Università degli studi di Modena e Reggio Emilia

Dipartimento di Ingegneria Enzo Ferrari

Matematica Discreta

Anno Accademico 2023/24

Indice

Capitolo 1

Complementi su insiemi e relazioni

1.1 Funzioni

Una **funzione** o **applicazione** tra due insiemi A e B è una legge per cui per ogni elemento del primo insieme esiste uno e un solo elemento del secondo insieme e viene rappresentata:

$$f : A \to B \; t.c. \; \forall a \in A \; \exists! b \in B \mid f(a) = b$$

b è l'**immagine** di a.

Proprietà delle Funzioni

1. la funzione si dice **iniettiva** se vale che: $\forall a, a' \in A, \; f(a) = f(a') \Rightarrow a = a'$.
2. la funzione si dice **suriettiva** sevale che: $\forall b \in B, \exists a \in A \mid f(a) = b$.
3. una funzione $f : A \to B$ si dice **biettiva** o **biunivoca** se è contemporaneamente *iniettiva* e *suriettiva* ovvero se:

$$\boxed{\forall b \in B} \quad \boxed{\exists! a \in A} \; t.c. \; f(a) = b$$

il box rosso identifica l'**iniettività**, mentre il box verde identifica la **suriettività**.

1.2 Insiemi Discreti

Due insiemi A e B si dicono **equipotenti** (o con la stessa **cardinalità**) se:

$$f : A \to B,\ f\ biunivoca$$

Siccome f è **biunivoca** avremo che ogni elemento di A avrà **uno e un solo** elemento di B distinto e B sarà formato da sole immagini di A portando i due insieme ad avere "lo stesso numero" di elementi, utilizzeremo come notazione: $\#A = \#B$. Un insieme A si dice **finito** se:

$$\exists n \in \mathbb{N},\ f : A \to \mathbb{N}_n,\ f\ biunivoca$$

$A = \{\square, \boxdot, \blacksquare\}$	contando i simboli dell'insieme A si va a creare
$\mathbb{N}_3 = \{1, 2, 3\}$	un'associazione tra gli elementi di A e di $\mathbb{N}_3$

In questo caso diremo che la **cardinalità** di A è **n**: $\#A = \#\mathbb{N}_n = n$
Un insieme A si dice **numerabile** se:

$$\exists f : A \to \mathbb{N},\ f\ biunivoca$$

In questo caso si dice che A ha cardinalità numerabile e si può rappresentare attraverso la lettera **aleph** (è la prima lettera dell'alfabeto ebraico): $\#A = \#\mathbb{N} = \aleph_0$ (si ricordi: **il Paradosso dell'albergo di Hilbert**).
Alcuni esempi:

1. l'insieme $\mathbb{Z}$ è **numerabile** ($\#\mathbb{N} = \#\mathbb{Z}$):

$$\begin{array}{cc} & 0 \to 1 \\ 1 \to 2 & -1 \to 3 \\ 2 \to 4 & -2 \to 5 \end{array}$$

   possiamo quindi mappare i valori **positivi** dell'insieme $\mathbb{Z}$ sono mappati nei valori **pari** dell'insieme $\mathbb{N}$ e in maniera complementare i valori **negativi** dell'insieme $\mathbb{Z}$ sono mappati nei valori **dispari** dell'insieme $\mathbb{N}$. È quindi possibile verificare la biunivocità dell'applicazione che mappa i valori da $\mathbb{Z}$ a $\mathbb{N}$.

2. l'insieme dei numeri **pari** $\mathbb{P}$ può definirsi numerabile, infatti: $\#\mathbb{P} = \#\mathbb{N}$, in questo caso avremo l'applicazione biunivoca del tipo:

$$f : \mathbb{P} \to \mathbb{N} \mid \forall p = 2n \in \mathbb{P},\ f(p) = \frac{1}{2}p = n$$

Se A è finito di cardinalità **n**, i suoi elementi possono essere etichettati con gli elementi di $\mathbb{N}_n$: $A = \{a_1, a_2, ..., a_n\}$

Se A è numerabile, gli elementi possono essere "etichettati" con gli elementi di $\mathbb{N}$: $A = \{a_1, a_2, ..., a_n, ...\} = \{a_i \mid i \in \mathbb{N}\}$

Un insieme A si dice **discreto** se è **finito** o **numerabile** (tutti gli insiemi *numerabili* sono infiniti, ma non tutti gli insimi infiniti sono numerabili)

Funzione Caratteristica: è un'applicazione ce determina se un elemento appartiene o meno ad un sottoinsieme Y di A ($Y \subseteq A$). Quindi diremo che dato un insieme discreto A ed un suo sottoinsieme $Y \subseteq A$ si dice **funzione caratteristica** di Y la funzione:

$$f_Y : A \to \{0, 1\} \; \forall a \in A \qquad f_Y(a) = \begin{cases} 1 & se\ a \in A \\ 0 & se\ a \notin A \end{cases}$$

Nel caso in cui A sia un insieme finito avremo che: $\#A = \sum_{a \in A} f_Y(a)$.
Se A è un insieme discreto, ed $f : A \to \{0, 1\}$ una applicazione a valori in $\{0, 1\}$, risulta univocamente determinato il sottoinsieme $Y \subseteq A$ tale che f sia una funzione caratteristica di Y:

$$Y = \{a \in A \mid f(a) = 1\}$$

Un esempio, definiamo $A = \mathbb{N}$ e sia $f : A \to \{0, 1\}$ definita da una **funzione caratteristica** del tipo: $n \to \frac{1+(-1)^n}{2}$. In questo caso la funzione f identifica, a partire dall'insieme $\mathbb{N}$, il sottoinsieme $\mathbb{P}$ dei numeri pari.
Utilizzando la **funzione caratteristica** si può ricavare la seguente proprietà degli insiemi discreti:

- se A è finito di cardinalità n, l'insieme $\mathcal{P}(a)$ delle **parti di A** è in corrispondenza biunivoca con l'**insieme delle n-ple** a valori in $\{0, 1\}$.
- se A è numerabile, l'insieme $\mathcal{P}(a)$ delle parti di A è in corrispondenza biunivoca con l'**insieme delle successioni** a valori in $\{0, 1\}$.

1.2.1 Proprietà 1

Se X e Y sono insiemi **finiti**, con $\#X = n$, $\#Y = m$ e con $X \cap Y = \emptyset$, allora $\#(X \cup Y) = n + m$.
Dimostrazione: per Hp. esistono due funzioni biettive $f : X \to \mathbb{N}_n$ e $g : Y \to \mathbb{N}_m$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}_{n+m}$. Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & se\ c \in X \\ g(c) + n & se\ c \in Y \end{cases}$$

1.2.2 Proprietà 2

Se X è un insieme **finito** con $\#X = n$ ed Y è un insieme **numerabile**, con $X \cap Y = \emptyset$ allora $\#(X \cup Y)$ è **numerabile**.

Dimostrazione: per Hp. esistono due funzioni biettive $f : X \to \mathbb{N}_n$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$. Possiamo porre $\forall c \in X \cup Y$ come:

$$h(c) = \begin{cases} f(c) & se\ c \in X \\ g(c) + n & se\ c \in Y \end{cases}$$

1.2.3 Proprietà 3

Se X e Y sono due insiemi **numerabili**, allora anche $X \cup Y$ è **numerabile**.

Dimostrazione: senza perdere di generalità, supponiamo che $X \cap Y = \emptyset$. Per ipotesi esistono due funzioni biettive $f : X \to \mathbb{N}$ e $g : Y \to \mathbb{N}$. Per dimostrare la proprietà occorre costruire una funzione biettiva $h : X \cup Y \to \mathbb{N}$. Ad esempio, $\forall c \in (X \cup Y)$, si può porre:

$$h(c) = \begin{cases} 2f(c) - 1 & se\ c \in X \\ 2g(c) & se\ c \in Y \end{cases}$$

Proposizione: se X è un insieme numerabile e $Y \subseteq X$ allora Y è un insieme **discreto**.

1.2.4 Proprietà 4

Se $\{A_i \mid i \in \mathbb{N}\} = \{A_1, A_2, ..., A_i, ...\}$ è un **insieme numerabile** di **insiemi numerabili**, si ha che:

$$\#(\bigcup_{i \in \mathbb{N}} A_i) = \#\mathbb{N}$$

Dimostrazione: senza perdere di generalità, supponiamo che gli insiemi siano fra loro **disgiunto**: $A_i \cap A_j = \emptyset, \ \forall i \in j$. Per dimostrare la tesi, utilizziamo il *procedimento diagonale di **Cantor***, enumerando per righe gli elementi di ciascun insieme, dove avremo come primo indice l'identificativo dell'insieme e come secondo indice quello della colonna:

$$\begin{array}{lllllll}
A_1\colon & a_{11} & a_{12} & a_{13} & \dots & a_{1h} & \dots \\
A_2\colon & a_{21} & a_{22} & a_{23} & \dots & a_{2h} & \dots \\
A_3\colon & a_{31} & a_{32} & a_{33} & \dots & a_{3h} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
A_i\colon & a_{i1} & a_{i2} & a_{i3} & \dots & a_{ih} & \dots \\
\dots & \dots & .. & \dots & \dots & \dots & \dots
\end{array}$$

Consideriamo le diagonali $D_1 = \{a_{11}\}$, $D_2 = \{a_{21}, a_{12}\}$, ..., D_k, ..., dove: $D_k = \{a_{ij} \mid i + j = k + 1\}$, dove il valore delle j identifica la posizione all'interno della diagonale D_k. Notiamo che sono composte da finiti elementi. Per dimostrare che $\#(\bigcup_{i\in\mathbb{N}} A_i)$ è **numerabile**, occorre costruire una applicazione biunivoca, tale che:

$$h : \bigcup_{i\in\mathbb{N}_n} A_i \to \mathbb{N}$$

Idealmente, vorremmo etichettare, ogni generico elemento a_{ij} che apparterrà alla $k-esima$ diagonale, in questo modo si creerà l'applicazione *biunivoca*.

