Didattica Matematica

Aritmetica 2011-12

Prof. S. Mantovani

1 Insiemi e terminologia

Assumeremo come intuitiva la nozione di insieme e ne utilizzeremo il linguaggio come strumento per studiare collezioni di oggetti.

Gli "Insiemi" sono generalmente indicati con le lettere latine maiuscole $A, B, X, Y \ldots$, e gli elementi di un insieme con lettere latine minuscole $a, b, x, y, ...$

Per indicare che un elemento x **appartiene** all'insieme X, si usa il simbolo $\in$ e si scrive: $x \in X$, mentre per indicare che y **non appartiene** all'insieme Y si scrive $y \notin Y$.

Si considera anche l'insieme privo di oggetti o **insieme vuoto**, che si indica con il simbolo $\emptyset$.

Ci sono diversi modi per descrivere un insieme: uno di questi consiste nell'elencare, se possibile, tutti i suoi elementi.

Esempio 1 *L'insieme X delle lettere dell'alfabeto che compongono la parola ITALIA è:*

$$X = \{I, T, L, A\}$$

Osservazione 2 *In genere gli elementi elencati sono intesi **distinti** e non ha importanza l'**ordine** in cui essi compaiono, cioè*

$$X = \{A, L, T, I\} = \{T, A, L, I\} = \{L, A, T, I\}....$$

Osservazione 3 *Si considerano anche gli insiemi "**singoletti**" formati da un unico elemento $\{a\}$.*

Esempio 4 *L'insieme W dei capoluoghi di provincia della regione Lombardia è:*

$$W = \{Milano, Varese, Sondrio, Lecco, Como, Cremona, Pavia, Bergamo, Brescia$$

Un altro modo per rappresentare un insieme X è quello di specificare X mediante una **condizione definitrice**, cioè una legge che permetta di stabilire se un oggetto appartiene oppure no all'insieme X.

Esempio 5 *L'insieme dei numeri naturali strettamente minori di 100, può essere indicato con la scrittura*

$$X = \{0, 1, 2, ..., 99\}$$

oppure

$$X = \{x \in \mathbb{N} \mid 0 \leq x \leq 99\}$$

Gli insiemi possono anche essere rappresentati graficamente utilizzando i **diagrammi di Venn**.

Definizione 6 *Un insieme Y si dice* ***sottoinsieme*** *di un insieme X e si scrive $Y \subseteq X$ se ogni elemento di Y è anche elemento di X, cioè se $\forall\, y \in Y$ si ha che $y \in X$, ove il simbolo $\forall$ si legge "****per ogni****".*

Esempio 7 *Detto $\mathbb{N}$ l'insieme dei numeri naturali, $\mathbb{Z}$ l'insieme dei numeri interi e $\mathbb{Q}$ l'insieme dei numeri razionali, si ha $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.*

Esempio 8 *Ogni insieme X è sottoinsieme di se stesso, cioè $X \subseteq X$. Inoltre $\emptyset \subseteq X, \forall X$.*

Definizione 9 *Se A e B sono due insiemi, scriveremo $A = B$ per indicare che $A \subseteq B$ e $B \subseteq A$.*

Notazione 10 *Con la scrittura $A \subset B$ (A sottoinsieme proprio di B) si vuole indicare che $A \subseteq B$ ma non è $A = B$; cioè $\forall\, a \in A \Rightarrow a \in B$ ma $\exists\, b \in B$ tale che $b \notin A$.*

Notazione 11 *Attenzione a non confondere i simboli, in particolare $\in$ e $\subseteq$. $\{a\} \subseteq A$, mentre $a \in A$.*

1.1 Operazioni sugli insiemi

Due insiemi possono essere combinati in modi diversi per ottenere nuovi insiemi.
Sia assegnato un universo U e siano $A, B \subseteq U$.

Definizione 12 *Si definisce* ***intersezione*** *di A e B, l'insieme degli elementi comuni ad A ed a B e la si indica con il simbolo $A \cap B$, cioè*
$A \cap B = \{x \in U \mid x \in A, x \in B\} = \{x \in U \mid x \in A \wedge x \in B\}$.

Osservazione 13 *L'intersezione $A \cap B$ è un sottoinsieme sia di A che di B, cioè $A \cap B \subseteq A, A \cap B \subseteq B$.*

Definizione 14 *Due insiemi A e B si dicono* ***disgiunti*** *se $A \cap B = \emptyset$.*

Proprietà dell'intersezione insiemistica:

1) $A \cap (B \cap C) = (A \cap B) \cap C$ (proprietà associativa)

2) $A \cap B = B \cap A$ (proprietà commutativa)

3) $A \cap A = A$ (proprietà di idempotenza)

4) $A \cap \emptyset = \emptyset$.

Definizione 15 *Si definisce* ***unione*** *di A e B l'insieme degli elementi che appartengono ad A o a B (o ad entrambi) e la si indica con il simbolo $A \cup B$, cioè*
$A \cup B = \{x \in U \mid x \in A \text{ o } x \in B\} = \{x \in U \mid x \in A \vee x \in B\}$.

Osservazione 16 *A e B sono sottoinsiemi di $A \cup B$, cioè $A \subseteq A \cup B$ e $B \subseteq A \cup B$.*

Proprietà dell'unione insiemistica:

1) $A \cup (B \cup C) = (A \cup B) \cup C$ (proprietà associativa)

2) $A \cup B = B \cup A$. (proprietà commutativa)

3) $A \cup A = A$ (proprietà di idempotenza)

4) $A \cup \emptyset = A$.

Esercizio 17 *Dimostrare che per ogni terna di sottoinsiemi $A, B, C \subseteq U$ valgono le seguenti proprietà:*

1) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (proprietà distributiva)

2) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (proprietà distributiva)

3) $A \subseteq B \Leftrightarrow A \cup B = B$

4) $A \cap B = A \Leftrightarrow A \subseteq B$

5) $A \cap (A \cup B) = A \cup (A \cap B) = A$ (proprietà di assorbimento)

Definizione 18 *Per ogni $A \subseteq U$ si dice* ***complemento*** *di A in U l'insieme*

$$A' = \{x \in U \mid x \notin A\}.$$

Valgono le seguenti proprietà:

1) $U' = \emptyset,\ \emptyset' = U$

2) $A \cup A' = U,\ A \cap A' = \emptyset$

3) $(A')' = A$

Verifichiamo per esercizio che valgono le uguaglianze seguenti (Leggi di De Morgan):

1) $(A \cap B)' = A' \cup B' \quad (\forall A, B \in U)$

2) $(A \cup B)' = A' \cap B' \quad (\forall A, B \in U)$.

Dimostrazione. Per dimostrare la 1) occorre provare la seguente doppia inclusione:

$(A \cap B)' \subseteq A' \cup B'$ e $A' \cup B' \subseteq (A \cap B)'$.

Sia $x \in (A \cap B)'$; allora $x \in U$, ma $x \notin A \cap B$ per cui x non appartiene ad almeno uno dei due insiemi A oppure B. Ne segue che x appartiene ad almeno uno degli insiemi A' o B' e quindi anche ad $A' \cup B'$.

Viceversa se $y \in A' \cup B'$ si ha che y appartiene ad almeno uno dei due insiemi A' o B'. Pertanto $y \in U$ ma non appartiene ad almeno uno degli insiemi A o B per cui $y \in (A \cap B)' \square$.

Per dimostrare la 2) occorre provare la seguente doppia inclusione:

$(A \cup B)' \subseteq A' \cap B'$ e $A' \cap B' \subseteq (A \cup B)'$.

Sia $x \in (A \cup B)'$: allora x non appartiene nè ad A nè a B e quindi x appartiene sia ad A' che a B', quindi $x \in A' \cap B'$.

Sia $y \in A' \cap B'$: allora y non sta in A e non sta in B. Si può concludere che y sta in $(A \cup B)'$. ■

Definizione 19 *Siano $A, B \subseteq U$; si dice **differenza** fra A e B l'insieme*

$$A \setminus B = \{x \in U \mid x \in A, x \notin B\}.$$

Osservazione 20 *Per ogni sottoinsieme $A \subseteq U \Rightarrow A' = U \setminus A$.*

Osservazione 21 *Per la differenza di insiemi non vale la proprietà commutativa.*

Infatti, siano a, b, c tre elementi distinti di un insieme U , si ponga $A = \{a, b\}$, $B = \{a, c\}$.

Si ha che $A \setminus B = \{b\} \neq B \setminus A = \{c\}$.

Osservazione 22 *Si possono utilizzare i diagrammi di Venn per visualizzare e risolvere con facilità problemi altrimenti piuttosto complicati.*

Un esempio è il cosiddetto "Problema del trifoglio"

Sia da risolvere il seguente problema: Una scuola serale propone l'insegnamento di tre lingue: Inglese, Francese e Tedesco. Al corso di Inglese sono iscritti 24 studenti, al corso di Francese 23 e al corso di Tedesco 18. Poichè 3 studenti frequentano sia il corso di Inglese sia quello di Francese, 10 frequentano sia Inglese che Tedesco, 9 sia Francese che Tedesco e 1 studente è iscritto a tutti e tre si domanda: "quanti sono gli iscritti alla scuola di lingue"?

La risposta è $12 + 7 + 5 + 9 + 8 + 2 + 1 = 44$.

1.2 Insieme delle parti

Definizione 23 *Fissato un insieme U, l'insieme i cui elementi sono tutti e soli i sottoinsiemi di U è detto **Insieme delle parti** di U, e lo si indica con il simbolo $\mathcal{P}(U)$. In simboli*

$$\mathcal{P}(U) = \{X \mid X \subseteq U\}$$

Esempio 24 *Se $U = \{1, 2, 3\}$ allora*

$$\mathcal{P}(U) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

1.3 Prodotto cartesiano di due insiemi

Definizione 25 *Dati due insiemi* A, B, *si dice* ***prodotto cartesiano*** *di* A *e* B *l'insieme:*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

costituito dalle coppie ***ordinate*** *degli elementi di* A *e di* B.

Osservazione 26 *Se* $A \neq B$ *si ha che* $A \times B \neq B \times A$.

Osservazione 27 *Se* $A = B$ *si usa anche scrivere* $A \times A = A^2$, *in particolare* $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

2 Relazioni binarie

Definizione 28 *Una* ***relazione binaria*** *fra due insiemi* X *e* Y *(non vuoti) è un sottoinsieme* $\mathcal{R}$ *del prodotto cartesiano* $X \times Y$, *cioè un insieme* $\mathcal{R}$ *di* ***coppie ordinate*** (x, y), $x \in X, y \in Y$.

1. Se $X = Y$ la relazione binaria si dice relazione su X.
2. Se $\mathcal{R}$ è una relazione fra X e Y e la coppia $(x, y) \in \mathcal{R}$ si scrive anche $x\mathcal{R}\, y$ e si dice che x è associato a y nella relazione $\mathcal{R}$.
3. Ogni sottoinsieme $\mathcal{R}$ di $X \times Y$ è una relazione fra X e Y; in particolare:
   - 3.1 $\mathcal{R} = \emptyset$ è la relazione **vuota** (nessun elemento di X è in relazione con elementi di Y).
   - 3.2 $\mathcal{R} = X \times Y$ è la relazione **totale** (ogni elemento di X è in relazione con ogni elemento di Y). Se $X = Y$, X^2 è la relazione universale (totale) su X.
4. Se $X = Y$, la diagonale di X^2 cioè $I_X = \{(x, x) |\ x \in X\}$, è la relazione **identica** su X.

Definizione 29 *Data una relazione* $\mathcal{R}$ *fra* X *e* Y *si dice* ***relazione trasposta*** *di* $\mathcal{R}$ *la relazione* $\mathcal{R}^T$ *così definita* $\mathcal{R}^T = \{(y, x) |\ (x, y) \in \mathcal{R}\ \}$.

Esempio 30 *Sia* $X = \{a, b.c\}$
$\mathcal{R} = \{(a, a), (b, b), (a, b), (a, c), (b, c)\}$
$\mathcal{R}^T = \{(a, a), (b, b), (b, a), (c, a), (c, b)\}$.

Osservazione 31 $(\mathcal{R}^T)^T = \mathcal{R}$.

Sia ora R una relazione definita su un insieme X.

Definizione 32 $\mathcal{R}$ *è* ***riflessiva*** *se* $I_X \subseteq \mathcal{R}$, *cioè se per ogni* $x \in X$ *si ha che* $(x, x) \in \mathcal{R}$, *ovvero* $x\mathcal{R}x, \forall x \in X$.

Definizione 33 $\mathcal{R}$ *è* ***simmetrica*** *se* $\mathcal{R}^T = \mathcal{R}$, *cioè se* $(x,y) \in \mathcal{R} \Rightarrow (y,x) \in \mathcal{R}$, *ovvero* $x\mathcal{R}y \Rightarrow y\mathcal{R}x$.

Definizione 34 $\mathcal{R}$ *è* ***antisimmetrica*** *se* $\mathcal{R} \cap \mathcal{R}^T \subseteq I_X$, *cioè se* $(x,y) \in \mathcal{R}$ *e* $(y,x) \in \mathcal{R} \Rightarrow x = y$, *(*$x\mathcal{R}y \ \wedge \ y\mathcal{R}x \Rightarrow x = y$*).*

Definizione 35 $\mathcal{R}$ *è* ***transitiva*** *se* $(x,y) \in \mathcal{R}$ *e* $(y,z) \in \mathcal{R} \Rightarrow (x,z) \in \mathcal{R}$ *(*$x\mathcal{R}\ y \wedge y\mathcal{R}\ z \Rightarrow x\mathcal{R}\ z$*).*

Esempio 36 *Sia* $X = \{a,b,c\}$ *e* $\mathcal{R}_1 = \{(a,a),(a,c),(b,b),(b,c),(c,b)\}$

1. *la relazione non è riflessiva perchè la coppia* $(c,c) \notin \mathcal{R}_1$;
2. *la relazione non è simmetrica perchè* $(a,c) \in \mathcal{R}_1$ *ma* $(c,a) \notin \mathcal{R}_1$
3. *la relazione non è transitiva perchè* $(a,c) \in \mathcal{R}_1$, $(c,b) \in \mathcal{R}_1$ *ma* $(a,b) \notin \mathcal{R}_1$.
4. *la relazione non è antisimmetrica perchè* (b,c), $(c,b) \in \mathcal{R}_1$ *con* $b \neq c$.

Esempio 37 $\mathcal{R}_2 = \{(a,a),(b,b),(c,c),(a,b),(a,c),(b,c),(c,a),(c,b)\}$

1. *la relazione è riflessiva*
2. *la relazione non è simmetrica:* $(a,b) \in \mathcal{R}_2$ *ma* $(b,a) \notin \mathcal{R}_2$;
3. *la relazione non è transitiva, infatti* $(b,c),(c,a) \in \mathcal{R}_2$ *ma* $(b,a) \notin \mathcal{R}_2$*;*
4. *la relazione non è antisimmetrica:* (b,c) *e* $(c,b) \in \mathcal{R}_2$.

Esempio 38 $\mathcal{R}_3 = \{(b,b),(c,c)\}$

1. *la relazione* $\mathcal{R}_3$ *non è riflessiva perchè* (a,a) *non appartiene ad* $\mathcal{R}_3$.
2. *la relazione* $\mathcal{R}_3$ *è simmetrica, antisimmetrica e transitiva.*

Definizione 39 *Una relazione che sia riflessiva, simmetrica e transitiva si dice* ***relazione di equivalenza****.*

Definizione 40 *Una relazione che sia riflessiva, antisimmetrica e transitiva si dice* ***relazione d'ordine****.*

2.1 Matrici di incidenza

Sia $X = \{x_1, x_2, \cdots, x_n\}$. Una relazione $\mathcal{R}$ su X si può rappresentare mediante una tabella a doppia entrata (matrice) $M_{\mathcal{R}}$ con n righe ed n colonne e così definita:

$$M_{\mathcal{R}} = (r_{ij}) = \begin{cases} r_{ij} = 1, \text{ se } (x_i, x_j) \in \mathcal{R} \\ r_{ij} = 0, \text{ se } (x_i, x_j) \notin \mathcal{R} \end{cases}$$

$M_{\mathcal{R}}$ è detta **matrice di incidenza** della relazione $\mathcal{R}$ (su X).

Esempio 41 *La matrice di incidenza della relazione* $\mathcal{R}_1$ *è* : $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

La matrice di incidenza della relazione $\mathcal{R}_2$ *è* : $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

Viceversa una matrice $M{=}(a_{ij})$ (a n righe ed n colonne), con $a_{ij} \in \{0,1\}$ può essere vista come la matrice di incidenza di una relazione su un insieme di ordine n.

Esempio 42

La matrice $M = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ *può essere vista come la matrice di incidenza di una relazione* $\mathcal{R}$ *su un insieme* X*, formato da quatto elementi. Se scegliamo* $X = \{a, b, c, d\}$ *avremo*

$$\mathcal{R} = \{(a,a),(a,b),(a,c),(b,b),(c,a),(c,b),(c,c),(c,d),(d,d)\}.$$

Osservazione 43 *Le proprietà di una relazione si possono dedurre molto agevolmente osservando la matrice di incidenza:*

a.1 $\mathcal{R} = \emptyset$ *(relazione vuota) se* $r_{ij} = 0 \quad \forall\, i, j = 1, 2, \cdots, n.$

a.2 $\mathcal{R} = X^2$ *(relazione totale) se* $r_{ij} = 1 \quad \forall\, i, j = 1, 2, \cdots, n.$

a.3 $\mathcal{R} = I_X$ *(relazione identica) se* $r_{ii} = 1\ \forall\ i \quad e \quad r_{ij} = 0\ \ \forall\ i \neq j.$

b.1 $\mathcal{R}$ *è riflessiva se* $r_{ii} = 1\ \ \forall\ i = 1, 2, \cdots, n.$

b.2 $\mathcal{R}$ *è simmetrica se* $r_{ij} = r_{ji}.$

b.3 $\mathcal{R}$ *è antisimmetrica se* $r_{ij} \cdot r_{ji} = 0,\ i \neq j.$

b.4 $\mathcal{R}$ *è transitiva se* $r_{ik} \cdot r_{kj} \leq r_{ij}\ \ \forall\ i, j, k = 1, 2, \cdots, n.$

Esempio 44 *La matrice* $M_{\mathcal{R}} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ *può essere la matrice di incidenza di una relazione sull'insieme* $X = \{a, b\}$*; tale relazione è riflessiva poichè è verificata la* $(b.1)$*, antisimmetrica per* $(b.3)$ *ma* <u>non</u> *simmetrica perchè non è verificata la* $(b.2)$ *ed è transitiva perchè è verificata la* $(b.4)$.

Esempio 45 *La relazione* $\mathcal{R}_1$ *non è transitiva perchè* $r_{13} \cdot r_{32} = 1 \not\leq r_{12} = 0.$

Osservazione 46 *Questa condizione per testare la transitività è equivalente alla condizione presentata a lezione, che fa uso del prodotto "booleano" tra due matrici di incidenza.*

$\mathcal{R}_1 \circ\mathcal{R}_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & \boxed{1} & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ e la relazione non è transitiva.

$\mathcal{R}_2 \circ\mathcal{R}_2 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ \boxed{1} & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ e la relazione non è transitiva.

Invece $\mathcal{R}_3 \circ\mathcal{R}_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ e la relazione è transitiva.

2.2 Relazioni di equivalenza

Definizione 47 *Ricordiamo che una relazione $\mathcal{R}$ su un insieme X si dice* ***relazione di equivalenza*** *se*

i) $a\ \mathcal{R}\ a \quad \forall a \in X$ *(proprietà riflessiva)*

ii) $a\ \mathcal{R}\ b \Rightarrow\ b\mathcal{R}\ a$ *(proprietà simmetrica)*

iii) $a\ \mathcal{R}\ b,\ b\mathcal{R}c \Rightarrow\ a\mathcal{R}\ c$ *(proprietà transitiva)*

Definizione 48 *Diremo* ***classe di equivalenza*** *individuata dall'elemento $a \in X$ l'insieme degli elementi di X che sono equivalenti ad a nella $\mathcal{R}$; in simboli*

$$[a]_{\mathcal{R}} = \{x \in X \mid x\ \mathcal{R}a\}.$$

Teorema 49 *Siano $a, b \in X$ e sia $\mathcal{R}$ una relazione di equivalenza su X. Allora si ha:*

1. $a \in [a]_{\mathcal{R}}$
2. $b\mathcal{R}\ a \Rightarrow [b]_{\mathcal{R}} = [a]_{\mathcal{R}}$ *(quindi* ***una classe di equivalenza è individuata da uno qualsiasi dei suoi elementi)***
3. $b \notin [\ a]_{\mathcal{R}} \Rightarrow [b]_{\mathcal{R}} \cap [a]_{\mathcal{R}} = \emptyset$ *(cioè* ***due classi di equivalenza distinte non hanno elementi in comune,*** *ovvero sono disgiunte****).***

Dimostrazione.

1. Immediato poichè $a\mathcal{R}a$ per la proprietà riflessiva.

2. Sia $x \in [b]_{\mathcal{R}}$ e quindi $x\mathcal{R}\ b$; poichè per ipotesi $b\mathcal{R}a$, per la transitività di $\mathcal{R}$ segue $x\mathcal{R}\ a$ cioè $x \in [a]_{\mathcal{R}}$. Quindi
$$[b]_{\mathcal{R}} \subseteq [a]_{\mathcal{R}}$$
Viceversa, sia $y \in [a]_{\mathcal{R}}$, allora $y\ \mathcal{R}\ a$ e, per la simmetria di $\mathcal{R}$, $a\mathcal{R}y$. Da $b\mathcal{R}\ a$ e $a\mathcal{R}\ y$ segue $b\ \mathcal{R}\ y$ cioè $y \in [b]_{\mathcal{R}}$ e quindi anche $[a]_{\mathcal{R}} \subseteq [b]_{\mathcal{R}}$, da cui segue l'uguaglianza delle classi.

