Indice

1. Insiemi 2
1.1. Definizione di insieme 2
1.2. Corrispondenze e relazioni 5
1.3. Funzioni 7
2. Numeri interi 10
2.1. Sistemi numerici 10
2.2. Divisione 12
2.3. Basi 15
2.4. Teorema Fondamentale dell'Aritmetica 16
2.5. Equazioni Diofantee 19
2.6. Congruenza Modulo n 21
2.7. Congruenze lineari 23

1. Insiemi

1.1. Definizione di insieme

Prende il nome di **insieme** una qualsiasi collezione di oggetti, detti *elementi* o *membri* dell'insieme. In genere, gli insiemi vengono denotati con le lettere maiuscole dell'alfabeto latino, mentre i loro elementi con le lettere minuscole. Per indicare che l'oggetto a é membro dell'insieme A viene usata la notazione $a \in A$, e si dice che a *appartiene* ad A.
Per rappresentare gli elementi che appartengono ad un insieme é possibile sia in maniera **estensionale**, ovvero semplicemente "elencandoli", oppure in maniera **intensionale**, ovvero specificando una certa proprietá che é posseduta da tutti ed i soli elementi di quell'insieme. Formalmente, viene usata questa notazione:

$$\underbrace{A = \{a_1, a_2, a_3, ...\}}_{\text{forma estensionale}} \qquad \underbrace{A = \{a : a \text{ possiede la proprietá caratteristica di } A\}}_{\text{forma intensionale}}$$

Esempio 1.1.1: Sia A l'insieme che contiene i colori che possono comparire in un pixel. A puó venire descritto equivalentemente nei due modi:

$$A = \{\text{rosso}, \text{verde}, \text{blu}\} \qquad A = \{a : a \text{ é uno dei colori presenti in un pixel}\}$$

Si noti come un insieme possa essere a sua volta trattato come un oggetto, e quindi essere membro di un'altro insieme. Inoltre, non é ammesso che un insieme contenga piú "copie" dello stesso oggetto. Infine, l'ordine in cui gli elementi di un insieme sono disposti non é rilevante.
Dato un insieme A, il numero di elementi che questo contiene é detto **cardinalitá** e si indica con $|A|$. La cardinalitá di un insieme puó essere sia *finita* che *infinita*, pertanto é ammesso che un insieme possa contenere infiniti elementi.
Siano A e B due insiemi. Si dice che B é un **sottoinsieme** di A se ogni membro di B é anche membro di A, e si indica con $B \subseteq A$. Equivalentemente, si dice che A é un **soprainsieme** di B se ogni membro di B é anche membro di A, e si indica con $A \supseteq B$. Formalmente:

$$B \subseteq A \text{ se e solo se } \forall x \in B, x \in A \qquad A \supseteq B \text{ se e solo se } \forall x \in B, x \in A$$

Due insiemi A e B sono **uguali** se contengono gli stessi elementi, ovvero se $A \subseteq B$ e $B \subseteq A$, e si indica con $A = B$. Due insiemi A e B sono diversi se esiste almeno un elemento di A che non é contenuto in B oppure se esiste almeno un elemento di B non contenuto in A, e si indica con $A \neq B$. Si noti come non sia ammesso che due insiemi siano uguali e distinti. Ovvero, se per due insiemi A e B vale $A = B$, allora A e B sono lo stesso insieme.
Siano A e B due insiemi. Se B é un sottoinsieme di A ed al contempo non é uguale ad A si dice che B é un **sottoinsieme proprio** di A, e si indica con $B \subset A$. Equivalentemente, se A é un soprainsieme di B ed al contempo non é uguale a B, si dice che A é un **soprainsieme proprio** di B, e si indica con $A \supset B$. Formalmente:

$$B \subset A \text{ se e solo se } \forall x \in B, x \in A \ \text{ e } B \neq A \qquad A \supset B \text{ se e solo se } \forall x \in B, x \in A \ \text{ e } B \neq A$$

Per indicare che l'insieme B *non* é un sottoinsieme di A viene usata la notazione $B \nsubseteq A$, mentre per indicare che B *non* é un sottoinsieme proprio di A viene usata la notazione $B \not\subset A$. Similmente, per indicare che l'insieme A *non* é un soprainsieme di B viene usata la notazione $A \nsupseteq B$, mentre per indicare che A *non* é un soprainsieme proprio di B viene usata la notazione $A \not\supset B$.

Lemma 1.1.1: Per qualsiasi insieme A valgono: $A \subseteq A$, $A \supseteq A$, $A = A$, $A \not\subset A$, $A \not\supset A$.

Dimostrazione:

1. Per definizione, $A \subseteq A$ se e solo se $\forall x \in A, x \in A$. Essendo $\forall x \in A, x \in A$ una tautologia, si ha $A \subseteq A$;
2. Analoga alla precedente;
3. Dato che $A \subseteq A$ e $A \supseteq A$, si ha $A = A$;

4. Dato che $A \subseteq A$ e $A = A$, si ha $A \not\subset A$;
5. Analoga alla precedente.

$\square$

L'insieme che non contiene alcun elemento viene detto **insieme vuoto**, e si indica con $\emptyset$ oppure con $\{\}$.

Lemma 1.1.2: L'insieme vuoto é sottoinsieme di ogni insieme (compreso di sé stesso).

Dimostrazione: Dato un qualsiasi insieme A, $\emptyset$ é un sottoinsieme di A se ogni membro di $\emptyset$ é anche membro di A. Dato che $\emptyset$ é l'insieme che non ha alcun membro, di fatto rispetta sempre questa definizione, anche nel caso in cui $A = \emptyset$. $\square$

A partire da un insieme A é possibile costruire l'**insieme potenza** di A, o **insieme delle parti** di A, come l'insieme che contiene tutti i sottoinsiemi di A. L'insieme potenza di A viene indicato con $\mathcal{P}(A)$.

Lemma 1.1.3: Per qualsiasi insieme A (compreso $\emptyset$), valgono $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$.

Dimostrazione: Dal Lemma 1.1.1 si ha $\emptyset \subseteq A$, mentre dal Lemma 1.1.2 si ha $A \subseteq A$. Avendo definito $\mathcal{P}(A)$ come l'insieme che contiene tutti i sottoinsiemi di A, $\mathcal{P}(A)$ conterrá certamente (almeno) questi due. $\square$

Esempio 1.1.2: Sia $A = \{\text{rosso}, \text{verde}, \text{blu}\}$. Si ha:

$$\mathcal{P}(A) = \{\emptyset, \{\text{rosso}\}, \{\text{verde}\}, \{\text{blu}\}, \{\text{rosso}, \text{verde}\}, \{\text{rosso}, \text{blu}\}, \{\text{verde}, \text{blu}\}, \{\text{rosso}, \text{verde}, \text{blu}\}\}$$

Dati due insiemi A e B, viene detto **unione** di A e di B l'insieme che contiene tutti gli elementi o di A o di B, e si indica con $A \cup B$:

$$A \cup B = \{x : x \in A \vee x \in B\}$$

Si noti come "$\vee$" non vada inteso in senso disgiuntivo. Ovvero, un certo elemento x appartiene ad $A \cup B$ se appartiene ad A, se appartiene a B oppure se appartiene ad entrambi.

Esempio 1.1.3: Siano $A = \{\text{rosso}, \text{verde}, \text{blu}\}$ e $B = \{\text{verde}, \text{giallo}, \text{rosa}, \text{nero}\}$. Si ha:

$$A \cup B = \{\text{rosso}, \text{verde}, \text{blu}, \text{giallo}, \text{rosa}, \text{nero}\}$$

Dati due insiemi A e B, viene detto **intersezione** di A e di B l'insieme che contiene tutti gli elementi di A e di B, e si indica con $A \cap B$:

$$A \cap B = \{x : x \in A \wedge x \in B\}$$

Si noti come "$\wedge$" vada inteso in senso disgiuntivo. Ovvero, un certo elemento x appartiene ad $A \cap B$ se e soltanto se appartiene contemporaneamente sia ad A che a B.
Se l'intersezione di due insiemi é l'insieme vuoto, ovvero se non esiste alcun elemento che sia presente contemporaneamente in entrambi gli insiemi, si dice che tali insiemi sono **disgiunti**.

Esempio 1.1.4: Siano $A = \{\text{rosso}, \text{verde}, \text{blu}\}$ e $B = \{\text{verde}, \text{giallo}, \text{rosa}, \text{nero}\}$. Si ha:

$$A \cap B = \{\text{verde}\}$$

É possibile generalizzare l'unione di k insiemi $A_1, A_2, A_3, ..., A_k$ come l'insieme che contiene tutti gli x che compaiono in almeno uno dei k insiemi:

$$\bigcup_{i=1}^{k} A_i = (...(A_1 \cup (A_2 \cup (A_3 \cup ...)))) \cup A_k = \{x : \exists i \in \{1, 2, ..., k\} : x \in A_i\}$$

Allo stesso modo, é possibile generalizzare l'intersezione di k insiemi $A_1, A_2, A_3, ..., A_k$ come l'insieme che contiene tutti gli x che compaiono in tutti e k gli insiemi:

$$\bigcap_{i=1}^{k} A_i = (...(A_1 \cap (A_2 \cap (A_3 \cap ...)))) \cap A_k = \{x : x \in A_i \forall i \in \{1, 2, ..., k\}\}$$

Lemma 1.1.4: Siano A, B e C tre insiemi. Per la loro unione e la loro intersezione valgono le proprietá:

Commutativa:
- $A \cap B = B \cap A$;
- $A \cup B = B \cup A$.

Associativa:
- $(A \cap B) \cap C = A \cap (B \cap C)$;
- $(A \cup B) \cup C = A \cup (B \cup C)$.

Distributiva:
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Il risultato viene generalizzato a k insiemi.

Dati due insiemi A e B, viene detta **differenza** di A e B l'insieme che contiene tutti gli elementi di A che non sono contenuti in B, e si indica con $A \setminus B$:

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

Siano A e B due insiemi tali per cui $B \subseteq A$. L'insieme $A - B$ viene detto **complemento** di B rispetto ad A, e si indica con $\overline{B}$. Quando é noto dal contesto rispetto a quale insieme un certo insieme viene complementato, questo viene omesso.

Teorema 1.1.1 (Leggi di De Morgan): Siano A e B due sottoinsiemi di un certo insieme U. Si ha:

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \qquad \overline{A \cup B} = \overline{A} \cap \overline{B}$$

Il risultato viene generalizzato a k insiemi.

Siano A e B due insiemi. Viene detto **prodotto cartesiano** di A e di B l'insieme costituito da tutte le possibili coppie ordinate costruite a partire dagli elementi di A e di B, e si indica con $A \times B$.

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

Esempio 1.1.5: Siano $A = \{\text{rosso}, \text{verde}, \text{blu}\}$ e $B = \{\text{verde}, \text{giallo}, \text{rosa}, \text{nero}\}$. Si ha:

$$\begin{aligned} A \times B = \{&(\text{rosso}, \text{verde}), (\text{rosso}, \text{giallo}), (\text{rosso}, \text{rosa}), (\text{rosso}, \text{nero}), \\ &(\text{verde}, \text{verde}), (\text{verde}, \text{giallo}), (\text{verde}, \text{rosa}), (\text{verde}, \text{nero}), \\ &(\text{blu}, \text{verde}), (\text{blu}, \text{giallo}), (\text{blu}, \text{rosa}), (\text{blu}, \text{nero})\} \end{aligned}$$

Il prodotto cartesiano fra due insiemi puó essere generalizzato a k insiemi $A_1, A_2, ..., A_k$ come all'insieme costruito da tutte le possibili k-uple ordinate costruite a partire dagli elementi di ogni A_i per $i = \{1, ..., k\}$:

$$\prod_{i=1}^{k} A_i = A_1 \times A_2 \times ... \times A_k = \{(a_1, a_2, ..., a_k) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge ... \wedge a_k \in A_k\}$$

Nel caso particolare in cui tutti e k gli insiemi $A_1, A_2, ..., A_k$ siano tutti uguali ad un certo insieme A, per indicare il loro prodotto cartesiano si scrive semplicemente A^k.

1.2. Corrispondenze e relazioni

Dati due insiemi A e B, viene detta **corrispondenza** fra A e B un sottoinsieme $\mathcal{R}$ del loro prodotto cartesiano; nel caso particolare in cui $A = B$, viene detta **relazione** su A.
Dato un insieme A ed una relazione $\mathcal{R}$ su A, per indicare che una coppia $(a, b) \in A \times A$ appartiene a $\mathcal{R}$ si usa dire che a é in *relazione* con b e si usa la dicitura $a\mathcal{R}b$.