$\#D_k = k$ $\quad\to$ ci serve la somma delle cardinalità delle $\to$ $\quad \sum_{k=1}^{i+j-2} \#D_k = \frac{(i+j-2)\cdot(i+j-1)}{2}$
diagonali precedenti alla diagonale tale
che $a_{ij} \in D_k$

In questo modo abbiamo "etichettato" tutti gli elementi appartenenti alle diagonali precedenti alla diagonale di riferimento D_k, ora ci mancano da "etichettare" gli elementi che precendo a_{ij} sulla diagonale, ma sapendo che a_{ij} è il **j-esimo** elemento allora basterà:

$$h(a_{ij}) = j + \frac{(i+j-2)(i+j-1)}{2}$$

In questo modo abbiamo "etichettato" anche tutti gli elementi che precedono il nostro a_{ij}, ma in direttamente abbiamo descritto un'applicazione **biunivoca** tra $\bigcup_{i\in\mathbb{N}_n} A_i$ e $\mathbb{N}$, ovvero $h(a_{ij})$ che quindi ci permette di dimostrare che anche $\bigcup_{i\in\mathbb{N}_n} A_i$ è **numerabile**.

Conseguenze:

- $\mathbb{Z}$ è numerabile: $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$.
- $\mathbb{N} \times \mathbb{N}$ è numerabile: $\mathbb{N} \times \mathbb{N} = \{(n, m) \mid n, m \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}}\{(n, m) \mid m \in \mathbb{N}\}$.
- $\mathbb{Q}$ è numerabile.

Off-Topic:

Paradosso del Grand Hotel di Hilbert: il paradosso del *Grand Hotel* inventato dal matematico *David Hilbert* per mostrare alcune caratteristiche del concetto di infinito e le differenze fra opzioni con insieme finiti ed infiniti. Hilbert immagina un hotel con infinite stanze, tutte occupate, e afferma che qualsiasi sia il numero di altri ospiti che sopraggiungano, sarà sempre possibile ospitarli tutti, anche se il loro numero è infinito, purché numerabile.
Nel caso semplice, arriva un singolo nuovo ospite. Il furbo albergatore sposterà tutti i clienti nella camera successiva (l'ospite della 1 alla 2, quello della 2 alla 3, etc.); in questo modo, benché l'albergo fosse pieno è comunque, essendo infinito, possibile sistemare il nuovo ospite.
Un caso meno intuitivo si ha quando arrivano infiniti nuovi ospiti. Sarebbe possibile procedere nel modo visto in precedenza, ma solo scomodando infinite volte gli ospiti (già spazientiti dal precedente spostamento): sostiene allora Hilbert che la soluzione sta semplicemente nello spostare ogni ospite nella stanza con numero doppio rispetto a quello attuale (dalla 1 alla 2, dalla 2 alla 4,etc.), lasciando ai nuovi ospiti tutte le camere con i numeri dispari, che sono essi stessi infiniti, risolvendo dunque il problema. Gli ospiti sono tutti dunque sistemati, benché l'albergo fosse pieno.

1.3 Confronto tra Cardinalità

Si dice che un insieme A ha **cardinalità minore o uguale** ad un insieme B (e si indica con: $\#A \leq \#B$) se: $\exists f : A \to B,\ f$ è *iniettiva*.

Proprietà:

- **riflessività**: $\forall A,\ \#A \leq \#A$.
- **transitività**: $\#A \leq \#B,\ \#B \leq \#C \Rightarrow \#A \leq \#C$.
- **antisimmetria**: $\#A \leq \#B,\ \#B \leq \#A \Rightarrow \#A = \#B$.
- **tricotomia**: $\forall A, B \Rightarrow \#A \leq \#B \ o\ \#B \leq \#A$.

La relazione "$\leq$" fra cardinalità è una relazione di ordine totale.

Lemma: $A \subseteq B \subseteq C$ con $\#A = \#B \Rightarrow \#A = \#B = \#C$.

Teorema di Cantor-Bernstein-Schroeder: Se $\exists f : A \to B,\ f$ *iniettiva* ed $\exists g : B \to A,\ g$ *iniettiva* allora $\exists h : A \to B,\ h$ *biunivoca*.

Dimostrazione: poiché f e g sono iniettive se le restriangamo alla loro immagine biunivoca:

$$\#A = \#f(A) \ con \ f(A) \subseteq B$$
$$\#B = \#g(B) \ con \ g(B) \subseteq A$$

Avremo:

$$g(f(A)) \subseteq g(B) \subseteq A \Rightarrow \#g(f(A)) = \#f(A) = \#A$$

e per il lemma possiamo dire che $\#g(B) = \#A$ e $\#g(B) = \#B$ e quindi avremo che $\#A = \#B$, questo implica che esiste una funzione $h : A \to B$ biunivoca.

Teorema di Cantor: se A è un insieme **numerabile** allora $\mathcal{P}(A)$ ha cardinalità **maggiore** di A:

$$\#A \leq \#\mathcal{P}(A) \ con \ \#A \neq \#\mathcal{P}(A)$$

Dimostrazione:

- dimostriamo per prima cosa che $\#A \leq \#\mathcal{P}(A)$ basta trovare una funzione definita $f : A \to \mathcal{P}(A)$ che sia **iniettiva** e non biunivoca.

  $$f(a) = \{a\}$$

  Utilizziamo una **dimostrazione per assurdo**: sappiamo che $\mathcal{P}(A)$ è in corrispondenza biunivoca con le successioni a valori in $\{0, 1\}$; allora se $\mathcal{P}(A)$ fosse numerabile sarebbe possibile elencare tutte le successioni a valori in $\{0, 1\}$:

$$\begin{array}{ccccccc}
S_1: & S_{11} & S_{12} & S_{13} & \dots & S_{1n} & \dots \\
S_2: & S_{21} & S_{22} & S_{23} & \dots & S_{2n} & \dots \\
S_3: & S_{31} & S_{32} & S_{33} & \dots & S_{3n} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots \\
S_j & S_{j1} & S_{j2} & S_{j3} & \dots & S_{jn} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}$$

Consideriamo la successione a valori in $\{0, 1\}$:

$$\bar{S} = \bar{S}_1,\ \bar{S}_2,\ \bar{S}_3,\ \dots,\ \bar{S}_j,\ \dots \ || \ \text{dove} \ \bar{S}_j \neq S_{jj}$$

In questo modo la successione $\bar{S}$ non coincide con nessuna delle successioni s_j, $\forall j \in \mathbb{N}$, poiché differisce dalla j-esima successione nel j-esimo elemento e quindi arriviamo ad un **assurdo**. Quindi l'insieme delle successioni a valori in $\{0, 1\}$ non può essere numerabile e, quindi, **non** è **numerabile** nemmeno $\mathcal{P}(A)$.

La Cardinalità di $\mathbb{R}$: anche $\mathbb{R}$ **non** è **numerabile**, infatti: $\#\mathbb{R} = \#]0, 1[$, consideriamo un'applicazione biunivoca tale che $f : \mathbb{R} \to]0, 1[$, ad esempio:

$$f(x) = \tfrac{x}{|x|+1} \; \forall x \in \mathbb{R}$$

che stabilisce biunivocità tra $\mathbb{R}$ e $]-1, 1[$ possiamo affermare che $\#\mathcal{P}(\mathbb{N}) = \#]0, 1[$, infatti considerando $\forall x \in]0, 1[$ come la rappresentazione binaria (con virgola) di x; se ϵ_n è l'n-esima cifra dopo la virgola di tale sviluppo $(\epsilon_1, \epsilon_2, ..., \epsilon_n, ...)$ è una successioni a valori in $\{0, 1\}$ quindi

$$0, \bar{9} = 1 \in \mathbb{R} \; || \text{ viene a perdersi la biunivocità}$$
$$\Rightarrow \#\mathbb{R} = \#\mathcal{P}(\mathbb{N})$$

Questa tipologia di cardinalità viene definita **cardinalità del continuo** e si denota con **c** o con $2^{\aleph_0}$.

> **Congettura** (*ipotesi del continuo*)
> non esistono cardinalità comprese fra $\#\mathbb{N}$ e $\#\mathbb{R}$.

> **Congettura** (*ipotesi generalizzata del continuo*)
> non esistono cardinalità comprese tra $\#X$ e $\mathcal{P}(X) = 2^{\#X}$ $\forall X$ di cardinalità non finita.

1.4 Relazioni di Equivalenza

Una **relazione** $\mathcal{R}$ tra due insiemi A e B è un **sottoinsieme** del **prodotto cartesiano** fra A e B, ovvero $\mathcal{R} \in A \times B$.

> **Esempio**
> $\mathcal{R} =' \leq '$ è relazione tra i due insiemi $A = \mathbb{N}$ e $B = \mathbb{N}$, poiché definisce un sottoinsieme del prodotto cartesiamo $\mathbb{N} \times \mathbb{N}$.
> Ad esempio: $(1, 2) \in \mathcal{R}$ e $(2, 1) \notin \mathcal{R}$.