3. Per assurdo sia $x \in [b]_{\mathcal{R}} \cap [a]_{\mathcal{R}}$ allora $x \mathcal{R} b$ e $x \mathcal{R} a$ e, per la simmetria di $\mathcal{R}$,

$b\mathcal{R} x$ e $x\mathcal{R}$a e quindi $b \mathcal{R} a$, contro l'ipotesi.

■

Definizione 50 *Si dice* ***partizione*** *di un insieme $X \neq \emptyset$ ogni collezione $\{A_i | \ i \in I\}$ di sottoinsiemi non vuoti A_i di X tali che:*

1) $A_i \cap A_j = \emptyset$ *per* $i \neq j$;

2) $\bigcup_{i \in I} A_i = X$;

In altre parole, ogni elemento di X appartiene ad uno ed un solo sottoinsieme A_i della partizione.

Teorema 51 *Ogni relazione di equivalenza $\mathcal{R}$ su un insieme X determina una partizione di X i cui elementi sono le classi di equivalenza (rispetto ad $\mathcal{R}$).*

Viceversa ogni partizione di X determina una relazione di equivalenza (su X) le cui classi di equivalenza sono gli elementi della partizione considerata.

Dimostrazione. 1. Mostriamo che le classi di equivalenza rispetto ad $\mathcal{R}$ sono gli elementi di una partizione di X.

Infatti ogni $a \in X$ sta in una classe poichè $a \in [a]_{\mathcal{R}}$. Inoltre appartiene ad una sola classe; infatti se $a \in [c]_{\mathcal{R}}$, $c \in X$, si avrebbe $a\mathcal{R}\ c$ e quindi $[a]_{\mathcal{R}} = [c]_{\mathcal{R}}$.

2. Viceversa, sia $\{A_i | \ i \in I\}$ una partizione di X e si consideri la relazione $\overline{\mathcal{R}}$ così definita:

per $x, y \in X$ poniamo $x\overline{\mathcal{R}}\ y \Leftrightarrow x, y \in A_i$ (con lo stesso i). Si verifica in modo immediato che $\overline{\mathcal{R}}$ è una relazione di equivalenza e quindi segue la tesi.

■

Definizione 52 *Data una relazione di equivalenza $\mathcal{R}$ su un insieme X, l'insieme delle classi di equivalenza prende il nome di* ***insieme quoziente*** di X *rispetto ad $\mathcal{R}$ e lo si indica con $X/_{\mathcal{R}}$.*

Esempio 53 *Sia $\mathcal{T}$ l'insieme dei triangoli del piano euclideo. Le note relazioni di* ***congruenza*** *e di* ***similitudine*** *sono relazioni di equivalenza.*

Esempio 54 *Sia $X = \{1, 2, 3, 4, 5, 6\}$ e sia $\mathrm{Y} = \{\{1, 3\}, \{2\}, \{4\}, \{5, 6\}\}$. Osserviamo che Y è una partizione dell'insieme X e individua, pertanto, la relazione di equivalenza ρ su X così definita:*

$\rho = \{(1, 3), (3, 1), (5, 6), (6, 5)\} \cup I_X$.

0.1 Applicazioni

Siano A e B due insiemi non vuoti e sia φ una relazione binaria tra A e B.

Definizione 1 *Diciamo che φ è un'**applicazione** (o **funzione** o mappa) tra A e B se per ogni $a \in A$ esiste uno ed un solo $b \in B$ tale che $(a, b) \in \varphi$.*

Di solito per indicare che φ è un'applicazione tra A e B si scrive

$$\varphi : A \longrightarrow B$$

e, invece di $(a, b) \in \varphi$, si pone $\varphi(a) = b$.

A è detto dominio e B codominio.

Definizione 2 *Date due applicazioni φ e ψ esse **coincidono** se e solo se hanno lo stesso dominio A, lo stesso codominio B e se $\varphi(a) = \psi(a)$ $\forall a \in A$.*

Esempio 3 1. $\varphi_1 : \mathbb{Z} \longrightarrow \mathbb{Z}$ *ove* $\varphi_1 = \{(x, x^2) | x \in \mathbb{Z}\}$. *In questo caso è* $\varphi_1(x) = x^2$.

2. $\varphi_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ *ove* $\varphi_2 = \{(x, 3x + 5) | x \in \mathbb{Z}\}$. *In questo caso* $\varphi_2(x) = 3x + 5$.

Notazioni
Se $\varphi : A \longrightarrow B$ è un'applicazione e a è un elemento del dominio A, l'elemento $\varphi(a)$ è detto **immagine** di a attraverso φ.
Se $A' \subseteq A$, l'insieme $\varphi(A') = \{\varphi(a) |\ a \in A'\}$, è detta **immagine** di A' mediante (o per) φ.
Nel caso in cui $A' = A$, $\varphi(A) = \{\varphi(a) |\ a \in A\}$ è detta **immagine dell'applicazione** φ.
Se, invece, $b \in B$, con la scrittura $\varphi^{-1}(b)$ si indica l'insieme degli elementi $a \in A$ tali che $\varphi(a) = b$, ovvero l'insieme delle **preimmagini** (o **controimmagini**) di b.
Ad esempio nel caso della φ_1 si ha $\varphi_1(2) = 4$, in altri termini l'immagine di 2 attraverso φ_1 è 4, mentre $\varphi_2^{-1}(5) = 0$, cioè 0 è una preimmagine di 5 attraverso φ_2.
Osserviamo invece che $\varphi_2^{-1}(7) \notin \mathbb{Z}$, quindi non tutti gli interi relativi hanno preimmagine per la φ_2.

Definizione 4 *Sia $\varphi : A \longrightarrow B$ un'applicazione. Diremo che*

i) φ è **iniettiva** se $\varphi(a_1) = \varphi(a_2)$ implica che $a_1 = a_2$, ovvero se ogni elemento di B ammette al più una preimmagine.

ii) φ è **suriettiva** se $\varphi(A) = B$, cioè se $\forall b \in B$ esiste almeno un $a \in A$ tale che $\varphi(a) = b$, cioè se ogni elemento di B ammette almeno una preimmagine.

iii) φ è **bijettiva** (o **biunivoca**) se è iniettiva ed anche suriettiva.

Consideriamo l'applicazione $\varphi_3 : \mathbb{Z} \longrightarrow \mathbb{Z}$ $(\varphi_3(x) = x^3 \ \ \forall x \in \mathbb{Z})$.
Essa **è iniettiva**, infatti, se $\varphi_3(x_1) = x_1^3 = x_2^3 = \varphi_3(x_2)$ si ha $x_1^3 - x_2^3 = 0$
cioè $(x_1 - x_2)(x_1^2 + x_1x_2 + x_2^2) = 0$ da cui si deduce $x_1 = x_2$.
Ma φ_3 **non è suriettiva**: infatti non tutti gli elementi di $\mathbb{Z}$ hanno controimmagine.
Basta considerare $5 \in \mathbb{Z}$: non esiste alcuno $z \in \mathbb{Z}$ tale che $\varphi_3(z) = 5$ (l'elemento $\sqrt[3]{5} \notin \mathbb{Z}$).

Osserviamo che, se per dominio e codominio per φ_3 assumessimo $\mathbb{R}$, allora φ_3 sarebbe biunivoca, quindi la suriettività (e l'iniettività) di una funzione dipendono dal dominio e dal codominio.

L'applicazione $\varphi_2 : \mathbb{Z} \longrightarrow \mathbb{Z}$ definita precedentemente ponendo $\varphi_2(x) = 3x + 5$ è ancora iniettiva ma non suriettiva.

Sia ora $\varphi_4 : \mathbb{Q} \longrightarrow \mathbb{Q}$ l'applicazione definita ponendo $\varphi_4(x) = \dfrac{x}{3}$. Essa è iniettiva ed anche suriettiva:

φ_4 è iniettiva: infatti se $\varphi_4(a) = \dfrac{a}{3} = \varphi_4(b) = \dfrac{b}{3}$, allora segue $a = b$;
φ_4 è suriettiva: infatti $\forall y \in \mathbb{Q}$ esiste $x \in \mathbb{Q}$ tale che $\varphi_4(x) = \dfrac{x}{3} = y$. Basta prendere $x = 3y$.

0.2 Insiemi finiti e infiniti

Definizione 5 *Dato un insieme X, si dice che è* ***finito*** *se esiste una applicazione biunivoca fra X e l'insieme $\{1, 2, \cdots, n\} \subseteq \mathbb{N}$. Il numero n si dice* ***ordine*** *o* ***cardinalità*** *di X e si scrive $|X| = n$.*

Definizione 6 *Un insieme X si dirà* ***infinito*** *se non è finito.*

Proprietà 7 *Un insieme X è infinito se e solo se esiste una applicazione biunivoca di X in un suo* ***sottoinsieme proprio*** *Y.*

Esempio 8 *Sia $X = \mathbb{N}$ (insieme dei numeri Naturali) e sia $\mathbb{P}$ il suo sottoinsieme proprio costituito dai numeri pari. Consideriamo l'applicazione $f : \mathbb{N} \to \mathbb{P}$ tale che $f(n) = 2n$, per ogni $n \in \mathbb{N}$.*

Questa applicazione è ben definita (ad ogni numero naturale associa il suo doppio).
Tale applicazione è iniettiva: infatti, se $f(n) = f(m)$ si ha che $2n = 2m \Rightarrow n = m$.
Inoltre è suriettiva perchè ogni numero pari ha controimmagine: $\forall 2t \in \mathbb{P}$, la controimmagine è t.

Definizione 9 *Un insieme X si dice* ***numerabile*** *se esiste un'applicazione biunivoca da $\mathbb{N}$ ad X.*

Quindi $\mathbb{N}$ è in particolare un insieme numerabile.

In generale, se un insieme X è numerabile, anche $X \times X$ è numerabile.

Esempio 10 *$\mathbb{Z}$ è numerabile. Infatti possiamo costruire la seguente applicazione biunivoca f (non è l' unica possibile) da $\mathbb{Z}$ ad $\mathbb{N}$ nel modo seguente:*

$$f(a) = \begin{cases} 2a - 1 & \text{se } a > 0 \\ -2a & \text{se } a \leq 0. \end{cases}$$

f è ben definita poichè ogni numero intero ha una ed una sola immagine in $\mathbb{N}$.
f è iniettiva: infatti se $a, b \in Z$ sono tali che $f(a) = f(b)$ si possono avere due casi:

1. *$f(a) = f(b)$ è un numero pari e quindi si ha $f(a) = f(b) = -2a = -2b \Rightarrow a = b$*
2. *$f(a) = f(b)$ è un numero dispari e quindi si ha $f(a) = f(b) = 2a - 1 = 2b - 1 \Rightarrow a = b$.*

f è suriettiva: infatti ogni elemento di $\mathbb{N}$ ha controimmagine in $\mathbb{Z}$, cioè $\forall n \in \mathbb{N}\ \exists\ x \in \mathbb{Z}$ tale che $f(x) = n$. Anche qui si hanno due casi:

1. *se n è pari consideriamo $x = -\dfrac{n}{2} \in \mathbb{Z}$ (negativo) ed è $f(x) = n$.*
2. *se n è dispari consideriamo $x = \dfrac{n+1}{2} \in \mathbb{Z}$ (positivo) ed è $f(x) = f\left(\dfrac{n+1}{2}\right) = 2\dfrac{n+1}{2} - 1 = n$.*

Si può mostrare che l'insieme dei numeri Razionali $\mathbb{Q}$ è numerabile, mentre l'insieme $\mathbb{R}$ dei numeri reali non lo è.

0.3 Alcune tecniche di enumerazione

Siano A e B due insiemi finiti: $A = \{a_1, a_2, \cdots, a_n\}$ e $B = \{b_1, b_2, \cdots, b_k\}$, cioè $| A |= n, | B |= k$.
Proposizione $| A \times B |= n \cdot k$.
Ci proponiamo di contare quante sono le applicazioni tra A e B, quante sono le applicazioni iniettive e quante le applicazioni biunivoche.

a) Contiamo le applicazioni. Sia f una applicazione da A a B. Allora l'immagine di a_1, cioè $f(a_1)$ può essere scelta in k modi diversi (perchè può essere un qualsiasi elemento di B). Analogamente $f(a_2)$ può essere scelta in k modi e così pure l'immagine di ogni altro elemento di A. Quindi per ogni scelta di $f(a_1), f(a_2), \cdots, f(a_n)$ si ha un'applicazione diversa e si può concludere che le applicazioni tra A e B sono

$$\underbrace{k \cdot k \cdot \cdots \cdot k}_{n \text{ volte}} = k^n$$

Esempio 11 *Siano* $A = \{a, b, c\}$ *e* $B = \{0, 1\}$. *Allora l'insieme delle applicazioni tra* A *e* B, *spesso denotato con il simbolo* B^A, *ha* 8 *elementi, precisamente:*

$$f_1 = \begin{cases} a \longrightarrow 0 \\ b \longrightarrow 0 \\ c \longrightarrow 0 \end{cases} \quad f_2 = \begin{cases} a \longrightarrow 0 \\ b \longrightarrow 0 \\ c \longrightarrow 1 \end{cases} \quad f_3 = \begin{cases} a \longrightarrow 0 \\ b \longrightarrow 1 \\ c \longrightarrow 0 \end{cases} \quad f_4 = \begin{cases} a \longrightarrow 1 \\ b \longrightarrow 0 \\ c \longrightarrow 0 \end{cases}$$

$$f_5 = \begin{cases} a \longrightarrow 1 \\ b \longrightarrow 1 \\ c \longrightarrow 1 \end{cases} \quad f_6 = \begin{cases} a \longrightarrow 1 \\ b \longrightarrow 1 \\ c \longrightarrow 0 \end{cases} \quad f_7 = \begin{cases} a \longrightarrow 1 \\ b \longrightarrow 0 \\ c \longrightarrow 1 \end{cases} \quad f_8 = \begin{cases} a \longrightarrow 0 \\ b \longrightarrow 1 \\ c \longrightarrow 1 \end{cases}$$

Si osserva che, delle 8 applicazioni sopra riportate, nessuna è iniettiva, mentre la f_1 e la f_5 non sono neppure suriettive.

Osservazione 12 *Si può stabilire una corrispondenza biunivoca tra le applicazioni sopra descritte e i sottoinsiemi del dominio* A, *associando ad ogni applicazione* f_i *il sottoinsieme di* A *costituito dall'insieme delle controimmagini dell'elemento* $1 \in B$. *(Il risultato si ottiene anche considerando le controimmagini dell'elemento* $0 \in B$*).*
Otteniamo che $f_1 \leftrightarrow \varnothing$, $f_2 \leftrightarrow \{c\}$, $f_3 \leftrightarrow \{b\}$, $f_4 \leftrightarrow \{a\}$, $f_5 \leftrightarrow A$, $f_6 \leftrightarrow \{a, b\}$, $f_7 \leftrightarrow \{a, c\}$, $f_8 \leftrightarrow \{b, c\}$.

Il procedimento può essere generalizzato:

Proposizione 13 *Dato un insieme* X *finito con* $|X| = n$, *i sottoinsiemi di* X *sono in corrispondenza biunivoca con le applicazioni di* X *nell'insieme* $Y = \{0, 1\}$ *e quindi sono* 2^n.

Vedremo che questo risultato si può ottenere anche usando la dimostrazione per induzione.

Osservazione 14 *Per il conteggio delle* ***applicazioni suriettive*** *tra due insiemi finiti* X *e* Y , *il risultato è molto più complicato da ottenere e ne omettiamo la dimostrazione. Si deve supporre che l'insieme dominio* X *abbia cardinalità minore della cardinalità dell'insieme immagine* Y.
Se $|X| = m$, *e* $|Y| = n$, *il numero delle applicazioni suriettive da* X *a* Y, *con* $m \leq n$, *è dato dalla formula*

$$n! S(m, n)$$

(ove $S(m, n)$ *sono i numeri di Stirling della seconda forma, definiti per ricorrenza nelle pagine seguenti).*

Proposizione 15 *Siano* A *e* B *due insiemi finiti con lo stesso numero* n *di elementi e sia* $f : A \longrightarrow B$ *un'applicazione. Allora* f *è iniettiva se e solo se* f *è suriettiva.*

Dimostrazione. Sia f iniettiva. Allora $|f(A)| = |A|$ ma $|A| = |B|$ quindi $|f(A)| = |B|$. Poichè $f(A) \subseteq B$ segue che $f(A) = B$, cioè la f è suriettiva.
Sia f suriettiva. Allora $f(A) = B$ da cui segue che $|f(A)| = |B|$. Poichè per ipotesi $|B| = |A|$ segue anche $|f(A)| = |A|$, cioè elementi distinti di A hanno immagini distinte e quindi f è iniettiva. ■

b) Supponendo che $k \geq n$, **contiamo** il numero di **applicazioni iniettive** tra l'insieme $A = \{a_1, a_2, \cdots, a_n\}$ e l'insieme $B = \{b_1, b_2, \cdots, b_k\}$,

Il discorso è analogo a quello fatto per contare le applicazioni tra A e B : si deve solo tener conto del fatto che elementi distinti debbono avere immagini distinte, quindi $f(a_1)$ può essere ancora scelto in k modi diversi, ma $f(a_2)$ dovrà essere diverso da $f(a_1)$ e quindi potrà essere scelto solo in $k - 1$ modi distinti, $f(a_3)$ potrà essere scelto solo in $k - 2$ modi e così via. Si ottiene:

$$|B^A| = k(k-1)(k-2)\cdots(k-n+1) = D_{k,n} \quad \text{(disposizioni di } k \text{ oggetti di classe } n\text{)}.$$

c) Nel caso in cui $|A| = |B| = n$, allora le applicazioni iniettive tra A e B sono anche suriettive e quindi bijettive ed è

$$|B^A| = n(n-1)(n-2)\cdots 2 \cdot 1 = n!$$

Queste applicazioni si dicono anche permutazioni.

Esempio 16 *Sia* $A = \{a_1, a_2, a_3\}, B = \{b_1, b_2, b_3\}$; *le* 6 *applicazioni bijettive tra* A *e* B *sono:*

$$f_1 = \begin{cases} a_1 \longrightarrow b_1 \\ a_2 \longrightarrow b_2 \\ a_3 \longrightarrow b_3 \end{cases} \qquad f_2 = \begin{cases} a_1 \longrightarrow b_1 \\ a_2 \longrightarrow b_3 \\ a_3 \longrightarrow b_2 \end{cases} \qquad f_3 = \begin{cases} a_1 \longrightarrow b_2 \\ a_2 \longrightarrow b_1 \\ a_3 \longrightarrow b_3 \end{cases}$$

$$f_4 = \begin{cases} a_1 \longrightarrow b_2 \\ a_2 \longrightarrow b_3 \\ a_3 \longrightarrow b_1 \end{cases} \qquad f_5 = \begin{cases} a_1 \longrightarrow b_3 \\ a_2 \longrightarrow b_2 \\ a_3 \longrightarrow b_1 \end{cases} \qquad f_6 = \begin{cases} a_1 \longrightarrow b_3 \\ a_2 \longrightarrow b_1 \\ a_3 \longrightarrow b_2. \end{cases}$$

Osservazione 17 *Nel caso in cui A coincide con B si parla di applicazioni sull'insieme A e tra queste c'è sempre l'applicazione* ***identica*** *(o* ***identità)*** *$I_A : A \longrightarrow A$ definita ponendo $I_A(a) = a, \forall\ a \in A$.*

0.4 Prodotto di applicazioni

Definizione 18 *Siano $f : A \longrightarrow B$ e $g : B \longrightarrow C$ due applicazioni. Si definisce* ***prodotto*** *delle due applicazioni l'applicazione $g \circ f : A \longrightarrow C$ così definita:*

$$g \circ f(a) = g\left[f(a)\right] \ , \forall a \in A$$

Si verifica che il prodotto di applicazioni è associativo, cioè per ogni terna di applicazioni f, g, h

$$f : A \longrightarrow B, \quad g : B \longrightarrow C, \quad h : C \longrightarrow D$$

è

$$(h \circ g) \circ f = h \circ (g \circ f)$$

Per ogni applicazione $f : A \longrightarrow B$ si ha che $I_B \circ f = f \circ I_A = f$, mentre in generale il prodotto non è commutativo, come si può vedere considerando il seguente

Esempio 19 *Siano $f : \mathbb{R} \longrightarrow \mathbb{R}$ e $g : \mathbb{R} \longrightarrow \mathbb{R}$ così definite:*

$$f(x) = 2x \qquad g(x) = (2x + 1)$$

si ha che
$(g \circ f)(x) = g\left[f(x)\right] = g(2x) = 2(2x) + 1 = 4x + 1$
$(f \circ g)(x) = f\left[g(x)\right] = f(2x + 1) = 2(2x + 1) = 4x + 2;$
e chiaramente sono applicazioni diverse perchè, per esempio, $(g \circ f)(0) = 1 \neq (f \circ g)(0) = 2$ e quindi **non vale la proprietà commutativa.**

Corollario 20 *Sia X un insieme. Il prodotto di applicazioni biunivoche su X è ancora una applicazione biunivoca su X.*

Esempio 21 *Sia $X = \{1, 2, 3\}$ e siano*
$\sigma = \begin{cases} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{cases} \qquad \tau = \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases}$ *due permutazioni.*

Il prodotto $\sigma \circ \tau = \begin{cases} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{cases}$; *infatti* $\begin{cases} (\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(2) = 3 \\ (\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(1) = 1 \\ (\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(3) = 2 \end{cases}$

invece $\tau \circ \sigma = \begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases}$; *infatti* $\begin{cases} (\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(1) = 2 \\ (\tau \circ \sigma)(2) = \tau(\sigma(2)) = \tau(3) = 3 \\ (\tau \circ \sigma)(3) = \tau(\sigma(3)) = \tau(2) = 1 \end{cases}$

Osserviamo quindi che, anche questa volta, $(\sigma \circ \tau)$ e $(\tau \circ \sigma)$ sono applicazioni diverse.