Esempio 1.2.1: Sia $A = \{\text{rosso}, \text{verde}, \text{blu}\}$. Si ha:

$$\begin{aligned} A \times A = \{&(\text{rosso}, \text{rosso}), (\text{rosso}, \text{verde}), (\text{rosso}, \text{blu}), (\text{verde}, \text{rosso}), \\ &(\text{verde}, \text{verde}), (\text{verde}, \text{blu}), (\text{blu}, \text{rosso}), (\text{blu}, \text{verde}), (\text{blu}, \text{blu})\} \end{aligned}$$

Una relazione $\mathcal{R}$ su A potrebbe essere:

$$\mathcal{R} \subseteq A \times A = \{(\text{rosso}, \text{rosso}), (\text{rosso}, \text{verde}), (\text{verde}, \text{verde}), (\text{blu}, \text{verde})\}$$

Dato un insieme A ed una relazione $\mathcal{R}$ su di esso, si dice che $\mathcal{R}$ é una relazione:

- **riflessiva** se $\forall a \in A$ si ha $a\mathcal{R}a$;
- **simmetrica** se $\forall a, b \in A$ $a\mathcal{R}b$ implica $b\mathcal{R}a$;
- **transitiva** se $\forall a, b, c \in A$ $a\mathcal{R}b$ e $b\mathcal{R}c$ implicano $a\mathcal{R}c$;
- **antisimmetrica** se $\forall a, b \in A$ $a\mathcal{R}b$ e $b\mathcal{R}a$ implicano $a = b$.

Una relazione puó rientrare in una, piú di una o anche nessuna di queste categorie.

Esempio 1.2.2: Sia $A = \{\text{rosso}, \text{verde}, \text{blu}\}$. Sia:

$$\mathcal{R}_1 = \{(\text{rosso}, \text{rosso}), (\text{verde}, \text{verde}), (\text{rosso}, \text{verde}), (\text{verde}, \text{rosso}), (\text{verde}, \text{blu})\}$$

- Non é riflessiva, perché $(\text{blu}, \text{blu}) \notin \mathcal{R}_1$;
- Non é simmetrica, perché $(\text{verde}, \text{blu}) \in \mathcal{R}_1$ ma $(\text{blu}, \text{verde}) \notin \mathcal{R}_1$;
- Non é transitiva, perché $(\text{rosso}, \text{verde}) \in \mathcal{R}_1$ e $(\text{verde}, \text{blu}) \in \mathcal{R}_1$ ma $(\text{blu}, \text{rosso}) \notin \mathcal{R}_1$;
- Non é antisimmetrica, perché $(\text{rosso}, \text{verde}) \in \mathcal{R}_1$ e $(\text{verde}, \text{rosso}) \in \mathcal{R}_1$ ma $\text{rosso} \neq \text{verde}$.

Sia invece:

$$\begin{aligned} \mathcal{R}_2 = \{&(\text{rosso}, \text{rosso}), (\text{verde}, \text{verde}), (\text{blu}, \text{blu}), (\text{rosso}, \text{verde}), \\ &(\text{verde}, \text{rosso}), (\text{verde}, \text{blu}), (\text{blu}, \text{verde}), (\text{rosso}, \text{blu}), (\text{blu}, \text{rosso})\} \end{aligned}$$

Tale relazione é riflessiva, simmetrica e transitiva, ma non é antisimmetrica. Sia infine:

$$\mathcal{R}_3 = \{(\text{rosso}, \text{rosso}), (\text{verde}, \text{verde}), (\text{blu}, \text{blu})\}$$

Tale relazione é riflessiva, simmetrica, transitiva e antisimmetrica.

Dato un insieme A, una relazione $\mathcal{R}$ su A che é (almeno) simmetrica, riflessiva e transitiva viene detta **relazione di equivalenza**. Le relazioni di equivalenza vengono anche spesso indicate con il simbolo $\sim$.
Siano A un insieme e $\sim$ una relazione di equivalenza su A. Preso un qualsiasi elemento $a \in A$, si definisce **classe di equivalenza** di a rispetto ad $\sim$ l'insieme:

$$[a]_{\sim} = \{b : b \in A \land b \sim a\}$$

Ovvero, l'insieme che contiene tutti gli elementi di A che sono in relazione con a. Un qualsiasi elemento di una classe di equivalenza viene detto **rappresentante** di tale classe.

Esempio 1.2.3: Sia $A = \{\text{rosso}, \text{verde}, \text{blu}, \text{giallo}\}$. Si consideri la relazione di equivalenza:

$$\begin{aligned} \sim \ = \{&(\text{rosso}, \text{rosso}), (\text{verde}, \text{verde}), (\text{blu}, \text{blu}), (\text{giallo}, \text{giallo}), (\text{rosso}, \text{giallo}), \\ &(\text{giallo}, \text{blu}), (\text{rosso}, \text{blu}), (\text{blu}, \text{rosso}), (\text{giallo}, \text{rosso}), (\text{blu}, \text{giallo})\} \end{aligned}$$

Si hanno le seguenti quattro classi di equivalenza:

$$[\text{verde}]_\sim = \{\text{verde}\} \qquad [\text{blu}]_\sim = [\text{giallo}]_\sim = [\text{rosso}]_\sim = \{\text{rosso}, \text{giallo}, \text{blu}\}$$

Lemma 1.2.1: Per qualsiasi insieme A, per qualsiasi relazione di equivalenza $\sim$ su A e per qualsiasi $a \in A$, si ha $[a]_\sim \neq \emptyset$.

Dimostrazione: Essendo $\sim$ una relazione di equivalenza, deve essere anche riflessiva, ovvero deve valere $a \sim a$. Pertanto, $[a]_\sim$ deve contenere almeno a, e quindi non é un insieme vuoto. □

Lemma 1.2.2: Siano A un insieme non vuoto e $\sim$ una relazione di equivalenza su A. Per ogni $a, b \in A$, si ha $[a]_\sim = [b]_\sim$ oppure $[a]_\sim \cap [b]_\sim = \emptyset$. Ovvero, o le classi di equivalenza di a e di b sono lo stesso insieme o sono due insiemi disgiunti.

Dimostrazione: Si supponga $[a]_\sim \cap [b]_\sim \neq \emptyset$, e sia $c \in [a]_\sim \cap [b]_\sim$. Per definizione di intersezione, si ha $c \in [a]_\sim$ e $c \in [b]_\sim$, ma questo equivale a dire $c \sim a$ e $c \sim b$. Essendo $\sim$ una relazione di equivalenza, deve essere simmetrica, pertanto valendo $c \sim a$ vale anche $a \sim c$. Per lo stesso motivo, deve essere anche transitiva, pertanto valendo $a \sim c$ e $c \sim b$ allora vale anche $a \sim b$, cioè $a \in [b]_\sim$. Essendo $\sim$ simmetrica, se vale $a \sim b$ allora vale anche $b \sim a$.
Sia $x \in A$ un elemento generico per cui vale $x \in [a]_\sim$, ovvero $x \sim a$. Avendo provato che vale $a \sim b$ ed essendo $\sim$ transitiva, vale anche $x \sim b$, ovvero $x \in [b]_\sim$. Essendo x un elemento generico, significa che questa proprietá vale per qualsiasi elemento di $[a]_\sim$, ovvero che qualsiasi elemento di $[a]_\sim$ é anche elemento di $[b]_\sim$. In altre parole, $[a]_\sim \subseteq [b]_\sim$.
Sia $y \in A$ un elemento generico per cui vale $y \in [b]_\sim$, ovvero $y \sim b$. Avendo provato che vale $b \sim a$ ed essendo $\sim$ transitiva, vale anche $y \sim a$, ovvero $y \in [a]_\sim$. Essendo y un elemento generico, significa che questa proprietá vale per qualsiasi elemento di $[b]_\sim$, ovvero che qualsiasi elemento di $[b]_\sim$ é anche elemento di $[a]_\sim$. In altre parole, $[b]_\sim \subseteq [a]_\sim$.
Avendo provato che vale sia $[a]_\sim \subseteq [b]_\sim$ sia $[b]_\sim \subseteq [a]_\sim$, per definizione di uguaglianza fra insiemi vale $[a]_\sim = [b]_\sim$. É stato allora provato che se $[a]_\sim \cap [b]_\sim \neq \emptyset$, allora $[a]_\sim = [b]_\sim$. Ma questa proposizione equivale ad asserire che vale o $[a]_\sim = [b]_\sim$ o $[a]_\sim \cap [b]_\sim = \emptyset$, e pertanto il lemma é provato. □

Dato un insieme A ed una relazione di equivalenza $\sim$ su A, viene detto **insieme quoziente** l'insieme $A/\sim$ che contiene tutte le classi di equivalenza (distinte) di $\sim$. Ovvero:

$$A/\sim \ = \left\{[a]_\sim, a \in A\right\}$$

Esempio 1.2.4: Nell'Esempio 1.2.3 si ha $A/\sim \ = \left\{[\text{blu}]_\sim, [\text{verde}]_\sim\right\}$.

Sia A un insieme diverso da $\emptyset$, e sia $\mathcal{F} = \{X_1, X_2, \ldots, X_k\}$ un insieme che contiene k sottoinsiemi di A. $\mathcal{F}$ viene detto **partizione** di A se:

- $\forall i \in \{1, \ldots, k\}$, si ha $X_i \neq \emptyset$;
- $\forall i, j \in \{1, \ldots, k\}$ si ha $X_i \cap X_j = \emptyset$. Ovvero, ciascun sottoinsieme é disgiunto da tutti gli altri;

- $\bigcup_{i=1}^{k} X_i = A$. Ovvero, l'unione di tutti i sottoinsiemi restituisce l'insieme di partenza.

Esempio 1.2.5: Sia $A = \{\text{rosso, verde, blu, giallo, rosa, nero, bianco, grigio}\}$. Una possibile partizione di tale insieme é data da:

$$\mathcal{F} = \{X_1, X_2, X_3\} = \{\{\text{rosso, nero, bianco, giallo, grigio}\}, \{\text{verde, blu}\}, \{\text{rosa}\}\}$$

Teorema 1.2.1 (Equivalenza fra insieme quoziente e partizioni): Sia A un insieme e sia $\sim$ una relazione di equivalenza su A. L'insieme quoziente $A/\sim$ determina una partizione su A. Allo stesso modo, sia $\mathcal{F} = \{X_1, X_2, \dots, X_k\}$ una partizione di A; la relazione $\mathcal{R}$ definita come $a\mathcal{R}b \Longleftrightarrow \{\exists i \in \{1, \dots, k\} \text{ t.c. } a, b \in X_i\}$ é una relazione di equivalenza su A.

Dimostrazione: Si osservi come:

- Per il Lemma 1.2.1, ogni classe di equivalenza di un qualsiasi insieme non é l'insieme vuoto;
- Per il Lemma 1.2.2, ogni classe di equivalenza di un qualsiasi insieme é o uguale ad un'altra o disgiunta da questa. Essendo l'insieme quoziente costituito da sole classi di equivalenza distinte, si ha che ciascuna classe che lo compone é distinta da tutte le altre;
- Dato che $[a]_\sim \subseteq A$ per qualsiasi $a \in A$, é evidente come $\bigcup_{a \in A} [a]_\sim \subseteq A$. Inoltre, sempre per il Lemma 1.2.1, ogni $a \in A$ appartiene a $[a]_\sim$, e quindi $A \subseteq \bigcup_{a \in A} [a]_\sim$. Unendo questo risultato al precedente, si ha $A = \bigcup_{a \in A} [a]_\sim$.

Ovvero, $A/\sim$ risponde alla definizione di partizione. D'altra parte, sia $\mathcal{R}$ la relazione definita come $a\mathcal{R}b \Longleftrightarrow \{\exists i \in \{1, \dots, k\} \text{ t.c. } a, b \in X_i\}$. Tale relazione é:

- Riflessiva, perché per definizione di partizione ogni X_i non é vuoto, pertanto esiste sempre almeno un $a \in A$ che vi appartenga, e quindi $a\mathcal{R}a$ é sempre verificato;
- Simmetrica, perché se $a, b \in X_i$ allora $b, a \in X_i$, dato che gli elementi di un insieme non sono ordinati;
- Transitiva, perché se $a, b \in X_i$ e $b, c \in X_i$, allora $a, c \in X_i$.