Una relazione $\mathcal{R}$ su A si dice **relazione di equivalenza** se sono vere le seguenti proprietà:

- *riflessività*: $\forall a \in A \Rightarrow a\mathcal{R}a$

- *simmetria*: $\forall a, b \in A \; : \; a\mathcal{R}b \Rightarrow b\mathcal{R}a$
- *transitività*: $\forall a, b, c \in A \; : \; a\mathcal{R}b \text{ e } b\mathcal{R}c \Rightarrow a\mathcal{R}c$

Definizione: sia $\mathcal{R}$ una **relazione di equivalenza** su A. Per ogni $a \in A$ si dice **classe di equivalenza** $[a] = \{x \in A \mid x\mathcal{R}a\}$.

Proprietà:

- $\forall a \in A, \; a \in [a]$

  Dimostrazione: è conseguenza diretta della proprietà riflessiva.
- $\forall a, b \in A, \; a \in [b] \Rightarrow [b] = [a]$

  Dimostrazione: poiché $a \in [b]$, $a\mathcal{R}b$. Se $x \in A$, $x \in [a]$, allora $x\mathcal{R}a$; per la **proprietà transitiva** segue $x\mathcal{R}v$ ovvero $x \in [b]$. Resta così dimostrato che $[a] \subseteq [b]$. Analogamente, se $y \in A$, $y \in [b]$, allora $y\mathcal{R}b$ per la **proprietà di simmetria**, $a\mathcal{R}b \Rightarrow b\mathcal{R}a$, per cui la transitività assicura $y\mathcal{R}a$, ovvero $y \in [a]$. Resta così dimostrato che $[b] \subseteq [a]$ e quindi $[b] = [a]$.
- $\forall a, b \in A, \; [a] = [b]$ *oppure* $[a] \cap [b] \neq \emptyset$

  Dimostrazione: se $\exists c \in [a] \cap [b]$, si ha $c \in [a] ec \in [b]$, ovvero $c\mathcal{R}a$ e $c\mathcal{R}b$. Applicando la **proprietà di simmetria** a $c\mathcal{R}a$ si ottiene $a\mathcal{R}c$, per cui la proprietà transitiva assicura $a\mathcal{R}b$, ovvero $a \in [b]$. La seconda proprietà implica $[a] = [b]$. Quindi, se due classi hanno un elemento in comune, le due classi coincidono.

Insieme Quoziente: sia A un insieme ed $\mathcal{R}$ una relazione di equivalenza su A. Si definisce **insieme quoziente** di A rispetto ad $\mathcal{R}$,

$$\tfrac{A}{\mathcal{R}} = \{[a] \mid a \in A\}$$

Rappresentante di una classe d'equivalenza: sia A un insieme ed $\mathcal{R}$ una relazione di equivalenza su A. Ogni elemento $x \in [a]$, si dice **Rappresentante** di $[a] \in \frac{A}{\mathcal{R}}$.

Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{R}$ definita da:

$$(a, b) \in \mathbb{R} \text{ se e solo se } a - b \in \mathbb{Z}$$

L'insieme quoziente $\frac{\mathbb{R}}{\mathcal{R}}$ è in corrispondenza biunivoca con $[0, 1[$: ogni classe può infatti avere come rappresentante significativo il suo unico elemento nell'intervallo $[0, 1[$.

Esempio: sia $\mathcal{R}$ la **relazione di equivalenza** su $\mathbb{N}_0 \times \mathbb{N}_0$ definita da:

$$(a,b)\mathcal{R}(a',b') \text{ se e solo se } a+b'=a'+b$$

In generale:

- se $a=b$, $[(a,b)] = \{(n,n) \mid n \in \mathbb{N}\}$
- se $a<b$, $[(a,b)] = \{(n, n+b-a) \mid n \in \mathbb{N}\}$
- se $a>b$, $[(a,b)] = \{n+a-b, n \ \mid n \in \mathbb{N}\}$

Allora l'insieme quoziente $\frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ è in relazione biunivoca con $\mathbb{Z}$.

Esempi

Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{N}$ definita da $(a,b) \in \mathcal{R}$ se e solo se $(-1)^a = (-1)^b$. L'**insieme quoziente** è formato da due classi $\frac{\mathbb{N}}{\mathcal{R}} = \{\mathbb{P}, \mathbb{D}\}$

Sia $\mathcal{R}$ la relazione di equivalenza su $\mathbb{R}$ definita da $(a,b) \in \mathbb{R}$ se e solo se $\lfloor a \rfloor = \lfloor b \rfloor$. L'**insieme quoziente** è in corrispondenza biunivoca con $\mathbb{Z}$ (il passaggio da $\mathbb{R}$ a $\frac{\mathbb{R}}{\mathcal{R}}$ è un esempio di **discretizzazione**): $\frac{\mathbb{R}}{\mathcal{R}} = \{[n, n+1[, n \in \mathbb{Z}\}$

1.5 Congruenza modulo n

Definizione: fissa un intero $n \in \mathbb{N}$, si definisce una relazione di equivalenza $\equiv_n$ su $\mathbb{Z}$:

$$x \equiv_n y \text{ se e solo se } \exists h \in \mathbb{Z} \mid y-x = h \cdot n$$

Verifichiamo che $\equiv_n$ è una **relazione di equivalenze**:

- **riflessività**: $\forall x \in \mathbb{Z}$, $x \equiv_n x$ è verificato, poiché $x-x = h \cdot n$ considerando $h=0 \in \mathbb{Z}$.
- **simmetria**: se $x \equiv_n y$, per definizione $\exists h \in \mathbb{Z}$ tale che $y-x = h \cdot n$. Per dimostrare che $y \equiv_n x$ devo trovare un $h' \in \mathbb{Z} \mid x-y = h' \cdot n$. Basta prendere $h' = -h$.
- **transitività**: se $x \equiv_n y$ e $y \equiv_n <$, allora $\exists h \in \mathbb{Z} \mid y-x = h \cdot n$ ed $\exists k \in \mathbb{Z} \mid z-y = k \cdot n$. Sommando membreo a membro, si ottiene $z-x = (h+k) \cdot n$; siccome $h+k \in \mathbb{Z}$ segue che $x \equiv_n z$.

Insieme delle classi resto modulo n: l'insieme quoziente $\mathbb{Z}/\equiv_n$ è detto **insieme delle classi resto modulo** n ed è indicato con $\mathbb{Z}_n$: $\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv_n}$.
L'insieme delle classi resto modulo n è costituito da:

$$\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$$

Dimostrazione: Per ogni $x \in \mathbb{Z}$, la divisione euclidea per n assicura che $\exists q, r \in \mathbb{Z},\ 0 \leq r < n$ tali che $x = q \cdot n + r$, ovvero che $x - r = q \cdot n$. Quindi, $x \equiv_n r$, da cui $[x] = [r]$, con $r \in \{0, 1, ..., n-1\}$. Occorre provare che le n classi $[0], [1], ..., [n-1]$ sono a due a due disgiunte, ovvero che $\forall r, s \in \mathbb{Z},\ 0 \leq r < s < n \Rightarrow [r] \neq [s]$. Per **assurdo** supponiamo $[r] = [s]$, questo significherebbe che che $\exists h \in \mathbb{Z} \mid s - r = h \cdot n$. Per ipotesi $s > r$, per cui $0 < s - r < n$; quindi $s - r$ **non** può essere multiplo intero di n.

Divisione euclidea: $\forall a, b \in \mathbb{Z},\ b \neq 0 \Rightarrow \exists q, r \in \mathbb{Z},\ 0 \leq r < |b| \mid a = b \cdot q + r$.

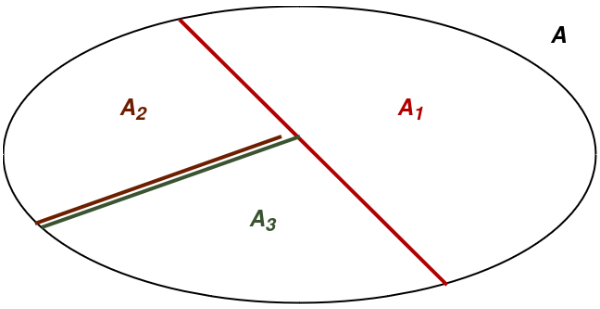


Figura 1.1: **Partizionamento**

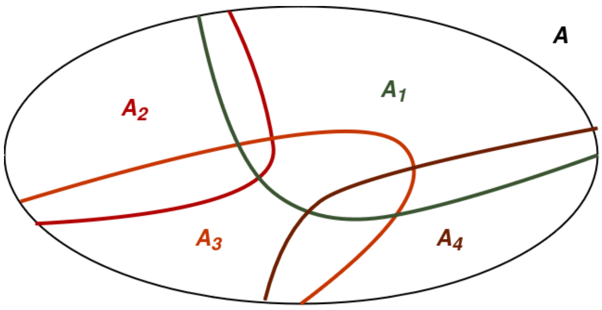


Figura 1.2: **Ricoprimento**

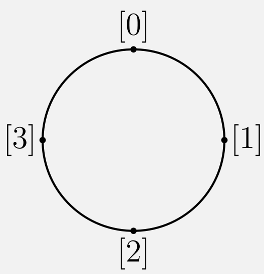
Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **partizione** di A se $\emptyset \notin \mathcal{B}$ e $\forall c \in A,\ \exists! B \in \mathcal{B} \mid x \in B$. Ovvero ogni sottoinsieme non ha intersezione con gli altri.

Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **ricoprimento** di A se $\forall x \in A,\ \exists B \in \mathcal{B} \mid x \in B$.