Esempio 22 *Consideriamo ora $\tau \circ \tau = \tau^2$. Abbiamo un caso particolare:*
$(\tau \circ \tau)(1) = 1, \qquad (\tau \circ \tau)(2) = 2 \qquad (\tau \circ \tau)(3) = 3$, *cioè $\tau^2 = i$ (applicazione identica).*

0.5 Principio di Induzione

Il "**Principio o postulato di induzione"** è un'importante tecnica dimostrativa, quando si tratti di dimostrare proposizioni in cui intervengano numeri interi.
Principio di induzione (**I forma**): Sia n_0 un intero e sia $P(n)$ un enunciato che ha senso per ogni $n \geq n_0$. Se:
i) $P(n_0)$ è vero
ii) per ogni $k > n_0$, $P(k-1)$ vero implica $P(k)$ vero,

allora $P(n)$ è vero per tutti gli $n \geq n_0$.

Diamo, ora, alcuni esempi di dimostrazioni che fanno uso del principio di induzione.

Esempio 23 *Dimostrare che la somma dei primi n numeri interi naturali è* $\frac{n(n+1)}{2}$, *cioè mostrare che è:*

$$1 + 2 + ... + (n-1) + n = \frac{n(n+1)}{2}$$

.

In questo caso $P(n)$ è $1 + 2 + ... + (n-1) + n = \frac{n(n+1)}{2}$.
i) $P(1)$ è vera; infatti il primo membro vale 1 e il secondo membro $\frac{1(1+1)}{2} = 1$
ii) Supposto vero $P(k-1)$ dimostriamo $P(k)$.
$P(k-1)$ è:

$$1 + 2 + ... + (k-1) = \frac{(k-1)k}{2}$$

quindi, poichè $1 + 2 + ... + (k-1) + k = [1 + 2 + ... + (k-1)] + k$,
sostituendo l'espressione tra parentesi quadra, che, per ipotesi induttiva, è $\frac{(k-1)k}{2}$, si ottiene che

$$1 + 2 + \ldots + (k-1) + k = [1 + 2 + ... + (k-1)] + k = \\ = \frac{(k-1)k}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k(k+1)}{2}.$$

Pertanto la proprietà è vera per tutti gli $n \geq 1$.

Esempio 24 *Dimostrare che la somma dei primi n numeri naturali pari (non nulli) è* $n(n+1)$, *cioè*

$$2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + \cdots 2 \cdot n = n(n+1).$$

i) $P(1)$ è vero: infatti il primo membro è $2 \cdot 1 = 2$, mentre il secondo membro è $1(1+1) = 2$.
ii) Supposto $P(k-1)$ vero, cioè supposto che valga l'uguaglianza

$$2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + \cdots 2 \cdot (k-1) = (k-1)k$$

proviamo $P(k)$.
$[2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + \cdots 2 \cdot (k-1)] + 2 \cdot k = [(k-1)k] + 2 \cdot k = k^2 - k + 2k = k^2 + k = k(k+1)$. □

Esempio 25 *Ricordando che si indica con* $|X|$ *il numero degli elementi di un insieme X, si può dimostrare, usando il principio di induzione, che, dato un insieme X con n oggetti, l'insieme delle parti di X possiede* 2^n *elementi, cioè il numero di sottoinsiemi di X è* 2^n.

In questo caso $P(n)$ può essere così riscritto :

$$|\mathcal{P}(X)| = 2^n.$$

i) $P(0)$ è vero: infatti in questo caso $X = \emptyset$ e qundi $\mathcal{P}(X)$ ha $\emptyset$ come unico sottoinsieme,
e quindi $|\mathcal{P}(X)| = 1 = 2^0$.

ii) Supposto l'asserto vero per $k-1$ dimostriamolo per k;
supponiamo cioè che un insieme dotato di $k-1$ oggetti possieda 2^{k-1}sottoinsiemi.

Consideriamo, ora, l'insieme X con k oggetti $X = \{a_1, a_2, a_3.....a_k\}$.
X può essere visto come unione di un insieme $Y = \{a_1, a_2, a_3.....a_{k-1}\}$ e del singoletto $\{a_k\}$:

$$X = Y \cup \{a_k\} = \{a_1, a_2, a_3.....a_{k-1}\} \cup \{a_k\}.$$

Per contare i sottoinsiemi di X dobbiamo tener conto dei sottoinsiemi di Y che per ipotesi induttiva sono in numero di 2^{k-1} e di quelli che si ottengono unendo a questi il singoletto $\{a_k\}$ e che, naturalmente, sono ancora in numero di 2^{k-1}.
(Osserviamo che tutti e soli i sottoinsiemi di X che non contengono a_k sono i sottoinsiemi di Y, mentre tutti e soli i sottoinsiemi di X che contengono a_k sono i sottoinsiemi ottenuti aggiungendo a_k ad un sottoinsieme di Y).
In totale si hanno: $2^{k-1} + \ 2^{k-1} = 2 \cdot 2^{k-1} = 2^k$.
Pertanto $|\mathcal{P}(X)| = 2^n$ per tutti gli $n \geq 0$.

Questo risultato è già stato dimostrato per altra via nel paragrafo sulle tecniche di enumerazione.

0.6 Dimostrare (per induzione) le seguenti relazioni

Se non è altrimenti specificato gli elementi in gioco sono numeri Naturali.

1. $\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + ... + (n-1)^2 + n^2 = \frac{n(n+1)(2n+1)}{6}$
2. $\sum_{1}^{n} i^3 = 1^3 + 2^3 + ... + (n-1)^3 + n^3 = \frac{n^2(n+1)^2}{4} = \left(\frac{n(n+1)}{2}\right)^2$
3. $\sum_{1}^{n} i^4 = 1^4 + 2^4 + ... + (n-1)^4 + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$
4. $\sum_{0}^{n-1} 2j + 1 = n^2$ (la somma dei primi n numeri positivi dispari)
5. $\sum_{0}^{n-1} (2j+1)^2 = \frac{n(2n-1)(2n+1)}{3}$
6. $(1+a)^n > na + 1$ per ogni $n \geq 2, a > -1$ (Disuguaglianza di Bernulli)
7. $1 + 2 + 2^2 + \cdots 2^{n-1} = 2^n - 1$.
8. $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) \cdots (1 - \frac{1}{n^2}) = \frac{n+1}{2n}$
9. $\frac{1^2}{2 \cdot 3} \cdot \frac{2^2}{3 \cdot 4} \cdot \frac{3^2}{4 \cdot 5} \cdots \frac{n^2}{(n+1) \cdot (n+2)} = \frac{2}{(n+1)^2(n+2)}$
10. $x + (x+y) + (x+2y) + \cdots (x+ny) = \frac{(n+1)(2x+ny)}{2}$ per ogni $x, y \in R$.
11. $\frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} = 2 - \frac{1}{2^n}$
12. $4^3 + 8^3 + 12^3 + \cdots + (4n)^3 = 16n^2(n+1)^2$
13. $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$ (Formula riportata in Talckys di Ibn Albanna nel 13^o secolo)
14. Verificare che $\forall n \in \mathbb{N} \setminus \{0\}$ si ha che $n^2 + n$ è un numero pari.
15. Verificare che $\forall n \in \mathbb{N} \setminus \{0\}$ si ha che $4^{n+1} + 5^{2n-1}$ è divisibile per 21.

Principio di induzione (II forma):
Sia n_0 un intero e sia $P(n)$ un enunciato che ha senso per ogni $n \geq n_0$. Se:
i) $P(n_0)$ è vero;
ii) per ogni $n > n_0$, $P(k)$ vero per ogni $n_0 \leq k < n$ implica $P(n)$ vero;
allora $P(n)$ è vero per tutti gli $n \geq n_0$.

Useremo nel seguito questa forma del principio di induzione per dimostrare vari teoremi sugli Interi.

0.7 Definizione di successioni per ricorrenza

Un problema frequente in matematica è quello di trovare il termine generico di una successione, cioè, dato $n \in \mathbb{N}$, si chiede di calcolare il numero f_n originato da qualche problema concreto.

0.7.1 I numeri di Fibonacci.

A Leonardo Fibonacci, mercante e matematico italiano vissuto tra il 1170 e il 1250, fu posto il seguente quesito relativo all'allevamento di conigli: data una coppia di conigli tale che:

a) generi una nuova coppia (maschio e femmina) ogni mese;

b) ogni coppia diventi fertile dopo un mese di vita.

Se nel periodo di tempo considerato non muore nessun coniglio, quante coppie sono presenti dopo n mesi?

La funzione è definita nel modo seguente: $f_n = \begin{cases} f_0 = 1,\ f_1 = 1 \\ f_n = f_{n-1} + f_{n-2} \end{cases}$

(Il problema fu risolto, nella forma che conosciamo, da De Moivre nel 1718.)[1]
Con f_n è indicato il numero di coppie di conigli dopo n mesi , mentre f_0 è la coppia iniziale (al tempo zero) ed f_1 è la stessa coppia (diventata fertile) dopo un mese.
I primi numeri di Fibonacci sono:

$$\begin{array}{ccccccccccc} 1 & = & 1 & & & & & & & & \\ 1 & + & 1 & = & 2 & & & & & & \\ & & 1 & + & 2 & = & 3 & & & & \\ & & & & 2 & + & 3 & = & 5 & & \\ & & & & & & 3 & + & 5 & = & 8 \\ & & & & & & & & 5 & + & 8 \\ & & & & & & & & . & . & . \end{array} \quad \begin{array}{c} \\ \\ \\ \\ \\ = \\ . \end{array} \quad \begin{array}{c} \\ \\ \\ \\ \\ 13 \\ . \end{array}$$

e così via.

0.7.2 I numeri di Stirling del secondo tipo[2].

Questi numeri contano il numero di partizioni di un insieme di n elementi in k classi: per esempio il numero di modi di formare k classi in una scuola con n studenti.

I numeri di Stirling (di II tipo), indicati con l'espressione $S(m+1, n)$ sono così definiti:
(i) $S(m, m) = 1, \forall m \geq 0$
(ii) $S(m, 0) = 0$, per $m > 0$
(iii) $S(m, n) = 0$, per $m < n$
(iv) $S(m+1, n) = S(m, n-1) + nS(m, n)$.
Esempio:
$S(2, 1) = S(1, 0) + 1S(1, 1) = 0 + 1 = 1$
$S(3, 2) = S(2, 1) + 2S(2, 2) = 1 + 2 \cdot 1 = 3.$
$S(4, 3) = S(3, 2) + 3S(3, 3) = 3 + 3 \cdot 1 = 6$

Valgono anche le proprietà seguenti:
$S(n, 2) = 2^{n-1} - 1$
$S(n, n-1) = \frac{(n^2-n)}{2}$

Osservazione 26 *I numeri di Stirling (di II tipo) si possono utilizzare per calcolare quante sono le* ***applicazioni suriettive*** *da un insieme X di ordine m ad un insieme Y di ordine n.*
Precisamente il numero di tali applicazioni suriettive è dato dal numero

$$n!S(m, n).$$

Ad esempio le applicazioni suriettive da X a Y, nel caso in cui $m = 3$ ed $n = 2$ sono $2!S(3, 2) = 2 \cdot 3 = 6$, mentre nel caso in cui $m = 4$ ed $n = 3$ sono $3!S(4, 3) = 3 \cdot 2 \cdot 6 = 36$ (in questo ultimo caso tutte le applicazioni sono 3^4)

[1] Se si cerca nel sito www.google.it "Fibonacci numbers" si trova moltissimo materiale
[2] Si può cercare "Stirling numbers"

0.7.3 I numeri di Bell

I numeri di Bell B_n rappresentano il numero di partizioni di un insieme di n elementi e quindi il numero di relazioni di equivalenza distinte che si possono introdurre in un insieme di cardinalità n.
Sono definiti nel seguente modo:

$$\begin{cases} B_0 = 1 \\ B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k. \end{cases}$$

I primi numeri di Bell sono:
$B_1 = \binom{0}{0} B_0 = 1 \cdot 1 = 1.$
$B_2 = \binom{1}{0} B_0 + \binom{1}{1} B_1 = 1 + 1 = 2.$
$B_3 = \binom{2}{0} B_0 + \binom{2}{1} B_1 + \binom{2}{2} B_2 = 1 + 2 + 2 = 5.$
$B_4 = \binom{3}{0} B_0 + \binom{3}{1} B_1 + \binom{3}{2} B_2 + \binom{3}{3} B_3 = 1 + 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 5 = 1 + 3 + 6 + 5 = 15.$

Osservazione 27 *Utilizzando i precedenti numeri di Bell, vediamo che le relazioni di equivalenza che si possono definire in un insieme di* 3 *elementi sono* 5*, mentre sono* 15 *le relazioni di equivalenza che si possono introdurre in un insieme di* 4 *elementi.*

0.1 Anello degli Interi

Introduciamo l'**insieme degli Interi**, come **ampliamento** dell'insieme dei Naturali.
Consideriamo l'insieme $\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$ e introduciamo la relazione seguente:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c.$$

La relazione introdotta è una relazione di equivalenza.
Infatti valgono le proprietà:
i) riflessiva: $\forall (a, b)$ si ha che $(a, b) \sim (a, b)$: infatti $a + b = b + a$ (Proprietà commutativa della somma di numeri naturali)
ii) simmetrica: se $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$; infatti per ipotesi

$$a + d = b + c \Rightarrow b + c = a + d \Rightarrow c + b = d + a \Rightarrow (c, d) \sim (a, b).$$

iii) transitiva se $(a, b) \sim (c, d)$ e se $(c, d) \sim (e, f) \Rightarrow (a, b) \sim (e, f)$.
Infatti per ipotesi valgono le uguaglianze:

$$\begin{cases} a + d = b + c \\ c + f = d + e \end{cases}$$

e da esse segue che

$$(a + d) + (c + f) = (b + c) + (d + e) \Rightarrow a + f = b + e \Rightarrow (a, b) \sim (e, f).$$

Poichè la relazione introdotta in $\mathbb{N} \times \mathbb{N}$ è di equivalenza, l'insieme $\mathbb{N} \times \mathbb{N}$ è suddiviso in classi di equivalenza (che rappresentano una partizione di $\mathbb{N} \times \mathbb{N}$: indichiamo con la scrittura $[(a, b)]_\sim$ la classe di equivalenza cui appartiene la coppia (a, b), cioè

$$[(a, b)]_\sim = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid (x, y) \sim (a, b)\} = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x + b = y + a\}$$

Scegliamo in ogni classe i rappresentanti "**canonici**".
Si possono presentare tre casi:
1) $a = b : [(a, b)]_\sim = \{(x, x) \mid x \in \mathbb{N}\} = [(0, 0)]_\sim$
2) $a > b : [(a, b)]_\sim = [(a - b, 0)]_\sim$
3) $b > a : [(a, b)]_\sim = [(0, b - a)]_\sim$

Consideriamo ora l'insieme delle classi di equivalenza $\mathbb{Z} = \mathbb{N} \times \mathbb{N}_{/\sim}$.

Osserviamo che in $\mathbb{Z}$ possiamo considerare il sottoinsieme $\bar{\mathbb{N}} = \{[(h, 0)]_{/\sim} \mid h \in \mathbb{N}\}$, che, in modo naturale, è in corrispondenza biunivoca con lo stesso $\mathbb{N}$.

Infatti se consideriamo l'applicazione $f : \mathbb{N} \to \bar{\mathbb{N}}$ tale che $f(a) = [(a, 0)]_{/\sim}$, si verifica immediatamente che f è ben definita e biunivoca.

Quindi possiamo porre $[(a, b)]_\sim = \begin{cases} 0 & \text{(ed è l'elemento neutro) se } a = b \\ +(a - b) & \text{se } a > b \text{ (e sono i numeri positivi)} \\ -(b - a) & \text{se } a < b \text{ (e sono i numeri negativi)} \end{cases}$

Operazioni in $\mathbb{Z} = \mathbb{N} \times \mathbb{N}_{/\sim}$.
Somma:
Definiamo la seguente operazione di **somma tra classi di equivalenza**:
$\forall [(a, b)]_\sim, [(c, d)]_\sim \in \mathbb{Z} = \mathbb{N} \times \mathbb{N}_{/\sim}$

$$[(a, b)]_\sim + [(c, d)]_\sim \quad = \quad [(a + c, b + d)]_\sim$$

Verifichiamo che questa somma è *ben definita*, cioè non dipende dai rappresentanti delle classi.
Mostriamo che, anche considerando altri rappresentanti delle stesse classi, cioè

$$(\bar{a}, \bar{b}) \in [(a, b)]_\sim e\ (\bar{c}, \bar{d}) \in [(c, d)]_\sim$$

otterremo, come risultato della somma, ancora la stessa classe.

Consideriamo

$$[(\bar{a},\bar{b})]_\sim + [(\bar{c},\bar{d})]_\sim = [(\bar{a}+\bar{c},\bar{b}+\bar{d})].$$

Poichè per ipotesi $(\bar{a},\bar{b}) \in [(a,b)]_\sim$ e $(\bar{c},\bar{d}) \in [(c,d)]_\sim$, si ha che

$$\begin{cases} \bar{a}+b = \bar{b}+a \\ \bar{c}+d = \bar{d}+c \end{cases}$$

sommando membro a membro, otteniamo

$$\bar{a}+b+\bar{c}+d = \bar{b}+a+\bar{d}+c = (\bar{a}+\bar{c})+(b+d) = (\bar{b}+\bar{d})+(a+c).$$

Questa uguaglianza ci permette di affermare che

$$(\bar{a}+\bar{c},\bar{b}+\bar{d}) \sim (a+c,b+d)$$

e quindi

$$[(\bar{a}+\bar{c},\bar{b}+\bar{d})]_\sim = [(a+c,b+d)]_\sim$$

Rispetto all'operazione di somma introdotta, valgono le proprietà:
Associativa: $\forall\ [(a,b)]_\sim,\ [(c,d)]_\sim,\ [(e,f)]_\sim$ si ha che

$$([(a,b)]_\sim + [(c,d)]_\sim) + [(e,f)]_\sim = [(a,b)]_\sim + ([(c,d)]_\sim + [(e,f)]_\sim)$$

Infatti, utilizzando la proprietà associativa valida in $\mathbb{N}$, si ha:

$$([(a,b)]_\sim + [(c,d)]_\sim) + [(e,f)]_\sim = [(a+c,b+d)]_\sim + [(e,f)]_\sim =$$

$$= [((a+c)+e,(b+d)+f)]_\sim = [(a+c+e,b+d+f)]_\sim$$

$$[(a,b)]_\sim + ([(c,d)]_\sim + [(e,f)]_\sim) = [(a,b)]_\sim + [(c+e,d+f)]_\sim =$$

$$= [(a+(c+e),b+(d+f)]_\sim = [(a+c+e,b+d+f)]_\sim$$

Commutativa:$\forall\ [(a,b)]_\sim,[(c,d)]_\sim$ si ha che

$$[(a,b)]_\sim + [(c,d)]_\sim = [(c,d)]_\sim + [(a,b)]_\sim$$

Infatti, utilizzando la proprietà commutativa valida in $\mathbb{N}$, si ha:

$$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c,b+d)]_\sim = [(c+a,d+b)]_\sim = [(c,d)]_\sim + [(a,b)]_\sim.$$

Esiste l'elemento neutro, cioè un elemento $[(x,y)]_\sim$ tale che :
$\forall\ [(a,b)]_\sim$ si abbia $[(a,b)]_\sim + [(x,y)]_\sim = [(a,b)]_\sim$.
Basta considerare l'elemento $[(0,0)]_\sim$:
infatti $[(a,b)]_\sim + [(0,0)]_\sim = [(a,b)]_\sim$.

Ogni elemento ammette **opposto**, cioè $\forall\ [(a,b)]_\sim\ \exists [(x,y)]_\sim$ tale che $[(a,b)]_\sim + [(x,y)]_\sim = [(0,0)]_\sim$.
Anche in questo caso, si vede subito che una soluzione è $[(b,a)]_\sim$:
infatti $[(a,b)]_\sim + [(b,a)]_\sim = [(a+b,a+b)]_\sim = [(0,0)]_\sim$.