Pertanto, é una relazione di equivalenza. □

1.3. Funzioni

Siano A e B due insiemi. Una **funzione** (o **applicazione**) da A a B é una legge f che ad ogni elemento di A associa uno ed un solo elemento di B:

$$f : A \mapsto B, f(a) = b$$

Dove A é detto **dominio** di f e B é detto **codominio** di f.
Di fatto, una funzione f da A a B é un caso particolare di una corrispondenza $\mathcal{R}_f$ da A a B dove il secondo termine di ciascuna coppia ordinata che la compone é sempre univoco:

$$f : A \mapsto B \;\; \text{equivale a} \; \mathcal{R}_f : \forall a \in A, \exists! b = f(a) \in B : (a, b) \in \mathcal{R}_f$$

Per ogni $a \in A$, il suo "corrispettivo" in B, ovvero $b = f(a)$, si dice **immagine** di A. L'insieme che contiene l'immagine di ciascun elemento dell'insieme A, ovvero $f(A) = \{f(a) : a \in A\}$, viene chiamato **immagine** di f, e viene indicato anche semplicemente con $\mathfrak{I}(f)$.
Per ogni $b \in B$, l'elemento a di A per il quale b ne é il "corrispettivo", ovvero $a : f(a) = b$, viene detto **controimmagine** di b. L'insieme che contiene le controimmagini di ciascun elemento dell'insieme B, ovvero $\{a \in A : f(a) \in B\}$, viene chiamato **controimmagine** di f, e viene indicato anche semplicemente con $\mathfrak{I}^{-1}(f)$.

Esempio 1.3.1:
- La legge che associa a ciascun numero razionale $\frac{a}{b}$ associa un numero intero $a+b$ non é una funzione. Questo perché $\frac{a}{b} = \frac{ha}{hb} \forall h \neq 0$, pertanto ad ogni $\frac{a}{b}$ é associata una moltitudine di valori, non uno soltanto. Ad esempio, alla frazione $\frac{2}{3}$ viene associato sia 5, sia 10;
- La legge $f : \mathbb{Z} \to \mathbb{Z}, f(z) = z^2$, che associa a ciascun numero intero il suo quadrato, é una funzione;
- Il sottoinsieme $\{(z, 7), z \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$, ovvero l'insieme composto da tutte le coppie ordinate del prodotto cartesiano di $\mathbb{Z}$ con sé stesso che hanno 7 come secondo elemento, é una funzione. Tale sottoinsieme puó essere scritto in maniera piú esplicita nella forma di legge come $f : \mathbb{Z} \to \mathbb{Z}, f(z) = 7$.

Siano dati due insiemi A e B ed una funzione $f : A \mapsto B$. Si dice che f é **iniettiva** se ad elementi distinti di A vengono sempre associati elementi distinti di B:

$$a_1, a_2 \in A : a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Si dice che f é **suriettiva** se il codominio B e l'insieme $f(A)$ coincidono, ovvero se ogni elemento di B ha almeno una controimmagine:

$$\forall b \in B, \exists a \in A : f(a) = b$$

Si dice che f é **biettiva**, o **biunivoca**, se é sia iniettiva sia suriettiva. In altre parole, f é biettiva se ad elementi distinti di A vengono associati elementi distinti di B e se ciascun elemento di B ha sempre una controimmagine:

$$\forall b \in B, \exists! a \in A : f(a) = b$$

Esempio 1.3.2:
- La funzione $f : \mathbb{Z} \to \mathbb{Z}, f(z) = 0$ non é iniettiva, perché ogni elemento di $\mathbb{Z}$ viene sempre associato allo stesso elemento di $\mathbb{Z}$ (lo 0, in questo caso). Inoltre, non é suriettiva, perché tutti gli elementi del codominio al di fuori di 0 non hanno una controimmagine;
- La funzione $f : \mathbb{Z} \mapsto \mathbb{Z}, f(z) = z^2$ non é iniettiva, perché se per un certo $a \in \mathbb{Z}$ vale $b = f(a)$, anche per $-a \in \mathbb{Z}$ vale $b = f(-a)$. Ad esempio, $f(4) = f(-4) = 16$). Inoltre, non é suriettiva, perché tutti gli elementi di $\mathbb{Z}$ che non sono quadrati perfetti non hanno una controimmagine. Ad esempio, non esiste un $a \in \mathbb{Z}$ tale per cui $f(a) = 13$. Infatti, sebbene esistano due a tali per cui $f(a) = 13$, ovvero $\pm\sqrt{13}$, questi non sono numeri interi, pertanto non appartengono al dominio;
- La funzione $f : \mathbb{N} \mapsto \mathbb{Z}, f(z) = z^2$ é iniettiva, perché ad ogni elemento di $\mathbb{N}$ viene associato un elemento distinto di $\mathbb{Z}$. Non é peró suriettiva, perché tutti gli elementi di $\mathbb{Z}$ che non sono quadrati perfetti non hanno una controimmagine;
- La funzione $f : \mathbb{Z} \mapsto \mathbb{Z}, f(z) = z + 1$ é iniettiva, perché per ogni numero intero esiste uno ed un solo numero intero ottenuto sommandovi uno. É inoltre anche suriettiva, perché per ogni numero intero é sempre possibile trovare un'altro numero intero ottenuto a partire dal precedente avendovi sommato uno. Pertanto, é una funzione biettiva.

Sia A un insieme non vuoto. La funzione $*$ viene detta **operazione binaria** su A se ha come dominio il prodotto cartesiano di A con sé stesso ed il codominio coincidente con A:

$$* : A \times A \mapsto A$$

Piú in generale, la funzione $*$ viene detta **operazione n-aria** su A se ha come dominio A^n e sé stesso come codominio:

$$* : A^n \mapsto A$$

Esempio 1.3.3:
- La funzione $f : \mathbb{Z} \times \mathbb{N} \mapsto \mathbb{Z}$, $f(a, b) = a^b$ non é un'operazione;
- La funzione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b) = \sqrt[b]{a}$ é un'operazione binaria;
- La funzione $f : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b, c) = \frac{a+b}{c}$ é un'operazione ternaria.

Sia $*$ una operazione su un insieme a, e siano $a, b, c \in A$ tre suoi elementi. Si dice che $*$ gode della **proprietá associativa** se applicare a c il risultato dell'applicazione di $*$ ad a e a b equivale all'applicare ad a il risultato dell'applicazione di $*$ a b e a c. In altri termini:

$$(a * b) * c = a * (b * c)$$

Dove le parentesi tonde determinano l'*ordine di precedenza* dell'applicazione di $*$.
Sia $*$ una operazione su un insieme a, e siano $a, b \in A$ due suoi elementi. Si dice che $*$ gode della **proprietá commutativa** se applicare a a b equivale ad applicare b ad a. In altri termini:

$$a * b = b * a$$

Esempio 1.3.4:
- L'operazione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b) = a + b$ gode sia della proprietá associativa che della proprietá commutativa;
- L'operazione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b) = a - b$ non gode né della proprietá associativa né della proprietá commutativa;
- L'operazione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b) = 2^{a+b}$ gode della proprietá commutativa, ma non di quella associativa. Infatti, sebbene sia vero che $f(a, b) = f(b, a)$ in quanto $2^{a+b} = 2^{b+a}$, non é vero che $f(a, f(b, c)) = f(f(a, b), c)$, in quanto $2^{a+2b+c} \neq 2^{2a+b+c}$.
- L'operazione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z}$, $f(a, b) = b$ gode della proprietá associativa, ma non di quella commutativa. Infatti, sebbene valga $f(a, f(b, c)) = f(f(a, b), c) = c$, si ha $f(a, b) = b$ e $f(b, a) = a$, pertanto $f(a, b) \neq f(b, a)$.

2. Numeri interi

2.1. Sistemi numerici

Sia $\mathbb{N}$ un insieme non vuoto, in cui si fissa un elemento detto *zero*, indicato con 0, ed una funzione $+$ da $\mathbb{N}$ in $\mathbb{N}$. Indicata con a^+ l'immagine di a tramite $+$ al variare di $a \in \mathbb{N}$, si dice che a^+ é *elemento successivo*, o *successore*, di a. Si assuma che per l'insieme $\mathbb{N}$ valgano i seguenti assiomi, detti **Assiomi di Peano**:

1. $0 \neq a^+ \ \forall a \in \mathbb{N}$. Ovvero, non esiste alcun elemento di $\mathbb{N}$ avente 0 come successore;
2. La funzione $+$ é iniettiva. Ovvero, non esistono due $a_1, a_2 \in S$ distinti che abbiano uno stesso a^+ come successore;
3. Se $S \subseteq \mathbb{N}, 0 \in S$ e $s^+ \in S \ \forall s \in S$, allora $S = \mathbb{N}$. Ovvero, se S é un sottoinsieme anche improprio di $\mathbb{N}$ che contiene (almeno) 0 e che, per ciascun elemento di S, ne contiene anche l'immagine tramite $+$, allora S e $\mathbb{N}$ sono lo stesso insieme.

L'insieme $\mathbb{N}$ cosí definito prende il nome di **insieme dei numeri naturali**.

Principio 2.1.1 (Principio del buon ordinamento): Sia S un sottoinsieme non vuoto di $\mathbb{Z}$ limitato inferiormente (esiste un $n_0 \in \mathbb{Z}$ tale che $s \geq n_0$, $\forall s \in S$). Allora S ha minimo, ovvero esiste un $m \in S$ tale che $s \geq m$, $\forall s \in S$.

Teorema 2.1.1 (Teorema di Ricorrenza): Dati un insieme S, un elemento a di S ed una funzione ϕ da S in sé stesso, esiste una ed una sola funzione $f : \mathbb{N} \to S$ tale che

$$f(0) = a, f(n^+) = \phi(f(n))$$

Principio 2.1.2 (Principio di induzione): Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$ é vera;
- $\forall n$, supponendo che sia vera $P(n)$ é possibile dimostrare che lo sia anche $P(n+1)$.

Allora $P(n)$ é vera $\forall n \in \mathbb{Z}$

Esempio 2.1.1: Si consideri la seguente proposizione, dipendente da n:

$$\sum_{i=1}^{n}(2i-1) = n^2, \forall n \geq 1$$

É possibile applicarvi il principio di induzione ponendo $n_0 = 1$. Nello specifico:

- $P(1)$ é vera. Infatti, $\sum_{i=1}^{1}(2i-1) = (2 \cdot 1) - 1 = 2 - 1 = 1$ e $1^2 = 1$;
- Supponendo che sia vera $P(n)$, si dimostri che é vera $P(n+1)$, ovvero che sia vera $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$. Si ha:

  $$\sum_{i=1}^{n+1}(2i-1) = (2(n+1)-1) + \sum_{i=1}^{n}(2i-1) = 2n+1+\sum_{i=1}^{n}(2i-1) = 2n+1+n^2$$

  Che é peró proprio la formula per il calcolo del quadrato di binomio. Pertanto $n^2 + 1 + 2n = (n+1)^2 = \sum_{i=1}^{n+1}(2i-1)$

Essendo verificate entrambe le ipotesi del principio di induzione, si ha che $P(n)$ é vera $\forall n \geq 1$

Il principio di induzione puó essere riespresso in termini diversi.

Principio 2.1.3 (Principio di induzione forte): Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:

- $P(n_0)$ é vera;
- $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$.

Allora $P(n)$ é vera $\forall n \in \mathbb{Z}$

L'aggettivo *forte* non sta ad indicare che il principio di induzione forte abbia un maggior potere espressivo del principio di induzione "standard"; indica semplicemente che si basa su una ipotesi (la seconda) piú forte di quella usata dalla formulazione precedente. Infatti, una dimostrazione compiuta mediante una delle due forme del principio di induzione puó essere convertita in una dimostrazione analoga compiuta nell'altra forma.

Teorema 2.1.2: Il principio di induzione, il principio di induzione forte ed il principio del buon ordinamento sono equivalenti.

Dimostrazione: La dimostrazione si compone di tre parti.

1. Assumendo come vero il principio di induzione, si dimostri la validitá del principio di induzione forte. Sia pertanto $P(n)$ una proposizione dipendente da n e sia $n_0 \in \mathbb{Z}$ un valore fissato. Si supponga che siano verificate le seguenti ipotesi:
   - $P(n_0)$ é vera;
   - $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$. In particolare, dunque, se $P(n-1)$ é vera allora $P(n)$ é vera. Il principio di induzione implica quindi che $P(n)$ é vera per ogni $n \geq n_0$;
2. Assumendo come vero il principio di induzione forte, si dimostri la validitá del principio del buon ordinamento. Sia pertanto $S \subseteq \mathbb{Z}$ un sottoinsieme non nullo dei numeri interi inferiormente limitato da n_0. Si supponga per assurdo il principio del buon ordinamento non sia valido, ovvero che S non ammetta minimo. Si consideri la proposizione $P(n)$ dipendente da n:

   $$P(n) = \textit{Non esiste alcun numero intero minore o uguale ad } n \textit{ che appartenga ad } S$$

É possibile applicare a $P(n)$ il principio di induzione forte. La prima ipotesi é verificata, perché se n_0 appartenesse ad S, essendone il limite inferiore, allora ne sarebbe necessariamente anche il minimo. Sia dunque n un intero maggiore di n_0. Si assuma allora che $\forall m$ tale che $n_0 \leq m < n$, supponendo che sia vera $P(m)$ é possibile dimostrare che lo sia anche $P(n)$. Si supponga che $P(n)$ sia falsa: esiste allora qualche $t \leq n, t \in S$. Ma questo non é possibile, perché $\forall t \in \mathbb{Z}, n_0 \leq t \leq n$ si suppone $P(t)$ vera, e quindi $t \notin S$. Occorre allora dedurre che S ammetta minimo, e quindi se si assume come valido il principio di induzione forte allora é valido il principio del buon ordinamento.

