Capitolo 0

Divisibilità negli interi

Indice

1 Principio di Induzione

Per numeri naturali, nel linguaggio comune, si intendono i numeri interi non negativi $0\,,\,1\,,\,2\,,\,3\,,\,\ldots\ldots.$

Da un punto di vista insiemistico–costruttivo, a partire dall'esistenza dell'insieme vuoto $\emptyset$, si possono definire i *numeri naturali* ponendo:

$$0 := \emptyset\,,\ 1 := \{0\}\,,\ 2 := \{0,1\}\,,\ 3 := \{0,1,2\}\,,\ \ldots\ldots$$

Si assume (nella teoria assiomatica degli insiemi) che la *costruzione ricorsiva* sopra descritta (ogni elemento è definito a partire dalla conoscenza di un elemento "che lo precede") dia luogo ad *un insieme* non finito:

$$\mathbb{N} := \{0, 1, 2, 3, \ldots\ldots, n, n+1, \ldots\ldots\}$$

detto *insieme dei numeri naturali* . (Il postulato dell'esistenza di un insieme costituito da una infintà di oggetti individuali, quale è $\mathbb{N}$, viene chiamato *Assioma dell'Infinito*).

Per ogni elemento (*numero naturale*) $x \in \mathbb{N}$, si pone:

$$\mathrm{succ}(x) := x + 1 := \{0, 1, 2, \ldots, x\}\,,$$

un tale elemento di $\mathbb{N}$ viene chiamato *il successivo del numero naturale* x.

Una descrizione assiomatica, puramente formale, dell'insieme dei numeri naturali $\mathbb{N}$ è stata data da G. Peano (1858-1932):

L'insieme $\mathbb{N}$ *è un insieme dotato di "una operazione di passaggio al successivo" (cioè, un'applicazione* $\mathbb{N} \to \mathbb{N}\,,\ x \mapsto \mathrm{succ}(x)$*) che verifica le seguenti proprietà:*

($\mathbb{N}$ 1) *Esiste un elemento* $0 \in \mathbb{N}$*, tale che* $0 \neq \mathrm{succ}(x)$*, per ogni* $x \in \mathbb{N}$*, (tale elemento viene chiamato* zero *o* primo elemento di $\mathbb{N}$*).*

($\mathbb{N}$ 2) *Se* $x, y \in \mathbb{N}$ *e se* $x \neq y$ *, allora* $\mathrm{succ}(x) \neq \mathrm{succ}(y)$.

($\mathbb{N}$ 3) *Se* U *è un sottoinsieme di* $\mathbb{N}$ *tale che*

$$\textbf{(a)}\ \ 0 \in U\,, \qquad \textbf{(b)}\ \ k \in U \quad \Rightarrow \quad \mathrm{succ}(k) \in U\,,$$

allora $U = \mathbb{N}$.

Le precedenti proprietà sono chiamate *Postulati (*od *Assiomi) di Peano.* La proprietà **($\mathbb{N}$ 3)** è chiamata *Principio di Induzione.*

I postulati di Peano *caratterizzano* l'insieme $\mathbb{N}$ dei numeri naturali, nel senso che è possibile dimostrare che *esiste ed è unico* (a meno di corrispondenze biunoviche che conservano il primo elemento e l'operazione di "passaggio al successivo") un insieme che verifica tali proprietà. Per tale ragione, il sistema di assioni di Peano si dice "un sistema monomorfo".

È importante evidenziare che, dagli assiomi di Peano, discendono tutte le ben note proprietà dell'insieme dei numeri naturali. In particolare le operazioni di somma e prodotto e le loro proprietà possono essere dedotte dagli assiomi di Peano. Per *somma di* $n, m \in \mathbb{N}$ si intende il numero naturale:

$$n+m := (\ldots((n+1)+1)+1\ldots) \ \ (m \text{ volte }), \ \ \text{se } m \geqslant 1 ; \quad n+0 := n ,$$

e per *prodotto di* $n, m \in \mathbb{N}$ si intende il numero naturale:

$$nm := n+n+n+\ldots+n \ \ (m \text{ volte }), \ \ \text{se } m \geqslant 1 ; \quad n0 := 0 .$$

La *relazione di ordine in* $\mathbb{N}$ è definita nella maniera seguente:

$$h \leqslant k \ \ :\Leftrightarrow \ \ k = h+n , \ \text{per un qualche } n \in \mathbb{N} .$$

Ovviamente, $h < k \ :\Leftrightarrow \ h \leqslant k$ e $h \neq k$. Dunque, $h < k \ \Rightarrow \ h+1 \leqslant k$.

Per semplicità di notazione, nel seguito, denoteremo con $\mathbb{N}^{+} := \mathbb{N} \setminus \{0\}$ *l'insieme dei numeri naturali positivi.* Porremo, poi, $\mathbb{N}^{-} := \{-n \ : \ n \in \mathbb{N}^{+}\}$ e $\mathbb{Z} := \mathbb{N}^{+} \cup \{0\} \cup \mathbb{N}^{-}$.

