Capitolo 0

Divisibilità negli interi

Versione Preliminare

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*

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

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:

$$x+1 := \{0,1,2,\ldots,x\}\,,$$

un tale elemento viene chiamato *il successivo del numero naturale* x (e l'operazione $x \mapsto x+1$ è detta *operazione di passaggio al successivo*).

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

L'insieme $\mathbb{N}$ *verifica le seguenti proprietà:*

($\mathbb{N}$ 1) *Esiste un elemento* $0 \in \mathbb{N}$, *tale che* $0 \neq x+1$, *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* $x+1 \neq y+1$.

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

$$\textbf{(a)}\ \ 0 \in U\,, \qquad \textbf{(b)}\ \ k \in U \ \ \Rightarrow \ \ k+1 \in U\,,$$

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 biunivoche 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, si deducono 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, $h < k \ \Rightarrow \ h + 1 \leqslant k$ (e viceversa).

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), 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, $0 = 0 - 0 = n - n$, per ogni $n \in \mathbb{N}$. Quindi, $\mathbb{N}^+ := \{n \in \mathbb{N} \ : \ n \neq 0\}$ e $\mathbb{N}^- := \{-m \ : m \in \mathbb{N}, \ n \neq 0\}$.
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:

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

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, se $x, y \in \mathbb{Z}$, allora:

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

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:

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

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:*

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

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 $n \in \mathbb{N}$. 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:*

$$\textbf{(a)}\ n_0 \in V\,, \quad \textbf{(b_A)}\ \{x \in \mathbb{Z} \mid n_0 \leqslant x \leqslant k\} \subseteq V \ \Rightarrow\ k+1 \in V\,,$$

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

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

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 $\{x \in \mathbb{Z} \mid n_0 \leqslant x \leqslant k\} \subseteq V$, 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 $m < n + 1$ (Legge di Tricotomia), 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 avesse che $a \geqslant nb$, allora il sottoinsieme $S := \{a - nb \ : \ n \in \mathbb{Z}\}$ di $\mathbb{N}$ dovrebbe 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:

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

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, ad esempio $x \in \mathbb{R}$, si ha:

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

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].

2 Algoritmo euclideo di divisione

In questo paragrafo intendiamo mostrare come molte delle proprietà dell'aritmetica elementare di $\mathbb{Z}$ traggano origine dalla validità in $\mathbb{N}$ del "Principio del Buon Ordinamento" (ovvero, equivalentemente, dal "Principio di Induzione", 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)** , 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 $(q - q')b = r' - r <\mid b \mid$, dunque $\mid q - q' \mid \cdot \mid b \mid <\mid b \mid$, 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 "$a \nmid b$".

Siano $a, b, c, x, y, z \in \mathbb{Z}$, notiamo che:

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

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

(b) Se $a, b \in \mathbb{Z}$ e se a e b non sono contemporaneamente nulli, allora si chiama *Massimo Comun Divisore* di a, b (in breve, $\mathrm{MCD}(a, b)$) un intero $d \in \mathbb{Z}$ che verifica le seguenti proprietà:

(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").

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

Teorema 2.3. *Siano $a, b \in \mathbb{Z}$, non entrambi nulli.*

(1) *Se d_1 e d_2 sono due Massimi Comun Divisori di a e b , allora $d_1 = \pm d_2$.*

(2) *Esiste sempre un Massimo Comun Divisore di a e b in $\mathbb{Z}$.*

(3) *Il Massimo Comun Divisore 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 $\mathrm{MCD}(a, b) =: d \in \mathbb{N}$ ha un significato univoco) e coincide con il minimo intero positivo nell'insieme:*

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

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

(5) *Esistono $x, y \in \mathbb{Z}$ in modo tale che:*

$$\mathrm{MCD}(a, b) = ax + by \quad \textbf{\textit{(Identità di Bézout)}}.$$

Dimostrazione. **(1)** è una conseguenza immediata di **(MCD2)**.

(2) discende da **(3)** (e da **(1)**).

