

2 Algoritmo euclideo di divisione

In questo paragrafo intendiamo mostrare come alcune importanti proprietà dell'aritmetica elementare di \mathbb{Z} traggano origine dalla validità in \mathbb{N} del “Principio del Minimo” (ovvero, equivalentemente, dal “Principio di Induzione”, cfr. Teorema 1.2).

Teorema 2.1. (Algoritmo euclideo di divisione) *Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora, esistono e sono univocamente determinati due interi $q \in \mathbb{Z}$ (detto, quoziente) ed $r \in \mathbb{N}$ (detto resto) in modo tale che:*

$$a = bq + r, \quad 0 \leq r < |b|.$$

Dimostrazione. Mostriamo, dapprima, l'esistenza di q ed r .

Caso 1. Supponiamo che $b > 0$. Notiamo, innanzitutto, che l'insieme:

$$S := \{a - nb : a - nb \geq 0, n \in \mathbb{Z}\} (\subseteq \mathbb{N})$$

è non vuoto (ad esempio, se $n' = -|a|$, allora $a - n'b \in S$). Per il “Principio del Minimo” (Teorema 1.2), possiamo trovare un primo elemento nell'insieme S , che denotiamo con $r := a - qb$. Mostriamo che $r < b$. Se, per assurdo, fosse $r \geq b$ allora si avrebbe:

$$r - b = a - qb - b = a - (q + 1)b \geq 0,$$

e, dunque, anche $r - b (< r)$ appartenerrebbe ad S . Ciò contraddice la minimalità di $r \in S$.

Caso 2. Supponiamo che $b < 0$. Applichiamo il Caso 1 alla coppia di interi $a, -b$ ed avremo l'esistenza di due interi $q, r \in \mathbb{Z}$ che verificano le seguenti condizioni:

$$a = -bq + r = b(-q) + r, \quad 0 \leq r < -b = |-b| = |b|.$$

Mostriamo, ora, l'unicità di q, r . Supponiamo di avere $q, q', r, r' \in \mathbb{Z}$ in modo tale che:

$$a = bq + r = bq' + r', \quad 0 \leq r, r' < |b|,$$

allora $(q - q')b = r' - r < |b|$, dunque $|q - q'| |b| < |b|$, cioè $|q - q'| < 1$, ovvero $q = q'$. Da ciò segue immediatamente che anche $r = r'$. \square

Definizione 2.2. Dati due elementi $a, b \in \mathbb{Z}$.

(a) Diremo che a divide b (oppure che b è divisibile per a), in breve scriveremo “ $a \mid b$ ”, se esiste un elemento $c \in \mathbb{Z}$ in modo tale che $ac = b$. Se ciò non accade, diremo che a non divide b , e scriveremo “ $a \nmid b$ ”. Notiamo che:

$$x \mid x, \quad x \mid 0, \quad 1 \mid x, \quad \text{per ogni } x \in \mathbb{Z};$$

$$\begin{aligned}
0 \mid x &\Leftrightarrow x = 0; \\
x \mid 1 &\Leftrightarrow x = \pm 1; \\
a \mid b \text{ e } b \mid a &\Leftrightarrow a = \pm b; \\
a \mid b \text{ e } b \mid c &\Rightarrow a \mid c; \\
z \mid a \text{ e } z \mid b &\Rightarrow z \mid ax + by, \quad \text{presi comunque } x, y \in \mathbb{Z}; \\
a \mid b &\Leftrightarrow ac \mid bc \quad \text{per ogni } c \in \mathbb{Z}.
\end{aligned}$$

(b) Se $ab \neq 0$ (cioè, se a e b non sono contemporaneamente nulli) si chiama *Massimo Comun Divisore* di a, b (in breve, $\text{MCD}(a, b)$) un intero $d \in \mathbb{Z}$ tale che:

$$\text{(MCD1)} \quad d \mid a, \quad d \mid b;$$

$$\text{(MCD2)} \quad d' \in \mathbb{Z}, \quad d' \mid a, \quad d' \mid b \Rightarrow d' \mid d.$$

Notiamo che se $a = 0$ e $b \neq 0$, allora b (ovvero, $-b$) è un Massimo Comun Divisore di 0 e b .

Infine, osserviamo che $\text{MCD}(0, 0)$ non è definito, in quanto ogni intero $x \in \mathbb{Z}$ è tale che $x \mid 0$ (e, quindi, non esiste un intero “massimo con tale proprietà”, cioè non esiste un intero che verifica anche la proprietà **(MCD2)**).

(c) Se a, b non sono entrambi nulli, diremo che a e b sono *relativamente primi* (ovvero, *coprimi*) se $\text{MCD}(a, b) = 1$. \square

Teorema 2.3. *Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esiste sempre un Massimo Comun Divisore d di a e b in \mathbb{Z} . Se d_1 e d_2 sono due Massimi Comun Divisori di a e b allora $d_1 = \pm d_2$.*

Il Massimo Comun Divisore d di a e b esiste ed è univocamente determinato in \mathbb{N} (in tal caso, esso è il più grande tra i divisori positivi comuni ad a e b , quindi la scrittura $d := \text{MCD}(a, b)$ ha un significato univoco quando si sceglie $d \in \mathbb{N}$) ed esso coincide con il minimo intero positivo nell'insieme:

$$S_{a,b} := \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}.$$

Dimostrazione. Sia $d := ax_0 + by_0$ il minimo intero (positivo) dell'insieme non vuoto $S_{a,b}$. Mostriamo che, preso comunque $z := ax + by \in \mathbb{Z}$, con $x, y \in \mathbb{Z}$ (dove z può anche non appartenere ad $S_{a,b}$), allora $d \mid z$. Possiamo, ovviamente, supporre che $z \neq 0$. Per il Teorema 2.1, possiamo trovare $q, r \in \mathbb{Z}$, in modo tale che:

$$z = dq + r, \quad 0 \leq r < d,$$

ovvero,

$$ax + by - (ax_0 + by_0)q = r \quad \text{cioè} \quad a(x - x_0q) + b(y - y_0q) = r$$

dunque se $r > 0$ allora $r (< d) \in S_{a,b}$. Per la minimalità di d possiamo concludere che $r = 0$, ovvero che $d \mid z$. In particolare, $d \mid a$ (per $x = 1$ e $y = 0$) e $d \mid b$ (per $x = 0$ e $y = 1$), (proprietà **(MCD1)** per d).