Se $\mathcal{R}$ è relazione di equivalenza su A, allora l'insieme quoziente $\frac{A}{\mathcal{R}} = \mathcal{B}$ è una partizione di A. Viceversa se $\mathcal{B}$ è una partizione di A, $\exists! \mathcal{R}$ relazione di equivalenza su A tale che $\frac{A}{\mathcal{R}} = \mathcal{B}$ allora $\mathcal{R}$ è definita da:

$$x\mathcal{R}y \Leftrightarrow \exists B \in \mathcal{B} \mid x, y \in B$$

$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$



$\mathbb{Z}$ è più facilmente rappresentabile tramite una circonferenza

Capitolo 2

Gli Interi e la Divisibilità

2.1 Strutture algebriche elementari

Una **operazione binaria intera** su un insieme G è un'applicazione

$$* \; : \; G \times G \rightarrow G$$

L'immagine della coppia (x, y) si denoterà con $x * y$.

- $e \in G$ si dice **elemento neutro** rispetto a $*$ se:

$$g * e = e * g = g \; \forall g \in G$$

- un elemento $g \in G$ si dice invertibile se esiste $\bar{g} \in G$ tale che $g * \bar{g} = \bar{g} * g = e$

2.1.1 Gruppi

La coppia $(G, *)$, con $*$ operazione su G, si dice **gruppo** se vengono rispettate le seguenti proprietà:

- $*$ è **associativa**: $\forall g, g', g'' \in G$ si ha $(g * g') * g'' = g * (g' * g'')$
- esiste l'elemento **neutro**
- ogni elemento di G è invertibile

Il gruppo si dice **abeliano** o **commutativo** se:

$$\forall g, g' \in G, \; g * g' = g' * g \text{ (proprietà } \textbf{commutativa}\text{)}$$

Alcuni esempi:

- $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$ non sono gruppi. In quanto non né in $\mathbb{N}$ né in $\mathbb{Z}$ è presente per ogni elemento dell'insieme l'elemento inverso, in $\mathbb{N}$ non sono presenti elementi negativi, quindi nessun elemento avrà un'altro elemento che sommato a se stesso dia 0, viceversa l'insieme $\mathbb{Z}$ dove sono presenti elementi positivi e negativi viene, invece, definita l'operazione $\cdot$ che richiede i reciproci dei singoli elementi affiché possano essere definiti gli elementi inversi.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, \cdot)$ sono gruppi abelliani

2.1.2 Anelli

La terna $(\mathbb{A}, +, \cdot)$ con $\mathbb{A}$ un insieme e $+, \cdot$ (somma e prodotto) due operazione binarie interne a $\mathbb{A}$, si dice **anello** se:

- $(\mathbb{A}, +, \cdot)$ è un gruppo **abeliano** (con elemento neutro 0).
- il prodotto è **associativo**.
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ e $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ (il prodotto è distribuito rispetto alla somma).

Un anello $(\mathbb{A}, +, \cdot)$ è detto **commutativa** se il prodotto è commutativo, mentre è detto **unitario** o con **unità** se $(\mathbb{A}, \cdot)$ ammette l'elemento neutro. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sono anelli.

2.1.3 Campi

La terna $(\mathbb{K}, +, \cdot)$ con $\mathbb{K}$ un insieme e $+, \cdot$ (somma e prodotto) due operazioni binarie interne a $\mathbb{K}$, si dice **campo** se:

- $(\mathbb{K}, +)$ è un gruppo **abeliano** (con elemento neutro 0).
- $(\mathbb{K} - \{0\}, \cdot)$ è un gruppo **abeliano** (con elemento neutro 1).
- per ogni $x, y, z \in \mathbb{K}$ si ha $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ quindi il prodotto è distribuito rispetto alla somma.

In qualunque campo vale la **legge di annullamento del prodotto**:

$$x \cdot y = 0 \rightarrow x = 0 \text{ oppure } y = 0$$

2.1.4 Domini d'integrità

Divisori dello zero: sia $(A, +, \cdot)$ un anello. Due elementi $a, b \in A$ si dicono **divisori dello zero** se $a \neq 0$, $b \neq 0$, ma $a \cdot b = 0$. Ovvero, può succedere che in un anello due elementi non nulli il cui prodotto fa 0.

Ad esempio l'anello delle matrici quadrate presenta dei divisori dello zero, infatti due matrici non nulle è possibile che il loro prodotto presenti la matrice nulla.

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$$

$$A \cdot B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} (1 \cdot 1 + 1 \cdot -1) & (1 \cdot -1 + 1 \cdot 1) \\ (1 \cdot 1 + 1 \cdot -1) & (1 \cdot -1 + 1 \cdot 1) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Dominio di Integrità: Un anello commutativo privo di divisori dello zero si dice **dominio di integrità**.

Ad esempio $(\mathbb{Z}, +, \cdot)$ è un **anello commutativo unitario** privo di divisori dello zero. Quindi è dominio di integrità.

2.2 L'anello dei numeri interi

È noto che $\exists h \mid h : \mathbb{Z} \to \frac{\mathbb{N}_0 \times \mathbb{N}_0}{\mathcal{R}}$ dove la relazione di equivalenza che si vuole definire è $\equiv_n$. Su questo insieme vengono **ben poste** le seguenti operazioni:

$$\boxplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$((m, n), (m', n')) \mapsto [(m, n)] \boxplus [(m', n')] \stackrel{\text{def}}{=} [(m + m', n + n')]$$
$$\boxdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$((m, n), (m', n')) \mapsto [(m, n)] \boxdot [(m', n')] \stackrel{\text{def}}{=} [(mm' + nn', mn' + m'n)]$$

Definito questo possiamo dire che $(\mathbb{Z}, \boxplus, \boxdot)$ è **dominio di integrità**.

2.3 Teoria della Divisibilità

Divisibilità: dati due numeri $a, b \in \mathbb{Z}$, si dice che a **divide** b (e si scrive $a|b$) se: $\exists c \in \mathbb{Z} \mid b = a \cdot c$

Esempi

- $2|12, \ \exists c \; t.c. \; 2 \cdot c = 2 \cdot 6 = 12$
- $3|7m \; \nexists c \; t.c. \; 3 \cdot c = 7 \; \forall c \in \mathbb{Z}$

Proprietà:

- **transitività**: se $n|m$ e $m|q$ allora $n|q$.

  Dimostrazione

  Hp. $\exists h \in \mathbb{Z} \mid m = h \cdot n \qquad \exists h' \in \mathbb{Z} \mid q = h' \cdot m$

  Sostituendo la prima relazione nella seconda si ottiene $q = h' \cdot h \cdot n$. Poichè $h' \cdot h \in \mathbb{Z}$ abbiamo definito che $n|q$.

- se $n|m$ e $m|n$, allora $m \pm n$.

  Dimostrazione

  Hp. $\exists h \in \mathbb{Z} \mid m = h \cdot n \qquad \exists h' \in \mathbb{Z} \mid n = h' \cdot m$

  Andiamo a sostituire la seconda alla prima equazione:

  $$n = h' \cdot h \cdot m$$
  $$n - h' \cdot h \cdot m = 0$$
  $$n \cdot (1 - h' \cdot h) = 0$$

  Essendo che $\mathbb{Z}$ è un **dominio di integrità**, segue che o $n = 0$ oppure $(1 - h' \cdot h) = 0 \rightarrow (h' \cdot h) = 1$, consideriamo che $n \leq 0$ e che quindi $h' \cdot h = 1$ sappiamo che h ammette un inverso h', da cui $h = h' = 1$ o $h = h' = -1$ (in $\mathbb{Z}$, gli unici elementi che ammettono inverso sono 1 e -1). In questo modo sappiamo che $m = n$ oppure $m = -n$.

2.4 Massimo Comune Divisore

Dati $a, b \in \mathbb{Z}$ non entrambi nulli, si dice che $d \in \mathbb{Z}$ è **UN massimo comune divisore** tra a e b se valgono contemporaneamente le due proprietà:

$$d|a \text{ e } d|b \qquad \forall d' \in \mathbb{Z} \mid d'|a,\ d'|b \Rightarrow d'|d$$

Se d e d' sono due massimi comuni divisori tra a e b allora $d' = \pm d$.

Dimostrazione

$\forall d' \in \mathbb{Z} \;\Rightarrow\; d'|a,\ d|b \;\Rightarrow\; d'|d \;\Rightarrow\; d = \pm d'$

$\forall d \in \mathbb{Z}\ d|a,\ d|b \;\Rightarrow\; d|d'$

Dati $a, b \in \mathbb{Z}$ non entrambi nulli, si dice che $d \in \mathbb{Z}^+$ è **IL massimo comune divisore** (***Greatest Common Divisor***) tra a, b se d è un *massimo comune divisore* fra a e b (fra i due possibili **MCD** prendo il massimo, quindi quello positivo).

$$d = \gcd(a, b)$$

Esempio

Se $a|b$, allora $\gcd(a, b) = |a|$ e in particolare $\gcd(a, 0) = |a|\ \forall a \in \mathbb{Z} - \{0\}$

Dati $a, b \in \mathbb{Z}$ non entrambi nulla, allora $\boxed{\exists!\,\gcd(a, b)}$ e viene inoltre definita l'**Identità di *Bezout*** che rappresenta il massimo comun divisore come combinazione lineare di a e b:

$$\gcd(a, b) = a \cdot \alpha + b \cdot \beta$$

Questi valori (α e β) però non sono strettamente univocamente determinata, infatti in generale una coppia di numeri interi hanno più di un α e un β definiti.