3. Assumendo come vero il principio del buon ordinamento, si dimostri la validitá del principio di induzione. Dato un numero fissato $n_0 \in \mathbb{Z}$, sia $P(n)$ una proposizione dipendente da $n \in \mathbb{Z}$, con $n \geq n_0$. Si supponga che siano verificate le seguenti ipotesi:
   - $P(n_0)$ é vera;
   - $\forall n$, supponendo che sia vera $P(n)$ é possibile dimostrare che lo sia anche $P(n+1)$.
     Si consideri l'insieme $S \subseteq \mathbb{Z}$ costituito da tutti gli $n \geq n_0$ per i quali $P(n)$ é falsa. Se il principio di induzione fosse verificato, tale insieme dovrebbe essere l'insieme vuoto. Si assuma per assurdo che tale insieme non sia vuoto: per il principio del buon ordinamento tale insieme deve ammettere un minimo, sia questo m, tale per cui $P(m)$ é falsa.
     Dato che l'insieme contiene solo interi n tali per cui $n \geq n_0$ (ma non tutti), dovrá aversi che $m > n_0$, ovvero che $m - 1 \geq n_0$. Ma allora $P(m-1)$ deve essere vera, perché altrimenti si avrebbe $m - 1 \in S$ ed m non sarebbe il minimo di S. Applicando la seconda ipotesi sopra definita, si ha che $P(m + 1 - 1) = P(m)$ é vera, ma questo é in contraddizione con quanto evidenziato in precedenza.
     Occorre allora dedurre che se si assume come valido il principio del buon ordinamento, allora é valido il principio di induzione forte.

□

2.2. Divisione

Dati due numeri interi n e m, con $n > m > 0$, l'operazione di **divisione** permette due interi q e r, chiamati rispettivamente *quoziente* e *resto*, tali che il prodotto fra m e q é il multiplo di m che piú si avvicina ad n per difetto ed il resto $r = n - mq$ misura lo scarto.

Teorema 2.2.1: Siano n e m due numeri interi, con $m \neq 0$. Esiste una ed una sola coppia di interi q ed r tali per cui $n = mq + r$ e $0 \leq r < |m|$

Siano a e b due numeri interi. Se esiste $c \in \mathbb{Z}$ tale che $a = bc$, si dice che b *divide* a, oppure analogamente che a é *divisibile* per b. Per indicare che b divide a viene usata la notazione $b \mid a$. Se b divide a, si dice anche che b é *multiplo* di a. É immediato verificare che, dato $a \in \mathbb{Z}$, sia ± 1 che $\pm a$ sono certamente divisori di a.
Siano $a, b \in \mathbb{Z}$ non entrambi nulli; si dice che $d \in \mathbb{Z}$ é un **Massimo Comun Divisore** tra a e b se sono verificate entrambe le seguenti due condizioni:

1. $d \mid a$ e $d \mid b$. Ovvero, d é divisore sia di a che di b;
2. Se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid d$. Ovvero, tutti i divisori di a che sono anche divisori di b sono anche divisori di d.

Teorema 2.2.2: Dati due numeri $a, b \in \mathbb{Z}$ non entrambi nulli, se d e $\tilde{d}$ sono due Massimi Comun Divisori fra a e b allora devono essere uguali in modulo, ovvero deve aversi $d = \pm\tilde{d}$.

Dimostrazione: Essendo d un Massimo Comun Divisore per a e b, deve valere $d \mid a$ e $d \mid b$. Inoltre, deve valere anche che se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid d$.
Essendo peró anche $\tilde{d}$ un Massimo Comun Divisore per a e b, deve valere $\tilde{d} \mid a$ e $\tilde{d} \mid b$. Allora é possibile sostituire c con $\tilde{d}$ nella seconda espressione ed ottenere che $\tilde{d} \mid d$.

É peró possibile operare anche in senso contrario: essendo $\tilde{d}$ un Massimo Comun Divisore per a e b, deve valere anche che se $c \in \mathbb{Z}$ é tale che $c \mid a$ e $c \mid b$, allora $c \mid \tilde{d}$, e valendo $d \mid a$ e $d \mid b$ deve aversi che $d \mid \tilde{d}$. Esistono allora due numeri $h, k \in \mathbb{Z}$ tali per cui $\tilde{d} = hd$ e $d = \tilde{d}$. Ne segue $\tilde{d} = (hk)\tilde{d}$, e quindi $hk = 1$. Deve allora aversi $h = k = 1$ e quindi $d = \tilde{d}$ oppure $h = k = -1$ e quindi $d = -\tilde{d}$. □

Dal teorema si evince immediatamente che se d é un Massimo Comun Divisore positivo di due numeri interi a e b, allora d é univoco. Tale valore viene indicato con $\text{MCD}(a, b)$.

Teorema 2.2.3 (Esistenza ed unicitá del Massimo Comun Divisore): Per una qualsiasi coppia di numeri interi a e b non entrambi nulli esiste sempre ed é univoco $d = \text{MCD}(a, b)$

Dimostrazione: Innanzitutto, é immediato riconoscere che se $d = \text{MCD}(a, b)$, allora é vero anche $d = \text{MCD}(-a, -b)$. É altrettanto immediato riconoscere che $\text{MCD}(a, b) = \text{MCD}(b, a)$ per qualsiasi a, b. Pertanto, senza perdita di generalitá, é possibile assumere che a e b siano numeri naturali con $a \geq b$.
Se $a = 0$ e $b \neq 0$ si verifica facilmente che $\text{MCD}(a, b) = a$; allo stesso modo, se $b = 0$ e $a \neq 0$ si ha $\text{MCD}(a, b) = b$. Si consideri pertanto il caso piú generale in cui $a \neq 0$ e $b \neq 0$. Devono allora esistere un quoziente q_1 ed un resto r_1 tali per cui é possibile eseguire la divisione:

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

Se $r_1 = 0$, allora $\text{MCD}(a, b) = b$, perché $a = bq_1$ é la definizione stessa di $b \mid a$ e q_1 é arbitrario. Se cosí non é, é possibile ripetere l'operazione e risvolgere i calcoli con un nuovo resto ed un nuovo quoziente. Piú in generale:

$$\begin{array}{lll}
(1) & a = bq_1 + r_1 & r_1 \neq 0 \\
(2) & b = r_1 q_2 + r_2 & r_2 \neq 0 \\
(3) & r_1 = r_2 q_3 + r_3 & r_3 \neq 0 \\
 & \dots & \\
(k-1) & r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} & r_{k-1} \neq 0 \\
(k) & r_{k-2} = r_{k-1} q_k &
\end{array}$$

Il fatto che prima o poi si giunga ad una k-esima iterazione in cui $r_k = 0$ é garantito dal fatto che tale successione é una successione strettamente crescente di numeri non negativi.
L'ultimo resto non nullo, ovvero r_{k-1}, é precisamente $\text{MCD}(a, b)$. Per verificarlo, é sufficiente osservare come questo possegga entrambe le proprietá enunciate nella definizione di Massimo Comun Divisore:

- Alla riga (k) si ha $r_{k-2} = r_{k-1} q_k$, ovvero $r_{k-1} \mid r_{k-2}$. Sostituendo la riga (k) nella riga $(k - 1)$ si ha:

  $$r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} = r_{k-1} q_k q_{k-1} + r_{k-1} = r_{k-1}(q_k q_{k-1} + 1)$$

  Ovvero, $r_{k-1} \mid r_{k-3}$ (Si noti come il raccoglimento é ammesso dato che r_{k-1} é definito come non nullo). Risalendo di riga in riga, é facile convincersi che dalla riga (2) si ottiene $r_{k-1} \mid r_1$ e $r_{k-1} \mid b$. Dalla riga (1) segue $r_{k-1} \mid a$. Avendo dimostrato che $r_{k-1} \mid a$ e $r_{k-1} \mid b$, si ha che r_{k-1} possiede la prima proprietá dell'MCD.
- Sia $c \in \mathbb{Z} - \{0\}$. Siano poi $a = c\overline{a}$ e $b = c\overline{b}$. Sostituendo nella riga (1) si ottiene:

  $$a = bq_1 + r_1 \Rightarrow c\overline{a} = c\overline{b}q_1 + r_1 \Rightarrow r_1 = c\overline{a} - c\overline{b}q_1 \Rightarrow r_1 = c\left(\overline{a} - \overline{b}q_1\right)$$

  Da cui si ha $c \mid r_1$. Ponendo $r_1 = c\overline{r_1}$ e sostituendo nella riga (2), si ha:

  $$b = r_1 q_2 + r_2 \Rightarrow c\overline{b} = c\overline{r_1} q_2 + r_2 \Rightarrow r_2 = c\overline{b} - c\overline{r_1} q_2 \Rightarrow r_2 = c\left(\overline{b} - \overline{r_1} q_2\right)$$

  Da cui si ha $c \mid r_2$. Discendendo di riga in riga ed applicando lo stesso procedimento, si arriva fino a $c \mid r_{k-1}$. Ma questo equivale a dire che, per un c numero intero generico, se $c \mid a$ e $c \mid b$, allora $c \mid r_{k-1}$, e quindi r_{k-1} possiede anche la seconda proprietá dell'MCD.

□

La dimostrazione del Teorema 2.2.3 fornisce implicitamente anche un algoritmo per calcolare, a partire da due numeri interi a e b non entrambi nulli, il loro MCD. Tale algoritmo é strutturato come segue:

1. Si calcola qual'é il piú grande intero q tale per cui é possibile moltiplicarlo per b ottenendo un valore inferiore ad a;
2. Si calcola r come differenza fra qb ed a. Se tale valore é nullo, allora q é MCD per a e b, e l'algoritmo termina;
3. b diventa il nuovo a, mentre r diventa il nuovo b. Dopodiché, si torna al punto 1.

Esempio 2.2.1: L'MCD dei numeri $a = 110143$ e $b = 665$ é 19. Infatti:

$$\begin{aligned}
110143 &= 665 \cdot 165 + 418 \\
665 &= 418 \cdot 1 + 247 \\
418 &= 247 \cdot 1 + 171 \\
247 &= 171 \cdot 1 + 76 \\
171 &= 76 \cdot 2 + 19 \\
76 &= 19 \cdot 4
\end{aligned}$$

Teorema 2.2.4 (Identitá di Bézout): Se a e b sono due numeri interi non entrambi nulli, allora esistono due numeri interi x e y tali per cui vale:

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

Dimostrazione: Facendo riferimento al Teorema 2.2.3, si consideri la successione di operazioni. In particolare, la riga (1), ovvero $a = bq_1 + r_1$, puó anche essere riscritta come $r_1 = a(1) + b(-q_1)$. Sostituendo nella riga (2), si ha:

$$b = r_1 q_2 + r_2 \Rightarrow b = (a - bq_1)q_2 + r_2 \Rightarrow r_2 = b - aq_2 + bq_1 q_2 \Rightarrow r_2 = a(-q_2) + b(q_1 q_2 + 1)$$

In questo modo, é possibile ciascun resto come combinazione lineare di a e di b. In particolare per il resto r_{k-1}, che é anche l'MCD di a e di b, esisteranno due valori x e y tali per cui é possibile esprimerlo come combinazione lineare di a e b, e quindi $r_{k-1} = \text{MCD}(a, b) = ax + by$. $\square$

La dimostrazione del Teorema 2.2.4 fornisce implicitamente anche un algoritmo per calcolare, a partire da due numeri interi a e b non entrambi nulli, una possibile coppia x, y di interi tali da soddisfare l'identitá per a e b, fintanto che il loro MCD é noto. Tale algoritmo é strutturato come segue:

1. Si esprime r in funzione di a e di b, spostando ques'ultimo a primo membro ed isolando r a secondo membro;
2. Se r é l'MCD di a e di b, l'algoritmo termina, perché le soluzioni particolari cercate sono i coefficienti di a e di b;
3. Si passa alla riga successiva e si ripete il procedimento, esprimendo i due nuovi a e b in funzione dei precedenti. Si noti come questi, ad ogni iterazione, cambiano di segno.