L'insieme $\mathbb{Z}$ dei *numeri interi,* o *numeri interi relativi*, viene introdotto in maniera più rigorosa come insieme-quoziente dell'insieme $\mathbb{N} \times \mathbb{N}$ rispetto alla relazione di equivalenza seguente:

$$(n, m) \sim (n', m') \ \ :\Leftrightarrow n+m' = m+n' .$$

Un elemento dell'insieme-quoziente $\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim$, determinato dalla classe di equivalenza di $(n, m) \in \mathbb{N} \times \mathbb{N}$, viene denotato con il simbolo $n-m$, i.e.

$$n-m := [(n, m)]_{\sim} := \{(n', m') \in \mathbb{N} \times \mathbb{N} \ : n+m' = m+n'\} .$$

Per semplicità di notazione, presi comunque $n, m \in \mathbb{N}$, nell'insieme $\mathbb{Z}$ si pone $-m := 0-m$, $n := n-0$ (identificando così $\mathbb{N}$ con la sua immagine canonica in $\mathbb{Z}$, tramite l'applicazione iniettiva $n \mapsto n-0$); dunque, in particolare, $0 = 0-0 = n-n$. In tal modo si definiscono, in modo rigoroso, $\mathbb{N}^{+} := \{n \ : \ n \in \mathbb{N}, \ n \neq 0\}$ e $\mathbb{N}^{-} := \{-m \ : \ m \in \mathbb{N}, \ m \neq 0\}$ come sottoinsiemi di $\mathbb{Z}$.

È subito visto che in $\mathbb{Z}$ possono essere (ben) definite in modo naturale, a partire da quelle di $\mathbb{N}$, le operazioni di somma, prodotto e una relazione di ordine:

$$\begin{aligned} (n-m)+(n'-m') \ &:= \ (n+n')-(m+m') , \\ (n-m)\cdot(n'-m') \ &:= \ (nn'+mm')-(nm'+mn') , \\ (n-m) \leq (n'-m') \ &:\Leftrightarrow \ n+m' \leq n'+m . \end{aligned}$$

In altri termini, l'insieme $\mathbb{Z}$ dei numeri interi (relativi) è "il più piccolo insieme" che contiene $\mathbb{N}$ nel quale è sempre possibile risolvere un'equazione lineare in una indeterminata X a coefficienti in $\mathbb{N}$ del tipo seguente:

$$m+X = n , \quad \text{con } \ n, m \in \mathbb{N} ,$$

la cui unica soluzione (in $\mathbb{Z}$) è data da $n - m$.

Si noti anche che, dalla decomposizione $\mathbb{Z} = \mathbb{N}^+ \cup \{0\} \cup \mathbb{N}^-$, si ricava la cosìdetta *Legge di Tricotomia* in $\mathbb{Z}$, cioè: *presi comunque $x, y \in \mathbb{Z}$ allora può accadere soltanto una delle seguenti eventualità:*

$$x < y \quad \textit{oppure} \quad x = y \quad \textit{oppure} \quad y < x \, .$$

Pertanto, $\mathbb{Z}$ è un *insieme totalmente* o *linearmente ordinato*, ciò significa che, presi comunque due elementi $x, y \in \mathbb{Z}$, allora:

$$x \nleqslant y \;\; \Rightarrow \;\; y < x \, .$$

È opportuno notare che la validità del Principio di Induzione si trasferisce da $\mathbb{N}$ ad appropriati sottoinsiemi di $\mathbb{Z}$, che sono in corrispondenza biunivoca naturale con $\mathbb{N}$. Precisamente, preso comunque un intero $n_0 \in \mathbb{Z}$, poniamo:

$$\mathbb{N}(n_0) := \{x \in \mathbb{Z} \ : \ x \geqslant n_0\} \, ,$$

allora possiamo affermare che in $\mathbb{N}(n_0)$ ($\subset \mathbb{Z}$) vale la seguente formulazione del:

(I) Principio di Induzione. *Sia $U \subseteq \mathbb{Z}$ tale che:*

$$\textbf{(a)} \;\; n_0 \in U \, , \qquad \textbf{(b)} \;\; k \in U \;\; \Rightarrow \;\; k + 1 \in U \, ,$$

allora $U = \mathbb{N}(n_0)$.

Sul Principio di Induzione si basa il cosìdetto Metodo di Prova per Induzione. Supponiamo che, dato un intero n_0, per ogni intero $n \geqslant n_0$, si possa formulare una proposizione $\mathbf{P}(n)$ (ad esempio, sia $n_0 = 1$, e sia $\mathbf{P}(n)$:= "se un insieme finito S ha n elementi, allora il suo insieme delle parti $\mathcal{B}(\mathcal{S})$ ha 2^n elementi"; oppure $\mathbf{P}(n)$:= "vale la seguente identità $1+2+\ldots+(n-1)+n = \frac{n(n+1)}{2}$"). Allora *il Metodo di Prova per Induzione* per la validità della proposizione $\mathbf{P}(n)$ consiste nel mostrare che:

(a) $\mathbf{P}(n_0)$ *è vera* (**Base dell'Induzione**);

(b) *per un qualsiasi intero $k \geqslant n_0$, si ha che:*
$\mathbf{P}(k)$ *è vera* $\Rightarrow$ $\mathbf{P}(k+1)$ *è vera* (**Passo Induttivo**) .