Per terminare, mostriamo che d verifica anche la proprietà **(MCD2)**. Se $d' \mid b$ e $d' \mid a$, allora è subito visto dalla definizione di divisibilità che $d' \mid a\alpha + b\beta$, presi comunque $\alpha, \beta \in \mathbb{Z}$. Dunque, in particolare, $d' \mid d$ (prendendo $\alpha = x_0$ e $\beta = y_0$). \square

Osservazione 2.4. Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, da quanto precede segue immediatamente che:

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

Corollario 2.5. (*Identità di Bézout (1730–1783)*) Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esistono $x, y \in \mathbb{Z}$ in modo tale che:

$$\text{MCD}(a, b) = ax + by. \quad \square$$

Corollario 2.6. (*Lemma di Euclide, IV–III Sec. A.C.*) Siano $a, b, c \in \mathbb{Z}$. Allora:

$$\text{MCD}(a, b) = 1 \text{ e } a \mid bc \Rightarrow a \mid c.$$

Dimostrazione. Dal Corollario 2.5 sappiamo che esistono $x, y \in \mathbb{Z}$ con $1 = ax + by$. Pertanto, $c = c \cdot 1 = acx + bcy$. Inoltre, per ipotesi, esiste un intero $k \in \mathbb{Z}$ in modo tale che $ak = bc$. Sostituendo abbiamo $c = acx + ak y = a(cx + ky)$, da cui ricaviamo che $a \mid c$. \square

Definizione 2.7. Dati due elementi $a, b \in \mathbb{Z}$. Si chiama *minimo comune multiplo di a, b* (in breve, $\text{mcm}(a, b)$) un intero $h \in \mathbb{Z}$ tale che:

$$\text{(mcm1)} \quad a \mid h, \quad b \mid h;$$

$$\text{(mcm2)} \quad h' \in \mathbb{Z}, \quad a \mid h', \quad \text{e } b \mid h' \Rightarrow h \mid h'.$$

Notiamo che, dalle proprietà della relazione di divisibilità, discende immediatamente che $\text{mcm}(a, 0) = \text{mcm}(0, b) = \text{mcm}(0, 0) = 0$.

Osservazione 2.8. Dati comunque $a, b \in \mathbb{Z}$, se h_1 e h_2 sono due minimi comuni multipli di a e b allora $h_1 = \pm h_2$. Pertanto, *un minimo comune multiplo h di a e b , se esiste, esso è univocamente determinato in \mathbb{N}* (in tal caso esso coincide con il minimo tra tutti gli interi positivi che seguono a e b e che sono multipli sia di a che di b , quindi *la scrittura $h := \text{mcm}(a, b)$ ha un significato univoco quando si sceglie $d \in \mathbb{N}$*). Il prossimo risultato mostra l'esistenza del $\text{mcm}(a, b)$, per ogni coppia di elementi $a, b \in \mathbb{Z}$. E' ovvio, da quanto precede, che $\text{mcm}(a, b) = \text{mcm}(|a|, |b|)$.

Teorema 2.9. *Dati comunque $a, b \in \mathbb{Z}$, non entrambi nulli, esiste ed è univocamente determinato in \mathbb{N} il $\text{mcm}(a, b)$ e risulta:*

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

Dimostrazione. Per le Osservazioni 2.8 e 2.4 non è restrittivo supporre che $a > 0$, $b > 0$. Sia $d := \text{MCD}(a, b)$. Allora, esistono $\alpha, \beta, x, y \in \mathbb{Z}$ in modo tale che:

$$a = d\alpha, \quad b = d\beta, \quad \text{e} \quad d = ax + by.$$

Poniamo $m := \frac{ab}{d} \in \mathbb{N}$. Allora abbiamo che $m = a\beta = b\alpha$ e quindi che $a \mid m$ e $b \mid m$ (proprietà **(mcm1)**). Sia ora h' un multiplo comune di a e b , cioè $a \mid h'$ e $b \mid h'$, ovvero $h' = a\alpha' = b\beta'$, per una qualche coppia $\alpha', \beta' \in \mathbb{N}$. Notiamo che:

$$\frac{h'}{m} = \frac{h'd}{ab} = \frac{h'(ax + by)}{ab} = \frac{h'}{b}x + \frac{h'}{a}y = \beta'x + \alpha'y \in \mathbb{Z},$$

pertanto $m \mid h'$ (proprietà **(mcm2)**). Da ciò ricaviamo che $\frac{ab}{d} = m = \text{mcm}(a, b)$ e, quindi, che $ab = \text{MCD}(a, b)\text{mcm}(a, b)$. \square

Osservazione 2.10. Per ogni $x \in \mathbb{Z}$, denotiamo con $x\mathbb{Z} := \{xk : k \in \mathbb{Z}\}$. Allora, si può facilmente verificare che:

- (a) $a\mathbb{Z} \supseteq b\mathbb{Z} \Leftrightarrow a \mid b$;
- (b) $\text{MCD}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} := \{ax + by \mid x, y \in \mathbb{Z}\}$;
- (c) $\text{mcm}(a, b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

Definizione 2.11. Un intero $p \geq 2$ si dice *primo* se dati $a, b \in \mathbb{Z}$ allora:

$$p \mid ab \quad \text{e} \quad p \nmid a \quad \Rightarrow \quad p \mid b.$$

Un intero $q \geq 2$ si dice *irriducibile* se dati $a, b \in \mathbb{Z}$ allora:

$$q = ab \quad \text{e} \quad q \neq \pm a \quad \Rightarrow \quad q = \pm b \quad (\text{e quindi } a = \pm 1).$$

Proposizione 2.12. Per un intero $p \geq 2$, le seguenti affermazioni sono tra loro equivalenti:

- (i) p è primo;
- (ii) p è irriducibile;
- (iii) i divisori positivi di p sono soltanto 1 e p .