Prodotto

Come si può definire un prodotto in modo che risulti "ben definito", cioè in modo che il risultato non dipenda dalla scelta dei rappresentanti delle classi?
Se lo definiamo in modo "naturale" nel modo seguente,
$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac,bd)]_\sim$
possiamo vedere che $[(1,2)]_\sim = [(0,1)]_\sim$, $[(3,5)]_\sim = [(1,3)]_\sim$ ma $[(1,2)]_\sim \cdot [(3,5)]_\sim = [(3,10)]_\sim$,
$[(0,1)]_\sim \cdot [(1,3)]_\sim = [(0,3)]_\sim$ ma $[(3,10)]_\sim \neq [(0,3)]_\sim$.

Quindi la precedente definizione non va bene. Come possiamo procedere?

Osserviamo che un'altra condizione alla quale dovrà soddisfare il prodotto tra classi è che vengano conservati i risultati tra gli elementi che corrispondono ai "*vecchi*" numeri naturali.
In particolare, se $[(a,b)]_\sim = [(a-b,0)]_\sim$ e $[(c,d)]_\sim = [(c-d,0)]_\sim$ (trattandosi delle classi corrispondenti ai naturali, devono essere $a \geq b, c \geq d$) si dovrà avere:

$[(a-b,0)]_\sim \cdot [(c-d,0)]_\sim = [(ac+bd-ad-bc,0)]_\sim = [(ac+bd,ad+bc)]_\sim$

Definiamo pertanto la seguente operazione di **prodotto tra classi di equivalenza**:
$\forall [(a,b)]_\sim, [(c,d)]_\sim \in Z = \mathbb{N} \times \mathbb{N}_{/\sim}$.

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]_\sim$$

Verifichiamo ora che il prodotto è **ben definito**.
Infatti se, come prima, consideriamo altri rappresentanti delle stesse classi, cioè
$(\bar{a},\bar{b}) \in [(a,b)]_\sim$ e $(\bar{c},\bar{d}) \in [(c,d)]_\sim$
otterremo

$[(\bar{a},\bar{b})]_\sim \cdot [(\bar{c},\bar{d})]_\sim = [(\bar{a}\bar{c}+\bar{b}\bar{d}, \bar{a}\bar{d}+\bar{b}\bar{c})]$.

Poichè per ipotesi $(\bar{a},\bar{b}) \in [(a,b)]_\sim$ e $(\bar{c},\bar{d}) \in [(c,d)]_\sim$, si ha che

$$\begin{cases} \bar{a}+b = \bar{b}+a \\ \bar{c}+d = \bar{d}+c \end{cases}$$

da cui si ottiene, con qualche passaggio,

$$\bar{a}\bar{c}+\bar{b}\bar{d}+ad+bc = ac+bd+\bar{a}\bar{d}+\bar{b}\bar{c}.$$

Questa uguaglianza ci permette di affermare che

$$(\bar{a}\bar{d}+\bar{b}\bar{c}, \bar{b}\bar{d}) \sim (ad+bc, bd)$$

e quindi

$$[(\bar{a}\bar{d}+\bar{b}\bar{c}, \bar{b}\bar{d})]_\sim = [(ad+bc,bd)]_\sim$$

Rispetto all'operazione di prodotto introdotta, valgono le proprietà:
Associativa: $\forall\ [(a,b)]_\sim,\ [(c,d)]_\sim,\ [(e,f)]_\sim$ si ha che

$$([(a,b)]_\sim \cdot [(c,d)]_\sim) \cdot [(e,f)]_\sim = [(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot\ [(e,f)]_\sim)$$

Infatti, utilizzando la proprietà associativa valida in $\mathbb{N}$, si ha:

$([(a,b)]_\sim \cdot [(c,d)]_\sim) \cdot\ [(e,f)]_\sim = [(ac+bd, ad+bc)]_\sim \cdot [(e,f)]_\sim =$
$= [((ac+bd)e+(ad+bc)f, (ac+bd)f+(ad+bc)e]_\sim =$
$= [(ace+bde+adf+bcf, acf+bdf+ade+bce)]_\sim;$
$[(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot\ [(e,f)]_\sim) = [(a,b)]_\sim \cdot [(ce+df, cf+de)]_\sim =$
$= [(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)]_\sim =$
$= [(ace+adf+bcf+bde, acf+ade+bce+bdf)]_\sim$

Commutativa:$\forall\ [(a,b)]_\sim, [(c,d)]_\sim$ si ha che

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(c,d)]_\sim \cdot [(a,b)]_\sim$$

Infatti, utilizzando la proprietà commutativa valida in $\mathbb{N}$, si ha:

$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]_\sim$
$[(c,d)]_\sim \cdot [(a,b)]_\sim. = [(ca+db, cb+da)]_\sim$

Esiste l'elemento neutro, cioè un elemento $[(x,y)]_\sim$ tale che :
$\forall\ [(a,b)]_\sim$ si abbia $[(a,b)]_\sim \cdot [(x,y)]_\sim = [(a,b)]_\sim$.
Basta considerare l'elemento $[(1,0)]_\sim$: infatti $[(a,b)]_\sim \cdot [(1,0)]_\sim = [(a,b)]_\sim$.

Invece **non è vero** che ogni elemento ammette **inverso**, cioè non è vero che
$\forall\ [(a,b)]_\sim\ \exists [(x,y)]_\sim$ tale che $[(a,b)]_\sim \cdot [(x,y)]_\sim = [(1,0)]_\sim$.

Elementi invertibili
Vediamo allora quali sono gli elementi che ammettono inverso, cioè gli elementi $[(a,b)]_\sim$ **per i quali** $\exists[(x,y)]_\sim$ **tale che**

$$[(a,b)]_\sim \cdot [(x,y)]_\sim = [(1,0)]_\sim.,$$

cioè che soddisfano l'uguaglianza:

$$[(ax+by, ay+bx)]_\sim = [(1,0)]_\sim.$$

Dobbiamo risolvere l'equazione (parametrica, di primo grado in due variabili) in $\mathbb{N}$**:**

$$ax+by+0 = ay+bx+1. \qquad (\star)$$

Poichè $ax+by \in \mathbb{N}, ay+bx \in \mathbb{N}$ **si ha che** $ax+by > ay+bx > 0$.
Si possono avere due situazioni: $a>b$ **oppure** $b>a$ **(**$a=b$ **è da escludere per l'ipotesi).**
Se $a>b$ **nella** $(\star)$ **possiamo raccogliere**
$(a-b)x-(a-b)y = (a-b)(x-y) = 1 \Rightarrow a-b=1, x-y=1.$
Se $a<b$ **nella** $(\star)$ **possiamo raccogliere**
$(b-a)y-(b-a)x = (b-a)(y-x) = 1 \Rightarrow b-a=1, y-x=1.$
Quindi gli elementi che ammettono inverso sono: $[(a,b)]_\sim = [(1+b,b)]_\sim = [(1,0)]_\sim$
e $[(a,b)]_\sim = [(a,a+1)]_\sim = [(0,1)]_\sim$

Sono questi gli interi 1 **e** -1.

Osservazione 1 ***Con il prodotto definito precedentemente si vede molto chiaramente la regola "meno per meno = più".***
Infatti $[(0,1)]_\sim \cdot [(0,1)]_\sim = [(0\cdot 0+1\cdot 1, 0\cdot 1+1\cdot 0)]_\sim = [(1,0)]_\sim.$

Osservazione 2 ***La stessa regola può essere dedotta utilizzando le proprietà distributive:***
$(-1)(-1) = (-1)(-1)+0\cdot(1) = (-1)(-1)+[(-1+1)](1) =$
$\underbrace{\text{utilizzando la proprietà distributiva}}(-1)(-1)+[(-1)(1)+(1)(1)]$
$= \underbrace{\text{utilizzando la proprietà associativa}}[(-1)(-1)+(-1)(1)]+(1)(1) =$
$\underbrace{\text{utilizzando la proprietà distributiva}}[(-1)(-1+1)]+(1)(1) = 0+(1)(1) = 1.$

Definizione 3 ***Per ogni*** $z \in \mathbb{Z}$ ***si definisce il valore assoluto o modulo di*** z ***e lo si indica con il simbolo*** $|z|$:

$$|z| = \begin{cases} z & z \geq 0 \\ -z & z < 0 \end{cases}$$

Osservazione 4 ***Per ogni*** $z_1, z_2 \in \mathbb{Z}$, ***vale l'uguaglianza*** $|z_1.z_2| = |z_1| \cdot |z_2|$.

Osservazione 5 ***Non vale invece, in generale, l'uguaglianza*** $|z_1+z_2| = |z_1| + |z_2|$.
Ad esempio se $z_1 = -5,\ z_2 = 3$ ***allora*** $|z_1+z_2| = 2 \neq 8 = |z_1| + |z_2|$.

Supponiamo familiari le principali proprietà delle operazioni sugli interi e la rappresentazione di $\mathbb{Z}$ **sulla retta orientata.**

0.1 I Numeri Razionali

Il procedimento di costruzione di $\mathbb{Q}$ come ampliamento di $\mathbb{Z}$, è molto simile al procedimeno visto per la costruzione di $\mathbb{Z}$, come ampliamento di $\mathbb{N}$.
Consideriamo l'insieme $\mathbb{Z} \times \mathbb{Z} \setminus \{0\} = \{(a,b) \mid a,b \in \mathbb{Z},\ b \neq 0\}$ e in esso introduciamo una relazione di equivalenza così definita:

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc$$

Verifichiamo che la relazione gode delle proprietà richieste.

1. Proprietà riflessiva: per ogni (a,b) si ha $(a,b) \sim (a,b)$. Infatti $ab = ba$.

2. Proprietà simmetrica: se $(a,b) \sim (c,d)$ segue che $(c,d) \sim (a,b)$.

Infatti da $ad = bc$ segue che $bc = ad$ e quindi $cb = da$ da cui segue $(c,d) \sim (a,b)$.

3. Proprietà transitiva: se $(a,b) \sim (c,d)$ e $(c,d) \sim (e,f) \Rightarrow (a,b) \sim (e,f)$.

Infatti per ipotesi $\begin{cases} (a,b) \sim (c,d) & \Rightarrow \quad ad = bc \\ (c,d) \sim (e,f) & \Rightarrow \quad cf = de \end{cases}$: $\qquad (\clubsuit)$

moltiplicando membro a membro si ha

$$adcf = bcde.$$

Poichè $d \neq 0$ si può semplificare, ottenendo $acf = bce$. si presentano ora due casi:

1. Se $c \neq 0$, si ottiene $af = be$ e quindi $(a,b) \sim (e,f)$.
2. Se $c = 0$, dalle ($\clubsuit$) si ha $ad = de = 0 \Rightarrow a = e = 0$ (essendo $d \neq 0$) e quindi ancora $(a,b) \sim (e,f)$.

Quindi è verificato che la relazione è di equivalenza.

Risulta perciò introdotta in $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ una **partizione in classi** di equivalenza.
Indichiamo con $\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})_\sim$ l'insieme delle classi di equivalenza e cerchiamo un rappresentante "canonico" per ogni classe.
Consideriamo $[(a,b)]_\sim = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\} \mid ay = bx\} = \left[(\bar{a},\bar{b})\right]_\sim$ ove $M.C.D.(\bar{a},\bar{b}) = 1$.

Osservazione 1 *Gli elementi di una stessa classe di equivalenza sono le coppie che possono essere rappresentate sul piano cartesiano come rette a coordinate intere passanti per l'origine e private dell'origine stessa.*

Osservazione 2 *Ogni classe di equivalenza* $[(a,b)]_\sim$ *è un numero razionale e può essere rappresentato da una "frazione". Precisamente* $[(a,b)]_\sim$ *può essere rappresentata dalla frazione* $\dfrac{a}{b}$ *oppure da una qualsiasi frazione* $\dfrac{c}{d}$ *equivalente alla data, cioè tale che* $ad = bc$ *(si ottiene* $\dfrac{c}{d} = \dfrac{ak}{bk},\ k \neq 0$) .
L'unica coppia (a,b) *con* a *e* b *coprimi, corrisponde alla frazione equivalente detta "ridotta ai minimi termini".*

Vale infatti la seguente

Proprietà 3 *Se* $a \neq 0$, *nella classe* $[(a,b)]_\sim$ *esiste una ed una sola coppia* $(\bar{a},\bar{b})$ *con* $M.C.D.(\bar{a},\bar{b}) = 1$ *e* $\bar{b} > 0$.

- Esistenza:

Sia $d = M.C.D.(a,b)$: allora $a = d\bar{a},\ b = d\bar{b}$ e $M.C.D.(\bar{a},\bar{b}) = 1$ (vedi capitolo sul $M.C.D.$).
Dalla definizione si vede subito che $(\bar{a},\bar{b}) \sim (a,b)$. Infatti $\bar{a}b = \bar{a}(d\bar{b}) = (\bar{a}d)\bar{b} = a\bar{b}$.

- Unicità:

Supponiamo che nella classe $[(a,b)]_\sim$, con $b>0$, ci siano due coppie, (m,n) ed (r,s) con $n,s>0$ e $M.C.D.(m,n)=M.C.D.(r,s)=1$.
Poichè le due coppie stanno nella stessa classe di equivalenza si avrà

$$(1) \qquad ms=nr.$$

Quindi m è un divisore del prodotto nr. Poichè m è primo con n (per le proprietà viste nel capitolo sulla divisibilità in $\mathbb{Z}$) necessariamente m dovrà essere un divisore di r. Quindi esisterà $h\in\mathbb{Z}$ tale che $r=mh$. Sostituendo nella (1) abbiamo

$$(2) \qquad ms=n(mh)$$

e semplificando per m $(\neq 0)$ otteniamo $s=nh$.
Sostituendo nella (1) si ottiene il sistema

$$\begin{cases} m\cdot nh=nr \\ s=nh \end{cases} \quad \text{da cui si deduce} \quad \begin{cases} r=mh \\ s=nh \end{cases}$$

Segue che h è un divisore comune, quindi necessariamente $h=1$ e $(m,n)=(r,s)$.
Si può concludere che esiste **una corrispondenza biunivoca** tra le classi di equivalenza e le coppie (a,b) con $b\neq 0$ e $M.C.D.(a,b)=1$.

Osservazione 4 *Gli elementi della classe* $[(kb,b)]_\sim=[(k,1)]_\sim$ *costituiscono un sottoisieme* $\mathbb{Z}'$ *di* $\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$ *che è in corrispondenza biunivoca con l'insieme degli Interi* $\mathbb{Z}$

Una corrispondenza può essere quella che associa alla classe $[(kb,b)]_\sim=[(k,1)]_\sim\in\mathbb{Z}'\subseteq\mathbb{Q}$ l'elemento $k\in\mathbb{Z}$.

Introduciamo ora le operazioni e studiamo la struttura di $\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$.

Somma:

Osservazione 5 *Come al momento di introdurre il prodotto in* $\mathbb{Z}$ *abbiamo dovuto scartare la definizione più immediata (componenete per componente), così qui non è accettabile la somma ottenuta componente per componente.*
Infatti se poniamo $[(a,b)]_\sim+[(c,d)]_\sim=[(a+c,b+d)]_\sim$ *ci accorgiamo subito che*
$[(3,1)]_\sim+[(1,2)]_\sim=[(4,3)]_\sim$ *mentre* $[(9,3)]_\sim+[(2,4)]_\sim=[(11,7)]_\sim$ *e* $[(4,3)]_\sim\neq[(11,7)]_\sim$
(osserviamo che $[(3,1)]_\sim=[(9,3)]_\sim$ *e che* $[(1,2)]_\sim=[(2,4)]_\sim$*)*

Introduciamo la seguente operazione di **somma tra classi di equivalenza**:
$\forall[(a,b)]_\sim,[(c,d)]_\sim\in\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$

$$[(a,b)]_\sim+[(c,d)]_\sim=[(ad+bc,bd)]_\sim$$

Verifichiamo che questa somma è *ben definita*, cioè non dipende dai rappresentanti delle classi. Intanto $bd\neq 0$ e quindi $[(ad+bc,bd)]_\sim\in\mathbb{Q}=(\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$.
Inoltre, cambiando i rappresentanti delle classi addende, otteniamo ancora la stessa classe.
Consideriamo infatti

$$(\bar a,\bar b)\in[(a,b)]_\sim e\ (\bar c,\bar d)\in[(c,d)]_\sim$$

Per definizione di somma

$$[(\bar a,\bar b)]_\sim+[(\bar c,\bar d)]_\sim \quad = \quad [(\bar a\bar d+\bar b\bar c,\bar b\bar d)]_\sim.$$

Mostriamo ora che $[(\bar a\bar d+\bar b\bar c,\bar b\bar d)]_\sim=[(ad+bc,bd)]_\sim$ (tesi).
Poichè per ipotesi $(\bar a,\bar b)\in[(a,b)]_\sim$ e $(\bar c,\bar d)\in[(c,d)]_\sim$, si ha che

$$\begin{cases} \bar a b=\bar b a \\ \bar c d=\bar d c \end{cases}$$

moltiplicando la prima uguaglianza per $d\bar d$ e la seconda per $b\bar b$ (che sono quantità $\neq 0$) si ottiene

$$\begin{cases} \bar{a}bd\bar{d} = \bar{b}ad\bar{d} \\ \bar{c}db\bar{b} = \bar{d}cb\bar{b} \end{cases}$$

da cui, sommando membro a membro e applicando la proprietà commutativa e distributiva, si ottiene:

$$\bar{a}bd\bar{d} + \bar{c}db\bar{b} = \bar{b}ad\bar{d} + \bar{d}cb\bar{b}$$

$$bd(\bar{a}\bar{d} + \bar{b}\bar{c}) = \bar{b}\bar{d}(ad + bc)$$

da cui segue che $(\bar{a}\bar{d} + \bar{b}\bar{c}, \bar{b}\bar{c}) \sim (ad + bc, bc)$ che è la tesi.

.

Rispetto all'operazione di somma introdotta, valgono le proprietà:
Associativa: $\forall\ [(a,b)]_\sim,\ [(c,d)]_\sim,\ [(e,f)]_\sim$ si ha che

$$([(a,b)]_\sim + [(c,d)]_\sim) + [(e,f)]_\sim = [(a,b)]_\sim + ([(c,d)]_\sim + [(e,f)]_\sim)$$

Infatti si ha:
I membro:

$$([(a,b)]_\sim + [(c,d)]_\sim) + [(e,f)]_\sim = [(ad+bc,bd)]_\sim + [(e,f)]_\sim = [((ad+bc)f + bde, (bd)f)]_\sim$$

II membro:

$$[(a,b)]_\sim + ([(c,d)]_\sim + [(e,f)]_\sim) = [(a,b)]_\sim + [(cf+de,df)]_\sim =$$

$$= [(adf + b(cf+de), b(df)]_\sim$$

e si vede che sono uguali, applicando la proprietà associativa valida in $\mathbb{Z}$.:
Commutativa:$\forall\ [(a,b)]_\sim, [(c,d)]_\sim$ si ha che

$$[(a,b)]_\sim + [(c,d)]_\sim = [(c,d)]_\sim + [(a,b)]_\sim$$

Infatti, utilizzando le proprietà di $\mathbb{Z}$, si ha:
$[(a,b)]_\sim + [(c,d)]_\sim = [(ad+bc,bd)]_\sim = [(cb+da,db)]_\sim = [(c,d)]_\sim + [(a,b)]_\sim$.

Esiste l'elemento neutro, cioè un elemento $[(x,y)]_\sim$ tale che :
$\forall\ [(a,b)]_\sim$ si abbia $[(a,b)]_\sim + [(x,y)]_\sim = [(a,b)]_\sim$.
Basta considerare l'elemento $[(0,1)]_\sim$:
infatti $[(a,b)]_\sim + [(0,1)]_\sim = [(a,b)]_\sim$.

Ogni elemento ammette **opposto**, cioè $\forall\ [(a,b)]_\sim\ \exists [(x,y)]_\sim$ tale che $[(a,b)]_\sim + [(x,y)]_\sim = [(0,1)]_\sim$.
Anche in questo caso, si vede subito che una soluzione è $[(-a,b)]_\sim$:
infatti $[(a,b)]_\sim + [(-a,b)]_\sim = [(ab + (-b)a, bb)]_\sim = [(0,bb)]_\sim = [(0,1)]_\sim$.

Prodotto

A differenza di quanto si verificava nel caso del prodotto di interi e nella somma precedentemente definita, il prodotto in $\mathbb{Q}$ si introduce in modo naturale, moltiplicando componente per componente

Definiamo il **prodotto tra classi di equivalenza**:
$\forall [(a,b)]_\sim, [(c,d)]_\sim \in \mathbb{Q} = (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})_\sim$

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac,bd)]_\sim$$

Verifichiamo ora che il prodotto è **ben definito**.
Infatti se consideriamo altri rappresentanti delle stesse classi, cioè
$(\bar{a},\bar{b}) \in [(a,b)]_\sim$ e $(\bar{c},\bar{d}) \in [(c,d)]_\sim$
otterremo

$$[(\bar{a},\bar{b})]_\sim \cdot [(\bar{c},\bar{d})]_\sim = [(\bar{a}\bar{c}, \bar{b}\bar{d})].$$

Poichè per ipotesi $(\bar{a},\bar{b}) \in [(a,b)]_\sim$ e $(\bar{c},\bar{d}) \in [(c,d)]_\sim$, si ha che

$$\begin{cases} \bar{a}b = \bar{b}a \\ \bar{c}d = \bar{d}c \end{cases}$$

da cui si ottiene, moltiplicando membro a membro

$$\bar{a}b\bar{c}d = \bar{b}a\bar{d}c \text{ cioè } ac\bar{b}\bar{d} = bd\bar{a}\bar{c}.$$

Questa uguaglianza ci permette di affermare che $[(ac,bd)]_\sim = [(\bar{a}\bar{c},\bar{b}\bar{d})]$.