Dimostrazione

Consideraiamo un insieme S costituito da tutte le combinazioni lineari intere di a, b che abbia però risultati strettamente positivi.

$$S = \{\lambda \cdot a + \mu \cdot b \mid \lambda, \mu \in \mathbb{Z},\ \lambda \cdot a + \mu \cdot b > 0\}$$

Osserviamo che l'insieme S non è vuoto ($S \neq \emptyset$), infatti almeno uno tra a e b non è nullo, infatti ponendo $a \neq 0$ è possibile affermare che:

$$|a| = (\text{segno}) \cdot a + 0 \cdot b \ \rightarrow \ |a| \in S$$

Osserviamo che S contiene unicamente numeri naturali possiamo dire che $S \subseteq \mathbb{N}$ non vuoto e che quindi $\exists \min(s) = d$ ovvero l'insieme è limitato inferiormente. Siccome $d \in S$ questo vuol dire che è rappresentabile come **combinazione lineare**, ovvero $\boxed{\exists \overline{\lambda}, \overline{\mu} \in \mathbb{Z}\ t.c.\ d = \overline{\lambda} \cdot a + \overline{\mu} \cdot b}$.

Adesso cerchiamo di dimostrare che questo d è proprio il massimo comune divisore che stavo cercando: $\boxed{\textbf{Th. } d = \gcd(a, b)}$ ovvero che $d|a$ e che $d|b$.

- partiamo dimostrando che $a|b$, andiamo a considerare la **divisione euclidea** tra a e d.

$$\exists q \in \mathbb{Z},\ \exists r \in \mathbb{Z},\ 0 \leq r < d \mid a = q \cdot d + r$$

$$\begin{aligned} r &= a - q \cdot d \\ &= a - q \cdot (\overline{\lambda} \cdot a + \overline{\mu} \cdot b) \\ &= a - q \cdot \overline{\lambda} \cdot a + q \cdot \overline{\mu} \cdot b \\ &= a \cdot \underbrace{\boxed{(1 - q \cdot \overline{\lambda})}}_{\in \mathbb{Z}} + b \cdot \underbrace{\boxed{q \cdot \overline{\mu}}}_{\in \mathbb{Z}} \end{aligned}$$

  In questo modo abbiamo scritto r come combinazione lineare di due interi, ma **se** $r \neq 0$ allora $r \in S$ siccome, però, $r < d$ e $d = \min(S)$ arriviamo ad un **assurdo**, quindi affinché vengano rispettati i vincoli bisogna che $r = 0 \quad \Rightarrow \quad a = q \cdot d + 0 = q \cdot d$ e quindi $\boxed{d|a}$

- in perfetta analogia si può dimostrare che $\boxed{d|b}$, partendo dalla **divisione euclidea** tra b e d.

- bisogna ora dimostrare che $\forall d' \in \mathbb{Z} \mid d'|a,\ d'|b \Rightarrow d'|d$. Poiché $d = \overline{\lambda} \cdot a + \overline{\mu} \cdot b$ allora bisognerà che $\boxed{\exists h \in \mathbb{Z} \mid a = d' \cdot h}$ e $\boxed{\exists k \in \mathbb{Z} \mid b = d' \cdot k}$. Usando queste due relazioni, segue che:

$$\begin{aligned} d &= \overline{\lambda} \cdot d' \cdot h + \overline{\mu} \cdot d' \cdot k \\ &= d' \cdot \underbrace{\boxed{[(\overline{\lambda} \cdot h) + (\overline{\mu} \cdot k)]}}_{\in \mathbb{Z}} \end{aligned}$$

  In questo modo siamo riusciti a dimostrare che $d'|d$.

Siamo riusciti a dimostrare il teorema di esistenza del **massimo comune divisore** in S, come il suo minimo: $d = \min(S) = \gcd(a, b)$

Siano $a, b \in \mathbb{Z}$, con $|a| \geq |b| > 0$. Se $a = b \cdot q + r$ è la **divisione euclidea** fra a e b allora avremo:

$$\{c \in \mathbb{Z} \mid c|a,\ c|b\} = \{c \in \mathbb{Z} \mid c|b,\ c|r\}$$

Ovvero l'insieme degli interi che dividono a e b sono gli stessi che dividono sia b che r, conseguenza di questo fatto è che:

$$\gcd(a, b) = \gcd(b, r)$$

Dimostrazione

- partiamo dal primo insieme: $\{c \in \mathbb{Z} \mid c|a,\ c|b\}$ andiamo a dimostrare che $\boxed{\textbf{Th. } c|r}$ (perché che $c|b$ è implicito per la costruzione del problema). Poiché $c|a$ e $c|b$ allora:

  $$\exists h \in \mathbb{Z} \text{ t.c. } a = c \cdot h \qquad \exists k \in \mathbb{Z} \text{ t.c. } b = c \cdot k$$

  Consideriamo ora la **divisione euclidea** tra a e b avremo che:

  $$\begin{aligned} r &= a - b \cdot q \\ &= c \cdot h - c \cdot k \cdot q \\ &= c \cdot \underbrace{(h - k \cdot q)}_{\in \mathbb{Z}} \end{aligned}$$

  Quindi in questo modo abbiamo dimostrato che $c|r$.

- affrontiamo ora il secondo insieme $\{c \in \mathbb{Z} \mid c|b,\ c|r\}$ e andiamo a dimostrare che $\boxed{\textbf{Th. } c|a}$ (perché che $c|b$ è implicito per la costruzione del problema). Poichè $c|b$ e $c|r$ allora:

  $$\exists h \in \mathbb{Z} \text{ t.c. } b = c \cdot h \qquad \exists k \in \mathbb{Z} \text{ t.c. } r = c \cdot k$$

  Consideriamo la **divisione euclidea** tra a e b avremo che:

  $$\begin{aligned} a &= b \cdot q + r \\ &= c \cdot h \cdot q + c \cdot k \\ &= c \cdot \underbrace{(h \cdot q + k)}_{\in \mathbb{Z}} \end{aligned}$$

  Quindi in questo modo abbiamo dimostrato che $c|a$.

Algoritmo delle Divisioni Successive (di Euclide)

Siano $a, b \in \mathbb{Z} - \{0\}$. Applicando ricorsivamente la divisione euclidea tra a e $|b|$, e poi tra **divisore** e **resto** della divisione:

$$
\begin{aligned}
a &= |b| \cdot q_1 + r_1 && \gcd(a, b) \\
b &= r_1 \cdot q_2 + r_2 && \gcd(b, r_1) \\
r_1 &= r_2 \cdot q_3 + r_3 && \gcd(r_1, r_2) \\
&\ldots && .. \\
r_{n-1} &= r_n \cdot q_{n+1} + 0 && \gcd(r_{n-1}, r_n) = r_n
\end{aligned}
$$

Poiché $r_1 > r_2 > r_3 > ... > r_i > ... \geq 0$, $\exists n \in \mathbb{N}$ t.c. $r_{n+1} = 0$ allora: $\gcd(a, b) = r_n$

Esempio: $\gcd(3522, 321) = ?$

$$
\begin{aligned}
3522 &= (10) \cdot 321 + \boxed{312} \\
321 &= (1) \cdot 312 + \boxed{9} \\
312 &= (34) \cdot 9 + \boxed{6} \\
9 &= (1) \cdot 6 + \boxed{3} \\
6 &= (2) \cdot 3 + 0
\end{aligned}
$$

Quindi: $\gcd(3522, 321) = 3$

È possibile utilizzando l'**Algoritmo delle Divisioni Successive** è possibile ricavare anche i parametri α e β dell'**Identità di Bezout** di a e b andando a ritroso e rappresentando il resto in funzione del valore di partenza e del dividendo.

Esempio:

$$
\begin{aligned}
\gcd(3522, 321) &= 3 \\
&= \boxed{9 - (1) \cdot 6} \\
&= 9 - (1) \cdot \boxed{[312 - (34) \cdot 9]} \\
&= 9 - 312 + (34) \cdot 9 \\
&= -312 + (35) \cdot 9 \\
&= -312 + (35) \cdot \boxed{[321 - (1) \cdot 312]} \\
&= -312 + (35) \cdot 321 - (35) \cdot 312 \\
&= (35) \cdot 321 - (36) \cdot 312 \\
&= (35) \cdot 321 - (36) \cdot \boxed{[3522 - (10) \cdot 321]} \\
&= (35) \cdot 321 - (36) \cdot 3522 + (360) \cdot 321 \\
&= \underbrace{\boxed{(-36)}}_{=\alpha} \cdot 3522 + \underbrace{\boxed{(395)}}_{=\beta} \cdot 321
\end{aligned}
$$

Avremo quindi: $\gcd(3522, 321) = 3 = \alpha \cdot 3522 + \beta \cdot 321 = (-36) \cdot 3522 + (395) \cdot 321$

Complessità computazionale: l'Algoritmo delle Divisioni Successive di Euclide per il calcolo del $\gcd(a, b)$ termina al più in $\boxed{2 \log_2 |b|}$ passi.