Dimostrazione. (i) \Rightarrow (ii). Supponiamo che $p = ab$ e che $p \neq \pm a$. Allora, ovviamente, $p \mid ab$. Inoltre, $p \nmid a$, perché se esistesse un intero $k \in \mathbb{Z}$ in modo tale che $pk = a$, allora avremmo che $p = ab = pkb$, da cui dedurremmo che $1 = kb$ (Legge di cancellazione, Esercizio 1.3 (c)), cioè $b = \pm 1$ ovvero $p = \pm a$, pervenendo così ad una contraddizione. Allora, avendo assunto la validità di (i), otteniamo che $p \mid b$. Pertanto, deve esistere un intero $h \in \mathbb{Z}$ in modo tale che $ph = b$. Quindi $p = ab = ahp$, cioè $1 = ah$ (Legge di cancellazione, Esercizio 1.3 (c)), dunque $a = \pm 1$ ovvero $p = \pm b$.

(ii) \Rightarrow (iii). Se, per assurdo la proprietà (iii) non fosse verificata, allora potremmo trovare due interi positivi $1 < a, b < p$ in modo tale che $p = ab$. Ma questo fatto contraddice (ii).

(iii) \Rightarrow (i). Se p verifica (iii) e $p \nmid a$, allora necessariamente $\text{MCD}(p, a) = 1$. Pertanto la conclusione che $p \mid b$ discende dal Lemma di Euclide (Corollario 2.6). \square

Teorema 2.13. (*Teorema Fondamentale dell'Aritmetica*, Euclide IV-III Sec. A.C.) *Un qualunque intero $a \in \mathbb{Z} \setminus \{0, 1, -1\}$ ammette una decomposizione unica (a meno dell'ordine dei fattori) del tipo:*

$$a = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$$

dove $r \geq 1$, p_i è un intero primo, $e_i \geq 1$, per ogni $1 \leq i \leq r$, ed inoltre $p_i \neq p_j$, se $1 \leq i \neq j \leq r$.

Dimostrazione. Non è ovviamente restrittivo limitare la dimostrazione del teorema al caso $a \geq 2$.

Dimostriamo dapprima l'esistenza della decomposizione. Procediamo per induzione su a .

Base dell'induzione: $a = 2$. L'enunciato è banalmente vero, essendo $a = 2$ un numero primo.

Passo Induttivo: Supponiamo, per ipotesi induttiva, che l'enunciato sia vero per ogni intero $2 \leq b < a$. Se a è un numero primo, non c'è nulla da dimostrare. Se a non è primo, allora $a = xy$, con $2 \leq x, y < a$. Per l'ipotesi induttiva (applicata ad x ed y), possiamo scrivere:

$$x = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n} \quad \text{e} \quad y = p_1^{g_1} p_2^{g_2} \dots p_m^{g_m}$$

dunque:

$$a = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n} p_1^{g_1} p_2^{g_2} \dots p_m^{g_m}.$$

Dopo aver raccolto gli eventuali fattori con la stessa base, otteniamo proprio una decomposizione del tipo enunciato.

Dimostriamo ora l'unicità della decomposizione. Supponiamo di avere due decomposizioni di a con le proprietà enunciate:

$$p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} = a = q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}.$$

Poiché p_1 è un numero primo e $p_1 \mid q_1^{f_1} q_2^{f_2} \dots q_s^{f_s}$, allora $p_1 \mid q_j$, per un qualche $1 \leq j \leq s$. Essendo anche q_j un numero primo (ovvero irriducibile), allora necessariamente $p_1 = q_j$. Dividendo le due decomposizioni di a per p_1 (quella di destra) e per q_j (quella di sinistra) (o, più precisamente, applicando la Legge di cancellazione, Esercizio 1.3 (c)) ed iterando il procedimento precedente, otteniamo necessariamente che $r = s$, $p_i = q_i$ (a meno di un cambiamento degli indici dei fattori ovvero del loro ordine) e $e_i = f_i$, per ogni $1 \leq i \leq r$. \square

2. Esercizi e Complementi

2.1. Siano $a_1, a_2, \dots, a_n \in \mathbb{Z}$ ($n \geq 2$) interi non tutti nulli. Un *Massimo Comun Divisore* di a_1, a_2, \dots, a_n (in breve, $\text{MCD}(a_1, a_2, \dots, a_n)$) è un intero $d \in \mathbb{Z}$ tale che:

(MCD1) $d \mid a_i$, per ogni $1 \leq i \leq n$;

(MCD2) $d' \in \mathbb{Z}$, $d' \mid a_i$, per ogni $1 \leq i \leq n \Rightarrow d' \mid d$.

