 \cdot 7$, $198 = 2 \cdot 3^2 \cdot 11$. Fattori comuni: 2 e 3, esponenti minimi 1 e 2. Quindi $\mathrm{MCD} = 2 \cdot 3^2 = 18$. ✓Lo stesso risultato si ottiene molto più rapidamente con Euclide quando i fattori sono difficili da trovare.

Nota — Estensione a più numeri

Per calcolare $\mathrm{MCD}(a, b, c)$ basta osservare che $\mathrm{MCD}(a, b, c) = \mathrm{MCD}(\mathrm{MCD}(a, b), c)$: si applica l'algoritmo a coppie. Idem per mcm.

10.7. Esempi svolti

quiz e materiali con l'AI

Esempio 10.11 — Applicazione dei criteri di divisibilità

Stabilire, senza fare le divisioni, se $n = 27\,720$ è divisibile per $2, 3, 4, 5, 8, 9, 10, 11$.

Soluzione.

- Ultima cifra 0: $2 \mid n$, $5 \mid n$, $10 \mid n$.
- Somma cifre: $2 + 7 + 7 + 2 + 0 = 18$; $3 \mid 18$, $9 \mid 18$: $3 \mid n$, $9 \mid n$.
- Ultime due cifre: 20; $4 \mid 20$: $4 \mid n$.
- Ultime tre cifre: 720; $720 = 8 \cdot 90$: $8 \mid n$.
- Cifre alternate da destra: $(0 + 7 + 2) - (2 + 7) = 9 - 9 = 0$; $11 \mid 0$: $11 \mid n$.

Sorprendentemente, n è divisibile per tutti i numeri proposti. È un esempio classico: $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.

Esempio 10.12 — Calcolo di MCD e mcm con la scomposizione

Calcolare MCD e mcm di 84 e 126.

Soluzione. Scomponiamo: $84 = 2^2 \cdot 3 \cdot 7$, $126 = 2 \cdot 3^2 \cdot 7$.

$$\mathrm{MCD}(84, 126) = 2^1 \cdot 3^1 \cdot 7^1 = 42,$$
$$\mathrm{mcm}(84, 126) = 2^2 \cdot 3^2 \cdot 7 = 252.$$

Verifica: $\mathrm{MCD} \cdot \mathrm{mcm} = 42 \cdot 252 = 10\,584$ e $a \cdot b = 84 \cdot 126 = 10\,584$. ✓

Esempio 10.13 — Algoritmo di Euclide per numeri grandi

Calcolare $\mathrm{MCD}(1071, 462)$.
Soluzione. Divisioni successive:

$$1071 = 462 \cdot 2 + 147$$
$$462 = 147 \cdot 3 + 21$$
$$147 = 21 \cdot 7 + 0$$

L'ultimo resto non nullo è 21. Quindi $\mathrm{MCD}(1071, 462) = 21$.

Esempio 10.14 — Problema concreto: la corsa

Due tapis roulant compiono un giro rispettivamente ogni 24 e 36 secondi. Se vengono fatti partire insieme, dopo quanti secondi si ritroveranno entrambi al punto di partenza?
Soluzione. Cerchiamo il primo istante *comune*: è $\mathrm{mcm}(24, 36)$. Scomposizioni: $24 = 2^3 \cdot 3$, $36 = 2^2 \cdot 3^2$. Esponenti massimi: 2^3, 3^2. Quindi

$$\mathrm{mcm}(24, 36) = 2^3 \cdot 3^2 = 72.$$

Si ritroveranno insieme al punto di partenza dopo 72 s (ossia 1 minuto e 12 secondi).

Esempio 10.15 — Frazione ai minimi termini

Ridurre la frazione $\dfrac{252}{198}$ ai minimi termini.
Soluzione. Dividere numeratore e denominatore per il loro MCD. Dall'esempio precedente, $\mathrm{MCD}(252, 198) = 18$. Allora

$$\frac{252}{198} = \frac{252 : 18}{198 : 18} = \frac{14}{11}.$$

La forma ridotta è $\frac{14}{11}$ (numeratore e denominatore ora coprimi).

10.8. Esercizi proposti

quiz e materiali con l'AI

Esercizio 10.1

1. Stabilisci, applicando i criteri, se i seguenti numeri sono divisibili per $2, 3, 4, 5, 9, 11$:
   (a) 4320; (b) 18 711; (c) 50 050; (d) 121 121.

2. Esegui la divisione euclidea, dando quoziente e resto: (a) $137 : 12$; (b) $1\,000 : 7$; (c) $-58 : 5$; (d) $1234 : 11$.
3. Calcola MCD e mcm con il metodo della scomposizione: (a) 24 e 36; (b) 45 e 75; (c) 84 e 90; (d) 120 e 180.
4. Per ciascuna coppia calcolata nell'esercizio precedente, verifica la relazione $\text{MCD} \cdot \text{mcm} = a \cdot b$.
5. Calcola MCD con l'algoritmo di Euclide: (a) $\text{MCD}(216, 144)$; (b) $\text{MCD}(1001, 777)$; (c) $\text{MCD}(2024, 506)$; (d) $\text{MCD}(4096, 2730)$.
6. Per ciascun caso del punto 5, ricava poi mcm usando la formula $\text{mcm} = \frac{ab}{\text{MCD}}$.
7. Riduci ai minimi termini, usando l'MCD: (a) $\frac{45}{75}$; (b) $\frac{84}{126}$; (c) $\frac{1\,000}{375}$.
8. Problema: due lampade lampeggiano rispettivamente ogni 15 secondi e 20 secondi. Se cominciano insieme, dopo quanti secondi torneranno a lampeggiare contemporaneamente?
9. (Discussione.) Un compagno afferma: "se $a \mid c$ e $b \mid c$, allora $a \cdot b \mid c$". È vero in generale? Trova un controesempio. Sotto quale condizione (su a e b) la frase diventa vera?

10.9. Riepilogo del capitolo

quiz e materiali con l'AI

Riepilogo

- $b \mid a$ significa: esiste $k \in \mathbb{Z}$ con $a = bk$. Equivalentemente, la divisione euclidea di a per b ha resto $r = 0$.
- *Divisione euclidea*: per ogni $a \in \mathbb{Z}$ e $b \in \mathbb{N}^*$, esistono e sono unici $q, r \in \mathbb{Z}$ con $a = bq + r$ e $0 \le r < b$.
- Proprietà: $a \mid b \wedge b \mid c \Rightarrow a \mid c$ (transitiva); $a \mid b \wedge a \mid c \Rightarrow a \mid (b \pm c)$.
- *Criteri di divisibilità*: ultima cifra (per 2, 5, 10); ultime due cifre (per 4, 25); somma delle cifre (per 3 e 9); somma alternata delle cifre (per 11).
- *MCD* di a e b: il più grande divisore comune. Si calcola per scomposizione (fattori comuni con esponente minimo) o con l'*algoritmo di Euclide* (divisioni euclidee successive finché il resto è 0). a e b *coprimi* $\Leftrightarrow \text{MCD}(a, b) = 1$.
- *mcm* di a e b: il più piccolo multiplo comune non nullo. Per scomposizione: tutti i fattori (anche non comuni) con esponente massimo.
- Relazione fondamentale: $\text{MCD}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$, da cui $\text{mcm} = \frac{ab}{\text{MCD}}$.
- Applicazione tipica: ridurre una frazione $\frac{a}{b}$ ai minimi termini dividendo numeratore e denominatore per $\text{MCD}(a, b)$. Sarà il fulcro del capitolo 12.