(3) 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,

$$ax + by - (ax_0 + by_0)q = r \quad \text{cioè} \quad a(x - x_0 q) + b(y - y_0 q) = r$$

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 $d' \in \mathbb{Z}$ e 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 $\beta := y_0$).

(4) segue immediatamente dalla definizione e da **(3)**; **(5)** discende immediatamente da **(3)**. □

Corollario 2.4. ***(Lemma di Euclide)*** *Siano $a, b, c \in \mathbb{Z}$. Allora:*

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

Dimostrazione. Dal Teorema 2.3 (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 $a \mid c$. □

Definizione 2.5. 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) $h' \in \mathbb{Z}\,, \quad a \mid h' \quad \text{e} \quad b \mid h' \quad \Rightarrow \quad h \mid h'.$

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

Teorema 2.7. *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 la Osservazione 2.6 e per il Teorema 2.3 (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 $m = a\beta = b\alpha$ (dove $\alpha := \frac{a}{d}$ e $\beta := \frac{b}{d}$) e quindi che $a \mid m$ e $b \mid m$ (proprietà **(mcm1)**). Sia ora $h' \in \mathbb{Z}$ 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 $\alpha', \beta' \in \mathbb{Z}$. 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 2.8. Nell'anello $\mathbb{Z}$, per ogni $x \in \mathbb{Z}$, denotiamo con $x\mathbb{Z} := \{xk \ : k \in \mathbb{Z}\}$ l'ideale generato da x in $\mathbb{Z}$. 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 2.9. 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 2.10. . *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 2.4). $\square$

Teorema 2.11. ***(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 b, con $2 \leqslant b < a$. 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:

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

dunque:

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

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:

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

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 j $(1 \leqslant j \leqslant s)$. Essendo anche q_j un numero primo (ovvero irriducibile, Proposizione 2.10), 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 $r = s$ e –a meno di un cambiamento dell'ordine dei fattori– che $p_i = q_i$ e $e_i = f_i$, per ogni i $(1 \leqslant i \leqslant r)$. $\square$

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:

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

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:

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

2.2. Siano a, b, c degli interi non nulli di $\mathbb{Z}$. Mostrare che (in $\mathbb{N}$) 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 $\mathrm{MCD}(a, b) = 1 \quad\Rightarrow\quad ab \mid c$.

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:

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

dove $n \geqslant 0$.
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:

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

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 Bezout, 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, $(x,y) \neq (x',y')$, 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 $y = y_0 - n\frac{\mathrm{mcm}(a,b)}{b}$.

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:

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

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

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

con $e_i \geqslant 0$ e $f_i \geqslant 0$, per ogni i $(1 \leqslant i \leqslant r)$. (Ammettendo, come abbiamo fatto ora, che alcuni esponenti possano essere ugali a 0, possiamo assumere che i fattori primi $\{p_1, p_2, \ldots, p_r\}$ che appaiono nella decomposizione di a e di b siano gli stessi (!), senza per questo perdere di generalità.)
Mostrare che:

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

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

2.7. **(a) (Euclide, IV 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 $\{p_1, p_2, \ldots, p_N\}$ l'insieme (finito) di tutti i numeri primi. L'intero positivo $n := p_1 p_2 \ldots p_N + 1$, come ogni intero non primo deve possedere un fattore primo (si osservi che $n > p_i$, per ogni $1 \leqslant i \leqslant N$). Dunque, deve esistere j, con $1 \leqslant j \leqslant N$, in modo tale che $p_j \mid n = p_1 p_2 \cdot \ldots \cdot p_N + 1$. Poiché, ovviamente, $p_j \mid p_1 p_2 \cdot \ldots \cdot p_N$, allora $p_j \mid 1 = n - p_1 p_2 \cdot \ldots \cdot p_N$. Si perviene così ad un assurdo.
(b) Basta considerare i seguenti N interi consecutivi:

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

e notare che $k \mid (N+1)! + k$, per ogni k $(2 \leqslant k \leqslant N+1)$.
(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 necessariamente $n < q \leqslant n! + 1$.]

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 $a = 0$, pervenendo così ad una contraddizione.]