Mostrare che *esiste un unico Massimo Comun Divisore* $d \in \mathbb{N}$ di a_1, a_2, \dots, a_n , il quale coincide con in minimo intero nell'insieme non vuoto:

$$S_{a_1, a_2, \dots, a_n} := \{a_1 y_1 + a_2 y_2 + \dots + a_n y_n : \begin{array}{l} y_i \in \mathbb{Z}, 1 \leq i \leq n, \\ a_1 y_1 + a_2 y_2 + \dots + a_n y_n > 0 \end{array}\}.$$

In particolare, esistono $x_1, x_2, \dots, x_n \in \mathbb{Z}$ in modo tale che il Massimo Comun Divisore (univocamente determinato in \mathbb{N}) si può esprimere nella forma seguente:

$$\text{MCD}(a_1, a_2, \dots, a_n) = a_1 x_1 + a_2 x_2 + \dots + a_n x_n \quad (\text{Identità di Bézout}).$$

[Suggestimento. Basta seguire, con le appropriate modifiche, la dimostrazione del Teorema 2.3.]

2.2. Siano a, b, c degli interi non nulli di \mathbb{N} . Mostrare che valgono le seguenti proprietà:

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

(b) $\text{MCD}(a, 1) = 1$.

(c) $\text{MCD}(ab, ac) = a \text{MCD}(b, c)$.

(d) $d = \text{MCD}(a, b) \Rightarrow \text{MCD}(\frac{a}{d}, \frac{b}{d}) = 1$.

(e) $\text{MCD}(a, b) = 1 = \text{MCD}(a, c) \Rightarrow \text{MCD}(a, bc) = 1$.

(f) $a \mid c, b \mid c, \text{ e } \text{MCD}(a, b) = 1 \Rightarrow ab \mid c$.

[Suggestimento. (a) Ci limitiamo a dimostrare la prima uguaglianza. Sia $d := \text{MCD}(a, b, c)$ e $\tilde{d} := \text{MCD}(a, \text{MCD}(b, c))$. Poiché $d \mid b$ e $d \mid c$, allora, $d \mid \text{MCD}(b, c)$ e, quindi $d \mid \tilde{d} = \text{MCD}(a, \text{MCD}(b, c))$. Viceversa, poiché \tilde{d} divide a, b, c , allora $\tilde{d} \mid d = \text{MCD}(a, b, c)$. Dunque, $d = \tilde{d}$.

(b) Segue dal fatto che $1 \mid a$ e se $x \mid 1$, allora $x = \pm 1$.

(c) Sia $t := \text{MCD}(b, c)$ e $\tilde{t} := \text{MCD}(ab, ac)$. E' ovvio che $at \mid ab$ e $at \mid ac$, quindi $at \mid \text{MCD}(ab, ac) = \tilde{t}$. Poiché $a \mid \text{MCD}(ab, ac) = \tilde{t}$ allora $\tilde{t} = ax$, per un qualche intero x . D'altra parte sappiamo che $at \mid \tilde{t} = ax$, quindi $t \mid x$. Inoltre $ax = \tilde{t} \mid ab$ e $ax = \tilde{t} \mid ac$, quindi $x \mid b$ e $x \mid c$, dunque $x \mid \text{MCD}(b, c) = t$. Pertanto $x = \pm t$, ovvero $\tilde{t} = \pm at$.

(d) Da (c) ricaviamo che $d = \text{MCD}(a, b) = \text{MCD}(d \frac{a}{d}, d \frac{b}{d}) = d \text{MCD}(\frac{a}{d}, \frac{b}{d})$, quindi $1 = \text{MCD}(\frac{a}{d}, \frac{b}{d})$.

(e) Per l'identità di Bézout, esistono $x, y, u, v \in \mathbb{Z}$ in modo tale che $ax + by = 1 = au + cv$. Quindi $1 = (ax + by)(au + cv) = a(axu + byu + cvx) + bc(yv) = a(u + cvx) + bc(yv)$, da cui si ricava che $1 = \text{MCD}(a, bc)$ (Teorema 2.3).

(f) Poiché $a \mid c$, allora $ab \mid cb$. Analogamente si prova che $ab \mid ac$. Dunque $ab \mid \text{MCD}(cb, ca) = c \text{MCD}(b, a) = c$.]

2.3. Algoritmo euclideo delle divisioni successive (metodo algoritmico per il calcolo del MCD di due elementi in \mathbb{Z}). Siano a e b due interi non nulli di \mathbb{Z} dei quali si vuole calcolare il MCD. Dal momento che $\text{MCD}(a, b) = \text{MCD}(|a|, |b|)$, allora possiamo supporre, senza perdere in generalità che $a \geq b > 0$. Applicando ricorsivamente l'Algoritmo di divisione abbiamo:

$$\begin{array}{ll} a = bq_1 + r_1, & 0 < r_1 < b =: r_0 \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_k = r_{k+1}q_{k+2} + r_{k+2}, & 0 < r_{k+2} < r_{k+1} \\ \vdots & \vdots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} + 0, & 0 = r_{n+1} < r_n \end{array}$$

dove $n \geq 0$.

Mostrare che:

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

(b) $r_n = ax_n + by_n$ (Identità di Bézout)

dove x_n e y_n in \mathbb{Z} sono calcolabili ricorsivamente tramite le seguenti formule:

$$\begin{array}{ll} x_0 := 0 & y_0 := 1 \\ x_1 := 1 & y_1 := -q_1 \\ \vdots & \vdots \\ x_k := x_{k-2} - q_k x_{k-1} & y_k := y_{k-2} - q_k y_{k-1}, \quad \text{per ogni } k \geq 2. \end{array}$$

[Suggerimento. (a) Osserviamo che se $a = bq + r$, con $0 \leq r < b$, allora $\text{MCD}(a, b) = \text{MCD}(b, r)$. Infatti l'insieme dei divisori comuni di a e b coincide con l'insieme dei divisori comuni di b ed $r = a - bq$ e quindi, ovviamente, il "massimo" elemento del primo insieme coincide con il "massimo" elemento del secondo insieme. Applicando ricorsivamente questa proprietà alla successione di divisioni euclidee, abbiamo $\text{MCD}(a, b) = \text{MCD}(b, r_1) = \text{MCD}(r_1, r_2) = \dots = \text{MCD}(r_{n-1}, r_n) = r_n$.