Ciò permette di concludere che la proposizione $\mathbf{P}(n)$ è vera per un qualunque $n \in \mathbb{N}(n_0)$. Infatti, la validità di tale metodo di prova è subito dimostrata, utilizzando il Principio di Induzione **(I)**, prendendo $U := \{k \in \mathbb{N} \ : \ \mathbf{P}(k)$ è vera $\}$.

Teorema 1.1. *I seguenti enunciati sono tra loro equivalenti:*

(I) ***Il Principio di Induzione.***

($\mathbf{I_A}$) ***Il Principio di "Ampia" Induzione*** *(o Formulazione "debole" del Principio di Induzione): Siano $n_0 \in \mathbb{Z}$ e $V \subseteq \mathbb{Z}$ tali che:*

$$\textbf{(a)}\ n_0 \in V\,, \quad \textbf{(b}_\mathbf{A}\textbf{)}\ \{x \in \mathbb{Z}\ :\ n_0 \leqslant x \leqslant k\} \subseteq V \ \Rightarrow\ k+1 \in V\,,$$

allora $V = \mathbb{N}(n_0)$ *.*

(BO) ***Il Principio del Buon Ordinamento*** *(o* ***Principio del Minimo****): Sia $n_0 \in \mathbb{Z}$ allora ogni sottoinsieme non vuoto T di $\mathbb{N}(n_0)$ ha* un primo elemento *o* minimo*, cioè un elemento $t \in T$ tale che $t \leqslant z$, per ogni altro elemento $z \in T$.*

Dimostrazione. È ovvio che **(I)** $\Rightarrow$ **($\mathbf{I_A}$)** , dal momento che l'ipotesi in **($\mathbf{b_A}$)** è (apparentemente) più restrittiva dell'ipotesi in **(b)** e, quindi, la condizione **(b)** è (apparentemente) più forte della condizione **($\mathbf{b_A}$)**.

($\mathbf{I_A}$) $\Rightarrow$ **(BO)**. Supponiamo, per assurdo, che esista un sottoinsieme non vuoto T di $\mathbb{N}(n_0)$ che non possieda un primo elemento (dunque, in particolare, T possiede necessariamente più di un elemento). Sia

$$V := \{x \in \mathbb{N}(n_0)\ :\ x \leqslant t\,, \quad \text{per ogni } t \in T\}.$$

Ovviamente, $n_0 \in V$, dunque $V \neq \emptyset$, ed inoltre $V \neq \mathbb{N}(n_0)$ (perché, se $t_1, t_2 \in T$ e se, ad esempio, $t_1 < t_2$ allora $t_2 \notin V$). Allora, per **($\mathbf{I_A}$)**, deve esistere un elemento k tale che $\{x \in \mathbb{Z}\ :\ n_0 \leqslant x \leqslant k\} \subseteq V$, ma $k+1 \notin V$. Osserviamo che un tale elemento k deve appartenere ad T (altrimenti, se fosse $k \notin T$, poiché $k \in V$, si avrebbe che $k < t$ e, dunque, che $k+1 \leqslant t$, per ogni $t \in T$, cioè si avrebbe che $k+1 \in V$). Dunque tale elemento k, che appartiene tanto a V quanto a T, risulta essere un primo elemento di T e ciò contraddice l'assunto.

(BO) $\Rightarrow$ **(I)**. Supponiamo, per assurdo, che esista un sottoinsieme proprio U di $\mathbb{N}(n_0)$ tale che $n_0 \in U$ ed inoltre soddisfacente alla condizione **(b)**. Sia $T := \mathbb{N}(n_0) \setminus U$. L'insieme T è non vuoto (perché abbiamo supposto che $U \subsetneq \mathbb{N}(n_0)$), allora per **(BO)**, deve esistere un primo elemento t in T. Ovviamente $n_0 < t$, perché $n_0 \in U$. Quindi l'insieme non vuoto degli elementi di $\mathbb{N}(n_0)$ che precedono t, deve essere contenuto in U, in particolare $t-1 \in U$. Quindi, per la proprietà **(b)**, dobbiamo avere che $(t-1)+1 = t \in U$ e ciò contraddice l'assunto. $\square$