Esempio 2.2.2: L'MCD dei numeri $a = 110143$ e $b = 665$ é 19. Una soluzione particolare che soddisfa l'identitá di Bézout per questa coppia é ricavata di seguito:

$$\begin{aligned}
110143 &= 665 \cdot 165 + 418 \Rightarrow a &&= 165b + 418 &&\Rightarrow a - 165b &&= 418 \\
665 &= 418 \cdot 1 + 247 \quad \Rightarrow b &&= a - 165b + 247 &&\Rightarrow 166b - a &&= 247 \\
418 &= 247 \cdot 1 + 171 \quad \Rightarrow a - 165b &&= 166b - a + 171 &&\Rightarrow 2a - 331b &&= 171 \\
247 &= 171 \cdot 1 + 76 \quad \Rightarrow 166b - a &&= 2a - 331b + 76 &&\Rightarrow 497b - 3a &&= 76 \\
171 &= 76 \cdot 2 + 19 \quad \Rightarrow 2a - 331b &&= 2(497b - 3a) + 19 &&\Rightarrow 8a - 1325b &&= 19
\end{aligned}$$

Se due numeri interi hanno 1 come Massimo Comun Divisore, allora si dice che tali numeri sono **coprimi** o **primi fra di loro**. Tale definizione puó essere riformulata anche rispetto al Teorema 2.2.4.

Lemma 2.2.1: Due numeri interi a e b sono primi fra di loro se e soltanto se esistono due numeri interi x e y tali per cui vale $ax + by = 1$.

Dimostrazione: Il primo verso dell'implicazione deriva direttamente dalla definizione di numeri coprimi. Infatti, due numeri interi a, e b si dicono coprimi se il loro MCD é 1; sostituendolo nell'identitá di Bézout, si ha precisamente $ax + by = 1$.
Ció che manca da dimostrare é il secondo verso, ovvero che se per due numeri interi a e b esistono due numeri interi x e y tali per cui $ax + by = 1$, allora a e b sono coprimi. Si supponga per assurdo che, se esistono x e y, tali per cui $ax + by = 1$, allora a e b non siano coprimi. Questo significa che il loro MCD non é 1, ovvero che $ax + by \neq 1$, ma questo é in contraddizione con l'ipotesi assunta per assurdo. □

2.3. Basi

Teorema 2.3.1 (Esistenza ed unicitá della rappresentazione dei numeri interi in una certa base): Sia b un intero maggiore o uguale a 2. Ogni numero intero n non negativo può essere scritto in uno ed un solo modo nella forma:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \ \forall i = 0, \ldots, k \ d_k \neq 0 \text{ per } k > 0$$

Dimostrazione: La dimostrazione prevede di applicare il principio di induzione forte su n. Per $n = 0$ la proposizione é verificata immediatamente. Si assuma allora che la proposizione sia vera per ogni m con $0 \leq m < n$ e la si dimostri per n.
Innanzitutto, si osservi come sia possibile dividere n per b, ottenendo:

$$n = bq + r \quad \text{con } 0 \leq r < b$$

per un certo q ed un certo r. Per la definizione di divisione, si ha $q < n$. Ma allora q é uno degli m per i quali é valida l'ipotesi assunta, ovvero che esiste uno ed un solo modo per scrivere q nella forma:

$$q = c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \ldots + c_1 b + c_0$$

Per certi k valori c_i tali per cui $0 \leq c_i < b$. Sostituendo la seconda espressione nella prima, si ha:

$$n = bq + r = b(c_{k-1} b^{k-1} + c_{k-2} b^{k-2} + \ldots + c_1 b + c_0) + r = c_{k-1} b^k + c_{k-2} b^{k-1} + \ldots + c_1 b^2 + c_0 b + r$$

Ponendo $d_k = c_{k-1}, d_{k-1} = c_{k-2}, \ldots, d_1 = c_0, d_0 = r$, si ha:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \ \forall i = 0, \ldots, k$$

Che é l'ipotesi che si voleva dimostrare.
Per quanto riguarda l'unicità di questa scrittura, questa segue dall'unicità di q e di r. □

Dati $b \in \mathbb{Z}$ con $b \geq 2$ e un numero naturale n tale che:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b + d_0 \quad \text{con } 0 \leq d_i < b \ \forall i = 0, \ldots, k \ d_k \neq 0 \text{ per } k > 0$$

Gli interi $d_0, d_1, \ldots, d_k$ si dicono le **cifre** di n in **base** b.
Per indicare in quale base n sta venendo espresso, se ne riportano ordinatamente le cifre aggiungendo la base in pedice alla cifra piú a destra. Nel caso in cui il pedice sia assente, si sta sottointendendo che tale numero sta venendo espresso in base 10.
Una base b fa uso di un numero di cifre pari a $b - 1$, partendo da 0; nel caso in cui la base sia maggiore di 10, si usano dei simboli extra per rappresentare le cifre mancanti.
Se é nota la (unica) rappresentazione di un numero intero non negativo in una certa base b, é sempre possibile ricavarne la rappresentazione in base 10 semplicemente svolgendo l'equazione della definizione. Si noti peró come tale equazione possa anche essere riscritta come:

$$\begin{aligned} n &= d_k b^k + d_{k-1} b^{k-1} + d_{k-2} b^{k-2} + d_{k-3} b^{k-3} + \ldots + d_1 b + d_0 \\ &= (d_k b + d_{k-1}) b^{k-1} + d_{k-2} b^{k-2} + d_{k-3} b^{k-3} + \ldots + d_1 b + d_0 \\ &= ((d_k b + d_{k-1}) b + d_{k-2}) b^{k-2} + d_{k-3} b^{k-3} + \ldots + d_1 b + d_0 \\ &= (((d_k b + d_{k-1}) b + d_{k-2}) b + d_{k-3}) b^{k-3} + \ldots + d_1 b + d_0 \\ &= \ldots \\ &= (\ldots(((d_k b + d_{k-1}) b + d_{k-2}) b + d_{k-3}) b^{k-3} + \ldots + d_1) b + d_0 \end{aligned}$$

Questa forma é nettamente piú convoluta, ma piú semplice da utilizzare per effettuare la conversione. Infatti, sono necessarie solo k moltiplicazioni per b e k addizioni.

Esempio 2.3.1:

$$61405_7 = (((6 \cdot 7 + 1)7 + 4)7 + 0)7 + 5 = ((42 + 1)7 + 4)49 + 5 = (301 + 4)49 + 5 = 14950$$

Per effettuare la conversione inversa, ovvero ricavare la rappresentazione di un numero n in base b a partire dalla sua rappresentazione in base 10, si osservi come le cifre $d_0, d_1, \ldots, d_k$ di n non siano altro che i resti delle divisioni:

$$\begin{aligned} n &= bq + d_0 & 0 \leq d_0 < b \\ q &= q_1 b + d_1 & 0 \leq d_1 < b \\ q_1 &= q_2 b + d_2 & 0 \leq d_2 < b \\ &\ldots \end{aligned}$$

E così via, finchè non si ottiene quoziente nullo.

Esempio 2.3.2:

$$\begin{aligned} 14950 &= 7 \cdot 2135 + 5 \\ 2135 &= 7 \cdot 305 + 0 \\ 305 &= 7 \cdot 43 + 4 \\ 43 &= 7 \cdot 6 + 1 \\ 6 &= 7 \cdot 0 + 6 \end{aligned}$$

Leggendo dal basso verso l'alto, si ha $14950 = 61405_7$

É facile verificare come maggiore é il numero di cifre che la base in cui un numero é espresso ha a disposizione, minore é il numero di cifre necessarie per rappresentarlo. In particolare, il numero di cifre in base b di un intero non negativo n è dato da:

$$k + 1 = \lfloor \log_b(n) \rfloor + 1 = \left\lfloor \frac{\ln(n)}{\ln(b)} \right\rfloor + 1$$

Perché $b^k \leq n < b^{k+1}$

2.4. Teorema Fondamentale dell'Aritmetica

Sia $p \in \mathbb{Z}$, con $p \geq 2$. Il numero intero p si dice **primo** se, per qualsiasi $a, b \in \mathbb{Z}$, $p \mid ab$ implica $p \mid a$ oppure $p \mid b$. Il numero intero p con $p \geq 2$ viene detto **irriducibile** se i suoi divisori sono solo e soltanto $\pm p$ e ± 1. In altre parole, se vale $a \mid p$ con $a \in \mathbb{Z}$, allora $a = \pm p$ oppure $a = \pm 1$.

Teorema 2.4.1: Il numero $p \in \mathbb{Z}$, con $p \geq 2$ é primo se e solo se é irriducibile (ovvero, le due definizioni sono equivalenti).

Dimostrazione:

- Si supponga che p sia un numero primo. Sia $a \in \mathbb{Z}$ un divisore di p, la cui esistenza é garantita per definizione. Deve allora esistere un certo $b \in \mathbb{Z}$ tale per cui $p = ab$; avendosi $p \mid p$ per qualsiasi numero intero, si ha $p \mid ab$. Essendo p un numero primo, per definizione deve aversi $p \mid a$ oppure $p \mid b$:
  - Se $p \mid a$, allora $p = \pm a$, perché avendo scelto a come divisore di p si ha sia $a \mid p$ che $p \mid a$;
  - Se $p \mid b$, allora deve esistere un certo $c \in \mathbb{Z}$ tale per cui $b = pc$. Ma per ipotesi $p = ab$, pertanto $p = a(pc)$, ovvero $\pm 1 = ac$, da cui si ha $a = \pm 1$.

  In entrambi i casi, p risponde alla definizione di numero irriducibile.
- Si supponga che p sia un numero irriducibile. Siano allora $a, b \in \mathbb{Z}$ tali per cui $p \mid ab$; deve allora esistere un certo $q \in \mathbb{Z}$ tale per cui $ab = pq$. Sia $d = \text{MCD}(a, b)$: per definizione, $d \mid p$. Essendo p un numero irriducibile, deve aversi o $d = p$ oppure $d = 1$:
  - Se $d = p$, allora p é uno dei divisori di a, e quindi $p \mid a$;
  - Se $d = 1$, allora esistono due numeri interi x e y tali per cui é valida l'identitá di Bézout, ovvero $1 = ax + py$. Moltiplicando tale identitá per b, si ha $b = abx + pby$, da cui si deduce $p \mid b$.

  In entrambi i casi, p risponde alla definizione di numero primo.

□

Un numero non primo (o, equivalentemente, un numero non irriducibile) viene detto **numero composto**.

Lemma 2.4.1 (Lemma di Euclide): Sia p un numero primo. Se p é il divisore del prodotto di $n \geq 2$ numeri interi, allora p é divisore di almeno uno dei fattori.

Dimostrazione: Si applichi il principio di induzione su n. Se $n = 2$, si ha $p \mid ab$ con $a, b \in \mathbb{Z}$, e per definizione $p \mid a$ oppure $p \mid b$.
Si supponga che la proposizione sia vera per n, ovvero che p sia il divisore di almeno uno dei fattori del prodotto $a_1 \cdot a_2 \cdot \ldots \cdot a_n$, con $a_1, \ldots, a_n \in \mathbb{Z}$ sapendo che é divisore del prodotto stesso. Si dimostri pertanto che p sia il divisore di almeno uno dei fattori del prodotto $a_1 \cdot a_2 \cdot \ldots \cdot a_{n+1}$ sapendo che vale $p \mid (a_1 \cdot \ldots \cdot a_{n+1})$. Sia $b = a_1 \cdot a_2 \cdot \ldots \cdot a_n$: é possibile allora scrivere $p \mid b \cdot a_{n+1}$. Si ha quindi $p \mid a_{n+1}$ oppure $p \mid b$: se vale $p \mid a_{n+1}$ il lemma é provato immediatamente, mentre se vale $p \mid b$ allora p divide almeno uno dei fattori di b per l'ipotesi induttiva, ed il lemma é provato comunque. □

Si dice che un numero naturale viene **fattorizzato in numeri primi** quando tale numero viene scritto come prodotto di soli numeri primi (non necessariamente distinti). In genere, una fattorizzazione viene espressa raccogliendo a fattor comune i numeri primi per mettere in evidenza la loro molteplicitá. Naturalmente, la fattorizzazione in numeri primi di un numero primo é sé stesso.

Esempio 2.4.1: Il numero 386672 puó venire riscritto come $11 \cdot 13 \cdot 13 \cdot 13 \cdot 2 \cdot 2 \cdot 2 \cdot 2$. Questa é una fattorizzazione in numeri primi, perché 11, 13 e 2 sono numeri primi. Tale fattorizzazione viene in genere scritta come $11 \cdot 13^3 \cdot 2^4$.

Teorema 2.4.2 (Teorema fondamentale dell'aritmetica): Per ogni numero $n \in \mathbb{N}$ tale che $n \geq 2$ esiste uno ed un solo modo per fattorizzarlo in numeri primi (a meno dell'ordine in cui si dispongono i fattori).