(b) Per induzione. Base dell'induzione:

$$\begin{array}{l} n = 0 : \quad r_0 := b = a \cdot 0 + b \cdot 1 \Rightarrow x_0 = 0, y_0 = 1. \\ n = 1 : \quad r_1 = a \cdot 1 - bq_1 \Rightarrow x_1 = 1, y_1 = -q_1. \end{array}$$

Passo induttivo. Supponiamo che, per ogni h , con $0 \leq h \leq k$, con $k \geq 1$, si abbia $r_h = ax_h + by_h$. Poiché:

$$r_{k-1} = r_k q_{k+1} + r_{k+1}, \quad \text{cioè } r_{k+1} = r_{k-1} - r_k q_{k+1},$$

allora l'espressione di r_{k+1} , come combinazione lineare di a e b , può essere calcolata ricorsivamente:

$$\begin{aligned} r_{k+1} &= r_{k-1} - r_k q_{k+1} = ax_{k-1} + by_{k-1} - (ax_k + by_k)q_{k+1} = \\ &= a(x_{k-1} - q_{k+1}x_k) + b(y_{k-1} - q_{k+1}y_k). \end{aligned}$$

2.4. Siano a e b due interi non nulli di \mathbb{Z} . Utilizziamo le notazioni dell'Esercizio 2.3. Per il calcolo del $\text{MCD}(a, b)$, abbiamo già osservato che non è restrittivo supporre che $a > b > 0$. Definiamo *lunghezza* $\lambda(a, b)$ dell'algoritmo euclideo della coppia (a, b) il numero $n + 1$ di divisioni necessarie per ottenere un resto $r_{n+1} = 0$. Definiamo *lunghezza euclidea di a* , $\lambda(a)$, il massimo valore raggiunto da $\lambda(a, b)$, al variare di b , con $a > b > 0$, i.e.

$$\lambda(a) := \text{Max}\{\lambda(a, b) : b \in \mathbb{N}, a > b > 0\}.$$

- (a) Mostrare che: $\lambda(a) = 1 \Leftrightarrow a = 2$.
 (b) Calcolare $\lambda(a)$ per tutti gli interi a , con $2 \leq a \leq 8$.

La *successione di Fibonacci* è la successione di numeri naturali definita induttivamente nella maniera seguente:

$$u_0 := 1, \quad u_1 := 1, \quad u_n := u_{n-1} + u_{n-2}, \quad \text{per ogni } n \geq 2.$$

Dunque, $u_2 := 2, u_3 := 3, u_4 := 5, u_5 := 8, u_6 := 13, \dots$

- (c) Mostrare che $\text{MCD}(u_{n+1}, u_n) = 1$ e che $\lambda(u_{n+1}, u_n) = n$, per ogni $n \geq 1$.

Date due coppie di interi positivi (a, b) , (a', b') con $a > b$ e $a' > b'$, diremo che (a, b) *precede* (a', b') se $\lambda(a, b) \leq \lambda(a', b')$.

- (d) Fissato $n \geq 1$, mostrare che (u_{n+1}, u_n) precede tutte le coppie (a, b) , con $a > b$, tali che $\lambda(a, b) = n$.

(e) (**Teorema di Lamé**, 1845) Mostrare che: $\lambda(u_{n+1}) = n$ e, se $\lambda(a) = n$, allora $a \geq u_{n+1}$.

- (f) Mostrare che $\lambda(a, b) \leq 2 \log_2(b) + 1$.

Osservare che tale stima è collegata al numero delle cifre, $\mathbf{cf}_2(b)$, del numero b nella sua scrittura in base 2 (ad esempio, se $b = 8 = (1000)_2$, $\mathbf{cf}_2(8) = 4$, $\log_2(8) = 3$).

Infatti, per ogni $b \geq 1$, $\log_2(b) < \mathbf{cf}_2(b)$.

- (g) Mostrare che $\lambda(a) < 2\mathbf{cf}_2(a) + 1$.

- (h) Mostrare per induzione su $n \geq 1$ che:

$$u_n \leq \left(\frac{7}{4}\right)^{n+1}.$$

Per ottenere una migliore approssimazione del valore di u_n , abbiamo bisogno di richiamare la nozione di numero aureo. Ricordiamo che il *rapporto aureo tra due lunghezze* era quella proporzione giudicata la più armoniosa secondo i canoni estetici classici tra le lunghezze a e b dei lati di un rettangolo e si ha quando $a > b$ e

$$\frac{a}{b} = \frac{a+b}{a} \quad \text{ovvero} \quad \frac{a}{b} = \frac{1+\sqrt{5}}{2} =: \omega,$$

(si noti che il numero reale ω (≈ 1.61803), detto *numero aureo*, è una delle due radici reali dell'equazione $X^2 - X - 1 = 0$, equazione determinata dalla relazione di rapporto aureo; l'altra soluzione è $\bar{\omega} := \frac{1-\sqrt{5}}{2}$ (≈ -0.618034)).