1. Esercizi e Complementi

1.1. Mostrare che:

(a) Se $n \in \mathbb{N}$, allora:

$$n < 1 \quad \Leftrightarrow \quad n = 0\,.$$

(b) Se $n, m \in \mathbb{Z}$, allora:

$$n < m \quad \Leftrightarrow \quad n + 1 \leqslant m\,.$$

[Suggerimento. **(a)** Supponiamo, per assurdo, che esista un $x \in \mathbb{N}$, tale che $0 < x < 1$. Allora, moltiplicando per $x\,(> 0)$, abbiamo che $0 < x^2 < x < 1$. Quindi, iterando il procedimento, per ogni $n \geqslant 1$, avremmo:

$$0 < \ldots\ldots < x^n < x^{n-1} < \ldots x^2 < x < 1\,.$$

Dunque, il sottoinsieme $S := \{x^n \ : n \geqslant 1\}\ (\subset \mathbb{N})$ non possiede un primo elemento. Ciò contraddice il Principio del Buon Ordinamento **(BO)**.
(b, $\Rightarrow$) Se $n < m$, allora $m - n > 0$. Se, per assurdo, $n + 1 \not\leqslant m$, allora $m < n + 1$, quindi $0 < m - n < 1$. Ciò contraddice il precedente punto (a).
(b, $\Leftarrow$) è banale.]

1.2. (Proprietà archimedea dell'insieme $\mathbb{Z}$, Archimede (III Sec. A.C.) **)**
Mostrare che: *Presi comunque $a, b \in \mathbb{Z}$, con $b \neq 0$, allora esiste sempre un intero $n \in \mathbb{Z}$ in modo tale che:*

$$a < nb\,.$$

[Suggerimento. Se, per assurdo, per ogni $n \in \mathbb{Z}$, si ha che $a \geqslant nb$, allora il sottoinsieme $S := \{a - nb \ \ : n \in \mathbb{Z}\}$ di $\mathbb{N}$ deve possedere un primo elemento $s_0 := a - n_0 b$ (Principio del Buon Ordinamento **(BO)**). Sia $s := a - (n_0 + 1)b \in S$. Allora, $s = s_0 - b$ (con $b > 0$ per ipotesi), quindi $s < s_0$. Ciò condraddice la proprietà di minimalità di s_0.]

1.3. Metodo di Prova per Induzione (II forma). Mostrare la validità del seguente enunciato:
Supponiamo che, dato un intero $n_0 \in \mathbb{Z}$, per ogni intero $n \geqslant n_0$, si possa formulare una proposizione $\mathbf{P}(n)$. Se:

(a) $\mathbf{P}(n_0)$ *è vera* (**Base dell'Induzione**);

(b) *per un qualsiasi intero h, con $n_0 \leqslant h \leqslant k$, si ha che:*
$\mathbf{P}(h)$ *è vera* $\Rightarrow$ $\mathbf{P}(k+1)$ *è vera* (**Passo Induttivo**);

allora la proposizione $\mathbf{P}(n)$ è vera per un qualunque $n \in \mathbb{Z}$, $n \geqslant n_0$.
[Suggerimento. Basta applicare la formulazione $(\mathbf{I_A})$ del Principio di Induzione all'insieme $V := \{n \in \mathbb{Z} \ : n \geqslant n_0\,,\ \mathbf{P}(n) \text{ è vera }\}$.]

1.4. Utilizzando il Metodo di Prova per Induzione, mostrare che per ogni $n \geqslant 1$ si ha:

(a) $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n\,.$
(b) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n\,.$
(c) $1^3 + 2^3 + 3^3 + \ldots + n^3 = (\frac{n(n+1)}{2})^2 = \frac{1}{4}n^4 + \frac{1}{2}n^3 + \frac{1}{4}n^2\,.$

[Suggerimento. È immediato che le formule precedenti sono verificate per $n = 1$ *(Base dell'Induzione)*. Procediamo, ora, nel dimostrare il *Passo Induttivo*.

(a) Se $1+2+3+\ldots+k = \frac{k(k+1)}{2}$, allora $1+2+3+\ldots+k+k+1 = \frac{k(k+1)}{2}+k+1 = (k+1)(\frac{k}{2}+1) = \frac{(k+1)(k+2)}{2}$.
(b) Se $1^2+2^2+3^2+\ldots+k^2 = \frac{1}{3}k^3+\frac{1}{2}k^2+\frac{1}{6}k$, allora $1^2+2^2+3^2+\ldots+k^2+(k+1)^2 = \frac{1}{3}k^3+\frac{1}{2}k^2+\frac{1}{6}k+(k+1)^2 = \frac{1}{3}k^3+\frac{1}{2}k^2+\frac{1}{6}k+k^2+2k+1 = \frac{1}{3}(k+1)^3+\frac{1}{2}(k+1)^2+\frac{1}{6}(k+1)$.
(c) Se $1^3+2^3+3^3+\ldots+k^3 = (\frac{k(k+1)}{2})^2$, allora $1^3+2^3+3^3+\ldots+k^3+(k+1)^3 = (\frac{k(k+1)}{2})^2+(k+1)^3 = (k+1)^2[(\frac{k}{2})^2+(k+1)] = (\frac{(k+1)(k+2)}{2})^2$.]

1.5. Utilizzando il Metodo di Prova per Induzione, mostrare che per ogni $n \geqslant 1$ si ha:

(a) $2n \geqslant n+1$.
(b) $2^n \geqslant 2n$.