Dimostrazione

Si verifica che, ogni due divisioni successive, il resto (almeno) si dimezza:

$$r_{2k} < \frac{r_{2k-2}}{2}$$

Allora, se k è tale che $\frac{|b|}{2^k} < 1$, si ha $r_{2k} = 0 \quad \forall k \in \mathbb{N}$. D'altra parte, $|b| < 2^k$ il che significa che $k > \log_2 |b|$. Siccome ad ogni variazione di k corrispondono due passi dell'algoritmo, allora questo terminerà in un numero intero di passi minore o uguale a $2 \log_2 |b|$

2.5 Equazioni Diofantee

Una **equazione diofantea** è un'equazione lineare di primo rado in due incognite a coefficienti interi, di cui si ricercano le soluzioni intere:

$$a \cdot x + b \cdot y = c, \qquad \text{con } a, b, c \in \mathbb{Z}$$

Le soluzioni (**se esistono**) sono coppie del tipo:

$$(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z} \text{ t.c. } a \cdot \overline{x} + b \cdot \overline{y} = c$$

L'equazione diofantea $ax + by = c$, con $a, b, c \in \mathbb{Z}$ **ammette soluzioni** (intere) se e solo se $\gcd(a, b)|c$. Inoltre se $(\overline{x}, \overline{y})$ è una soluzione, allora esistono infinite soluzioni:

$$\text{Sol} = \{(\overline{x}, \overline{y}) + k \cdot \tfrac{(-b,a)}{\gcd(a,b)} \text{ t.c. } k \in \mathbb{Z}\}$$

Dimostrazione: quando bisogna dimostrare un **se e solo se** ($\longleftrightarrow$), la dimostrazine sarà divisia in due parti: la prima parte dimostrerà il "$\rightarrow$", mentre la seconda il "$\leftarrow$"

Prima Parte

Hp: $\exists(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ t.c. $a\overline{x} + b\overline{y} = c$

Th: $\underbrace{\gcd(a, b)}_{d \in \mathbb{Z}} | c$

Per definizione avremo che $d|a$ e che $\Rightarrow$ $\quad \exists h \in \mathbb{Z}$ t.c. $a = d \cdot h$

$d|b$ $\quad \exists k \in \mathbb{Z}$ t.c. $b = d \cdot k$

Allora:

$$d \cdot h \cdot \overline{x} + d \cdot k \cdot \overline{y} = c$$
$$d \cdot \underbrace{\boxed{(h \cdot \overline{x} + k \cdot \overline{y})}}_{\in \mathbb{Z}} = c$$

$d|c$ in questo modo abbiamo dimostrato che $\gcd(a, b)$ divide il termine noto c

Seconda Parte

Hp: $\gcd(a, b)|c$

Th: $\exists(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z}$ t.c. $a\overline{x} + b\overline{y} = c$

Poniamo $d \in \mathbb{Z}$, $d = \gcd(a, b)$ è possibile scriverlo attraverso l'**identità di bezout** come:

$$\exists \alpha, \beta \in \mathbb{Z} \text{ t.c. } d = \alpha \cdot a + \beta \cdot b$$

Poiché $d|c$ allora $\exists h \in \mathbb{Z}$ t.c. $c = d \cdot h$ andando a sostituire avremo che:

$$\begin{aligned} c = d \cdot h &= (\alpha \cdot a + \beta \cdot b) \cdot h \\ &= a \cdot \underbrace{(\alpha \cdot h)}_{\in \mathbb{Z}} + b \cdot \underbrace{(\beta \cdot h)}_{\in \mathbb{Z}} \end{aligned}$$

In questo modo abbiamo dimostrato che $(\overline{x}, \overline{y}) = (a \cdot h, b \cdot h)$ e che quindi **se esiste** è soluzione.

Terza Parte

L'ultima parte della dimostrazione ci permette di verificare che **se esiste** una soluzione, ne **esistono infinite**, ovvero se:

$$\exists(\overline{x}, \overline{y}) \in \mathbb{Z} \times \mathbb{Z} \rightarrow \exists\infty \text{ soluzioni}$$

Facciamo riferimento a un sistema lineare completo come insieme delle soluzioni, quello che si ottiene è una soluzione "particolare" alla verrà aggiunto l'insieme di tutte le soluzioni del **sistema omogeneo associato**: $\mathcal{S}$ è un sistema e $\mathcal{S}_0$ è il sistema omogeneo associato (ovvero sostituiso il vettore colonna dei termini noti con degli 0) allora la mia soluzione sarà:

$$Sol(\mathcal{S}) = \{\overline{x} + Sol(\mathcal{S}_0)\}$$

Nel nostro caso avremo come $\mathcal{S} : \; a \cdot x + b \cdot y = c$ e quindi avremo che $\boxed{(\overline{x}, \overline{y}) \in Sol(\mathcal{S})}$

Mentre $\mathcal{S}_0 : \; a \cdot x + b \cdot y = 0$ è quindi immediato che $(-b, a) \in Sol(\mathcal{S}_0)$, ma quindi faranno parte di $Sol(\mathcal{S}_0)$ tutti i loro multipli e sottomultipli.

$$\boxed{Sol(\mathcal{S}_0) = k \cdot \frac{(-b,a)}{\gcd(a,b)}}$$

Quindi avremo che $Sol(\mathcal{S}) = \{(\overline{x}, \overline{y}) + k \cdot \frac{(-b,a)}{\gcd(a,b)} \text{ t.c. } k \in \mathbb{Z}\}$

2.6 Numeri Primi e Coprimi

Numeri Coprimi: due interi $a, b \in \mathbb{Z}$ si dicono **coprimi** se $\gcd(a, b) = 1$.

Proprietà:

- due interi consecutivi sono sempre coprimi.

  Dimostrazione: è possibile dimostrarlo tramite due metodi:

  1. **divisione euclidea**: $(n + 1) = n \cdot (n) + 1$ quindi utilizzando l'**algoritmo delle divisioni successive** ottengo che $n = 1 \cdot (n) + 0$. Quindi avremo che $\boxed{\gcd(n, n+1) = 1}$
  2. **identità di bezout**: $1 = (n+1) \cdot (1) + n \cdot (-1) \;\Rightarrow\; 1 \in \mathcal{S}$ dove $\mathcal{S}$ è l'insieme delle combinazioni lineari. Siccome $\min(\mathcal{S}) = \gcd(n+1, n) \;\Rightarrow\; \boxed{\gcd(n+1, n) = 1}$

- due dispari consecutivi sono sempre coprimi.

Dimostrazione: anche in questo caso è possibile dimostrarlo tramite gli stessi due approcci della proprioetà precedente, visualizziamo solo quello con l'**identità di bezout**:

$$2 = (2 \cdot n - 1)(1) + (2 \cdot n + 1)(-1) \ \Rightarrow \ 2 \in \mathcal{S}$$

Ma siccome 2 non corrisponde all'$\gcd(2 \cdot n - 1, 2 \cdot n + 1)$

Allora $\boxed{\gcd(2 \cdot n - 1, 2 \cdot n + 1) = 1}$

- $\forall a, b \in \mathbb{Z} - \{0\}$, $\frac{a}{\gcd(a,b)}$ e $\frac{b}{\gcd(a,b)}$ sono coprimi.

Dimostrazione: per l'**identità di bezout** sappiamo che:

$$\exists \alpha, \beta \in \mathbb{Z} \text{ t.c. } \gcd(a, b) = \alpha \cdot a + \beta \cdot b$$

Se si va dividere ambo i membri per l'$\gcd(a, b)$ avremo che:

$$\begin{aligned} \gcd(a,b) &= \alpha \cdot a + \beta \cdot b \\ \frac{1}{\gcd(a,b)} \cdot \gcd(a,b) &= \frac{1}{\gcd(a,b)} \cdot (\alpha \cdot a + \beta \cdot b) \\ 1 &= \alpha \cdot \underbrace{\boxed{\frac{a}{\gcd(a,b)}}}_{\in \mathbb{Z}} + \beta \cdot \underbrace{\boxed{\frac{1}{\gcd(a,b)}}}_{\in \mathbb{Z}} \\ 1 &= \gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) \end{aligned}$$

Numeri Primi: un intero $p \in \mathbb{Z}$ si dice **primo** se gli unici suoi divisori sono ± 1 e $\pm p$.

Lemma di Euclide: se $a, b \in \mathbb{Z}$ sono **coprimi**:

$$a | (bc) \ \Rightarrow \ a | c$$

Dimostrazione: se $a | (bc)$ allora $\exists h \in \mathbb{Z}$ t.c. $\boxed{b \cdot c = h \cdot a}$, poiché $\gcd(a, b) = 1$, per l'**identità di bezout** $\exists \alpha, \beta \in \mathbb{Z}$ t.c. $1 = \alpha \cdot a + \beta \cdot b$.

Moltiplicando entrambi i membri per c si ottiene:

$$\begin{aligned} c \cdot 1 &= c \cdot (\alpha \cdot a + \beta \cdot b) \\ c &= c \cdot \alpha \cdot a + \boxed{c \cdot b} \cdot \beta \\ c &= c \cdot \alpha \cdot a + h \cdot a \cdot \beta \\ c &= a \cdot (\underbrace{\boxed{\alpha \cdot c + h \cdot \beta}}_{\in \mathbb{Z}}) \end{aligned}$$

In questo modo abbiamo dimostrato che $a | c$.

Proprietà

Se $a, b \in \mathbb{Z} - \{0\}$ sono coprimi

$$a|c,\ b|c \ \Rightarrow\ (ab)|c$$

Dimostrazione: siccome $b|c$ allora $\exists h \in \mathbb{Z}$ t.c. $c = h \cdot b$. In questo modo $a|c \to a|(hb)$ che per il **Lemma di Euclide** implica che $a|h$, ovvero che $\exists h' \in \mathbb{Z}$ t.c. $h = h' \cdot a$, sostituendo avremo:

$$c = h \cdot b = h' \cdot ab \to \boxed{(ab)|c}$$

Teorema della Caratterizzazione dei Numeri Primi

Sia $p \in \mathbb{Z}$

$$p \text{ è primo} \iff (\forall m, n \in \mathbb{Z} \text{ t.c. } p|(mn) \text{ allora o } p|m \text{ o } p|n)$$

Dimostrazione

Prima Parte "$\Rightarrow$"

Sia p primo. Per **Hp.** supponiamo esistano $n, m \in \mathbb{Z}$ tali che $p|(mn)$, con p **non divide** n. Poichè p è primo significa che n non è multiplo di p e quindi $\gcd(p, n) = 1$ per il **Lemma di Euclide**, da $\gcd(p, n) = 1$ e $p|(mn)$ (le nostre ipotesi) segue che $p|m$, ovvero la tesi.