- (i) Mostrare per induzione su $n \geq 0$ che:

$$u_n = \frac{\omega^{n+1} - \bar{\omega}^{n+1}}{\sqrt{5}}.$$

- (j) Dedurre dal punto precedente che, per ogni $n \geq 1$,

$$\left|u_n - \frac{\omega^{n+1}}{\sqrt{5}}\right| < \frac{1}{2},$$

dunque u_n è l'intero più prossimo al numero reale $\frac{\omega^{n+1}}{\sqrt{5}}$ e quindi:

$$u_n \approx \frac{\omega^{n+1}}{\sqrt{5}}.$$

(k) Sia a un intero positivo, denotiamo con $\mathbf{cf}_{10}(a)$ il numero delle cifre di a nella sua scrittura decimale (ad esempio, se $a = 9705$ allora $\mathbf{cf}_{10}(a) = 4$). Mostrare che:

$$\begin{aligned} \lambda(a) &\lesssim \log_{\omega}(a) + \frac{1}{2} \log_{\omega}(5) - 2 \approx \log_{\omega}(a) - 0.327724 \approx \\ &\approx 4.78497 \cdot \text{Log}(a) - 0.327724 < 5\mathbf{cf}_{10}(a). \end{aligned}$$

[Suggesto. (a, \Leftarrow) Se $a = 2$, allora $b = 1$, quindi $a = 2b + 0$, cioè, in questo caso, $r_1 = 0$, dunque $\lambda(a) = 1$.

(a, \Rightarrow) Se, per assurdo, $a > 2$, prendiamo $b := a - 1$, allora:

$$a = b \cdot 1 + 1, \quad b = 1 \cdot b + 0,$$

dunque $\lambda(a) \geq \lambda(a, a - 1) = 2$.

(b) $\lambda(3) = \lambda(4) = \lambda(6) = 2$; $\lambda(5) = \lambda(7) = 3$; $\lambda(8) = 4 (= \lambda(8, 5))$.

(c) Dalla definizione stessa dei numeri di Fibonacci abbiamo che:

$$\begin{aligned} u_{n+1} &= u_n \cdot 1 + u_{n-1}, & 0 < u_{n-1} < u_n \\ u_n &= u_{n-1} \cdot 1 + u_{n-2}, & 0 < u_{n-2} < u_{n-1} \\ &\vdots & \vdots \\ u_3 &= u_2 \cdot 1 + u_1, & 0 < 1 = u_1 < u_2 \\ u_2 &= u_1 \cdot 2 + 0. \end{aligned}$$

(d) Per minimalizzare il valore di a , in un algoritmo euclideo che conta n divisioni con il resto, dobbiamo prendere gli interi q_1, q_2, \dots, q_n ed r_{n-1} il più piccoli possibile e, poi, ricavare attraverso le equazioni dell'algoritmo i valori di $r_{n-2}, r_{n-1}, \dots, r_1, b, a$. Poiché $q_1, q_2, \dots, q_{n-1} \geq 1$ e $q_n \geq 2$ (dal momento che $q_n r_{n-1} = r_{n-2} > r_{n-1}$) ed, inoltre, $r_{n-1} \geq 1$ (dal momento che $r_{n-1} > r_n = 0$), allora prendendo esattamente $q_1 = q_2 = \dots = q_{n-1} = 1$, $q_n = 2$ e $r_{n-1} = 1$, otteniamo proprio che a deve coincidere con u_{n+1} (in tal caso, poi, $b = u_n$).

(e) Se $u_{n+1} \geq a > b > 0$ e se $\lambda(a, b) = m$ allora, per il punto (d), $a \geq u_{m+1}$ e quindi $u_{n+1} \geq u_{m+1}$. Pertanto $m \leq n$, dunque $\lambda(a) \leq n$. In particolare, per $a = u_{n+1}$, ricaviamo $\lambda(u_{n+1}) \leq n$. Quindi, utilizzando (c), concludiamo che $\lambda(u_{n+1}) = n$.

(f) Supponiamo che $\lambda(a, b) = n + 1$. E' subito visto che $r_{-1} := a > 2r_1$ e $r_0 := b > 2r_2$. In generale, $r_{k-2} > 2r_k$, per ogni k , con $1 \leq k \leq n$. Pertanto, se n è pari, allora $b > 2^{\frac{n}{2}}$; se n è dispari, allora $b > 2^{\frac{n-1}{2}}$. In ogni caso, $b > 2^{\frac{n-1}{2}}$, dunque $\log_2(b) > \frac{n-1}{2}$. Pertanto, $2\log_2(b) + 1 > n$, quindi $2\log_2(b) + 1 \geq n + 1 = \lambda(a, b)$.

(g) è una conseguenza immediata di (f), dal momento che $a > b$ e, quindi, $\log_2(a) > \log_2(b)$.

(h) Per $n = 0, 1, 2$ la disuguaglianza è banalmente verificata:

$$\begin{aligned} u_0 &= 1 = \left(\frac{7}{4}\right)^0 \\ u_1 &= 1 < \left(\frac{7}{4}\right)^1 = 1.75 \\ u_2 &= 2 < \left(\frac{7}{4}\right)^2 \approx 3.0625. \end{aligned}$$

Sia $n \geq 3$, applicando l'ipotesi induttiva ai casi $n - 1$ ed $n - 2$, allora possiamo concludere:

$$u_n = u_{n-1} + u_{n-2} < \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2} = \left(\frac{7}{4}\right)^{n-2} \left(\frac{7}{4} + 1\right) < \left(\frac{7}{4}\right)^{n-2} \left(\frac{7}{4}\right)^2.$$

(i) Per $n = 0$ e per $n = 1$ l'uguaglianza è banalmente verificata:

$$\begin{aligned} u_0 &= \frac{\omega - \bar{\omega}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 \\ u_1 &= \frac{\omega^2 - \bar{\omega}^2}{\sqrt{5}} = \\ &= \frac{\omega + 1 - (\bar{\omega} + 1)}{\sqrt{5}} = 1 \end{aligned}$$