Dimostrazione: Per provare l'esistenza della fattorizzazione in numeri primi di n, si proceda per induzione forte su n. Sia $P(n)$ la proposizione *esiste una fattorizzazione in numeri primi per il numero* n, con $n_0 = 2$.
La proposizione $P(n_0)$ é verificata, perché 2 é un numero primo ed é quindi fattorizzabile in numeri primi.
Si consideri pertanto la validitá della proposizione $P(n)$ assumendo che questa sia valida per tutti gli m tali per cui $2 \leq m < n$. Se n é un numero primo, allora $P(n)$ é verificata immediatamente; se invece é un

numero composto, allora sará certamente scrivibile come prodotto di due interi, siano questi a e b. Si ha allora $n = ab$, con $2 \leq a$ e $b < n$. Essendo sia a che b minori di n, vale per questi l'ipotesi induttiva, ed esiste quindi una fattorizzazione in numeri primi sia per a che per b, siano queste rispettivamente $a_1 \cdot ... \cdot a_h$ e $b_1 \cdot ... \cdot b_k$. É allora possibile fattorizzare n in numeri primi come $(a_1 \cdot ... \cdot a_h) \cdot (b_1 \cdot ... \cdot b_k)$, pertanto (almeno) una fattorizzazione in numeri primi per n esiste.
Per provare l'unicitá della fattorizzazione in numeri primi di n, si proceda nuovamente per induzione forte su n. Sia $P(n)$ la proposizione *esiste una sola fattorizzazione in numeri primi per il numero* n, con $n_0 = 2$. La proposizione $P(n_0)$ é verificata, perché 2 é un numero primo ed é quindi fattorizzabile in numeri primi in un solo modo (sé stesso). Si dimostri quindi che esista un solo modo per fattorizzare in numeri primi n assumendo che esista un solo modo per fattorizzare tutti gli m con $0 \leq m < n$. Dato che almeno una fattorizzazione in numeri primi per n esiste, si supponga $n = p_1 p_2 ... p_s = q_1 q_2 ... q_t$, dove ciascun p_i con $1 \leq i \leq s$ e ciascun q_j con $1 \leq j \leq t$ é un numero primo (non necessariamente distinto dagli altri). Si vuole dimostrare sia che $s = t$, ovvero che entrambe le fattorizzazioni sono costituite dallo stesso numero di elementi, sia che ogni p_i ha un q_j al quale é equivalente, e che quindi le due fattorizzazioni sono equivalenti membro a membro. Poiché $p_1 \mid p_1, p_2, ..., p_s$ si ha che $p_1 \mid q_1 q_2 ... q_t$, e dunque esiste almeno un j con $1 \leq j \leq t$ per il quale vale $p_1 \mid q_j$. Senza perdita di generalitá, é possibile assumere che il j in questione sia 1 (eventualmente, é sufficiente riordinare i fattori $q_1, ..., q_t$ per fare in modo che sia cosí), ed é quindi possibile assumere che valga $p_1 \mid q_1$. Essendo peró entrambi numeri primi, se ne deduce che $p_1 = q_1$. Ma allora:

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_t \Rightarrow \cancel{p_1} p_2 ... p_s = \cancel{q_1} q_2 ... q_t \Rightarrow p_2 ... p_s = q_2 ... q_t$$

Che essendo necessariamente entrambe minori di n, vale per queste l'ipotesi induttiva. □

Per calcolare la (univoca) fattorizzazione di un numero primo occorre trovare un numero primo qualsiasi che ne sia un divisore e ripetere il procedimento sul risultato di tale divisione fintanto che é possibile procedere, ovvero fintanto che tale risultato sia diverso da 1.

Esempio 2.4.2:

$$\begin{aligned} 13796146 \div 13 &= 1061242 \\ 1061242 \div 13 &= 81634 \\ 81634 \div 17 &= 4802 \\ 4802 \div 7 &= 686 \\ 686 \div 7 &= 98 \\ 98 \div 7 &= 14 \\ 14 \div 7 &= 2 \\ 2 \div 2 &= 1 \end{aligned}$$

Teorema 2.4.3 (Teorema di Euclide sui numeri primi): Esistono infiniti numeri primi.

Dimostrazione: Si supponga per assurdo che questo non sia vero, e che i numeri primi siano quindi un insieme finito: sia tale insieme $\{p_1, p_2, ..., p_k\}$. Sia $M = 1 + (p_1 \cdot p_2 \cdot ... \cdot p_k)$: essendo 2 il numero primo piú piccolo, si avrá certamente $M \geq 2$. Essendo poi l'insieme $\mathbb{Z}$ chiuso rispetto al prodotto e alla somma, si ha $M \in \mathbb{Z}$. Sono allora valide le ipotesi del Teorema 2.4.2, ed esiste quindi una ed una sola fattorizzazione in numeri primi per M. Se tale fattorizzazione esiste, allora ciascun elemento p_i di tale fattorizzazione deve esserne anche un divisore. Questo peró non é possibile, perché se si avesse $p_i \mid M$ per un qualsiasi $1 \leq i \leq k$ allora si avrebbe anche $p_i \mid 1 = M - (p_1 \cdot p_2 \cdot ... \cdot p_k)$, e non esiste alcun numero che sia divisore di 1. Occorre pertanto assumere che i numeri primi siano infiniti. □

Siano $a, b \in \mathbb{Z}$ non entrambi nulli; si dice che $m \in \mathbb{Z}$ é un **Minimo Comune Multiplo** tra a e b se sono verificate entrambe le seguenti due condizioni:

1. $a \mid m$ e $b \mid m$. Ovvero, sia a che b sono divisori di m;

2. Se $c \in \mathbb{Z}$ é tale che $a \mid c$ e $b \mid c$, allora $m \mid c$. Ovvero, se sia a che b sono divisori di un generico c, allora anche m é divisore di c.

Teorema 2.4.4: Dati due numeri $a, b \in \mathbb{Z}$ non entrambi nulli, se m e $\widetilde{m}$ sono due Minimi Comuni Multipli fra a e b allora devono essere uguali in modulo, ovvero deve aversi $m = \pm\widetilde{m}$.

Dal teorema si evince immediatamente che se m é un Minimo Comune Multiplo positivo di due numeri interi a e b, allora m é univoco. Tale valore viene indicato con $\mathrm{mcm}(a, b)$.

Teorema 2.4.5 (Esistenza ed unicitá del Minimo Comune Multiplo): Per una qualsiasi coppia di numeri interi a e b non entrambi nulli esiste sempre ed é univoco $m = \mathrm{mcm}(a, b)$. In particolare, $\mathrm{mcm}(a, b) = \frac{ab}{\mathrm{MCD}(a,b)}$.

Dimostrazione: Sia $d = \mathrm{MCD}(a, b)$. Siano poi $a = \tilde{a}d$, $b = \tilde{b}d$ e $m = \frac{ab}{d}$. Sostituendo le espressioni di a e b in m, si ha $m = \frac{\tilde{a}d\tilde{b}\cancel{d}}{\cancel{d}} = \tilde{a}\tilde{b}d = a\tilde{b} = b\tilde{a}$, da cui si evince $a \mid m$ e $b \mid m$, provando il primo requisito della definizione di Minimo Comune Multiplo.
Preso un $c \in \mathbb{Z}$ tale per cui $a \mid c$ e $b \mid c$, ossia tale per cui $c = as = bt$ per certi $s, t \in \mathbb{Z}$, si ha $c = \tilde{a}sd = \tilde{b}td$, ovvero $\tilde{a}s = \tilde{b}t$. Poiché $\mathrm{MCD}\left(\tilde{a}, \tilde{b}\right) = 1$, deve aversi $\tilde{a} \mid t$ e $\tilde{b} \mid s$, ovvero deve valere $t = h\tilde{a}$ e $s = k\tilde{b}$ per certi $h, k \in \mathbb{Z}$. Sostituendo $t = h\tilde{a}$ nell'espressione per c, si ha $c = b\tilde{a}h = mh$, da cui si deduce $m \mid c$, provando il secondo requisito della definizione di Minimo Comune Multiplo. □

2.5. Equazioni Diofantee

Viene detta **equazione diofantea** una equazione nella forma:

$$ax + by = c \qquad \text{con } a, b, c, x, y \in \mathbb{Z} \ \text{ e } a, b, c \neq 0$$

Dove a, b, c sono i *termini noti* e x, y sono le *incognite*.
Essendo x e y interi, le *soluzioni* di tale equazione sono tutte e sole le coppie $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ tali per cui $ax_0 + by_0 = c$.

Esempio 2.5.1: Si consideri l'equazione diofantea $6x + 5y = 3$. Le coppie $(3, -3)$ e $(8, -9)$ sono sue possibili soluzioni.

Teorema 2.5.1 (Condizione necessaria e sufficiente per la solubilitá delle equazioni diofantee): Si consideri l'equazione diofantea $ax + by = c$, con termini noti non nulli $a, b, c \in \mathbb{Z}$ e incognite $x, y \in \mathbb{Z}$. Tale equazione ammette soluzione se e soltanto se $\mathrm{MCD}(a, b) \mid c$.

Dimostrazione: Si supponga che $ax + by = c$ ammetta una certa soluzione $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$. Deve allora valere $ax_0 + by_0 = c$. Valendo $\mathrm{MCD}(a, b) \mid ax_0 + by_0$ si ha $\mathrm{MCD}(a, b) \mid c$. Pertanto, se una equazione diofantea $ax + by = c$ é risolubile, allora $\mathrm{MCD}(a, b) \mid c$.
Viceversa, si supponga che per l'equazione diofantea $ax + by = c$ valga $\mathrm{MCD}(a, b) \mid c$. Questo equivale a dire che vale $c = \mathrm{MCD}(a, b)\tilde{c}$ per un qualche $\tilde{c} \in \mathbb{Z}$. Per l'identità di Bezout esistono certi $s, t \in \mathbb{Z}$ tali per cui $\mathrm{MCD}(a, b) = as + bt$. Sostituendo nell'equazione precedente, si ha $c = (as + bt)\tilde{c} = as\tilde{c} + bt\tilde{c}$. Ponendo $x_0 = s\tilde{c}$ e $y_0 = t\tilde{c}$, si ha $c = ax_0 + by_0$. Essendo $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$, tale coppia é una possibile soluzione per l'equazione. Pertanto, se per l'equazione diofantea $ax + by = c$ vale $\mathrm{MCD}(a, b) \mid c$, allora tale equazione ha (almeno) una soluzione. □

Esempio 2.5.2: Si consideri l'equazione diofantea $74x + 22y = 10$. Ci si chiede se tale equazione ammetta soluzione. Si calcoli pertanto $\text{MCD}(a, b)$:

$$\begin{aligned} 74 &= 22 \cdot 3 + 8 \\ 22 &= 8 \cdot 2 + 6 \\ 8 &= 6 \cdot 1 + 2 \\ 6 &= 2 \cdot 3 \end{aligned}$$

Da cui si ricava $\text{MCD}(74, 22) = 2$. Essendo $2 \mid 10$, si ha che l'equazione ammette soluzione.

Corollario 2.5.1 (Determinare una soluzione particolare di una equazione diofantea): Si consideri l'equazione diofantea risolubile $ax + by = c$, con termini noti non nulli $a, b, c \in \mathbb{Z}$ e incognite $x, y \in \mathbb{Z}$. Una soluzione particolare $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ di tale equazione puó essere ottenuta dall'identitá di Bézout che ha a e b per termini noti.

Dimostrazione: Sia $ax + by = \text{MCD}(a, b)$ l'identitá di Bézout per a e b. Moltiplicando ambo i membri per un certo $\tilde{c} \in \mathbb{Z}$, si ha $(ax + by)\tilde{c} = ax\tilde{c} + by\tilde{c} = \text{MCD}(a, b)\tilde{c}$. Sostituendo $x\tilde{c} = x_0$, $y\tilde{c} = y_0$ e $\text{MCD}(a, b)\tilde{c} = c$, si ha $ax_0 + by_0 = c$. Questa é una equazione diofantea, essendo costituita da soli coefficienti interi, e la coppia (x_0, y_0) ne é soluzione. Tale equazione é infatti risolubile perché essendo $\text{MCD}(a, b)\tilde{c} = c$, si ha $c \mid \text{MCD}(a, b)$. □

Il Corollario 2.5.1 suggerisce che per ricavare una soluzione particolare di una equazione diofantea risolubile $ax + by = c$ sia sufficiente trovare una soluzione particolare dell'identitá di Bézout che ha a e b per termini noti e moltiplicare il risultato per $\frac{c}{\text{MCD}(a,b)}$.

Esempio 2.5.3: Si consideri l'equazione diofantea risolubile $74x + 22y = 10$. É giá stato calcolato che $\text{MCD}(74, 22) = 2$, pertanto l'identitá di Bézout che ha 74 e 22 come termini noti é $74x' + 22y' = 2$. Se ne determini una soluzione particolare $({x_0}', {y_0}')$:

$$\begin{aligned} 74 &= 22 \cdot 3 + 8 \Rightarrow a = 3b + 8 \Rightarrow a - 3b = 8 \\ 22 &= 8 \cdot 2 + 6 \Rightarrow b = 2(a - 3b) + 6 \Rightarrow 7b - 2a = 6 \\ 8 &= 6 \cdot 1 + 2 \Rightarrow (a - 3b) = (7b - 2a) + 2 \Rightarrow 3a - 10b = 2 \end{aligned}$$

Si ha quindi $({x_0}', {y_0}') = (3, -10)$. Essendo $\frac{10}{\text{MCD}(74,22)} = 5$, si ha che una soluzione particolare dell'equazione diofantea $74x + 22y = 10$ é $(15, -50)$.