Rispetto all'operazione di prodotto introdotta, valgono le proprietà:
Associativa: $\forall\ [(a,b)]_\sim,\ [(c,d)]_\sim,\ [(e,f)]_\sim \in \mathbb{Q} = (\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$ si ha che

$$([(a,b)]_\sim \cdot [(c,d)]_\sim)\cdot [(e,f)]_\sim = [(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot\ [(e,f)]_\sim)$$

Infatti, utilizzando la proprietà associativa valida in $\mathbb{N}$, si ha:
$([(a,b)]_\sim \cdot [(c,d)]_\sim)\cdot\ [(e,f)]_\sim = [(ac+bd, ad+bc)]_\sim \cdot [(e,f)]_\sim =$
$= [((ac+bd)e + (ad+bc)f, (ac+bd)f + (ad+bc)e]_\sim =$
$= [(ace+bde+adf+bcf, acf+bdf+ade+bce)]_\sim;$
$[(a,b)]_\sim \cdot ([(c,d)]_\sim \cdot\ [(e,f)]_\sim) = [(a,b)]_\sim \cdot [(ce+df, cf+de)]_\sim =$
$= [(a(ce+df)+b(cf+de), a(cf+de)+b(ce+df)]_\sim =$
$= [(ace+adf+bcf+bde, acf+ade+bce+bdf)]_\sim$

Commutativa:$\forall\ [(a,b)]_\sim, [(c,d)]_\sim$ si ha che

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(c,d)]_\sim \cdot [(a,b)]_\sim$$

Infatti, utilizzando la proprietà commutativa valida in $\mathbb{N}$, si ha:
$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]_\sim$
$[(c,d)]_\sim \cdot [(a,b)]_\sim. = [(ca+db, cb+da)]_\sim$

Esiste l'elemento neutro, cioè un elemento $[(x,y)]_\sim$ tale che :
$\forall\ [(a,b)]_\sim$ si abbia $[(a,b)]_\sim \cdot [(x,y)]_\sim = [(a,b)]_\sim$.
Basta considerare l'elemento $[(1,0)]_\sim$: infatti $[(a,b)]_\sim \cdot [(1,0)]_\sim = [(a,b)]_\sim$.

Ogni elemento diverso da $[(0,b)]_\sim$**ammette inverso**, cioè
$\forall\ [(a,b)]_\sim\ \neq [(0,b)]_\sim\ \exists [(x,y)]_\sim$ tale che $[(a,b)]_\sim \cdot [(x,y)]_\sim = [(1,0)]_\sim$.
Si vede subito che un possibile risultato è $[(x,y)]_\sim = [(b,a)]_\sim$

Valgono inoltre le proprietà distributive (destre e sinistre), cioè $\forall\ [(a,b)]_\sim,\ [(c,d)]_\sim,\ [(e,f)]_\sim \in \mathbb{Q} = (\mathbb{Z}\times\mathbb{Z}\setminus\{0\})_\sim$ si ha che
$\{[(a,b)]_\sim +\ [(c,d)]_\sim\}\cdot\ [(e,f)]_\sim = \{[(a,b)]_\sim\ \cdot [(e,f)]_\sim\} + \{\ [(c,d)]_\sim \cdot\ [(e,f)]_\sim\}$

Osservazione 6 *Una struttura come quella che abbiamo appena ottenuto si dice Campo.*

1 La divisione in $\mathbb{Z}$

Teorema 1 *Siano* a *e* $b \in \mathbb{Z},\ b \neq 0$; *allora* ***esistono*** *e* ***sono univocamente determinati*** *due interi* q *ed* $r \in \mathbb{Z}$ *tali che*
1) $a = bq + r$
2) $0 \leq r < |b|$

Dimostrazione.
1) **Esistenza della coppia** $q, r \in \mathbb{Z}$. Distinguiamo quattro casi:

i) $a \geq 0,\ b > 0$

ii) $a \geq 0,\ b < 0$

iii) $a < 0,\ b > 0$

iv) $a < 0,\ b < 0$

i) Procediamo per induzione su a, fissato b.
Se $a = 0$ si ha che $a = b \cdot 0 + 0$ (e quindi $q = 0 = r$).
Se $0 < a < b$ si ha che $a = b \cdot 0 + a$ (ove $q = 0$ ed $r = a$).
Se $a \geq b$ allora $0 \leq a - b < a$ e, utilizzando l'ipotesi di induzione nella II forma, si ha che esistono due interi $\tilde{q},\ \tilde{r}$ tali che

$$a - b = b\tilde{q} + \tilde{r} \ \text{ con } 0 \leq \tilde{r} < b$$

e quindi

$$a = b + b\tilde{q} + \tilde{r} = b(1 + \tilde{q}) + \tilde{r} \ \text{ da cui si conclude } \ q = \tilde{q} + 1,\ r = \tilde{r}.$$

ii) $a \geq 0,\ b < 0$. Poniamo $b' = -b > 0$. Allora poichè $a \geq 0,\ b' > 0$, per il punto i) $\exists\ \bar{q},\ \bar{r} \in \mathbb{Z}$ tali che

$$a = b'\bar{q} + \bar{r} \ \text{ con } \ 0 \leq \bar{r} < b' = |b|.\text{Allora}$$

$$a = (-b)\bar{q} + \bar{r} = b(-\bar{q}) + \bar{r}, \quad \text{ e quindi } q = -\bar{q},\ r = \bar{r}.$$

iii) $a < 0,\ b > 0$. Poniamo $a' = -a > 0$; quindi, essendo $a' > 0,\ b > 0$, per il punto i) $\exists\ q_1, r_1 \in \mathbb{Z}$ tali che

$$a' = bq_1 + r_1, \quad 0 \leq r_1 < b$$

cioè

$$-a = bq_1 + r_1$$

da cui moltiplicando membro a membro per (-1) si ottiene:

$$a = b(-q_1) + (-r_1).$$

Se $r_1 = 0$ allora $q = -q_1,\ r = -r_1 = 0$;
se $r_1 > 0$ allora, aggiungendo $+b$ e $-b$ al secondo membro, si ottiene

$$a = b(-q_1) + b - b + r_1 = b(-q_1 - 1) + (b - r_1)$$

e quindi si ha $q = -q_1 - 1$ e $r = b - r_1$ (osservando che $0 \leq b - r_1 < |b|$.)
iv) $a < 0,\ b < 0$.
Poniamo $b' = -b > 0$, come nel punto ii). Allora, per il punto iii), esistono $q_2,\ r_2 \in \mathbb{Z}$ tali che

$$a = b'q_2 + r_2, \ \text{ con } \ 0 \leq r_2 < b' = |b|$$

e quindi otteniamo

$$a = b(-q_2) + r_2 \ \text{, ove } q = -q_2,\ r = r_2.$$

2) **Unicità della coppia** $q,\ r$, nell'ipotesi in cui $0 \leq r < |b|$.
Supponiamo che, accanto a q ed r, esistano $\bar{q},\ \bar{r}$ tali che

$$a = bq + r,\ a = b\bar{q} + \bar{r}, \text{ con le condizioni } 0 \leq r < |b|,\ 0 \leq \bar{r} < |b|.$$

dalla relazione precedente, uguagliando e supponendo $r \geq \bar{r}$, si ottiene:

$$bq + r = b\bar{q} + \bar{r}, \quad 0 \leq r - \bar{r} < |b|$$

da cui

$$r - \bar{r} = b(\bar{q} - q) \quad \text{e quindi} \quad r - \bar{r} = |b| \cdot |(\bar{q} - q)|.$$

Si conclude che $r - \bar{r}$, dovendo essere un multiplo non negativo di $|b|$ e strettamente minore di $|b|$, dovrà essere nullo, cioè $\bar{r} = r,\ \bar{q} = q$. ■

Definizione 2 *Gli interi q ed r si dicono* ***quoziente*** *e* ***resto*** *della divisione di a per b.*

Definizione 3 *Dati $a,\ b \in \mathbb{Z}$ diciamo che $b \mid a$ (b divide a) se $b \neq 0$ ed esiste $c \in \mathbb{Z}$ tale che $a = bc$.*

Osservazione 4 *Se $b \neq 0,\ b \mid a \Leftrightarrow$ il resto della divisione di a per b è 0.*

Osservazione 5 *$\forall a \in \mathbb{Z}$ si ha sempre che $\pm 1,\ \pm a$ sono divisori di a (detti* ***divisori banali****).*

Proprietà 6 *Se $a \neq 0, b \neq 0,$ allora $b|a$ e $a|b \Leftrightarrow a = \pm b$ $(ab \neq 0)$.*

Infatti, per ipotesi $b|a$ e $a|b,\ \exists\ q_1, q_2 \in \mathbb{Z}$ tali che $a = bq_1,\ b = aq_2$, da cui si ha $a = bq_1 = aq_2q_1$ e quindi $q_2q_1 = 1$. In $\mathbb{Z}$ le soluzioni sono $q_2 = q_1 = \pm 1$ e quindi $a = \pm b$.
Il viceversa è banale.

Definizione 7 *Dati $a,\ b,\ c \in \mathbb{Z}$, se esistono due interi $x,\ y$ tali che $(ax + by) = c$, si dice che c è* ***combinazione lineare*** *di a e di b.*

Osservazione 8 *Se $a,\ b,\ c \in \mathbb{Z}$, $c|a,\ c|b \Rightarrow c|(ax + by), \forall x, y \in \mathbb{Z}$.*

Infatti, $c|a \Rightarrow \exists\ q_1 \in \mathbb{Z}$ tale che $a = cq_1,\ c|b \Rightarrow \exists\ q_2$ tale che $b = cq_2$.
Allora $ax + by = cq_1x + cq_2y = c(q_1x + q_2y)$ e quindi $c|(ax + by)$.

1.1 Massimo comun divisore (M.C.D.) e Minimo comune multiplo (m.c.m.)

Definizione 9 *Un intero d si dirà massimo comun divisore degli interi $a,\ b$ (non entrambi nulli) e lo si indicherà con $M.C.D.(a, b)$, se e solo se*

i) $d|a,\ d|b$;

ii) se t è un intero tale che $t|a,\ t|b$ allora $t|d$.

Osservazione 10 *Si verifica facilmente che , se $d = M.C.D.(a, b)$ allora è pure*
$d = M.C.D.(-a, b) = M.C.D.(a, -b) = M.C.D.(-a, -b)$
$d = M.C.D.(b, a) = M.C.D.(b, -a) = M.C.D.(-b, a) = M.C.D.(-b, -a)$

Osservazione 11 $M.C.D.(0, b) = b = M.C.D.(b, 0)$.

Basterà quindi provare l'esistenza di un massimo comun divisore per ogni coppia di interi $a,\ b > 0$.
Daremo una dimostrazione di tipo costruttivo, utilizzando una procedura detta
"**Algoritmo euclideo delle divisioni successive**",
che permette l'effettiva determinazione di un $M.C.D.(a, b)$. e che può essere facilmente tradotta in un programma per calcolo automatico.

Teorema 12 *Per ogni coppia $a,\ b \in \mathbb{Z},\ a > 0,\ b > 0$, esiste un massimo comun divisore d fra a e b.*

Dimostrazione. Si supponga $a \geq b$ e si eseguano le divisioni successive

$$a = bq_1 + r_1 \qquad \text{con} \quad 0 \leq r_1 < b \qquad (1)$$

Se $r_1 = 0$ abbiamo finito e un Massimo Comun Divisore di a e b è b stesso.

$$\text{se } r_1 \neq 0 \qquad b = r_1q_2 + r_2 \qquad \text{con} \quad 0 \leq r_2 < r_1 \qquad (2)$$

$$\text{se } r_2 \neq 0 \qquad r_1 = r_2q_3 + r_3 \qquad \text{con} \quad 0 \leq r_3 < r_2 \qquad (3)$$

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$\text{se } r_{h-1} \neq 0 \qquad r_{h-2} = r_{h-1}q_h + r_h \qquad \text{con} \quad 0 \leq r_h < r_{h-1} \qquad (h)$$

$$\text{se } r_h \neq 0 \qquad r_{h-1} = r_hq_{h+1}. \qquad (h+1)$$

Poichè $r_h < r_{h-1} < r_{h-2} < \ldots < r_3 < r_2 < r_1 < b$,
dopo un numero finito di divisioni si otterrà un resto nullo, cioè $\exists\ h$ tale che $r_{h+1} = 0$.
Un Massimo Comun Divisore è allora **l'ultimo resto non nullo** nelle divisioni precedenti cioè $r_h = d = M.C.D.(a,b)$.
Infatti se $r_1 \neq 0,\ r_h \neq 0$ e $r_{h+1} = 0$, mostriamo che $r_h = M.C.D.(a,b)$, cioè che r_h verifica le condizioni i), ii) della definizione.
i) $r_h|\ a$ e $r_h|\ b$. Infatti dalla uguaglianza sulla riga $(h+1)$ segue $r_h|\ r_{h-1}$, dalla uguaglianza sulla riga (h) e, sostituendo, si ha $r_{h-2} = (r_h q_{h+1})q_h + r_h = r_h(q_{h+1}q_h + 1) \Rightarrow r_h|\ r_{h-2}$.
Così risalendo si ottiene dalla (2) e dalla (1) che $r_h|\ b$ ed $r_h|\ a$.
ii) se $t|\ a$ e $t|\ b \Rightarrow t|\ r_n$.
Infatti dalla (1) si ha che $r_1 = a - bq_1$, cioè r_1 è combinazione lineare di a e di b e quindi si ha che $t|\ r_1$.
Poichè $t|\ r_1$ e $t|\ b$, dalla (2) si ha che $t|\ r_2$.
Così proseguendo, alla fine si ottiene che $t|\ r_h$ e quindi si conclude che r_h è un $M.C.D.(a,b)$. ■

Teorema 13 *Nelle ipotesi del teorema precedente, esistono due interi x e y tali che $d = ax + by$.*

Dimostrazione. Riprendendo le divisioni del teorema precedente, osserviamo che la (1) permette di esprimere r_1 nella forma

$$r_1 = a + b(-q_1).$$

Sostituendo l'espressione di r_1 nella (2) si ha:

$$r_2 = b - r_1 q_2 = b - [a + b(-q_1)]q_2 = a(-q_2) + b(1 + q_1 q_2)$$

e così via.
In questo modo si esprime ciascun resto come "combinazione lineare " a coefficienti interi di a e di b.
In particolare esisteranno $x,\ y \in \mathbb{Z}$ tali che:

$$d = M.C.D.(a,b) = r_h = xa + yb, \qquad x, y \in \mathbb{Z}.$$ ■

Esempio 14 *Determinare un $M.C.D.(24, 39)$.*

Effettuiamo le divisioni successive:

$$39 = 24 \cdot 1 + 15$$
$$24 = 15 \cdot 1 + 9$$
$$15 = 9 \cdot 1 + 6$$
$$9 = 6 \cdot 1 + \underline{3}$$
$$6 = 3 \cdot 2 + 0$$

Poichè 3 è l'ultimo resto non nullo, $3 = M.C.D.(39, 24)$.
Possiamo inoltre scrivere 3 come combinazione lineare di 39 e di 24.
Utilizzando le uguaglianze trovate, ricaviamo 3 dalla penultima cioè
$3 = 9 \cdot 1 + 6 \cdot (-1)$ e, procedendo a ritroso con le sostituzioni, si ottiene:
$6 = 15 \cdot 1 - 9 \cdot 1 \Rightarrow 3 = 9 \cdot 1 + 6 \cdot (-1) = 3 = 9 \cdot 1 + [15 \cdot 1 - 9 \cdot 1] \cdot (-1) = 9 \cdot 2 + 15 \cdot (-1)$
$9 = 24 + 15 \cdot (-1) \Rightarrow 3 = 9 \cdot 2 + 15 \cdot (-1) = [24 + 15 \cdot (-1)] \cdot 2 + 15 \cdot (-1) = 24 \cdot 2 + 15 \cdot (-3)$
$15 = 39 + 24 \cdot (-1) \Rightarrow \underline{3} = 24 \cdot 2 + 15 \cdot (-3) = 24 \cdot 2 + [39 + 24 \cdot (-1)] \cdot (-3) = \underline{24 \cdot 5 + 39 \cdot (-3)}$

Esempio 15 *Trovare un $M.C.D.(210, 182)$ ed esprimerlo come combinazione lineare di 210 ed 182.*

Come prima effettuiamo le divisioni:

$$210 = 182 \cdot 21 + 28$$
$$182 = 28 \cdot 6 + 14$$
$$28 = 14 \cdot 2$$

Quindi un $M.C.D.(210, 182)$ è 14. Una combinazione lineare si otterrà nel modo seguente:
$14 = 182 + 28 \cdot (-6) = 182 + [210 - 182 \cdot (-1)] \cdot (-6) = 182 \cdot 7 + 210 \cdot (-6)$.

Definizione 16 *Due interi a e b si dicono **relativamente primi** (o primi tra loro o **coprimi**) se $M.C.D.(a,b) = 1$, ovvero se (e solo se) esistono due interi relativi x e y tali che valga l'uguaglianza:*

$$1 = ax + by \qquad \textit{(identità di Bézout).}$$

Osservazione 17 *Se $a,\ b \in \mathbb{Z}$ e $d = M.C.D.(a,b)$, posto $a = d\bar{a},\ b = d\bar{b}$, si ha che $M.C.D.(\bar{a}, \bar{b}) = 1$.*

Infatti, detto $t = M.C.D.(\bar{a}, \bar{b})$ si ha che $t|\bar{a},\ t|\bar{b} \Rightarrow\ td \mid t\bar{a} = a,\ td|\ t\bar{b} = b$ quindi $t = \pm 1$.

Osservazione 18 *Sia $d = M.C.D.(a,b) = 1$ e $a \mid bc \Longrightarrow a \mid c$.*

Infatti, poichè $M.C.D.(a,b)=1$, esistono $x,y\in\mathbb{Z}$ tali che $1=ax+by$; poichè $a\mid bc\ \exists\ q\in\mathbb{Z}$ tale che $bc=aq$. Allora si ha $c=cax+cby$ e, sostituendo, si ottiene $c=cax+aqy=a(cx+qy)$.
Segue quindi che $a\mid c$.

Esercizio 19 *Se $a\mid c$ e $b\mid c$ con $M.C.D.(a,b)=1$ allora il prodotto $ab\mid c$.*
Infatti poichè $M.C.D.(a,b)=1$ esistono $x,y\in\mathbb{Z}$ tali che $ax+by=1$. Inoltre da $a\mid c$ e $b\mid c$ segue che esistono due interi, h,k, tali che $c=ha$, $c=kb$.
Dall'uguaglianza $ax+by=1$, moltiplicando entrambi i membri per c otteniamo

$$cax+cby=c$$

e, sostitendo a c nel primo addendo kb e nel secondo ha, otteniamo$(kb)ax+(ha)by=c\Rightarrow ab(kx+hy)=c\Rightarrow ab\mid c$.

Osservazione 20 *L'ipotesi che $M.C.D.(a,b)=1$ è essenziale: se per esempio $a=10,b=6,c=30$ si ha che $a\mid c$ e $b\mid c$ ma $ab\nmid c$.*

Definizione 21 *Siano $a,b\in\mathbb{Z},\ a\neq 0,b\neq 0$. Si dice minimo comune multiplo di a e b, e lo si indica con il simbolo $m.c.m.(a,b)$, ogni intero m tale che :*

1) $a\mid m,\ b\mid m$;

2) se $t\in\mathbb{Z}$ è tale che $a\mid t,\ b\mid t$ allora $t\mid m$.

Esistenza ed unicità a meno del segno sono garantiti dal seguente

Teorema 22 *Siano $a,b\in\mathbb{Z},\ a\neq 0,b\neq 0$ (non lede la generalità supporre $a>0,b>0$) allora, detto $d=M.C.D.(a,b)$ si ha che $m=\dfrac{a\cdot b}{d}$ è un minimo comune multiplo fra a e b;*

Dimostrazione. Posto $a=d\bar{a},\ b=d\bar{b}$, si ha

$$\frac{ab}{d}=\frac{d\bar{a}d\bar{b}}{d}=\bar{a}b=a\bar{b}$$

quindi $a|\dfrac{ab}{d},\ b|\dfrac{ab}{d}$ ed è soddisfatto il punto 1) della definizione.
Sia ora $t\in\mathbb{Z}$tale che $a\mid t,\ b\mid t$, mostriamo che $\dfrac{ab}{d}|t$. Infatti

$$t=at_1=bt_2\longrightarrow\bar{a}dt_1=\bar{b}dt_2\longrightarrow\bar{a}t_1=\bar{b}t_2$$

e, per le osservazioni precedenti, si ha che $M.C.D.(\bar{a},\bar{b})=1$ da cui si deduce che $\bar{a}\mid t_2$, $t_2=\bar{a}t_3$ e quindi

$$t=bt_2=b\bar{a}t_3=\frac{ab}{d}t_3\Longrightarrow\frac{ab}{d}|\ t.$$

■

Osservazione 23 *Se $m=m.c.m.(a,b)$, l'unico altro $m.c.m.(a,b)$ è $-m$.*

Esercizio 24 *Verificare che $\forall k\in\mathbb{Z}$ sono coprimi i numeri $a=22k+5$ e $b=33k+7$.*

Dimostrazione. Sia $d=M.C.D.(a,b)$.
Allora esisteranno $\bar{a},\bar{b}\in Z$ tali che $a=22k+5=d\bar{a},\ b=33k+7=d\bar{b}$.
Se moltiplichiamo la prima uguaglianza per 3 e la seconda per 2, si ottiene:

$$\begin{cases}3a=3\cdot 22k+15=3d\bar{a}\\ 2b=2\cdot 33k+14=2d\bar{b}.\end{cases}$$

Sottraendo membro a membro si ottiene $3a-2b=1=(3\bar{a}-2\bar{b})d\Rightarrow d\mid 1\Rightarrow M.C.D.(a,b)=1$. ■

1.2 Equazioni Diofantee.

Si dicono diofantee equazioni del tipo

$$ax + by = c, \text{ ove } a, b, x, y \in \mathbb{Z}.$$

Si possono avere due casi:

1) non ci sono soluzioni (intere): per esempio $2x + 6y = 5$.