(si ricordi che $\omega^2 - \omega - 1 = 0 = \bar{\omega}^2 - \bar{\omega} - 1$). Supponiamo, per ipotesi induttiva che, per $n \geq 2$, $u_{n-1} = \frac{\omega^{n-1} - \bar{\omega}^{n-1}}{\sqrt{5}}$ e $u_{n-2} = \frac{\omega^{n-2} - \bar{\omega}^{n-2}}{\sqrt{5}}$. Allora:

$$\begin{aligned} u_n = u_{n-1} + u_{n-2} &= \frac{\omega^{n-1} - \bar{\omega}^{n-1}}{\sqrt{5}} + \frac{\omega^{n-2} - \bar{\omega}^{n-2}}{\sqrt{5}} = \\ &= \frac{\omega^{n-1}(\omega + 1) - \bar{\omega}^{n-1}(\bar{\omega} + 1)}{\sqrt{5}} = \frac{\omega^{n+1} - \bar{\omega}^{n+1}}{\sqrt{5}}. \end{aligned}$$

(j) Basta osservare che, per ogni $n \geq 1$,

$$\left| \frac{\bar{\omega}^n}{\sqrt{5}} \right| < \left| \frac{\bar{\omega}}{\sqrt{5}} \right| \approx 0.276393 < \frac{1}{2}.$$

(k) Se $n = \lambda(a)$ allora $a \geq u_{n+1} \gtrsim \frac{\omega^{n+2}}{\sqrt{5}}$, dunque:

$$\log_\omega(a) \gtrsim n + 2 - \log_\omega(\sqrt{5}) \Rightarrow n \lesssim \log_\omega(a) + \frac{1}{2} \log_\omega(5) - 2.$$

La conclusione discende dal momento che $\log_\omega(5) \approx 3.34455$, $\frac{1}{2} \log_\omega(5) - 2 \approx -0.327724$, $\log_\omega(a) = \text{Log}(a)/\text{Log}(\omega) \approx 4.78497 \cdot \text{Log}(a)$, $\text{Log}(a) < \mathbf{cf}_{10}(a)$.]

2.5. Siano a e b due interi non nulli di \mathbb{Z} e sia $d := \text{MCD}(a, b)$.

- (a) Mostrare che, nell'espressione $d = ax + by$, nota come Identità di Bézout, la coppia di interi $x, y \in \mathbb{Z}$ non è univocamente determinata (mostrare con un esempio esplicito, ad esempio $a = 4$, $b = 6$, $d = 2$, che possono esistere due coppie distinte di interi in modo tale che $d = ax + by = ax' + by'$).
- (b) Siano $x_0, y_0 \in \mathbb{Z}$ tali che $ax_0 + by_0 = 1$. Preso comunque $n \in \mathbb{Z}$, poniamo $x_n := x_0 + nb$ e $y_n := y_0 - na$. Verificare che, per ogni $n \in \mathbb{Z}$, risulta $ax_n + by_n = 1$.
- (c) Mostrare che, se $ax_0 + by_0 = 1 = ax + by$, con $x_0, y_0, x, y \in \mathbb{Z}$, allora esiste un intero $n \in \mathbb{Z}$ in modo tale che $x = x_0 + nb$ e $y = y_0 - na$.
- (d) Mostrare che, se $ax_0 + by_0 = d = ax + by$ con $x_0, y_0, x, y \in \mathbb{Z}$, allora esiste un intero $n \in \mathbb{Z}$ in modo tale che $x = x_0 + n \frac{\text{mcm}(a,b)}{a}$ e $y = y_0 - n \frac{\text{mcm}(a,b)}{b}$.

[Suggerimento. (a) Basta prendere, ad esempio, $(x, y) = (-1, 1)$ e $(x', y') = (2, -1)$.

(b) $ax_n + by_n = a(x_0 + nb) + b(y_0 - na) = ax_0 + by_0 = 1$.

(c) Se $ax_0 + by_0 = 1$, allora $\text{MCD}(a, b) = 1$ (Teorema 2.3). Da $ax_0 + by_0 = 1 = ax + by$, ricaviamo che $a(x - x_0) = b(y_0 - y)$, cioè $a \mid b(y_0 - y)$, quindi $a \mid y_0 - y$. Se poniamo $n := \frac{(y_0 - y)}{a}$ allora abbiamo $x = x_0 + nb$ e $y = y_0 - na$.

(d) Poiché

$$a \frac{x_0}{d} + b \frac{y_0}{d} = 1 = a \frac{x}{d} + b \frac{y}{d},$$

allora, per (c), $x = x_0 + n \frac{b}{d}$ e $y = y_0 - n \frac{a}{d}$. Per concludere basta ricordare che:

$$\text{mcm}(a, b) = \text{mcm}(a, b) \frac{\text{MCD}(a, b)}{d} = \frac{ab}{d}.]$$

2.6. Mostrare la validità della seguente variante dell'algoritmo euclideo di divisione (Teorema 2.1):

Siano $a, b \in \mathbb{Z}$, $b \neq 0$. Allora, esistono e sono univocamente determinati due interi $q, r \in \mathbb{Z}$ in modo tale che:

$$a = bq + r, \quad -\frac{1}{2} |b| \leq r < \frac{1}{2} |b|.$$

[Suggerimento. Sappiamo (Teorema 2.1) che esistono e sono univocamente determinati due interi $q, r \in \mathbb{Z}$ in modo tale che $a = bq + r$, con $0 \leq r < |b|$. Se $(0 \leq) r < \frac{1}{2} |b|$, allora non c'è null'altro da dimostrare. Supponiamo, dunque, che $\frac{1}{2} |b| \leq r < |b|$. In tal caso, $0 < |b| - r \leq |b| - \frac{1}{2} |b| = \frac{1}{2} |b| \leq r < |b|$. Scriviamo $r = (|b| - r) + r'$, con $r' := 2r - |b|$. Dunque, per un'opportuna scelta del segno (dipendente dal segno di $|b|$), abbiamo $a = qb + r = (q \pm 1)b + (r' - r)$. Se poniamo $q'' := q \pm 1$ e $r'' := r' - r = r - |b|$, allora abbiamo $a = q''b + r''$, con $q'', r'' \in \mathbb{Z}$ ed, inoltre, $-\frac{1}{2} |b| \leq r'' < 0$. Si vede facilmente che q'' e r'' sono univocamente determinati perché q ed r (da cui sono dedotti) sono univocamente determinati.