Teorema 2.5.2 (Soluzioni di una equazione diofantea): Si consideri l'equazione diofantea risolubile $ax + by = c$, con termini noti non nulli $a, b, c \in \mathbb{Z}$ e incognite $x, y \in \mathbb{Z}$. Se la coppia $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ é soluzione per tale equazione, allora lo sono tutte e sole le coppie $(x_h, y_h) \in \mathbb{Z} \times \mathbb{Z}$ cosí costruite:

$$x_h = x_0 + h\left(\frac{b}{\text{MCD}(a, b)}\right) \qquad y_h = y_0 - h\left(\frac{a}{\text{MCD}(a, b)}\right) \qquad \text{con } h \in \mathbb{Z}$$

Dimostrazione: Le coppie (x_h, y_h) cosí costruite sono certamente soluzioni di $ax + by = c$, dato che sostituendo si ha:

$$ax_h + by_h = c \Rightarrow a\left(x_0 + h\left(\frac{b}{\mathrm{MCD}(a,b)}\right)\right) + b\left(y_0 - h\left(\frac{a}{\mathrm{MCD}(a,b)}\right)\right) = c$$
$$\Rightarrow ax_0 + \frac{ahb}{\cancel{\mathrm{MCD}(a,b)}} + by_0 - \frac{ahb}{\cancel{\mathrm{MCD}(a,b)}} = c \Rightarrow ax_0 + by_0 = c$$

Viceversa, sia $(\overline{x}, \overline{y})$ una generica soluzione di $ax + by = c$. Dato che anche (x_0, y_0) lo é, é possibile scrivere:

$$a\overline{x} + b\overline{y} = c = ax_0 + by_0 \Rightarrow a(\overline{x} - x_0) = -b(\overline{y} - y_0) \Rightarrow \overline{a}(\overline{x} - x_0) = \overline{b}(y_0 - \overline{y}) \quad \text{con} \quad \begin{aligned} \overline{a} &= \tfrac{a}{\mathrm{MCD}(a,b)} \\ \overline{b} &= \tfrac{b}{\mathrm{MCD}(a,b)} \end{aligned}$$

Dall'espressione si ricava che $\overline{a} \mid \overline{b}(y_0 - \overline{y})$, da cui si ha $\overline{a} \mid y_0 - \overline{y}$. Ma allora esiste un certo $h \in \mathbb{Z}$ tale per cui $y_0 - \overline{y} = h\overline{a}$, cioé $\overline{y} = y_0 - h\overline{a}$. Sostituendo nella precedente, si ha:

$$\overline{a}(\overline{x} - x_0) = \overline{b}(\cancel{y_0} - \cancel{y_0} + h\overline{a}) \Rightarrow \cancel{\overline{a}}(\overline{x} - x_0) = \overline{b}h\cancel{\overline{a}} \Rightarrow \overline{x} - x_0 = \overline{b}h \Rightarrow \overline{x} = x_0 + \overline{b}h$$

Risostituendo il valore di $\overline{a}$ e $\overline{b}$ nelle rispettive formule, si ottiene la forma presente nell'enunciato del teorema:

$$\overline{x} = x_0 + h\left(\frac{b}{\mathrm{MCD}(a,b)}\right) \qquad \overline{y} = y_0 - h\left(\frac{a}{\mathrm{MCD}(a,b)}\right) \qquad \text{con } h \in \mathbb{Z}$$

Essendo $(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ una soluzione generica, si ha quindi che qualsiasi soluzione puó essere espressa in tale forma. □

Esempio 2.5.4: Si consideri l'equazione diofantea risolubile $74x + 22y = 10$, del quale é nota la soluzione particolare $(15, -50)$ ed é noto che $\mathrm{MCD}(74, 22) = 2$. Avendosi $\frac{74}{2} = 37$ e $\frac{22}{2} = 11$, é possibile ricavare la famiglia di soluzioni $(x_h, y_h) \in \mathbb{Z} \times \mathbb{Z}$:

$$x_h = 15 + 11h \qquad y_h = -50 - 37h \qquad \text{con } h \in \mathbb{Z}$$

2.6. Congruenza Modulo n

Sia $n \in \mathbb{Z}$ con $n > 0$. Dati due interi a e b sono **congrui modulo** n se $n \mid a - b$, e si scrive $a \equiv b \bmod n$. In altre parole, $a \equiv b \bmod n$ vale se e solo se esiste un certo $k \in \mathbb{Z}$ tale per cui $a - b = nk$. In maniera equivalente, é possibile dire che due numeri a e b sono congruenti modulo n se la loro divisione per n restituisce il medesimo resto.

Esempio 2.6.1: Avendosi $12 \mid 38 - 14$, é possibile scrivere $38 \equiv 14 \bmod 12$. Si noti inoltre come sia 38 sia 14, divisi per 12, diano resto 2.

La definizione puó essere estesa anche al caso in cui $n = 0$. Si noti infatti come, se vale $n = 0$, si ha $a - b = 0 \cdot k$, ovvero $a = b$. Pertanto, la congruenza modulo 0 coincide semplicemente con la relazione di uguaglianza in $\mathbb{Z}$.
La definizione puó essere inoltre estesa anche al caso in cui $n < 0$. Infatti, basta osservare che $n \mid a - b$ se e solo se $-n \mid a - b$ per concludere che $a \equiv b \bmod n$ se e solo se $a \equiv b \bmod -n$. Per questo motivo, non é limitativo considerare $n > 0$.

Lemma 2.6.1: Sia $n \in \mathbb{Z}$ con $n > 0$. Dati quattro interi a, b, c e d, se vale $a \equiv b \bmod n$ e $c \equiv d \bmod n$ allora vale $a + b \equiv c + d \bmod n$.

Lemma 2.6.2: Sia $n \in \mathbb{Z}$ con $n > 0$. Dati quattro interi a, b, c e d, se vale $a \equiv b \bmod n$ e $c \equiv d \bmod n$ allora vale $ab \equiv cd \bmod n$.

Teorema 2.6.1: Per ogni numero intero $n > 0$, la congruenza modulo n é una relazione di equivalenza su $\mathbb{Z}$.

Dimostrazione: La congruenza modulo n definisce su $\mathbb{Z}$ la relazione $\mathcal{R}$ data da:

$$\forall a, b \in \mathbb{Z}, (a, b) \in \mathcal{R} \text{ se e solo se } a \equiv b \bmod n$$

La relazione in questione é:

1. Riflessiva: $\forall a \in \mathbb{Z}$ vale $a \equiv a \bmod n$. Infatti, $a \equiv a \bmod n$ equivale a dire $a - a = 0 = kn$, che é valido per $k = 0$ e per qualsiasi $a \in \mathbb{Z}$;
2. Simmetrica: $\forall a, b \in \mathbb{Z}$, $a \equiv b \bmod n$ implica $b \equiv a \bmod n$. Infatti, $a \equiv b \bmod n$ equivale a dire $a - b = kn$ per un certo $k \in \mathbb{Z}$. Moltiplicando per -1 ambo i membri si ha $-(a - b) = -(kn)$, ovvero $b - a = (-k)n$, cioé $b \equiv a \bmod n$;
3. Transitiva: $\forall a, b, c \in \mathbb{Z}$, $a \equiv b \bmod n$ e $b \equiv c \bmod n$ implicano $a \equiv c \bmod n$. Infatti, $a \equiv b \bmod n$ e $b \equiv c \bmod n$ equivalgono a dire, rispettivamente, $a - b = kn$ e $b - c = hn$ per certi $h, k \in \mathbb{Z}$. Sommando la seconda alla prima:

$$a - b + (b - c) = kn + (b - c) \Rightarrow a - \cancel{b} + \cancel{b} - c = kn + hn \Rightarrow a - c = (k + h)n \Rightarrow a \equiv c \bmod n$$

Pertanto, é una relazione di equivalenza. □

Essendo la congruenza modulo n una relazione di equivalenza, é possibile identificare delle classi di equivalenza. Preso n intero con $n > 0$ ed un certo $a \in \mathbb{Z}$, la classe di equivalenza di a rispetto alla congruenza modulo n viene indicata con $[a]_n$.
Tale classe di equivalenza corrisponde all'insieme $\{b : b \in \mathbb{Z} \land a \equiv b \bmod n\}$, ovvero all'insieme che contiene tutti i numeri interi che, divisi per n, restituiscono lo stesso resto della divisione fra n e a.

Lemma 2.6.3: Sia n un numero intero maggiore di 0. Sia a un numero intero qualsiasi e sia b il resto della divisione di a per n. Vale $[a]_n = [b]_n$.

Dimostrazione: Se b é il resto della divisione di a per n, allora vale $a = nk + b$ per un certo $k \in \mathbb{Z}$, da cui si ha $a - b = nk$, che é la definizione di congruenza modulo n. □

L'insieme quoziente di $\mathbb{Z}$ rispetto alla relazione di congruenza modulo n con $n > 0$ si dice **insieme delle classi di resti modulo** n e si denota con $\mathbb{Z}_n$.

Teorema 2.6.2: Per ogni numero intero $n > 0$, l'insieme delle classi di resti modulo n ha cardinalitá n. In particolare, tale insieme é:

$$\mathbb{Z}_n = \left\{[0]_n, [1]_n, ..., [n-1]_n\right\} = \{\{nk : k \in \mathbb{Z}\}, \{1 + nk : k \in \mathbb{Z}\}, ..., \{n - 1 + nk : k \in \mathbb{Z}\}\}$$

Dimostrazione: Sia $a \in \mathbb{Z}$. La divisione con resto fornisce $a = nq + r$ con $0 \leq r < n$. Poichè $a - r = qn$ si ha che $a \equiv r \bmod n$. Ciò mostra che ogni intero a è congruo, modulo n, a uno degli interi $0, 1, ..., n - 1$. D'altra parte se i e j sono interi, con $0 \leq i < n$ e $0 \leq j < n$ si ha, assumendo $i \geq j$, che $0 \leq i - j \leq n - 1$ e quindi $i - j = kn$ se e solo se $k = 0$, cioè $i = j$. □

Esempio 2.6.2:

Con $n = 2$, si ha $\mathbb{Z}_2 = \left\{[0]_2, [1]_2\right\}$:

$[0]_2 = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$

$[1]_2 = \{..., -5, -3, -1, 1, 3, 5, 7, ...\}$

Con $n = 3$, si ha $\mathbb{Z}_3 = \left\{[0]_3, [1]_3, [2]_3\right\}$:

$[0]_3 = \{..., -9, -6, -3, 0, 3, 6, 9, ...\}$

$[1]_3 = \{..., -8, -5, -2, 1, 4, 7, 10, ...\}$

$[2]_3 = \{..., -7, -4, -1, 2, 5, 8, 11, ...\}$

Ad esempio, la classe di resto $[5]_7$ rappresenta, oltre al numero 5, anche il numero 12 $(1 \times 7 + 5)$, il numero 19 $(2 \times 7 + 5)$, il numero 2308 $(329 \times 7 + 5)$, il numero -2 $(-1 \times 7 + 5)$ il numero -9 $(-2 \times 7 + 5)$, ecc...

2.7. Congruenze lineari

Viene detta **congruenza lineare modulo** n qualunque espressione nella forma:

$$ax \equiv b \bmod n \qquad \text{con } a, b, n \in \mathbb{Z}$$

Dove a, b ed n sono termini noti ed x é una incognita. Naturalmente, le *soluzioni* di una congruenza lineare sono tutti e soli quei $c \in \mathbb{Z}$ tali che, sostituiti ad x, rendono valida l'espressione. Se esiste almeno un c con queste caratteristiche, si dice che la congruenza lineare *ammette* soluzione.

Esempio 2.7.1: Si consideri la congruenza lineare $2x \equiv 3 \bmod 7$. Una possibile soluzione per tale congruenza é $c = 5$, dato che $2 \cdot 5 = 10$ ed effettivamente $10 \equiv 3 \bmod 7$. Anche $c = 26$ é una possibile soluzione, dato che $2 \cdot 26 = 52 \equiv 3 \bmod 7$.

Teorema 2.7.1: Siano $a, b, n \in \mathbb{Z}$, con $a \neq 0$. La congruenza lineare $ax \equiv b \bmod n$ ammette soluzione se e soltanto se $\mathrm{MCD}(a, n) \mid b$.