2) Ci sono infinite soluzioni (intere): per esempio $2x + 3y = 5$.

Osserviamo che invece in $\mathbb{R}$ l'equazione $ax + by = c$, ha sempre infinite soluzioni che possono essere interpretate come gli infiniti punti di una retta.

Per quanto riguarda il caso in $\mathbb{Z}$, vale il seguente

Teorema 25 *L'equazione $ax + by = c$, con $a, b \in \mathbb{Z}$ ha soluzioni intere x, y, se e solo se, detto $d = M.C.D.(a, b)$, si ha che $d \mid c$.*

Dimostrazione. Supponiamo dapprima che $d \mid c$. Per le proprietà del massimo comun divisore si ha che esistono due interi $\bar{x}$ e $\bar{y} \in \mathbb{Z}$ tali che

$$a\bar{x} + b\bar{y} = d. \qquad (\star)$$

Poichè $d \mid c$ esiste un $k \in \mathbb{Z}$ tale che $dk = c$. Moltiplicando entrambi i membri della $(\star)$ per k si ottiene

$$a(\bar{x}k) + b(\bar{y}k) = dk = c$$

e quindi l'equazione data ammette soluzioni intere (che sono $x = \bar{x}k, y = \bar{y}k$). Viceversa supponiamo che esistano $x', y' \in \mathbb{Z}$ tali che $ax' + by' = c$. Poichè $d = M.C.D.(a, b)$ si ha che $a = d\bar{a}, b = d\bar{b}$ da cui segue che $c = d\bar{a}x' + d\bar{b}y' = d(\bar{a}x' + \bar{b}y') \Rightarrow d \mid c$. ■

Teorema 26 *Sia data l'equazione diofantea*

$$ax + by = c \qquad (\star)$$

che ammetta soluzioni $\bar{x}$, $\bar{y}$. Allora tutte e sole le soluzioni sono

$$\begin{cases} x = \bar{x} + \bar{b}t \\ y = \bar{y} - \bar{a}t \end{cases} . \qquad (\star\star)$$

ove $M.C.D.(\bar{a}, \bar{b}) = 1, a = d\bar{a}, b = d\bar{b}, d = M.C.D.(a, b), t \in \mathbb{Z}$.

Dimostrazione. Cominciamo col mostrare che ogni coppia del tipo $(\star\star)$ è soluzione dell'equazione $(\star)$. Infatti, sostituendo si ha

$$a(\bar{x} + \bar{b}t) + b(\bar{y} - \bar{a}t) = a\bar{x} + a\bar{b}t + b\bar{y} - b\bar{a}t = c.$$

Viceversa, sia la coppia x, y, soluzione della $(\star)$ e quindi si abbia

$$ax + by = c = a\bar{x} + b\bar{y}.$$

Poichè $a = d\bar{a}, b = d\bar{b}$, (ove $d = M.C.D.(a, b)$), sostituendo si ottiene

$$d\bar{a}x + d\bar{b}y = d\bar{a}\bar{x} + d\bar{b}\bar{y} \quad \text{e, semplificando } \bar{a}\ x + \bar{b}y = \bar{a}\bar{x} + \bar{b}\bar{y}$$

raccogliendo

$$\bar{a}(x - \bar{x}) = \bar{b}(\bar{y} - y) \qquad (\Diamond)$$

Poichè $M.C.D.(\bar{a}, \bar{b}) = 1$, dal fatto che $\bar{a} \mid \bar{b}(\bar{y} - y)$ segue che $\bar{a} \mid (\bar{y} - y)$ e quindi esiste un intero t tale che $\bar{y} - y = \bar{a}t \Rightarrow y = \bar{y} - \bar{a}t$.
Sostituendo nella $(\Diamond)$ si ottiene $\bar{a}(x - \bar{x}) = \bar{b}(\bar{a}t) \Rightarrow x = \bar{x} + \bar{b}t$. ■

1.3 Numeri primi e Teorema fondamentale dell'Aritmetica

Definizione 27 *Un numero* $p \in \mathbb{Z},\ p \neq 0,\ p \neq \pm 1$, *si dice* ***primo*** *se, ogni volta che* p *divide il prodotto di due interi* a *e* b *esso divide almeno uno dei due fattori. In simboli:*

$$p \mid ab \Longrightarrow p \mid a \text{ o } p \mid b.$$

Definizione 28 *Un numero* $p \in \mathbb{Z},\ p \neq 0,\ p \neq \pm 1$, *si dice* ***irriducibile*** *se e solo se* p *è divisibile solo per* ± 1 *e* $\pm p$.

Teorema 29 *Sia* $p \in Z,\ p \neq 0,\ p \neq \pm 1$. *Allora* p *è irriducibile se e solo se* p *è primo.*

Dimostrazione.
Assumiamo per ipotesi che p sia primo e dimostriamo che p è irriducibile.
Sia q un divisore di p cioè sia $p = q\overline{p}$. Poichè p è primo e $p \mid p$, segue che o $p|q$ oppure $p|\overline{p}$.
Se $p \mid q$ allora $q = p\overline{q} \Rightarrow q = q\overline{p}\overline{q}$ cioè $1 = \overline{p}\overline{q}$ da cui si ottiene $\overline{p} = \overline{q} = \pm 1$ e si conclude che $p = \pm q$.
Se $p \mid \overline{p}$ allora $\overline{p} = p\widetilde{p} \Rightarrow p = qp\widetilde{p}$ cioè $q\widetilde{p} = 1$, da cui si ottiene $q = \widetilde{p} = \pm 1$.

Viceversa supponiamo p irriducibile e dimostriamo che p è primo. Sia p un divisore di ab, cioè $p|ab$ e quindi $\exists q \in \mathbb{Z}$ tale che $ab = pq$. Sia $d = M.C.D.(p, b)$; allora $d \mid p$ che è irriducibile e quindi $d = \pm p$ oppure $d = \pm 1$.
1) $d = \pm p \ \Rightarrow p|\ b$;
2) $d = \pm 1 \Rightarrow \exists\, x, y \in Z$ tali che si abbia $1 = px+by$. Allora segue che $a = apx+aby = apx+pqy = p(ax+qy)$ $\Rightarrow p|a$. ■

Teorema 30 ***(TEOREMA fondamentale dell'Aritmetica)****: Ogni numero intero* n, *diverso da* 0 *e da* ± 1, *può essere scritto come prodotto di* $s \geq 1$ *numeri primi (non necessariamente distinti). Tale fattorizzazione è essenzialmente unica, cioè se*

$$n \ = \ p_1 p_2 \cdots p_s = \ q_1 q_2 \cdots q_t$$

ove ogni $p_i\ (1 \leq i \leq s)$ *e ogni* $q_j\ (1 \leq j \leq t)$ *è un numero primo, allora si possono ordinare i fattori in modo che sia*
1) $s = t$
2) $p_1 = \pm q_1, \cdots, p_s = \pm q_s$.

Dimostrazione. Supponiamo $n > 1$ e procediamo per induzione (II forma) osservando che per $n = 2$ il Teorema è vero essendo 2 un numero primo.
Esistenza della fattorizzazione:
Supponiamo che il Teorema sia vero per ogni intero m con $2 \leq m \leq n$ e proviamolo per n. Se n è un numero primo, il teorema è vero; se n non è primo, allora sarà fattorizzabile nella forma $n = ab$ con $1 < a < n$ e $1 < b < n$. Per ipotesi induttiva

$$a = a_1 a_2 \cdots a_h \quad \text{e} \quad b = b_1 b_2 \cdots b_k$$

ove i fattori a_i e b_j sono primi $\forall i = 1, \cdots, h$ e $j = 1, \cdots, k$.
Quindi $n = a_1 a_2 \cdots a_h b_1 b_2 \cdots b_k$ cioè è esprimibile come prodotto di un numero finito di numeri primi.
Unicità della fattorizzazione:
Sia $n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ $\qquad (\circ)$
con i p_i e i q_j numeri primi $\forall i = 1, \cdots, s$ e $j = 1, \cdots, t$.
Dimostriamo che $s = t$ e che, a meno dell'ordine in cui compaiono e del loro segno, i fattori del primo membro sono uguali a quelli del secondo membro.
Poichè $p_1|q_1(q_2 \cdots q_t)$, per definizione di numero primo si ha che o $p_1|q_1$ e allora $p_1 = \pm q_1$, oppure $p_1|(q_2 \cdots q_t)$.
Se $p_1 \nmid q_1$ allora $p_1|[q_2(q_3 \cdots q_t)]$ quindi o $p_1|q_2$ e allora $p_1 = \pm q_2$ oppure $p_1|(q_3 \cdots q_t)$.
Procedendo in questo modo, essendo finito il numero dei fattori, esisterà qualche q_i tale che $p_1 = \pm q_i$.
Allora dalla $(\circ)$, semplificando, si ottiene

$$p_2 \cdots p_s = q_2 \cdots q_t. \qquad (\circ\circ)$$

Non può essere $s < t$ altrimenti, dopo s passaggi si avrebbe $1 = \pm q_{s+1} \cdots q_t$. (Analogamente non può essere $t < s$). Quindi in ogni caso è provata l'unicità della fattorizzazione. ■

Corollario 31 *Ogni numero intero n ha una fattorizzazione (essenzialmente unica) come prodotto di potenze di primi distinti, cioè ogni numero intero n si può scrivere nella forma*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} \qquad p_i \neq p_j \text{ se i} \neq \text{j}, \alpha_\text{i} > 0.$$

Corollario 32 *Sia $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$: possiamo agevolmente contare quanti sono i suoi divisori (propri ed impropri). Infatti, sia d un divisore di n. Allora $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ con $0 \leq \beta_i \leq \alpha_i$ e quindi i divisori di n saranno tanti quanti sono i valori distinti di d ottenuti al variare delle potenze β_i.*
Poichè ogni β_i può essere scelto in $\alpha_i + 1$ modi, i divisori di n saranno

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Esempio: quanti sono i divisori (propri ed impropri) di 50?
Poichè $50 = 2 \cdot 5^2$ si ha che $\alpha_1 = 1$ e $\alpha_2 = 2$. I divisori saranno $2 \cdot 3 = 6$. Infatti
$X = \{d \in \mathbb{N} | d|50\} = \{1, 2, 5, 10, 25, 50\}$.

Teorema 33 *Esistono infiniti numeri primi.*

Dimostrazione. Sia $P = \{p_1, p_2, \cdots, p_t\}$ l'insieme dei numeri primi.
Procediamo per assurdo e supponiamo che P sia finito.
Consideriamo ora il numero $m = p_1 p_2 \cdots p_t + 1$. Esso risulta coprimo con ogni elemento dell'insieme P quindi non è divisibile per nessuno di essi. Inoltre non è un numero primo perchè $m \notin P$ (infatti $m > p_i, \forall i$) e quindi si ha l'assudo. ■

Si può anche dimostrare che sono infiniti i numeri primi della forma $4k - 1$ e anche quelli della forma $4k + 1$.
Non è a tuttoggi conosciuta una formula che permetta di rappresentare tutti i numeri primi.

1.4 Numerazione in base n.

Teorema 34 *Sia n un intero $n \geq 2$. Ogni intero $a \geq 0$ può essere scritto in uno ed un sol modo nella forma:*

$$a = r_h n^h + r_{h-1} n^{h-1} + \cdots r_1 n^1 + r_0 n^0$$

per ogni $i = 0, 1, \cdots, h$ ed $r_h \neq 0$, per $h > 0$.

Dimostrazione. Si procede per induzione su a.
1. Se $a = 0$ la tesi è dimostrata poichè $0 = 0 \cdot n^0$.
2. Supposto che l'asserto sia vero per ogni k con $0 < k < a$, mostriamo che è vero anche per a.
Dividiamo a per n : si ottiene
$a = qn + r$ con $0 \leq r < n$. Poichè $q < a$, per l'ipotesi di induzione, q ammette la scrittura:
$q = s_{h-1} n^{h-1} + s_{h-2} n^{h-2} + \cdots + s_1 n^1 + s_0 n^0$ con $0 \leq s_i < n$
e quindi, sostituendo. si ha:
$a = nq + r = s_{h-1} n^h + s_{n-2} n^{h-1} + \cdots + s_1 n^2 + s_0 n^1 + r n^0 = r_h n^h + r_{h-1} n^{h-1} + \cdots r_1 n^1 + r_0 n^0$
ove $r_h = s_{h-1}$, $r_{h-1} = s_{h-2}, \cdots, r_1 = s_0$, $r_0 = r$.

L'unicità dell'espressione segue dall'unicità di q ed r. ■

Osservazione 35 *$r_0, r_1, \cdots, r_h$ sono i resti della sequenza di divisioni:*

$$\begin{array}{ll} a = qn + r_0 & 0 \leq r_0 < n \\ q = q_1 n + r_1 & 0 \leq r_1 < n \\ q_1 = q_2 n + r_2 & 0 \leq r_2 < n \\ \vdots \quad \vdots & \vdots \\ q_{h-1} = q_h n + r_h & 0 \leq r_h < n \ . \end{array}$$

Osservazione 36 *: Sia X un insieme di n simboli (cifre) distinti, il numero $a = r_h r_{h-1} \cdots r_0$ con $r_i \in X$ è rappresentato in base n.*

Esempio 37 *1.* $n = 10$ *: abbiamo l'usuale rappresentazione in base* 10*, che utilizza le cifre appartenenti all'insieme* $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
Il numero $(2002)_{10} = 2 \cdot 10^3 + 0 \cdot 10^2 + 0 \cdot 10^1 + 2 \cdot 10^0$.
2. $n = 2$ *: utilizziamo i simboli 0 e 1. Rappresentiamo il numero* $(2002)_{10}$ *in base 2.*

$$2002 = 2 \cdot 1001 + 0$$
$$1001 = 2 \cdot 500 + 1$$
$$500 = 2 \cdot 250 + 0$$
$$250 = 2 \cdot 125 + 0$$
$$125 = 2 \cdot 62 + 1$$
$$62 = 2 \cdot 31 + 0$$
$$31 = 2 \cdot 15 + 1$$
$$15 = 2 \cdot 7 + 1$$
$$7 = 2 \cdot 3 + 1$$
$$3 = 2 \cdot 1 + 1$$
$$1 = 2 \cdot 0 + 1$$

e quindi $(2002)_{10} = (11111010010)_2$.
3. $n = 8$ *: utilizziamo le cifre* $0, 1, 2, 3, 4, 5, 6, 7$,
ancora, utilizzando l'osservazione precedente si ha

$$2002 = 8 \cdot 250 + 2$$
$$250 = 8 \cdot 31 + 2$$
$$31 = 8 \cdot 3 + 7$$
$$3 = 8 \cdot 0 + 3$$

e quindi $(2002)_{10} = (3722)_8$

1.5 Operazioni in base 2

Le operazioni in una qualsivoglia base si impostano e si risolvono in modo analogo a quanto si fa nel caso della numerazione in base 10.
Nel caso della numerazione in base 2 è molto agevole fare i calcoli.

Esempio 38 *In base* 10 *si sa che* $8 + 12 = 20$. *e* $8 \times 12 = 96$.
In base 2 si ha: $(8)_{10} = (1000)_2$, $(12)_{10} = (1100)_2$ *e quindi:*

$$\begin{array}{r} 1000+ \\ 1100 = \\ \hline 10100 \end{array}$$

mentre

$$\begin{array}{r} 1000\times \\ 1100 = \\ \hline 0000 \\ 0000 \\ 1000 \\ 1000 \\ \hline 1100000 \end{array}$$

1.6 Relazione di congruenza in $\mathbb{Z}$

Diamo ora un esempio importante di relazione di equivalenza: la **relazione di congruenza** *modn* in $\mathbb{Z}$.

Definizione 39 *Sia* $X = \mathbb{Z}$, $a, b \in \mathbb{Z}$ *ed* n *un intero* $n > 1$. *Si dice che* a *è congruo* a b *modulo* n *e si scrive*

$$a \equiv b(modn) \qquad \text{se } \exists\ h \in \mathbb{Z} \text{ tale che} \qquad a - b = hn.^1$$

Proposizione 40 *La relazione di congruenza* $(modn)$ *è una relazione di equivalenza in* $\mathbb{Z}$.

Dimostrazione.

Proprietà riflessiva: $\forall a \in \mathbb{Z}$ è $a \equiv a(modn)$: infatti $a - a = 0 \cdot n$.

Proprietà simmetrica: sia $a \equiv b(modn) \Rightarrow \exists\ h \in \mathbb{Z}$ tale che $a-b = h \cdot n$; ma è anche $b-a = (-h)\cdot n$, $(-h) \in \mathbb{Z}$ quindi $b \equiv a(modn)$.

Proprietà transitiva: $a \equiv b(modn) \Rightarrow \exists\ h_1 \in \mathbb{Z}$ tale che $a - b = h_1 \cdot n$; $b \equiv c(modn) \Rightarrow \exists\ h_2 \in \mathbb{Z}$ tale che $b - c = h_2 \cdot n$. Sommando membro a membro si ottiene

$$a - c = (h_1 + h_2) \cdot n$$

da cui segue che $a \equiv c(modn)$.

■

1.7 Classi di resti modulo n.

Fissato $n > 1$, l'insieme $\mathbb{Z}$ può essere ripartito in classi di congruenza (includendo in una stessa classe tutti e soli gli $z \in \mathbb{Z}$ a due a due congrui tra loro modulo n), quindi la classe di congruenza individuata da x è:

$$[x]_n = \{x + hn |\ h \in Z\} = \{y |\ y \equiv x(modn)\}.$$

Proposizione 41 *Fissato* $n > 1$, *si hanno esattamente* n *classi di equivalenza distinte, che possono essere rappresentate dai numeri* $0, 1, \ldots, n-1$. *L'insieme di queste classi di è indicato con il simbolo* $\mathbb{Z}_n$ *e viene usualmente chiamato "**insieme delle classi di resti modulo** n". Si ha quindi*

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Dimostrazione. Sia $x \in Z$; per l'algoritmo della divisione $\exists!\ q,\ r \in Z$ tali che $x = nq + r$, con $0 \leq r < n$. Si ha quindi che $x \equiv r(modn)$, cioè $[x]_n = [r]_n$. D'altro canto, due classi $[x]_n, [y]_n$ con $0 \leq x < y < n$ sono sempre distinte. Infatti se $[x]_n = [y]_n$ avremmo $x \equiv y(modn)$ cioè $n|(x - y)$. Poichè x e y sono entrambi minori di n l'unica soluzione è $x - y = 0$ cioè $x = y$. ■

Osserviamo ora i legami che sussistono tra le operazioni di somma e di prodotto definiti in $\mathbb{Z}$ e la relazione di congruenza modulo n.

Proposizione 42 *La relazione di congruenza* $(modn)$ *è compatibile con le operazioni di somma e di prodotto di* $\mathbb{Z}$, *cioè se* $a, b \in \mathbb{Z}$ *da* $a \equiv b(modn)$ *e* $c \equiv d(modn)$ *segue*

$$a + c \equiv b + d(modn)$$

$$a \cdot c \equiv b \cdot d(modn).$$

Dimostrazione. Poichè $a \equiv b(modn)$ e $c \equiv d(modn)$ esistono $h, k \in Z$ tali che $a - b = hn,\ c - d = kn$. Sommando membro a membro otteniamo

$$(a - b) + (c - d) = hn + kn$$

cioè $(a + c) - (b + d) = (h + k)n$, da cui segue $a + c \equiv b + d(modn)$. Analogamente, moltiplicando membro a membro, si ottiene $ac = (b + hn)(d + kn) = bd + (bk + hd + hk)n \Longrightarrow ac \equiv bd(modn)$. ■

Valgono anche le seguenti proprietà

Proposizione 43 *Sia* $n > 1$ *e siano* $a,\ b,\ t \in \mathbb{Z},\ t \geq 0$.

[1] Otteniamo la stessa relazione se poniamo $a \equiv b(modn) \Leftrightarrow \exists k \in Z$ tale che $b - a = kn$

1) *se* $at \equiv bt(modn)$ *e* t *è primo con* n *allora* $a \equiv b(modn)$ *(cioè si può semplificare, se* t *ed* n *sono coprimi!)*;

2) *se* $a \equiv b(modn)$ *allora* $n| \ a \Leftrightarrow n| \ b$.