Si noti che, utilizzando tale versione dell'algoritmo di divisione, si ottiene una versione modificata dell'algoritmo euclideo delle divisioni successive (Esercizio 2.3; nel caso attuale $-\frac{|r_k|}{2} \leq r_{k+1} < \frac{|r_k|}{2}$) che tende ad arrestarsi più rapidamente del tradizionale algoritmo euclideo, dal momento che i resti si avvicinano più rapidamente allo zero.]

2.7. Siano $a, b \in \mathbb{Z} \setminus \{0, 1, -1\}$ due interi dei quali sia nota la fattorizzazione in numeri primi:

$$a = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \quad \text{e} \quad b = \pm p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$$

con $e_i \geq 0$ e $f_i \geq 0$, per ogni $1 \leq i \leq r$ (ammettendo, come abbiamo fatto ora, che alcuni esponenti possano essere uguali a 0, possiamo assumere che i fattori primi che appaiono nella decomposizione di a e di b siano gli stessi (!), senza per questo perdere di generalità). Mostrare che:

(a) $\text{MCD}(a, b) = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$, dove $u_i := \text{Min}(e_i, f_i)$, per ogni $1 \leq i \leq r$.

(b) $\text{mcm}(a, b) = p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$, dove $v_i := \text{Max}(e_i, f_i)$, per ogni $1 \leq i \leq r$.

[Suggerimento. (a) Se p è un divisore primo di a e di b allora, necessariamente, $p = p_i$, per un qualche i , con $1 \leq i \leq r$. Pertanto un divisore comune t di a e b ha una decomposizione in numeri primi del tipo $t = p_1^{\tau_1} p_2^{\tau_2} \dots p_r^{\tau_r}$, con $\tau_i \leq u_i$, per ogni i . Pertanto il massimo di questi divisori comuni di a e b è dato da $d = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$.

(b) Se m è un multiplo comune di a e b , allora $p_i^{v_i} \mid m$, per ogni i , con $1 \leq i \leq r$. Quindi $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r} \mid m$. Pertanto il minimo tra questi multipli comuni di a e b è proprio $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$.]

2.8. (a) (Euclide, IV–III Sec. A.C.). Mostare che esistono infiniti interi primi.

(b) Dimostrare che, preso comunque un intero $N > 0$ (grande come si vuole), è possibile trovare N interi consecutivi, nessuno dei quali è primo.

(c) Mostrare che, per ogni intero $n > 0$, esiste sempre un primo p in modo tale che $n < p \leq n! + 1$.

[Suggestimento. **(a)** Per assurdo sia $\{p_1, p_2, \dots, p_N\}$ l'insieme (finito) di tutti i numeri primi. L'intero positivo $n := p_1 p_2 \dots p_N + 1$ ($> p_i$, per ogni $1 \leq i \leq N$), come ogni intero non primo, deve possedere un fattore primo. Dunque, deve esistere j , con $1 \leq j \leq N$, in modo tale che $p_j \mid n = p_1 p_2 \dots p_N + 1$. Poiché, ovviamente, $p_j \mid p_1 p_2 \dots p_N$, allora $p_j \mid 1 = n - p_1 p_2 \dots p_N$. Si perviene così ad un assurdo.

(b) Basta considerare i seguenti N interi consecutivi:

$$(N+1)! + 2, (N+1)! + 3, (N+1)! + 4, \dots, (N+1)! + N + 1,$$

e notare che $k \mid (N+1)! + k$, per ogni $2 \leq k \leq N+1$.

(c) Se p è un numero primo e se $p \leq n$ allora ovviamente $p \mid n!$ (dunque, $p \nmid n! + 1$). Pertanto, se q è un fattore primo di $n! + 1$, allora $n < q \leq n! + 1$.]

2.9. Utilizzare le proprietà dei numeri primi ed il Teorema Fondamentale della Aritmetica per dimostrare:

(a) (Pitagora, VI Sec. A.C.) $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. (Con un argomento simile si dimostri che, più generalmente, $\sqrt{p} \in \mathbb{R} \setminus \mathbb{Q}$, per ogni numero primo p .)

(b) Presi $n, r \in \mathbb{N}$, con $\sqrt[n]{n}$ non intero, allora $\sqrt[n]{n} \in \mathbb{R} \setminus \mathbb{Q}$.

(c) $\log_{10}(2) \in \mathbb{R} \setminus \mathbb{Q}$.

[Suggestimento. **(a)** Per assurdo, se $\sqrt{p} \in \mathbb{Q}$, allora $b^2 p = a^2$ per una qualche coppia di interi $a, b \in \mathbb{Z}$, con $b \neq 0$ e $\text{MCD}(a, b) = 1$. Da cui ricaviamo che $p \mid a^2$, dunque $p \mid a$. Pertanto $pk = a$, per un qualche $k \in \mathbb{Z}$. Quindi $b^2 p = a^2 = p^2 k^2$, cioè $b^2 = pk^2$, dunque $p \mid b$. Questo contraddice il fatto che $\text{MCD}(a, b) = 1$.

La dimostrazione di **(b)** è del tutto simile a quella di **(a)**.

(c) Per assurdo, se $\log_{10}(2) \in \mathbb{Q}$, allora $b \log_{10}(2) = a$, per una qualche coppia di interi $a, b \in \mathbb{N}$, con $b \neq 0$ e $\text{MCD}(a, b) = 1$. Dunque, $2^b = 10^a = 2^a 5^a$. Per il Teorema Fondamentale dell'Aritmetica deve essere $b = a$ ed $a = 0$, perveniamo così ad una contraddizione.]