Seconda Parte "$\Leftarrow$"

Supponiamo ora che $\forall m, n \in \mathbb{Z}$ t.c. $p|(mn)$ allora o $p|m$ o $p|n$. Immaginiamo di scrivere p come prodotto di due fattori

$$p = a \cdot b, \text{ con } a, b \in \mathbb{Z}$$

Da $p = a \cdot b$ segue che $p|(ab)$; per ipotesi, allora, $p|(ab)$ implica che o $p|a$ oppure $p|b$, supponiamo che $p|a$. Siccome $p = a \cdot b$ allora sicuramente $a|p$, ma visto che $p|a$ e $a|p \to a = \pm p$.

Se $a = p$, allora $b = 1$, mentre se $a = -p$ allora $b = -1$. In entrambi i casi gli unici divisori di p sono $\pm p$ e ± 1, per cui p è **primo**.

Minimo Comune Multiplo

Dati $a, b \in \mathbb{Z} - \{0\}$ si dice che $M \in \mathbb{Z}$ è **UN minimo comune multiplo** tra a e b se:

- $a|M$ e $b|M$
- $\forall c \in \mathbb{Z}$ t.c. $a|c,\ b|c \Rightarrow M|c$

Mentre si definisce il **IL minimo comune multiplo** tra a e b l'unico *minimo comune multiplo* **positivo**:

$$M = mcm(a, b) \in \mathbb{Z}^+$$

tale che $a|M,\ b|M$; $\forall c \in \mathbb{Z}$ t.c. $a|c,\ b|c \Rightarrow M|c$

Teorema dell'Esistenza del Minimo Comune Multiplo

Dati $a, b \in \mathbb{Z} - \{0\},\ \exists M = mcm(a, b)$:

$$M = \frac{|ab|}{\gcd(a,b)}$$

Dimostrazione

$a, b \in \mathbb{Z} - \{0\},\ \exists M = mcm(a, b) \iff \boxed{a|M \text{ e } b|M}\ \boxed{\forall c \in \mathbb{Z} \text{ t.c. } a|c,\ b|c \Rightarrow M|c}$

Dimostriamo per primo $\boxed{a|M \text{ e } b|M}$ ovvero che il **minimo comune multiplo** divide contemporaneamente a e b.

$mcm(a, b) = mcm(|a|, |b|)$ possiamo quindi supporre che entrambi i valori siano positivi. So che $\exists d = \gcd(a, b) \in \mathbb{Z}$ e vado a considerare:

$$M = \frac{a \cdot b}{d}$$

Posso verificare che M sia il *minimo comune multiplo* perché se $d|a \to \exists h \in \mathbb{Z}$ t.c. $a = h \cdot d$ e contemporaneamente $d|b \to \exists k \in \mathbb{Z}$ t.c. $b = k \cdot d$ posso riscrivere la relazione di prima come:

$$M = \frac{a \cdot b}{d} = \frac{(d \cdot h)(d \cdot k)}{d} = dhk$$

In questo modo abbiamo che $M = (d \cdot h) \cdot k = a \cdot k$ quindi $\boxed{a|M}$ e che $M = (d \cdot k) \cdot h = b \cdot h$ quindi $\boxed{b|M}$

Dimostriamo ora che $\boxed{\forall c \in \mathbb{Z} \text{ t.c. } a|c,\ b|c \Rightarrow M|c}$ ovvero che M è il **minimo**. Sappiamo che $a|c$ significa che $\exists \alpha \in \mathbb{Z}$ t.c. $c = a \cdot \alpha = (d \cdot h) \cdot \alpha$ e che $b|c$ significa che $\exists \beta \in \mathbb{Z}$ t.c. $c = b \cdot \beta = (d \cdot k) \cdot \beta$, in questo modo possiamo dire che $\exists c' \in \mathbb{Z}$ t.c. $c = d \cdot c'$ con $c' = h \cdot \alpha$ oppure $c' = k \cdot \beta$.

Poiché:

$$h = \frac{a}{\gcd(a,b)} \qquad k = fracb\gcd(a, b)$$

h e k sono **coprimi** e sono entrambi divisiori di c', segue che $hk|c'$, ma allora $\exists \gamma \in \mathbb{Z}$ t.c. $hk \cdot \gamma = c'$, moltiplicando per d avremo che $dhk \cdot \gamma = d \cdot c' = c$ e $dhk = M \Rightarrow \boxed{M|c}$

Teorema Fondamentale dell'Aritmetica

Per ogni $n \in \mathbb{Z},\ \exists p_1, p_2, ..., p_s$ con p_i **primo** $\forall i \in \mathbb{N}_s,\ s \geq 1$ e $p_i \neq p_j\ \forall i \neq j$ ed $\exists h_1, h_2, ..., h_s \in \mathbb{Z}^+$:

$$n = sign(n) \cdot p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_s^{h_s}$$

Inoltre se

$$n = sign(n) \cdot q_1^{k_1} \cdot q_2^{k_2} \cdot ... \cdot q_r^{k_r}$$

con q_j **primo** $\forall j \in \mathbb{N}_r,\ r \geq 1$ e $q_j \neq q_l\ \forall j \neq l$ e $k_j \in \mathbb{Z}^+,\ \forall j \in \mathbb{N}_r$, allora $r = s$ ed $\exists \phi : \mathbb{N}_r \to \mathbb{N}_s$ biunivoca tale che $p_i = q_{\phi(i)}$ e $h_i = k_{\phi(i)} \forall i \in \mathbb{N}_s$

Ovvero che i numeri primi che compongono n sono sempre gli stessi ma cambiati di posizione (combinazione unica, può solo permutare la poszione.)

Conseguenza: Dati due numeri $a, b \in \mathbb{Z}$ posso sempre rappresentarli come il prodotto di numeri primi (ad eccezione di quelli con esponente nullo) ad esempio:

$$a = p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_r^{h_r} \qquad \mathcal{S}_a = \{p_1^{h_1}, p_2^{h_2}, ..., p_r^{h_r}\}$$
$$b = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_s^{k_s} \qquad \mathcal{S}_b = \{p_1^{k_1}, p_2^{k_2}, ..., p_s^{k_s}\}$$

avremo che:

- $\gcd(a, b)$ è la sequenza di tutti i numeri primi con esponente minore che sta nell'intersezione della rappresentazione: $\mathcal{S}_a \cap \mathcal{S}_b$.
- $mcm(a, b)$ è la sequenza dei numeri primi comuni e non con esponente maggiore presenti nell'unione: $\mathcal{S}_a \cup \mathcal{S}_b$

Esempio

$12 = 2^2 \cdot 3^1 \to \mathcal{S}_a = \{2^2, 3^1\}$ $\qquad 45 = 3^2 \cdot 5^1 \to \mathcal{S}_b = \{3^2, 5^1\}$

$\gcd(12, 45) = 3^1 = 3$ $\qquad mcm(12, 45) = 2^2 \cdot 3^2 \cdot 5^1 = 180$

Teorema dell'Esistenza di infiniti numeri primi: esistono **infiniti** numeri **primi**.

Dimostrazione: supponiamo **per assurdo** che i numeri primi siano **finiti**, ovvero che $\exists N \in \mathbb{N}$, t.c. $p_1, p_2, ..., p_N$ siano tutti e soli i numeri primi. Consideriamo ora $\overline{n} = p_1 \cdot p_2 \cdot p_N + 1$, sicuramente $\forall i \in \mathbb{N}_N$, non può essere vero che $p_i | \overline{n}$ poiché il resto della **divisione euclidea** tra $\overline{n}$ e p_i vale 1. Tuttavia per il **teorema fondamentale dell'aritmetica**, anche $\overline{n}$ deve essere rappresentabile come il prodotto di potenze di numeri primi, ma se $p_1, p_2, ..., p_N$ sono gli unici numeri primi allora si ottiene **assurdo**.

Proprietà: $\sqrt{3}$ è **irrazionale**.

Dimostrazione: supponiamo per **assurdo** che $\sqrt{3}$ sia *razionale*, ovvero che:

$$\sqrt{3} = \frac{m}{n},\ m, n \in \mathbb{Z}^+$$

Allora avremo che $m = \sqrt{3} \cdot n$ elevando entrambi i membri al quadrato avremo che $\underbrace{m^2}_{c'} = \underbrace{3 \cdot n^2}_{c''}$

Poiché per il **teorema fondamentale dell'aritmetica** la scomposizione in fattori primi è unica a meno dell'ordine dei fattori, da $c' = m^2$ segue che gli esponenti di tutti i fattori primi di c' sono pari, mentre da $c'' = 3n^2$ segue che il fattore primo 3 compare in c'' con esponente dispari, ma visto che $c' = c''$ avremo dimostrato l'**assurdo**.