Dimostrazione. 1) Per ipotesi si ha che $at - bt = hn$ e quindi $(a-b)t = hn$. Poichè $M.C.D.(t,n) = 1$ segue che $n \mid (a-b)$ e quindi $a \equiv b(modn)$.
2) Per ipotesi sia $a = nq$ e $a - b = hn$. Allora $b = a - nh = nq - nh = n(q-h)$ da cui si ha $n|b$.
Il viceversa segue sfruttando la proprietà simmetrica della relazione di congruenza e scambiando b con a. ■

1.8 Un po' di nomenclatura.

Sia dato un insieme (non vuoto) nel quale siano introdotte delle operazioni, che possiamo indicare con i simboli "+", " $\cdot$ ", " $*$ ", " $\times$ ", " $\cup$ ", " $\cap$ ", ...
Rispetto ad una o più di queste operazioni possono valere varie proprietà (commutativa, associativa, distributive), possono esistere elementi neutri e/o elementi reciproci, ecc.
Sono particolarmente interessanti i casi delle seguenti strutture:
1) **Semigruppo**: $(S, *)$: è un insieme non vuoto dotato di legge di composizione $*$ che sia associativa, cioè tale che $\forall a, b, c \in S$ valga l'uguaglianza $(a * b) * c = a * (b * c)$.
2) **Monoide**: è un semigruppo in cui esista l'elemento neutro, cioè un elemento $u \in S$ tale che $u * a = a * u, \forall a \in S$.
3) **Gruppo**: è un monoide G in cui ogni elemento ammetta inverso, cioè $\forall a \in G \ \exists \bar{a} \in G$ tale che $a * \bar{a} = \bar{a} * a = u$.
4) **Gruppo abeliano:** è un gruppo in cui valga la proprietà commutativa, cioè $\forall a, b \in G$ valga l'uguaglianza $a * b = b * a$.
5) **Anello**: è un insieme non vuoto dotato di due leggi di composizione, che possiamo indicare con "+" e " $\cdot$" : $(A+, \cdot)$ che sia gruppo abeliano, rispetto alla somma e sia semigruppo rispetto al prodotto. Devono inoltre valere le proprietà distributive, cioè $\forall a, b, c \in A$ devono valere le uguaglianze: $(a+b)c = ac + bc$ e $a(b+c) = ab + ac$.
6) **Campo:** è un anello in cui gli elementi non nulli formano un gruppo abeliano.

Gli insiemi numerici che generalmente si usano sono esempi notevoli:
$\mathbb{N}$, l'insieme dei numeri Naturali è monoide rispetto alla somma e rispetto al prodotto usuale .
$\mathbb{Z}$, l'insieme dei numeri Interi relativi è un anello commutativo rispetto alla somma e al prodotto usuali.
$\mathbb{Q}$, l'insieme dei numeri Razionali è un campo rispetto alla somma e al prodotto.
$\mathbb{R}$, l'insieme dei numeri Reali è un campo rispetto alla somma e al prodotto.
$\mathbb{C}$, l'insieme dei numeri Complessi è un campo rispetto alla somma e al prodotto in esso definito.

1.9 L'anello delle classi di resto modulo n

Se, fissato $n \geq 2$, consideriamo l'insieme delle n classi di resto modulo n, e lo indichiamo con $\mathbb{Z}_n$, possiamo introdurre in tale insieme due operazioni inducendole in modo naturale da $\mathbb{Z}$.
Somma di classi di resto: $\forall \ [a]_n, \ [b]_n \in \mathbb{Z}_n$ definiamo una somma:

$$[a]_n + [b]_n = [a+b]_n$$

e un prodotto

$$[a]_n \cdot [b]_n = [ab]_n$$

Utilizzando le proprietà riportate nel precedente paragrafo (compatibilità della relazione di equivalenza con le operazioni), si può dimostrare che tali operazioni non dipendono dalla scelta dei rappresentanti delle classi e che sono associative e commutative.
Inoltre vediamo che la classe $[0]_n$ è l'elemento neutro rispetto alla somma: infatti $\forall \ [a]_n \in \mathbb{Z}_n$ si ha che $[0]_n + \ [a]_n = \ [a]_n$
e $\forall \ [a]_n \in \mathbb{Z}_n$ esiste un elemento $[\bar{a}]_n$ (opposto) tale che $[a]_n + [\bar{a}]_n = [0]_n$: basta considerare la classe $[-a]_n$.
Esiste inoltre l'elemento neutro rispetto al prodotto che è evidentemente la classe $[1]_n$.
Valendo anche le proprietà distributive, possiamo concludere che $\mathbb{Z}_n$ è un anello commutativo per ogni $n \geq 2$.

1.10 Il Campo delle classi di resti mod p, con p numero primo.

Tutto quello che è stato detto per un qualsiasi numero n, continua a velere se $n = p$ cioè se il modulo è un numero primo.
In questo caso però abbiamo un'altra proprietà: ogni elemento (classe) diverso da 0, possiede inverso e quindi $\mathbb{Z}_p$ risulta essere un campo (finito).
Per verificare che ogni classe $[a]_p \neq [0]_p$ ammette inverso, bisogna verificare che $\forall [a]_p \neq [0]_p \exists [x]_p$ tale che $[a]_p \cdot [x]_p = [1]_p$.
Si tratta di trovare soluzione alla equazione (diofantea) di primo grado con coefficienti in $\mathbb{Z}$

$$ax = 1 + kp$$

cioè

$$ax + kp = 1$$

Abbiamo visto che una tale equazione nelle incognite x e k ha soluzioni (intere) se e solo se $M.C.D.(a, p) = 1$.
Essendo p un numero primo e poichè a non è un multiplo di p (poichè per ipotesi $[a]_p \neq [0]_p$) segue la tesi.

1.11 Criteri di divisibilità

Le congruenze modulo n sono strumenti di grande utilità nello studio delle proprietà aritmetiche degli interi. Ad esempio giocano un ruolo primario nella dimostrazione dei cosiddetti "criteri di divisibilità". Abbiamo visto che, dato un intero $a > 0$, se $a = r_h r_{h-1} \dots r_1 r_0$ si può scrivere

$$a = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \dots + r_1 \cdot 10 + r_0 \cdot 10^0,\ r_h \neq 0,\ h \geq 0.$$

Osserviamo ora che $10 \equiv 0(mod2)$; $10 \equiv 0(mod5)$; $10 \equiv 0(mod10)$, e quindi anche
$10^t \equiv 0(mod2) \equiv 0(mod5) \equiv 0(mod10) \equiv 0(mod100),\ \forall t > 1$.

Segue che

Criterio 44 *Dato un numero*

$$a \quad = \quad r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \dots + r_1 \cdot 10 + r_0 \cdot 10^0,\ r_h \neq 0,\ h \geq 0,$$

1. a è divisibile per 2 se e solo se $2|r_0$, cioè se e solo se l'ultima cifra $r_0 \in \{0, 2, 4, 6, 8\}$
2. a è divisibile per 5 se e solo se $5|r_0$, cioè se e solo se $r_0 \in \{0, 5\}$
3. a è divisibile per 10 se e solo se $r_0 = 0$
4. a è divisibile per 100 se e solo se $r_0 = r_1 = 0$.

Con ragionamento analogo, osservando che $10 \equiv 1(mod3) \equiv 1(mod9)$ possiamo concludere che

Criterio 45 *Dato un numero $a = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \dots + r_1 \cdot 10 + r_0 \cdot 10^0,\ r_h \neq 0,\ h \geq 0$*
1. $3|a \leftrightarrow 3|(r_h + r_{h-1} + \dots + r_1 + r_0)$
2. $9|a \leftrightarrow 9|(r_h + r_{h-1} + \dots + r_1 + r_0)$,
cioè 3, (rispettivamente 9), dividono un numero intero a se e solo se 3 (rispettivamente 9) ne dividono la somma delle cifre.

Criterio 46 *Dato un numero a, nelle ipotesi dei precedenti criteri, allora $11|a \Leftrightarrow 11|\sum_0^h (-1)^i a_i$ cioè, come noto, un numero è divisibile per 11 quando, eseguita la somma delle cifre di posto pari e la somma delle cifre di posto dispari, la differenza è un multiplo di 11.*

Dimostrazione. Osserviamo che $10 \equiv -1(mod11)$ e quindi $10^2 \equiv 1(mod11), \dots, 10^r \equiv (-1)^r(mod11)$.
Si ha quindi che

$$10^t \equiv (-1)^t = \begin{cases} 1 \text{ se t è pari} \\ -1 \text{ se } t \text{ èdispari} \end{cases}$$

Allora $a \equiv r_h(-1)^h + r_{h-1}(-1)^{h-1} + \dots + r_1(-1) + r_0(mod11)$ e quindi $11|a \Leftrightarrow 11|(r_h(-1)^h + r_{h-1}(-1)^{h-1} + \dots + r_1(-1) + r_0)$. ■

Osservazione 47 *Si possono enunciare molti altri criteri di divisibilità, ma questi presentati sono quelli più utilizzati perchè più vantaggiosi.*

Osservazione 48 *Un criterio di divisibilità per* $2^2,\ 2^3,\ 2^4, \ldots, 2^n$ *:*

Abbiamo precendetemente osservato che , poichè $10 \equiv 0(mod\ 2)$, segue che $2|\ a \Leftrightarrow 2|\ r_0$.
In modo analogo, poichè $10^2 \equiv 0\ (mod\ 2^2)$, avremo che $2^2|\ a \Leftrightarrow 4|(\ r_1 \cdot 10 + r_0)$; cioè "un numero è divisibile per 4 se (e solo se) lo è il numero formato dalle due ultime cifre".
Generalizzando, poichè $10^n \equiv 0(mod\ 2^n)$, si potrà dire che un numero a è divisibile per 2^n se (e solo se) è divisibile per 2^n il numero formato dalle ultime n cifre, cioè il numero $(r_n \cdot 10^n + \ldots + r_1 \cdot 10 + r_0)$.

Osservazione 49 *Un criterio di divisibilità per* 25*.*

Con ragionamento analogo a quello usato nell'osservazione precedente, si vede che $10^2 \equiv 0(mod\ 5^2)$ e quindi "un numero è divisibile per 25 se (e solo se) lo è il numero formato dalle ultime due cifre".

Osservazione 50 *Un criterio di divisibilità per* 7*.*

Poichè il numero

$$a = r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \ldots + r_1 \cdot 10 + r_0 \cdot 10^0,\ (r_h \neq 0,\ h \geq 0)$$

è divisibile per 7 se e solo se

$$[a]_7 = [r_h \cdot 10^h + r_{h-1} \cdot 10^{h-1} + \ldots + r_1 \cdot 10 + r_0 \cdot 10^0]_7. = [0]_7$$

e poichè valgono le seguenti congruenze

$10^0 \equiv 1 \ (mod\ 7)$, $10^4 \equiv -3 \ (mod\ 7)$
$10^1 \equiv 3 \ (mod\ 7)$, $10^5 \equiv -2 \ (mod\ 7)$
$10^2 \equiv 2 \ (mod\ 7)$, $10^6 \equiv 1 \ (mod\ 7)$
$10^3 \equiv -1 \ (mod\ 7)$ $\cdots$

avremo che

$$[a]_7 = [a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + \cdots]_7 = [0]_7$$

e quindi a è divisibile per 7 se e solo se è divisibile per 7 il numero

$$(a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - \cdots$$

Esempio:
Decidere se il numero $a = 11188821$ è divisibile per 7.
Usando il criterio sopra esposto, poichè
$(a_0 - a_4 + a_7) + 3(a_1 - a_5 + a_8) + 2(a_2 - a_6 + a_9) = (1 - 8 + 1) + 3(2 - 8 + 1) + 2(8 - 1 + 0) = -6 + -15 + 14 = -7$,
si conclude che il numero dato è multiplo di 7.

Osservazione 51 *Per alcuni criteri si possono dare giustificazioni (potrebbero anche diventare dimostrazioni) che e possibile proporre agli studenti della scuola media inferiore.*

Divisibilità per 3 e per 9.

Esempio 52 *Consideriamo il numero* 2421 *e scriviamolo come somma di potenze di* 10*, ovvero:*
$2421 = 2 \cdot 1000 + 4 \cdot 100 + 2 \cdot 10 + 1$
poi scriviamo $1000 = 999 + 1; 100 = 99 + 1; 10 = 9 + 1$ *e sostituiamo:*
$2421 = 2 \cdot (999 + 1) + 4 \cdot (99 + 1) + 2 \cdot (9 + 1) + 1$
usando ora la proprietà distributiva
$2421 = \underline{2 \cdot 9 \cdot 111} + 2 + \underline{4 \cdot 9 \cdot 11} + 4 + \underline{2 \cdot 9} + 2 + 1 = 9(222 + 44 + 2) + [2 + 4 + 2 + 1]$.
Si può concludere che il numero proposto è divisibile per 3 *o per* 9 *se e solo se è divisibile per* 3 *o, rispettivamente, per* 9 *il numero* $[2 + 4 + 2 + 1]$ *che corrisponde alla somma delle cifre. In questo caso si deduce che* 2421 *è divisibile per* 9 *e quindi anche per* 3*.*

Esempio 53 *Consideriamo il numero* 42015*. Ancora possiamo scriverlo*
$42015 = 4 \cdot 10000 + 2 \cdot 1000 + 0 \cdot 100 + 1 \cdot 10 + 5 = 4 \cdot (9999 + 1) + 2 \cdot (999 + 1) + 1 \cdot (9 + 1) + 5 =$
$\underline{4 \cdot (9 \cdot 1111)} + 4 + \underline{2 \cdot (9 \cdot 111)} + 2 + \underline{1 \cdot 9} + 1 + 5 =$
$\underline{9(4444 + 222 + 1)} + \underline{[4 + 2 + 1 + 5]} = 9k + 12.$
Si deduce che 42015 *è divisibile per* 3 *(e non è divisibile per* 9*)*

Se invece di un esempio consideriamo un intero scritto in forma polinomiale, si può utilizzare il procedimento esposto per dare una dimostrazione. Osserviamo pure che con procedimento analogo possiamo giustificare (e dimostrare) il criterio di divisibilità per 2, 4, 5, 10, 100, ecc.

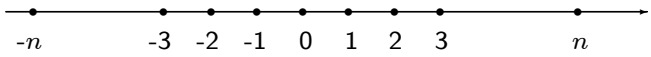
Numeri

Se consideriamo l'insieme $\mathbb{N} = \{0, 1, 2, 3, ..., n, ...\}$ dei numeri naturali (incluso 0), le operazioni che possiamo eseguire all'interno di questo insieme sono solo la *somma* e il *prodotto*. Ciò implica che equazioni di I grado in un'incognita x del tipo:

$$ax - b = 0, \text{ con } a, b \in \mathbb{N} \qquad (\bigstar)$$

sono risolubili in $\mathbb{N}$ solo in questi casi: $\begin{cases} a = b = 0 \\ a \neq 0, \ a \text{ divisore di } b. \end{cases}$

Se vogliamo quindi avere soluzioni per equazioni di tipo ($\bigstar$), dobbiamo estendere l'insieme $\mathbb{N}$. La prima estensione riguarda la possibilità di eseguire differenze e questo ci porta all'insieme $\mathbb{Z}$ dei numeri interi (relativi), ottenuto "aggiungendo a $\mathbb{N}$ una sua copia negativa", cioè $\mathbb{Z} = \{(\pm, n) | n \neq 0, n \in \mathbb{N}\} \cup \{0\} = \{\pm n, n \in \mathbb{N}\}$, dopo aver identificato ± 0 con 0. $\mathbb{N}$ risulta immerso in $\mathbb{Z}$, una volta identificato n con $+n$.



Anche lavorando in $\mathbb{Z}$ però abbiamo soluzioni solo per: $\begin{cases} a = b = 0 \\ a \neq 0, \ a \text{ divisore di } b. \end{cases}$

Tutto ciò perchè neppure in $\mathbb{Z}$ siamo in grado di eseguire l'operazione che ci serve per ottenere sempre (tranne quando $a = 0$ e $b \neq 0$) una soluzione: la divisione. Per fare questo, dobbiamo estendere ulteriormente $\mathbb{Z}$, considerando dapprima le frazioni: $\pm\frac{n}{m}$, con $n, m \in \mathbb{N}$, $m \neq 0$. Volendo definire delle operazioni sulle frazioni ed in particolare la divisione, ci accorgiamo presto che ci sono più (infinite) frazioni che rappresentano lo stesso numero: sono frazioni *equivalenti,* cioè frazioni $\pm\frac{n}{m}$, $\pm\frac{r}{s}$ tali che $ns = mr$. Dobbiamo quindi "identificare tutte le frazioni equivalenti", cioè considerare l'insieme delle classi di equivalenza rispetto a questa relazione di equivalenza tra frazioni (notiamo che in ogni classe di equivalenza ci sono infinite frazioni tutte riconducibili mediante semplificazione ad una stessa frazione "ridotta ai minimi termini", cioè con numeratore e denominatore primi tra loro, frazione che possiamo eleggere a rappresentante "privilegiato"). In questo modo otteniamo l'insieme $\mathbb{Q}$ dei *numeri razionali,* in cui sono definite le operazioni di somma, opposto, prodotto, reciproco (quest'ultimo solo per numeri diversi da 0).

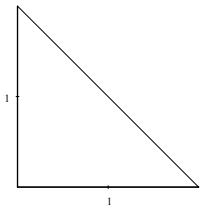
A questo punto abbiamo esteso a sufficienza il nostro insieme di partenza per riuscire ad ottenere sempre (tranne in un caso) una soluzione (in $\mathbb{Q}$) di una qualunque equazione

Un'equazione di 1° grado in un'incognita a coefficienti in $\mathbb{Q}$ (e quindi anche in $\mathbb{N}$ o in $\mathbb{Z}$)

$$ax = b, \text{ con } a, b \in \mathbb{Q} \text{ ha: } \begin{cases} \text{come soluzione } x = \dfrac{b}{a}, \text{ se } a \neq 0 \\ \text{come soluzione ogni } x \in \mathbb{Q}, \text{ se } a = b = 0 \\ \text{nessuna soluzione, } a = 0 \text{ e } b \neq 0. \end{cases}$$

Per poter risolvere in $\mathbb{Q}$ un'equazione del tipo $\boxed{x^2 - 2 = 0}$, dovremmo trovare un numero razionale $\dfrac{p}{q}$ tale che $\left(\dfrac{p}{q}\right)^2 - 2 = 0$, con p e q che possiamo prendere primi tra loro. Avremmo allora che $\left(\dfrac{p}{q}\right)^2 = 2 \Leftrightarrow \dfrac{p^2}{q^2} = 2 \Leftrightarrow p^2 = 2q^2 \Leftrightarrow p^2$ pari $\Leftrightarrow p$ pari, cioè $p = 2k \Leftrightarrow p^2 = 4k^2 \Leftrightarrow 2q^2 = p^2 = 4k^2 \Leftrightarrow q^2 = 2k^2 \Rightarrow q^2$ pari $\Leftrightarrow q$ pari, il che è impossibile, visto che p e q non hanno divisori in comune.

Questa equazione non può quindi avere soluzioni razionali, ma almeno una soluzione deve pure averla, visto che x rappresenta l'ipotenusa di un triangolo rettangolo isoscele di cateto 1, grazie al Teorema di Pitagora: $x^2 = (1)^2 + (1)^2 = 2$:



Allora dove cercare le soluzioni, se non tra i razionali? Apriamo una breve parentesi: ogni numero razionale si può scrivere in forma decimale, o finita o illimitata periodica. Esiste però una terza possibilità: una forma decimale illimitata non periodica, forma che rappresenta un numero *irrazionale*. Ci sono infiniti numeri irrazionali, tra cui il famoso π ed anche il numero di Nepero e, per esempio tutte le radici di indice n di numeri (positivi, nel caso n pari) che non siano potenze n-sime. Aggiungendo a $\mathbb{Q}$ i numeri irrazionali otteniamo l'insieme $\mathbb{R}$ dei numeri reali. Dal punto di vista algebrico, in $\mathbb{R}$ si possono fare somme, opposti, prodotti, reciproci (di reali non nulli) ed in più radici, non tutte però, visto che, se n è pari, $x^n \geq 0$, per ogni x :

$$\begin{cases} n \text{ pari : } \sqrt[n]{x} \text{ è definita solo per } x \geq 0 \\ n \text{ dispari : } \sqrt[n]{x} \text{ è definita per ogni } x \end{cases}.$$

L'estrazione di radici ci permette allora di risolvere in $\mathbb{R}$ l'equazione $x^2 - 2 = 0$, in quanto da $x^2 = 2$ otteniamo che $x = \pm\sqrt{2}$.

Polinomi

Un'espressione (letterale) è una scrittura che indica operazioni o funzioni da eseguire sui numeri o sulle lettere che vi compaiono, dove i numeri appartengono ad un fissato insieme (che pensiamo essere quello dei razionali o dei reali) e le lettere rappresentano numeri di tale insieme: $\frac{\pi x - 2^y}{\cos^2 z + 1}$. Un'espressione si dice *algebrica intera (fratta)* se le operazioni da eseguire sulle lettere sono solo somma, sottrazione, prodotto (e quoziente) : $3a^2b^3 - \frac{2}{3}abc^4, \frac{\sqrt{2}v^2u - 3s^3t}{-4uv(3ts^2)}$. Quindi in un'algebrica intera possono comparire solo potenze con esponente positivo, mentre in una fratta possono comparire anche quelle con esponente negativo, del tipo $a^{-n} = \frac{1}{a^n}$. $\frac{a^2-2b}{3ab}$ è un'espressione algebrica fratta, come pure $3a^2 - 2b^{-3}c$, mentre $3^{-2}a^3c + \frac{2bc^2}{5}$ è algebrica intera.