[Suggerimento. È immediato che le disuguaglianze precedenti sono verificate per $n = 1$ *(Base dell'Induzione)*. Procediamo, ora, nel dimostrare il *Passo Induttivo.*
(a) Se $2k \geqslant k+1$, allora $2(k+1) = 2k+2 \geqslant k+1+2 > (k+1)+1$.
(b) Se $2^k \geqslant 2k$, allora $2^{k+1} = 2 \cdot 2^k \geqslant 2 \cdot 2k \geqslant 2(k+1)$.]

1.6. Utilizzando il Metodo di Prova per Induzione, mostrare che per ogni $n \geqslant 0$ e per ogni elemento $x \neq 1$ (ad esempio, $x \in \mathbb{R}$) si ha:

$$(1-x)^{-1} = 1+x+x^2+x^3+\ldots+\frac{x^n}{(1-x)}\,.$$

[Suggerimento. È immediato che la formula precedente è verificata per $n = 0$ *(Base dell'Induzione)* e per $n = 1$:

$$(1-x)^{-1} = 1+\frac{x}{(1-x)}\,.$$

Passo induttivo: Se

$$(1-x)^{-1} = 1+x+x^2+x^3+\ldots+\frac{x^k}{(1-x)}\,,$$

allora:

$$\begin{aligned}(1-x)^{-1} = 1+\tfrac{x}{(1-x)} \quad &= 1+x\cdot(1-x)^{-1} = \\ &= 1+x\cdot[1+x+x^2+x^3+\ldots+\tfrac{x^k}{(1-x)}] = \\ &= 1+x+x^2+x^3+\ldots+\tfrac{x^{k+1}}{(1-x)}\,.\,]\end{aligned}$$

1.7. Utilizzando il Metodo di Prova per Induzione, mostrare che:
(a) Per ogni $n \geqslant 1$ e per ogni x, ad esempio $x \in \mathbb{R}$, si ha:

$$(x^n-1) = (x-1)(x^{n-1}+x^{n-2}+\ldots+x^2+x+1)\,.$$

(b) (Progressione Aritmetica) Per ogni $n \geqslant 0$ e presi comunque x, y, ad esempio $x, y \in \mathbb{R}$, si ha:

$$x+(x+y)+(x+2y)+(x+3y)+\ldots+(x+(n-1)y)+(x+ny) = \frac{(n+1)(2x+ny)}{2}\,.$$

(c) (Progressione Geometrica) Per ogni $n \geqslant 0$ e presi comunque x e $y \neq 1$, ad esempio $x, y \in \mathbb{R}$, con $y \neq 1$, si ha:

$$x+xy+xy^2+xy^3+\ldots+xy^{n-1}+xy^n = \frac{x(y^{n+1}-1)}{(y-1)}\,.$$

(d) Presi comunque due interi $m \geqslant 0$ ed $n \geqslant m$ e presi comunque x e $y \neq 1$, ad esempio $x, y \in \mathbb{R}$, con $y \neq 1$, si ha:

$$xy^m + xy^{m+1} + xy^{m+2} + \ldots + xy^{n-1} + xy^n = \frac{x(y^{n+1} - y^m)}{(y-1)}\,.$$

[Suggerimento. **(a)** Se $n = 1$ l'uguaglianza è banalmente verificata. Per $n \geq 2$, si ha:

$$\begin{aligned}(x^n - 1) &= (x+1)(x^{n-1} - 1) - x(x^{n-2} - 1) = \\ &= (x+1)(x-1)(x^{n-2} + \ldots + x + 1) - x(x-1)(x^{n-3} + \ldots + x + 1) = \\ &= (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1)\,.\end{aligned}$$

(b) Se $n = 0$ l'uguaglianza è banalmente verificata. Per $n \geq 1$, si ha:

$$\begin{aligned}&[x\ +(x+y) + (x+2y) + (x+3y) + \ldots + (x+(n-1)y)] + (x+ny) = \\ &= \tfrac{n(2x+(n-1)y)}{2} + (x+ny) = \tfrac{n(2x+(n-1)y)+(2x+2ny)}{2} \\ &= \tfrac{(n+1)(2x+ny)}{2}\,.\end{aligned}$$

La dimostrazione di **(c)** è analoga a quella di **(b)**.
(d) è conseguenza diretta di **(c)** dal momento che:

$$\begin{aligned}xy^m &+ xy^{m+1} + xy^{m+2} + \ldots + xy^{n-1} + xy^n = \\ &= (x + xy + + \ldots + xy^{n-1} + xy^n) - (x + xy + \ldots + xy^{m-2} + xy^{m-1})\,.\ ]\end{aligned}$$