Dimostrazione: Da definizione di congruenza modulo n, si ha che $ax \equiv b \bmod n$ equivale a $n \mid ax - b$, che a sua volta equivale a $ax - b = nk$ per un certo $k \in \mathbb{Z}$. Spostando b al secondo membro, si ha $ax - nk = b$; dato che tutti i numeri che figurano in questa equazione sono numeri interi, si sta avendo a che fare con una equazione diofantea, nello specifico nelle variabili x e k. Per il Teorema 2.5.1, l'equazione ha soluzione se e soltanto se $\mathrm{MCD}(a, n) \mid b$, ma dato che tale equazione é solamente una riscrittura di $ax \equiv b \bmod n$, allora anche quest'ultima avrá soluzione se e solo se sono rispettate tali condizioni. □

Esempio 2.7.2:
- La congruenza lineare dell'Esempio 2.7.1 ha soluzioni, perché $\mathrm{MCD}(a, n) = 1$ ed é vero che $1 \mid 3$;
- La congruenza lineare $2x \equiv 3 \bmod 4$ non ha soluzioni, perché $\mathrm{MCD}(a, n) = 2$ ed é falso che $2 \mid 3$.

Il Teorema 2.7.1 fornisce implicitamente un approccio per cercare una soluzione particolare di una congruenza lineare, ovvero costruendo una equazione diofantea a questa equivalente e risolvendola. La soluzione particolare é data dalla componente x della soluzione particolare di tale equazione.

Esempio 2.7.3: Si consideri la congruenza lineare $21x \equiv 6 \bmod 30$. L'equazione diofantea associata é $21x - 30k = 6$. Si ha:

$$\begin{aligned} 30 &= 21 \cdot 1 + 9 \\ 21 &= 9 \cdot 2 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned} \qquad \begin{aligned} b &= a \cdot 1 + 9 \Rightarrow 9 = b - a \\ a &= 2(b - a) + 3 \Rightarrow 3 = 3a - 2b \end{aligned} \qquad (6)21 - (4)30 = 6$$

Da cui si ricava la soluzione particolare $c = 6$ per la congruenza lineare.

Teorema 2.7.2: Siano $a, b, n \in \mathbb{Z}$, con $a \neq 0$. Si consideri la congruenza lineare $ax \equiv b \bmod n$: se $x_0 \in \mathbb{Z}$ ne é una soluzione, allora lo sono anche tutti ed i soli numeri interi x_h nella forma:

$$x_h = x_0 + h\left(\frac{n}{\text{MCD}(a, n)}\right) \quad \text{con } h \in \mathbb{Z}$$

In particolare, fra queste ne esistono esattamente $\text{MCD}(a, n)$ non congruenti modulo n fra di loro.

Dimostrazione: Per il Teorema 2.7.1, $ax \equiv b \bmod n$ ha soluzione se e soltanto se ha soluzione l'equazione diofantea equivalente $ax - nk = b$ con $k \in \mathbb{Z}$. Per il Teorema 2.5.2 si ha che se $(x_0, k_0) \in \mathbb{Z} \times \mathbb{Z}$ é una soluzione particolare di tale equazione, allora lo sono tutte e sole le coppie $(x_h, k_h) \in \mathbb{Z} \times \mathbb{Z}$ nella forma:

$$x_h = x_0 + h\left(\frac{n}{\text{MCD}(a, n)}\right) \qquad k_h = k_0 - h\left(\frac{n}{\text{MCD}(a, n)}\right) \qquad \text{con } h \in \mathbb{Z}$$

L'espressione per x_h é quella cercata. Per provare che la congruenza lineare ha esattamente $\text{MCD}(a, n)$ soluzioni non congruenti modulo n fra di loro, si consideri $h_1, h_2 \in \mathbb{Z}$. Si ha:

$$x_0 + h_1\left(\frac{n}{\text{MCD}(a, n)}\right) \equiv x_0 + h_2\left(\frac{n}{\text{MCD}(a, n)}\right) \bmod n \Longleftrightarrow \left(\frac{n}{\text{MCD}(a, n)}\right)(h_1 - h_2) \equiv 0 \bmod n$$

Deve allora esistere un certo $q \in \mathbb{Z}$ tale per cui:

$$\left(\frac{n}{\text{MCD}(a, n)}\right)(h_1 - h_2) \equiv 0 \bmod n \Rightarrow \left(\frac{\cancel{n}}{\text{MCD}(a, n)}\right)(h_1 - h_2) = q\cancel{n} \Rightarrow h_1 - h_2 = q \ \text{MCD}(a, n)$$

Pertanto, le $\text{MCD}(a, n)$ soluzioni non congruenti modulo n fra di loro che si stavano cercando sono tutte e sole le soluzioni con $h = 0, 1, \ldots, (\text{MCD}(a, n) - 1)$. □

Esempio 2.7.4: La congruenza lineare dell'Esempio 2.7.3, che aveva per soluzione particolare $c = 5$. Avendosi $\text{MCD}(21, 30) = 3$, si ha $\frac{30}{3} = 10$. Pertanto, tale congruenza lineare ha per soluzioni ogni intero nella forma $6 + 10h$ con $h \in \mathbb{Z}$. In particolare, le soluzioni non congruenti modulo n fra di loro sono $c = 6$, $c = 16$ e $c = 26$.

Viene detto **sistema di congruenze lineari** qualunque espressione nella forma:

$$A_i x \equiv B_i \bmod N_i = \begin{cases} a_1 x \equiv b_1 \quad \bmod n_1 \\ a_2 x \equiv b_2 \quad \bmod n_2 \\ \vdots \\ a_m x \equiv b_m \bmod n_m \end{cases} \quad \text{con } a_1, \ldots, a_m, b_1, \ldots, b_m, n_1, \ldots, n_m \in \mathbb{Z}$$

Dove $a_1, \ldots, a_m, b_1, \ldots, b_m$ e $n_1, \ldots, n_m$ sono termini noti ed x é una incognita. Le *soluzioni* di un sistema di congruenze lineari sono tutti e soli quei $c \in \mathbb{Z}$ tali che, sostituiti ad x, verificano contemporaneamente tutte le m

congruenze lineari modulo n_i che lo compongono. Se esiste almeno un c con queste caratteristiche, si dice che il sistema di congruenze lineari *ammette* soluzione.

Lemma 2.7.1 (Condizione necessaria per la solubilitá di un sistema di congruenze lineari): Un sistema di congruenze lineari $A_i x \equiv B_i \bmod N_i$ ha soluzione soltanto se, per ogni $i = 1, ..., m$, si ha $\mathrm{MCD}(a_i, n_i) \mid b_i$.

Dimostrazione: Per il Teorema 2.7.1, si ha che $ax \equiv b \bmod n$ ha soluzione se e soltanto se $\mathrm{MCD}(a, n) \mid b$. Dato che un sistema di congruenze lineari ha soluzione soltanto se tutte le congruenze che lo compongono hanno soluzione, tale sistema avrá soluzione soltanto se $\mathrm{MCD}(a_i, n_i) \mid b_i$ é valido per ogni $i = 1, ..., m$.□

Si noti come il Lemma 2.7.1 sia una implicazione a senso unico, ovvero potrebbero esistere dei sistemi di congruenze lineari che lo verificano ma che comunque non hanno soluzione. Infatti, le congruenze lineari che costituiscono un sistema potrebbero essere solubili individualmente, ma nessuna di queste avere una soluzione che sia comune a tutte.

Teorema 2.7.3 (Teorema Cinese del Resto): Si consideri un sistema di congruenze lineari come quello presentato di seguito:

$$\begin{cases} x \equiv b_1 \mod n_1 \\ \vdots \\ x \equiv b_2 \mod n_2 \\ x \equiv b_m \mod n_m \end{cases} \quad \text{con } b_1, ..., b_m, n_1, ..., n_m \in \mathbb{Z}$$

Ovvero, dove i termini $a_1, ..., a_m$ sono tutti pari ad 1. Si assuma inoltre che i termini $n_1, ..., n_m$ siano tutti positivi e che siano a due a due coprimi, ovvero $\mathrm{MCD}(n_i, n_j) = 1$ per ogni $1 \leq i \leq m$ e $1 \leq j \leq m$ tali per cui $i \neq j$.
Allora il sistema é risolubile. In particolare, se c e c' sono due soluzioni, allora vale:

$$c \equiv c' \bmod N \quad \text{dove } N = n_1 \cdot n_2 \cdot ... \cdot n_m = \prod_{i=1}^{m} n_i$$

Dimostrazione: Per ogni $i = 1, ..., m$, sia $N_i = \frac{N}{n_i}$ (essendo $N = \prod_{i=1}^{m} n_i$ é garantito che N_i sia un numero intero, perché n_i é uno dei fattori di N). Per ipotesi, si ha $\mathrm{MCD}(n_i, n_j) = 1$ per $i \neq j$. Tuttavia, é facile verificare che anche $\mathrm{MCD}(N_i, n_i) = 1$.
Infatti, si supponga per assurdo che $\mathrm{MCD}(N_i, n_i) \neq 1$. Deve allora esistere un numero primo p tale per cui $p \mid n_i$ e $p \mid N_i$, ovvero che é divisore sia di n_i che di N_i. Essendo $N_i = n_1 \cdot ... \cdot n_{i-1} \cdot n_{i+1} \cdot ... \cdot n_m$, per il Lemma 2.4.1 deve esistere un n_j con $j \neq i$ tale per cui $p \mid n_j$. Ma allora, valendo sia $p \mid n_i$ sia $p \mid n_j$, si ha che n_i ed n_j hanno un divisore in comune, e quindi non sono primi, contro l'ipotesi che invece lo siano. Occorre allora assumere che $\mathrm{MCD}(N_i, n_i) = 1$.
Si consideri la congruenza lineare $N_i y \equiv 1 \bmod n_i$ nell'incognita y, che ha y_i per soluzione. Per il Teorema 2.7.1, tale congruenza lineare ha soluzione se vale $\mathrm{MCD}(N_i, n_i) \mid 1$, ed é stato appena mostrato che $\mathrm{MCD}(N_i, n_i) = 1$, pertanto é garantito che y_i esista. Sia c definito come:

$$c = \sum_{i=1}^{m} N_i y_i b_i = N_1 y_1 b_1 + ... + N_m y_m b_m$$

É possibile verificare che c é una soluzione del sistema, ovvero che $c \equiv b_j \bmod n_j$ per $j \neq i$. Valendo $n_j \mid N_i$ per qualsiasi $j \neq i$, é possibile scrivere $N_i \equiv 0 \bmod n_j$, e quindi $c \equiv N_j y_j b_j \bmod n_j$. Avendo trovato che vale $N_j n_j \equiv 1 \bmod n_j$, moltiplicando ambo i membri per b_j si ha $N_j n_j b_j \equiv b_j \bmod n_j$ (questo é legittimo perché $N_j n_j$ e 1 sono primi fra di loro, esiste un lemma che lo prova).
Avendosi la soluzione c, sia c' un'altra soluzione del sistema. Allora deve valere $c \equiv c' \bmod n_i$, ovvero $n_i \mid c - c'$ per ogni i = $1, ..., m$. Poichè gli n_i sono a due a due coprimi, segue che anche N é divisore di

$c - c'$, ovvero $c \equiv c' \bmod N$. Questo dimostra che c è l'unica soluzione del sistema modulo N, a meno di multipli di N. $\square$

Esempio 2.7.5: Si consideri il seguente sistema di congruenze lineari, e lo si risolva:

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

Tale sistema rispetta le ipotesi del Teorema 2.7.3, dato che tutti i termini noti a sinistra dell'equivalenza sono pari ad 1, i termini noti a destra sono tutti positivi e sono tutti coprimi fra di loro a due a due.
Si ha allora $N = 3 \cdot 5 \cdot 7 = 105$. Per ciascuna congruenza lineare del sistema si calcoli $N_i = \frac{N}{n_i}$:

$$N_1 = \frac{N}{n_1} = \frac{105}{3} = 35 \qquad N_2 = \frac{N}{n_2} = \frac{105}{5} = 21 \qquad N_3 = \frac{N}{n_3} = \frac{105}{7} = 15$$

Da cui si ottengono le congruenze lineari:

$$\begin{aligned} N_1 y \equiv 1 \bmod n_1 &\Rightarrow 35y \equiv 1 \bmod 3 \Rightarrow 2y \equiv 1 \bmod 3 \Rightarrow y_1 = 2 \\ N_2 y \equiv 1 \bmod n_2 &\Rightarrow 21y \equiv 1 \bmod 5 \quad \Rightarrow y \equiv 1 \bmod 5 \Rightarrow y_2 = 1 \\ N_3 y \equiv 1 \bmod n_3 &\Rightarrow 15y \equiv 1 \bmod 7 \quad \Rightarrow y \equiv 1 \bmod 7 \Rightarrow y_3 = 1 \end{aligned}$$

La soluzione del sistema é allora data da:

$$c = \sum_{i=1}^{3} N_i y_i b_i = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

E da tutti gli interi a questo congruenti modulo N.