Si dice *monomio (intero)* un'espressione algebrica (letterale) in cui figurano solo operazioni di prodotto: $3ac^2(-4)b^3\left(\frac{c}{2}\right)^2$. Un monomio si dice *ridotto a forma normale* se si presenta come il prodotto di un unico fattore numerico (detto *coefficiente*) per la sua *parte letterale*, in cui ogni lettera presente compare una sola volta con un esponente positivo: $-3ab^3c^4$. Chiaramente ogni monomio si può ridurre in forma normale,

---

eseguendo i prodotti numerici, e applicando le proprietà delle potenze. Due monomi sono *uguali* quando ridotti in forma normale hanno stesso coefficiente e stessa parte letterale, *simili* se hanno la stessa parte letterale. Si dice *grado di un monomio* la somma degli esponenti delle sue lettere (se non compaiono lettere, ma solo un numero diverso da 0, si dice di grado 0). Il monomio formato dal solo 0 non ha grado. Si può definire *il prodotto* di due monomi qualunque, mentre la somma si può eseguire solo tra monomi simili. Chiamiamo *polinomio* una somma di monomi: $3ab, 2a^2 - 3, 2c - 3ab, 0$ sono tutti polinomi (da notare che consideriamo i monomi come particolari polinomi). Si dice *grado di un polinomio* il massimo dei gradi dei monomi che lo compongono e *grado di un polinomio rispetto ad una lettera* il massimo esponente con cui quella lettera compare nei monomi che lo compongono.Tra polinomi sono possibili le operazioni di somma, differenza e prodotto, che si ottiene dalla somma dei prodotti di tutti i termini (monomi) di un polinomio per tutti i termini dell'altro polinomio. I *"prodotti notevoli"* (quadrato e cubo di un binomio, quadrato di un polinomio, somma per differenza, somma e differenza di cubi, ect) sono ottenuti attraverso l'applicazione della definizione di prodotto, seguita da opportune semplificazioni; sono quindi utili da ricordare per ottenere conti più semplici e per non dover rifare per ogni caso particolare le semplificazioni che valgono per il caso più generale. Sono regole mnemoniche, ma non campate per aria, ed utili per fare i conti! Non solo: conoscere i prodotti notevoli

diventa particolarmente importante quando si vuole compiere l'operazione "opposta" rispetto al prodotto, la *scomposizione di un polinomio in fattori*: prendere un polinomio e volerlo scrivere sotto forma di un prodotto di due o più fattori e quindi è utile quando ci sono da fare quozienti e, se possibile, semplificare. Attenzione all'uso di questa parola: purtroppo con il termine "semplificazione" si indicano operazioni ben diverse, che hanno però lo stesso effetto, cioè quello di rendere l'espressione data più semplice. Questo uso genera spesso confusione negli alunni, quindi è bene specificare ogni volta il tipo di semplificazione che si esegue ed il perchè:

$(a+b)^2 - 2ab + b^2 = a^2 + 2ab + b^2 - 2ab + b^2 = a^2 + 2b^2$, in quanto $2ab - 2ab$ sono termini opposti e la loro SOMMA è 0, quindi non dà contributo in una somma

$$\frac{(a^2 - b^2) - (a-b)}{a-b} = \frac{(a-b)(a+b) - (a-b)}{a-b} = \frac{(a-b)\cdot(a+b-1)}{a-b} = (a+b-1),$$

in quanto $a - b$ è un fattore comune al numeratore e al denominatore e posso cancellarlo sia sopra che sotto ottenendo 1 (e non 0!). Bisogna essere molto chiari e spiegare che questo tipo di semplificazione si può fare solo quando si è in presenza di un prodotto sia sopra che sotto: non capita di rado (purtroppo) vedere miei studenti (I anno Università) che tranquillamente semplificano in questo modo: $\frac{a+b}{b} = a$!

Polinomi in una indeterminata (o incognita)

Sia K un campo ($\mathbb{Q}, \mathbb{R}$) ed x una lettera che rappresenta un'indeterminata. Allora un polinomio di grado n a coefficienti in K è un'espressione del tipo:

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \text{ con } a_i \in K, \quad i = 1, .., n \text{ e } a_n \neq 0.$$

L'insieme di tutti i polinomi in x a coefficienti in K si indica con $K[x]$. Da notare il ruolo profondamente diverso delle lettere in questa espressione: x rappresenta un'incognita (un "buco"), gli a_i, detti *coefficienti* del polinomio, sono da pensarsi dati, nel senso che questa scrittura rappresenta *tutti i polinomi* di grado n su K, al variare dei coefficienti in K, e ogni assegnazione degli a_i dà luogo ad un polinomio: $4x^5 - 3x^4 + x^2 - 5$ è un polinomio di grado 5 con coefficienti $(4, -3, 0, 1, 0, -5)$. Quindi un polinomio di grado n è individuato dalla $n + 1 - pla$ ordinata $(a_n, a_{n-1}, ..., a_1, a_0)$ e due polinomi dello stesso grado sono uguali, per definizione, quando hanno coefficienti di ugual potenza uguali: $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = b_n x^n + b_{n-1} x^{n-1} + ... + b_1 x + b_0 \Leftrightarrow a_i = b_i$, $\forall i = 1, .., n$ (polinomi di diverso grado non possono essere uguali).

Le operazioni di somma e prodotto indicate prima per polinomi generici valgono ovviamente anche per polinomi in $K[x]$, con semplificazioni di calcolo dovuti alla forma

più semplice: la somma, per esempio, tra un polinomio di grado n ed uno di grado m, dove $m \geq n$, si ottiene sommando i coefficienti di potenze di ugual grado fino a grado n e lasciando invariate quelli del polinomio di grado maggiore da $n+1$ a m. $\left(3x^5 - 2x^3 + x - 7\right) + \left(3x^3 - x^2 + 2x + 5\right) = 3x^5 + x^3 - x^2 + 3x - 2$. Per il prodotto possiamo notare che un polinomio in x di grado n moltiplicato per uno di grado m dà luogo ad un polinomio di grado $n+m$. Come per i numeri interi, non è ovunque definita una operazione di divisione: $\frac{x^2-2x}{x+1}$ non dà luogo ad un polinomio intero (mentre $\frac{x^2-2x}{x-2}$ si!). Nel caso di polinomi in un'incognita esiste un algoritmo di divisione del tutto analogo a quello tra interi che permette di dimostrare che, dati due polinomi $f(x)$ e $g(x)$, se il gr$(f) \geq$ gr(g), allora esistono due polinomi $q(x)$ e $r(x)$, detti rispettivamente *quoziente* e *resto* tali che $f(x) = g(x) \cdot q(x) + r(x)$, con gr$(r) <$ gr(g), oppure $r(x) = 0$. In quest'ultimo caso, cioè quando il resto è nullo, si dice che $f(x)$ è *divisibile* per $g(x)$ o che $g(x)$ è un *divisore* di $f(x)$ e vale allora che $f(x) = g(x) \cdot q(x)$ (e allora anche $q(x)$ è divisore).

Caso semplice si ottiene quando si divide per un polinomio di I grado, del tipo $x - \alpha$. In questo caso, c'è un teorema (*Teorema del resto*) che ci permette di conoscere il resto di tale divisione senza eseguirla:

Il resto della divisione del polinomio $f(x)$ per $x - \alpha$ coincide con il valore $f(\alpha)$.

Infatti $f(x) = (x - \alpha) \cdot q(x) + r$ e quindi $f(\alpha) = (\alpha - \alpha) \cdot q(\alpha) + r = 0 + r = r$.

Se chiamiamo *radice* in K di $f(x) \in K[x]$ un numero $\alpha \in K$ tale che $f(\alpha) = 0$, (per cui α è radice del polinomio $f(x)$ se e solo α è soluzione della equazione algebrica $f(x) = 0$) otteniamo come corollario che

Il numero α è radice del polinomio $f(x)$ se e solo $f(x)$ è divisibile per $x - \alpha$.

Se un polinomio ha radici α e β, sarà divisibile per $(x - \alpha)$ e per $(x - \beta)$, quindi per $(x - \alpha) \cdot (x - \beta)$. Quindi se $\alpha_1, \alpha_2, ..., \alpha_k$ sono k radici distinte di un polinomio $f(x)$, allora $(x - \alpha_1) \cdot (x - \alpha_2) \cdot .... \cdot (x - \alpha_k)$, che ha grado k, divide $f(x)$ e quindi gr$(f) \geq k$. Come conseguenza immediata otteniamo che:

Un polinomio di grado n non può avere più di n radici distinte.*

*[In $\mathbb{Q}$ ed in $\mathbb{R}$ ci sono polinomi che non ammettono radici razionali o reali: $x^2 + 1$ ne è il più classico esempio. In realtà si può estendere $\mathbb{R}$ al campo $\mathbb{C}$ *dei numeri complessi*, in cui vale il seguente: *Teorema fondamentale dell'algebra*. Ogni polinomio di grado n a coefficienti in $\mathbb{C}$ ha in $\mathbb{C}$ n radici (ognuna contata con la propria molteplicità).]

Consideriamo ora un polinomio $f(x) \in \mathbb{R}[x]$ di grado n, cioè con coefficienti reali. Ci interessa sapere se ha delle radici reali ed, in tal caso, quante e, come obiettivo massimale, quali. Il problema è completamente risolto nel caso di $n = 2$, dove sappiamo esistere una formula risolutiva per un'equazione di II grado ad un'incognita a coefficienti in $\mathbb{R}$ del tipo

$$\boxed{ax^2 + bx + c = 0 \qquad (\diamondsuit)}$$

con $a \neq 0$, (altrimenti si torna al caso di I grado). Se vale la condizione $\boxed{b^2 - 4ac \geq 0 \quad (\clubsuit)}$, si ottiene la ben nota formula risolutiva $x_{1,2} = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.

[Infatti, questa equazione può essere scritta attraverso un semplice completamento di quadrati come:

$$ax^2+bx+c = a(x^2+\tfrac{b}{a}x+\tfrac{c}{a}) = a\left[x^2+\tfrac{b}{a}x+\left(\tfrac{b}{2a}\right)^2-\left(\tfrac{b}{2a}\right)^2+\tfrac{c}{a}\right] =$$
$$a\left[\left(x+\tfrac{b}{2a}\right)^2-\tfrac{b^2-4ac}{4a^2}\right] = 0 \iff \left(x+\tfrac{b}{2a}\right)^2 = \tfrac{b^2-4ac}{4a^2}$$

La prima osservazione da farsi è che se cerchiamo soluzioni reali, $\frac{b^2-4ac}{4a^2}$ deve necessariamente essere positivo o nullo, in quanto il quadrato di un qualunque reale è positivo o nullo. Otteniamo quindi una

condizione per avere soluzioni reali: $\boxed{b^2 - 4ac \geq 0 \quad (\clubsuit)}$. Una volta verificatesi questa condizione, per risolvere l'equazione abbiamo bisogno di estrarre radice quadrata, che nel campo reale si può fare, a patto che il radicando sia positivo o nullo, cosa vera grazie a $(\clubsuit)$: $x + \frac{b}{2a} = \pm\sqrt{\frac{b^2-4ac}{4a^2}} \iff x = \frac{-b\pm\sqrt{b^2-4ac}}{2a} \in R$.]

Cosa succede quando il grado del polinomio cresce? Per quanto riguarda il grado 3, c'è una formula dovuta a Cardano che permette di trovare le soluzioni di un'equazione di terzo grado:

$$x = \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

Per il quarto grado abbiamo una formula analoga, anche se ancora più complicata, che esprime le soluzioni per mezzo di radicali. Da notare che, se il metodo per risolvere le equazioni di 2^o grado era noto già agli antichi greci, per arrivare a queste formule si è dovuto aspettare fino al XVI secolo. E per i successivi tre secoli si è cercato di trovare formule analoghe esprimenti le radici di un polinomio di grado 5 mediante (somma, prodotto, quoziente e) radicali dei suoi coefficienti, fino a quando, intorno al 1820, Abel

dimostrò che non può esistere una tale formula per un generico polinomio di grado $n \geq 5$. In altri termini Abel dimostrò che un generico polinomio di grado $n \geq 5$ non è *risolubile per radicali* (come invece accade per i polinomi di grado inferiore). Questo non vuol dire che per particolari polinomi ciò non possa accadere, ma solo che non vale per tutti. Dopo una decina d'anni, Galois trovò una completa caratterizzazione delle condizioni a cui devono soddisfare polinomi di grado $n \geq 5$ per essere risolubili per radicali, trovando esplicitamente polinomi che non possono essere risolti per radicali (come ad esempio, $x^5 - 4x - 2$: in tal caso, si possono trovare soluzioni approssimate, mediante vari algoritmi numerici ed analitici, in questo caso $x \simeq -1.24, -0.51, 1.52$). Il lavoro di Galois (morto in un duello a soli 21 anni) fu fondamentale per la nascita e lo sviluppo dell'algebra moderna, ma questa è un'altra storia.

Equazioni

Abbiamo visto il caso delle equazioni (od algebriche intere) in un'incognita. Ma cos'è un'equazione? In modo molto generale, possiamo dire che *un'equazione è un'uguaglianza tra due espressioni che contengono una o più incognite*, che rappresentano elementi (all'inizio sconosciuti) in un certo insieme che, una volta determinati (sempre che esistano) e sostituiti nell'equazione, soddisfano l'uguaglianza tra le due espressioni date. In particolare, se le espressioni che compaiono in questa uguaglianza sono polinomi interi, avremo a che fare con *equazioni algebriche*; se le incognite che compaiono sono $x_1, x_2, ..., x_n$ avremo a che fare con equazioni in $x_1, x_2, ..., x_n$. Da notare che se nelle espressioni compaiono più lettere, bisogna specificare a priori quali sono le incognite e quali fungono da parametro o coefficiente. Ad esempio, l'uguaglianza che dà l'area A di un rettangolo di base b e altezza h, data da $A = b \cdot h$, diventa un'equazione nell'incognita A se conosciamo b e h, mentre è un'equazione in b, se conosciamo A e h. (perchè quindi dover sempre imparare le cosiddette "formule inverse", una o più d'una per ogni formula diretta, quando si può imparare una volta per tutte a risolvere le equazioni?). Da qui l'importanza di non dare peso al "nome" delle incognite, ma alla sostanza, cioè al fatto che le incognite rappresentano dei "vuoti" che si cerca di riempire con elementi di un dato insieme in cui si cercano le soluzioni e di solito tale

insieme dipende dal problema. Per esempio se vogliamo sapere quante arance ha mangiato Mario, sapendo che in totale erano 12 e che Giovanni ne ha mangiate il doppio di Mario,indicando con x il numero di arance mangiate da Mario, necessariamente la soluzione del problema $x + 2x = 12$ va ricercata in $\mathbb{N}$, visto che si richiede un numero intero. In tal senso la soluzione del problema predente partendo da 10 arance in totale non ha soluzioni in $\mathbb{N}$, ma solo in $\mathbb{Q}$, visto che la soluzione diventa $x = \frac{10}{3}$ (soluzione che diventa accettabile per il nostro problema solo se pensiamo di riuscire a dividere un'arancia in tre parti uguali!). Data quindi un'equazione, sostituendo al posto delle incognite numeri appartenenti ad un dato insieme, si ottiene un'uguaglianza tra due numeri che può risultare vera o falsa. Si chiama *soluzione* in K di un'equazione in $x_1, x_2, ..., x_n$ una $n - pla$ di numeri $(k_1, k_2, ..., k_n) \in K^n$ che, sostituiti (con ordine!) nell'equazione si ottenga un'uguaglianza numerica vera, cioè tali da *verificare (o soddisfare*) l'equazione. Risolvere in $K = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ un'equazione nelle incognite $x_1, x_2, ..., x_n$ significa trovare soluzioni dell'equazione che appartengono a K. Ci sono vari casi :

1) Se non esistono soluzioni che appartengono a K, l'equazione è impossibile in K, mentre, se non esistono soluzioni in alcun insieme, l'equazione si dirà *impossibile.*

$x+3 = 0$, $2x+3y+2 = 0$ sono impossibili in $\mathbb{N}$, ma non in $\mathbb{Z}$, mentre $(x + 1)^2 = x^2+2x$ è impossibile in ogni insieme.

2) Se esistono soluzioni che appartengono a K, l'equazione si dice *risolubile in* K. In particolare si dirà *determinata*, se ammette un numero finito di soluzioni, indeterminata se ne ammette un numero *infinito*. $x + 3 = 0, 2x + 3y = 0$ sono rispettivamente determinata ed indeterminata in $\mathbb{Z}$.

3) Se l'equazione in $x_1, x_2, ..., x_n$ viene verificata da qualunque $n - pla$ di numeri $(k_1, k_2, ..., k_n)$ reali, si dirà un'*identità*: $(x + y)^2 = x^2 + 2xy + y^2, x = x, 0x^3 = 0$, sono tutti esempi di identità.

Attenzione a non confondere le equazioni indeterminate con le equazioni identiche, in quanto nel caso algebrico ad un'incognita vanno a coincidere, ma con più incognite sono ben diverse:

$2x + 3y = 0$ ha infinite soluzioni, tutte le coppie del tipo $(3k, -2k)$, ma non è un'identità: $(1, 3)$ non la soddisfa!

Risoluzione di equazioni

Per risolvere equazioni, si cerca di ridurre l'equazione data ad un'equazione più semplice, ma *equivalente* a quella di partenza, cioè che abbia le stesse soluzioni. Per ottenere ciò, si utilizzano i famosi "principi di equivalenza", che si possono enunciare in varie forme:

I Principio di equivalenza: aggiungendo o sottraendo *uno stesso numero* ad entrambi i membri di un'equazione, si ottiene un'equazione equivalente alla data.

II Principio di equivalenza: moltiplicando o dividendo per *uno stesso numero diverso da zero* entrambi i membri di un'equazione, si ottiene un'equazione equivalente alla data.

Oppure:

I Principio di equivalenza: aggiungendo o sottraendo *una stessa espressione* ad entrambi i membri di un'equazione, si ottiene un'equazione equivalente alla data.

In questo caso non ci sono problemi solo l'espressione che si aggiunge o si toglie non modifica il campo di variabilità delle incognite che compaiono nell'equazione data:

$2x + 1 = \frac{x}{3} - 4$ NON è equivalente a $2x + 1 + \sqrt{x} = \frac{x}{3} - 4 + \sqrt{x}$, in quanto l'unica soluzione ($x = -3$) della prima non appartiene al campo di variabilità dell'incognita della seconda ($x \geq 0$). Ovviamente questo problema non sussiste se l'espressione da aggiungere e togliere è un polinomio intero (dove l'incognita varia su tutto il campo).

A maggior ragione nascono problemi se esprimiamo il II Principio di equivalenza in modo analogo:

Moltiplicando o dividendo per *una stessa espressione diversa da zero* ad entrambi i membri di un'equazione, si ottiene un'equazione equivalente alla data.

$x - 2 = 1$ NON è equivalente a $(x - 2)(x + 2) = x + 2$,perché la seconda ha la radice $x = -2$, assente nella prima. Si è infatti moltiplicato per il fattore $C = x + 2$, che si annulla per $x = -2$.

$2x = 4$ ammette la soluzione $x = 2$ mentre l'equazione $2x\sqrt{x-3} = 4\sqrt{x-3}$ non ammette soluzioni.

Per quanto riguarda la trattazione delle equazioni di I grado, intere o fratte, per non correre rischi basterà usare il I principio nella seconda forma (serve anche aggiungere o togliere monomi del tipo kx) ed il II nella prima (serve solo dividere per il coefficiente dell'incognita, quando diverso da zero).

Problemi da risolvere con equazioni

A parte la ovvia osservazione che sarebbe opportuno partire da problemi concreti proprio per introdurre le equazioni, ovviamente si possono (e si devono) riprendere dopo aver svolto la parte relativa alla risoluzione delle equazioni. Attenzione comunque alla scelta dei problemi, soprattutto quelli introduttivi.

Problema 1. Gianni ha 3 anni e suo padre 25. Tra quanti anni l'età del padre sarà il triplo di quella del figlio?

Problema 2. Due fratelli hanno complessivamente 28 anni. Qual è l'età di ciascuno dei due fratelli, se gli anni del minore sono i 3/4 di quelli del maggiore?

Questi 2 problemi presentano aspetti differenti: nel primo caso c'è solo un dato incognito, il numero di anni necessario affinché venga verificata l'unica condizione richiesta: l'età del padre diventi il triplo di quella del figlio. Chiamando x (o anche n, visto che stiamo cercando un numero intero) tale dato incognito, otterremo immediatamente l'equazione risolutiva, cioè: $(x + 25) = 3\,(3 + x)$,cioè $x = 8$. Nel secondo caso ci sono 2 dati incogniti, l'età del minore, x, e l'età del maggiore, y, che sono legati da due condizioni, che devono valere contemporaneamente, cioè $x + y = 28$ e $x = \frac{3}{4}y$. Quindi siamo di fronte ad un *sistema di due equazioni in due incognite:* $\begin{cases} x + y = 28 \\ x = \frac{3}{4}y \end{cases}$, che ovviamente ha come immediata equazione risolutiva un'equazione in una sola incognita (che può essere sia x che y) $\frac{3}{4}y + y = 28$, da cui $y = 16$ e sostituendo nella seconda equazione risolviamo $x = \frac{3}{4}16 = 12$.

Concettualmente i due problemi sono molto diversi e come tali devono essere proposti agli alunni. In realtà i libri di testo sono pieni di tali problemi, ma non trattano assolutamente i sistemi due equazioni in due incognite!