1.8. (Disuguaglianza di Jakob Bernoulli (1654-1705)**)** Utilizzando il Metodo di Prova per Induzione, mostrare che, per ogni $n \geqslant 0$ e per ogni $x \in \mathbb{R}$, si ha:

$$(1+x)^n \geqslant 1 + nx\,.$$

[Suggerimento. Se $n = 0$ la disuguaglianza è banalmente verificata. Per $n \geq 1$, si ha:

$$\begin{aligned}(1+x)^n = (1+x)^{n-1}(1+x) \quad &\geqslant (1+(n-1)x)(1+x) = 1 + nx + (n-1)x^2 \geqslant \\ &\geqslant 1 + nx\,.\ ]\end{aligned}$$

1.9. (Principio di G.P. Lejeune Dirichlet (1805-1859) detto anche **Principio delle "gabbie dei piccioni"** ovvero **Principio delle "caselle postali")**

Siano $n > m \geqslant 1$. Utilizzando il Metodo di Prova per Induzione, mostrare che: *Se un insieme finito con* n *elementi* [lettere] *deve essere ripartito in* m *: sottoinsieni* [caselle postali], *allora almeno un sottoinsieme* [casella postale] *deve contenere più di un elemento* [lettera].
[Suggerimento. Se $n \geqslant 2$, allora $m = 1$. In tal caso il Principio enunciato è ovvio. Supponiamo $n \geqslant 3$. Sia $A := \{a_1, a_2, \ldots, a_n\}$ e sia $\mathcal{F} := \{A_1, A_2, \ldots, A_m\}$ una famiglia di m sottoinsiemi di A, con $m < n$, $\cup_{1 \leq i \leq m} A_i = A$ e $A_i \cap A_j = \emptyset$, se $1 \leqslant i \neq j \leqslant m$. Supponiamo per semplicità di notazione che $a_1 \in A_1$ (altrimenti, modifichiamo gli indici degli insiemi della famiglia $\mathcal{F}$) e che $A_1 = \{a_1\}$ (altrimenti abbiamo concluso). Poniamo $A' := A \setminus \{a_1\}$ e $\mathcal{F}' := \{A_2, \ldots, A_m\}$. Applicando l'ipotesi induttiva ad A' ed $\mathcal{F}'$ concludiamo facilmente.]

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 del Buon Ordinamento", cfr. Teorema 1.1).

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:*

$$a = bq + r\,, \qquad 0 \leqslant r <\mid b \mid .$$

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

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

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

è non vuoto (ad esempio, se $n' = -\mid a \mid$, allora $a - n'b \in S$). Per il "Principio del Buon Ordinamento" **(BO)** (Teorema 1.1), possiamo trovare un primo elemento nell'insieme S, che denotiamo con $r := a - qb$. Mostriamo che $r < b$. Se, per assurdo, fosse $r \geqslant b$ allora si avrebbe:

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

e, dunque, anche $r - b\,(< r)$ apparterrebbe 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:

$$a = -bq + r = b(-q) + r\,, \qquad 0 \leqslant r < -b =\mid -b \mid=\mid b \mid .$$

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

$$a = bq + r = bq' = r'\,, \qquad 0 \leqslant r, r' <\mid b \mid,$$

allora $(q - q')b = r' - r <\mid b \mid b$, dunque $\mid q - q' \mid\mid b \mid<\mid b \mid$, cioè $\mid q - q' \mid< 1$, 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:

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

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

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

(MCD1) $d \mid a\,,\ \ d \mid b\,;$

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

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 $\mathrm{MCD}(0, 0)$ *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 $\mathrm{MCD}(a, b) = 1$. $\square$

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 $d := \mathrm{MCD}(a, b)$ ha un significato univoco) 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:

$$z = dq + r, \qquad 0 \leqslant r < d,$$

ovvero,

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

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 $d' \mid b$, 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:

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

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:*

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

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

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

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 $c = acx + aky = a(cx + ky)$, 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, $\mathrm{mcm}(a, b)$) un intero $h \in \mathbb{Z}$ tale che:

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

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

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

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 somo multipli sia di a che di b, quindi la scrittura $h := \mathrm{mcm}(a, b)$ ha un significato univoco). Il prossimo risultato mostra l'esistenza del $\mathrm{mcm}(a, b)$, per ogni coppia di elementi $a, b \in \mathbb{Z}$. E' ovvio, da quanto precede, che $\mathrm{mcm}(a, b) = \mathrm{mcm}(|\, a\, |, |\, b\, |)$.

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

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

Dimostrazione. Per le Osservazioni 2.8 e 2.4 non è restrittivo supporre che $a > 0$, $b > 0$. Sia $d := \mathrm{MCD}(a, b)$. 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 $\frac{ab}{d} = m = \mathrm{mcm}(a,b)$ e, quindi, che $ab = \mathrm{MCD}(a,b)\mathrm{mcm}(a,b)$. $\square$

Osservazione 2.10. Nell'anello $\mathbb{Z}$, per ogni $x \in \mathbb{Z}$, debnotiamo con $xZ := \{xk \ : \ k \in \mathbb{Z}\}$ l'ideale generato da x. Allora, si può facilmente verificare che

(a) $a\mathbb{Z} \supseteq b\mathbb{Z} \quad \Leftrightarrow \quad a \mid b$:

(b) $\mathrm{MCD}(a,b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$;

(c) $\mathrm{mcm}(a,b)\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

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

$$q = ab \quad \text{e} \quad q \neq \mid a \mid \quad \Rightarrow \quad q = \pm b\,.$$

Proposizione 2.12. *Per un intero $p \geqslant 2$, 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 $p \neq \mid a \mid$. 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 $1 = kb$, cioè $\mid b \mid = 1$ ovvero $p = \mid a \mid$, 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 $1 = ah$, dunque $\mid a \mid = 1$ 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 $\mathrm{MCD}(p,a) = 1$. 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 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:*

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

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

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

Dimostramo 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 $2 \leqslant b < a$. Se a è un numero primo, non c'è nulla da dimostrare. Se a non è primo, allora $a = xy$, con $2 \leqslant x, y < a$. Per l'ipotesi induttiva (applicata ad x ed y), possiamo scrivere:

$$x = {p'}_1^{f_1} {p'}_2^{f_2} \ldots {p'}_n^{f_n} \quad \text{e} \quad y = {p''}_1^{g_1} {p''}_2^{g_2} \ldots {p''}_m^{g_m}$$

dunque:

$$a = {p'}_1^{f_1} {p'}_2^{f_2} \ldots {p'}_n^{f_n} {p''}_1^{g_1} {p''}_2^{g_2} \ldots {p''}_m^{g_m} .$$

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:

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

Poiché p_1 è un numero primo e $p_1 \mid q_1^{f_1} q_2^{f_2} \ldots q_s^{f_s}$, allora $p_1 \mid q_j$, per un qualche $1 \leqslant j \leqslant s$. 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) 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 $1 \leqslant i \leqslant r$. $\square$

2. Esercizi e Complementi

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

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

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

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

$$S_{a_1, a_2, \ldots, a_n} := \{a_1y_1 + a_2y_2 + \ldots + a_ny_n \ : \quad \begin{array}{l} y_i \in \mathbb{Z}\,,\ 1 \leqslant i \leqslant n\,, \\ a_1y_1 + a_2y_2 + \ldots + a_ny_n > 0\}. \end{array}$$

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

$$\mathrm{MCD}(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n \qquad \text{(Identità di Bézout)}.$$

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

2.2. Siano a, b, c degli interi non nulli di $\mathbb{Z}$. Mostrare che (a meno del segno) valgono le seguenti proprietà:

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

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

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

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

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

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

[Suggerimento. **(a)** Ci limitiamo a dimostrare la prima uguaglianza. Sia $d := \mathrm{MCD}(a, b, c)$ e $\tilde{d} := \mathrm{MCD}(a, \mathrm{MCD}(b, c))$. Poiché $d \mid b$ e $d \mid c$, allora, $d \mid \mathrm{MCD}(b, c)$ e, quindi $d \mid \tilde{d} = \mathrm{MCD}(a, \mathrm{MCD}(b, c))$. Viceversa, poché $\tilde{d}$ divide a, b, c, allora $\tilde{d} \mid d = \mathrm{MCD}(a, b, c)$. Dunque, $d = \pm\tilde{d}$.
(b) Segue dal fatto che $1 \mid a$ e se $x \mid 1$, allora $x = \pm 1$.
(c) Sia $t := \mathrm{MCD}(b, c)$ e $\tilde{t} := \mathrm{MCD}(ab, ac)$. E' ovvio che $at \mid ab$ e $at \mid ac$, quindi $at \mid \mathrm{MCD}(ab, ac) = \tilde{t}$. Poiché $a \mid \mathrm{MCD}(ab, ac) = \tilde{t}$ 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 $x \mid \mathrm{MCD}(b, c) = t$. Pertanto $x = \pm t$, ovvero $\tilde{t} = \pm at$.
(d) Da **(c)** ricaviamo che $d = \mathrm{MCD}(a, b) = \mathrm{MCD}(d\frac{a}{d}, d\frac{b}{d}) = d\mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$, quindi $1 = \mathrm{MCD}(\frac{a}{d}, \frac{b}{d})$.
(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 $1 = \mathrm{MCD}(a, bc)$ (Teorema 2.3).
(f) Poiché $a \mid c$, allora $ab \mid cb$. Analogamente si prova che $ab \mid ac$. Dunque $ab \mid \mathrm{MCD}(cb, ca) = c\mathrm{MCD}(b, a) = c$.]

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 $\mathrm{MCD}(a,b) = \mathrm{MCD}(\mid a \mid, \mid b \mid)$, allora possiamo supporre, senza perdere in generalità che $a \geqslant b > 0$. Applicando ricorsivamente l'Algoritmo di divisione abbiamo:

$$\begin{array}{ll}
a = bq_1 + r_1\,, & 0 < r_1 < b =: r_0 \\
b = r_1 q_2 + r_2\,, & 0 < r_2 < r_1 \\
r_1 = r_2 q_3 + r_3\,, & 0 < r_3 < r_2 \\
\vdots & \vdots \\
r_k = r_{k+1} q_{k+2} + r_{k+2}\,, & 0 < r_{k+2} < r_{k+1} \\
\vdots & \vdots \\
r_{n-2} = r_{n-1} q_n + r_n\,, & 0 < r_n < r_{n-1} \\
r_{n-1} = r_n q_{n+1} + 0\,, & 0 = r_{n+1} < r_n
\end{array}$$

dove $n \geqslant 0$.
Mostrare che:

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

(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:

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

[Suggerimento. **(a)** Osserviamo che se $a = bq + r$, con $0 \leqslant r < b$, allora $\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r)$. 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 propietà alla successione di divisioni euclidee, abbiamo $\mathrm{MCD}(a,b) = \mathrm{MCD}(b,r_1) = \mathrm{MCD}(r_1,r_2) = \ldots = \mathrm{MCD}(r_{n-1},r_n) = r_n$.

(b) Per induzione. Base dell'induzione:

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

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

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

allora l'espessione 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 $\mathbb{Z}$ e sia $d := \mathrm{MCD}(a,b)$.

(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 $x = x_0 + n\frac{\mathrm{mcm}(a,b)}{a}$ e $y = y_0 - n\frac{\mathrm{mcm}(a,b)}{b}$.

[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 $\mathrm{MCD}(a, b) = 1$ (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:

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

2.5. 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:

$$a = bq + r\,, \qquad -\frac{1}{2} \mid b \mid \leqslant r < \frac{1}{2} \mid b \mid .$$

[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 $0 \leqslant r < \mid b \mid$. Se $(0 \leqslant)\ r < \frac{1}{2} \mid b \mid$, allora non c'è null'altro da dimostrare. Supponiamo, dunque, che $\frac{1}{2} \mid b \mid \leqslant r\ (< \mid b \mid)$. In tal caso, $0 < \mid b \mid - r \leqslant \mid b \mid - \frac{1}{2} \mid b \mid = \frac{1}{2} \mid b \mid \leqslant r < \mid b \mid$. Scriviamo $r = (\mid b \mid - r) + r'$, con $r' := 2r - \mid b \mid$. Dunque, per un'opportuna scelta del segno (dipendente dal segno di $\mid b \mid$), abbiamo $a = qb + r = (q \pm 1)b + (r' - r)$. Se poniamo $q'' := q \pm 1$ e $r'' := r' - r = r - \mid b \mid$, allora abbiamo $a = q''b + r''$, con $q'', r'' \in \mathbb{Z}$ ed, inoltre, $-\frac{1}{2} \mid b \mid \leqslant r'' < 0$. 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) che si arresta dopo un numero approssimativamente dimezzato di passi.]

2.6. 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 $e_i \geqslant 0$ e $f_i \geqslant 0$, per ogni $1 \leqslant i \leqslant r$ (ammettendo, come abbiamo fatto ora, che alcuni esponenti possano essere ugali 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) $\mathrm{MCD}(a, b) = p_1^{u_1} p_2^{u_2} \dots p_r^{u_r}$, dove $u_i := \mathrm{Min}(e_i, f_i)$, per ogni $1 \leqslant i \leqslant r$.

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

[Suggerimento. **(a)** Se p è un divisore primo di a e di b allora, necessariamente, $p = p_i$, per un qualche i, con $1 \leqslant i \leqslant r$. 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 $1 \leqslant i \leqslant r$. 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 $p_1^{v_1} p_2^{v_2} \dots p_r^{v_r}$.]

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

(b) Dimostare 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 $n < p \leqslant n! + 1$.

[Suggerimento. **(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 $1 \leqslant i \leqslant N$), come ogni intero non primo, deve possedere un fattore primo. Dunque, deve esistere j, con $1 \leqslant j \leqslant N$, 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:

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

e notare che $k \mid (N+1)! + k$, per ogni $2 \leqslant k \leqslant N + 1$.
(c) Se p è un numero primo e se $p \leqslant n$ allora ovviamente $p \mid n!$ (dunque, $p \nmid n! + 1$). Pertanto, se q è un fattore primo di $n! + 1$, allora $n < q \leqslant n! + 1$.]

2.8. 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 $\sqrt[r]{n}$ non intero, allora $\sqrt[r]{n} \in \mathbb{R} \setminus \mathbb{Q}$.

(c) $\mathrm{Log}_{10}(2) \in \mathbb{R} \setminus \mathbb{Q}$.

[Suggerimento. **(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 $\mathrm{MCD}(a, b) = 1$. 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 $\mathrm{MCD}(a, b) = 1$.
La dimostrazione di **(b)** è del tutto simile a quella di **(a)**.

(c) Per assurdo, se $\mathrm{Log}_{10}(2) \in \mathbb{Q}$, allora $b\mathrm{Log}_{10}(2) = a$, per una qualche coppia di interi $a, b \in \mathbb{N}$, con $b \neq 0$ e $\mathrm{MCD}(a, b) = 1$. 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.]