Lemma: se n è dispari, fattorizzare n equivale a scrivere n come differenza di due quadrati.

$$n = x^2 - y^2 = (x + y) \cdot (x - y)$$

Dimostrazione: siccome $n \in \mathbb{D}$, una sua fattorizzazione $n = a \cdot b$ implica che anche $a, b \in \mathbb{D}$, mentre $(a + b), (a - b) \in \mathbb{P}$. Allora

$$n = a \cdot b = (\tfrac{a+b}{2})^2 - (\tfrac{a-b}{2})^2 = \frac{a^2+b^2+2ab}{4} - \frac{a^2+b^2-2ab}{4} = \frac{4ab}{4} = a \cdot b, \quad \text{con } \tfrac{a+b}{2}, \tfrac{a-b}{2} \in \mathbb{Z}$$

Metodo di Fattorizzazione di Fermat

Senza perdere di generalità, si consideri $n \in \mathbb{Z}^+$ dispari. Per cercare due interi x e y tali che $n = x^2 - y^2$ si cerca un intero x tale che $x^2 - n$ sia un quadrato perfetto. Allora:

- inizialmente si pone $x = \lfloor \sqrt{n} \rfloor + 1$ e si verifica se $n - x^2$ è un quadrato perfetto, o no.
- in caso affermativo si ottiene una decomposizione di n e l'algoritmo termina; altrimenti, si pone $x := x + 1$ e si itera il procedimento.

Il procedimento avrà sicuramente termine, poiché al limite si arriva ad $x := \frac{n+1}{2}$ in cui la condizione diventa

$$(\tfrac{n+1}{2})^2 - n = (\tfrac{n-1}{2})^2 \rightarrow n = (\tfrac{n+1}{2})^2 - (\tfrac{n-1}{2})^2$$

Se si arriva a questo punto, significa che l'unica decomposizione è quella banale, per cui n è primo; altrimenti si ottiene una decomposizione non banale di n e si procede ripetendo l'algoritmo su ciascuno dei fattori.

Esempio

$$n = 194333 \qquad x = \lfloor \sqrt{n} \rfloor + 1 = 440 + 1 = 441$$

$$441^2 - 194333 = 148 \rightarrow \text{non è un quadrato perfetto} \rightarrow x = x + 1 = 442$$

$$\ldots$$

$$447^2 - 19433 = 5476 = 74^2 \Rightarrow n = 447^2 - 74^2 = (447 + 74) \cdot (447 - 74) = \boxed{521 \cdot 373}$$

Capitolo 3

Aritmetica Modulare

È nota la definizione di **insieme delle classi resto modulo** n $\mathbb{Z}_n$ ($\forall n \in \mathbb{N}, n \geq 2$), come insime quoziente di $\mathbb{Z}$ rispetto alla **relazione di congruenza** modulo n:

$$a \equiv_n b \iff \exists h \in \mathbb{Z} \text{ t.c. } b - a = h \cdot n$$

Inoltre:

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

3.1 Operazioni in $\mathbb{Z}_n$

Su $\mathbb{Z}_n = \frac{\mathbb{Z}}{\equiv_n}$ sono ben poste la **somma** e il **prodotto**

3.1.1 Somma in $\mathbb{Z}_n$

$$\boxplus : \mathbb{Z}_n \times \mathbb{Z}_n \mapsto \mathbb{Z}_n$$
$$([a], [b]) \mapsto [a] \boxplus [b] \stackrel{\text{def}}{=} [a+b]$$

Dimostrazione: per provare che la somma è ben posta, occorre provare che, $\forall a' \in [a]$ e $\forall b' \in [b]$, si ha $[a' + b'] = [a + b]$.

Per **Hp.** avremo che $\exists h \in \mathbb{Z}$ t.c. $a' - a = h \cdot n$ ed $\exists h' \in \mathbb{Z}$ t.c. $b' - b = h' \cdot n$. Facendo la somma otteniamo:

$$(a' - a) + (b' - b) = (h' \cdot n) + (h \cdot n)$$
$$(a' + b') - (a + b) = n \cdot \underbrace{\boxed{(h' - h)}}_{\in \mathbb{Z}}$$

In questo modo siamo riusciti a provare la nostra **Th.**

3.1.2 Prodotto in $\mathbb{Z}_n$

$$\boxdot : \mathbb{Z}_n \times \mathbb{Z}_n \mapsto \mathbb{Z}_n$$
$$([a],[b]) \mapsto [a] \boxdot [b] \stackrel{\text{def}}{=} [a \cdot b]$$

Dimostrazione: per provare che il prodotto è ben posto, occorre provare che $\forall a' \in [a]$ e $\forall b' \in [b]$, si ha $[a' \cdot b'] = [a \cdot b]$.

Per **Hp.** avremo che $\exists h \in \mathbb{Z}$ t.c. $a' - a = h \cdot n$ ed $\exists h' \in \mathbb{Z}$ t.c. $b' - b = h' \cdot n$. Moltiplicando membro a membro $a' = a + hn$ e $b' = b + h'n$ otteniamo:

$$a' \cdot b' = (a + hn) \cdot (b + h'n) = ab + ah'n + bhn + hh'n^2$$
$$a'b' - ab = ah'n + bhn + hh'n^2 = n \cdot (\underbrace{\boxed{ah' + bh + hh'n}}_{\in \mathbb{Z}})$$

In questo modo siamo riusciti a provare la nostra **Th.**

Proposizione: $(\mathbb{Z}_n, \boxplus, \boxdot)$ è un anello commutativo con unità, $\forall n \in \mathbb{N}, n \geq 2$

Teorema: $(\mathbb{Z}_n, \boxplus, \boxdot)$ è un campo *se e solo se* n è **primo**.

Dimostrazione

Prima Parte "$\Rightarrow$": se n non è primo avremo che $n = a \cdot b$, con $\{a, b\} \neq \{n, 1\}$ ma allora in $\mathbb{Z}_n$ avremo che $[a] \cdot [b] = [a \cdot b] = n = [0]$ il che significa che $\mathbb{Z}_n$ ammette divisori dello zero e quindi non può essere un campo.

Seconda Parte "$\Leftarrow$": se n è primo, bisogna dimostrare che ogni elemento non nullo ammette l'inverso. Si può dire che $[a] \neq [0] \Rightarrow a \not\equiv_n 0$ quindi che a non è multiplo di n.

Quindi il $\gcd(a, n) = 1$, quindi per l'**identità di bezout** $\exists \alpha, \beta \in \mathbb{Z}$ t.c. $1 = \alpha \cdot a + \beta \cdot n$ che si può riscrivere come:

$$1 - \underbrace{\boxed{a \cdot \alpha}}_{\in [1]} = n \cdot \beta$$

Ma se $a \cdot \alpha \in [1]$ questo implica che $[a \cdot \alpha] = [1]$ ovvero $[a] \cdot [\alpha] = [1]$ e quindi siccome 1 è l'elemento neutro per la moltiplicazione, avremo che $[\alpha]$ è l'inverso.

Se n non è primo, occorre prestare attenzione ai calcoli in $\mathbb{Z}_n$. Ad esempio:

$$3 \cdot 5 \equiv_9 3 \cdot 8, \text{ ma non è vero che } 5 \equiv_9 8$$

Teorema: $a \cdot c \equiv b \cdot b \pmod{n} \Rightarrow a \equiv b \pmod{\frac{n}{d}}$ con $d = \gcd(c, n)$

Corollario: se $\gcd(c, n) = 1 \Rightarrow a \equiv b \pmod{n}$. Nel caso di n **primo** avremo che

$$\forall c \in \mathbb{Z}_n,\ c \neq 0 \rightarrow \gcd(c, n) = 1$$

Teorema: ogni numero intero n è congruo modulo 9 alla somma delle sue cifre.

Dimostrazione: esplicitando la natura posizionale del sistema decimale avremo:

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + ... + a_k \cdot 10^k =$$

$$= a_0 + a_1 \cdot (1+9) + a_2 \cdot (1+99) + a_3 \cdot (1+999) + ... + a_k \cdot (1 + \underbrace{99...999}_{k}) =$$

$$= (a_0 + a_1 + a_2 + a_3 + ... + a_k) + 9 \cdot a_1 + 99 \cdot a_2 + 999 \cdot a_3 + ... + \underbrace{99...999}_{k} =$$

$$= (a_0 + a_1 + a_2 + a_3 + ... + a_k) + 9 \cdot (a_1 + 11a_2 + 111a_3 + ... + \underbrace{11...111}_{k} a_k)$$

Quindi n si ottiene dalla somma delle sue cifre, agiungendone un multiplo di 9 il che prova la tesi. **Conseguenza**: prova del nove.

Proprietà:

- **Criterio di Divisibilità per 3** (*per 9*): un numero intero è divisibile per 3 (*per 9*) se e solo se la somma delle sue cifre è divisibile per 3 (*per 9*).

  Dimostrazione

  $n \equiv a_k + a_{k-1} + ... + a_0$ sia modulo 3 che modulo 9

- **Criterio di Divisibilità per 2 e per 5**: un numero intero è divisibile per 2 (*o per 5*) se e solo se la cifra delle unità a_0 è divisibile per 2 (*o per 5*).

  Dimostrazione

  Per ogni $k > 1$, $10^k \equiv 10$ sia modulo 2 che modulo 5. Quindi di avrebbe $n \equiv a_0$ sia modulo 2 che modulo 5

- **Criterio di Divisibilità per 4 e per 25**: un numero intero è divisibile per 4 (o per 25) se e solo se il numero a_1a_0 formato dalle sue ultime due cifre è divisibile per 4 (o per 25).

  Dimostrazione

  $100 = 2^2 5^2 \equiv 0$ sia modulo 4 che modulo 25. Allora ogni intero n è congruo modulo 4 o 25 se le ultime due cifre sono divisibili per 4 o per 25

- **Criterio di Divisibilità per 2^r**: un numero intero è divisibile per 2^r se e solo se 2^r divide il numero costituito dalle ultime r cifre di n

  Dimostrazione

  È sufficente osservare che $10^k = 2^k 5^k \equiv 0 \pmod{2^r}$ $\forall k \geq r$

- **Criterio di Divisibilità per 11**: un numero intero è divisibile per 11 se e solo se è divisibile per 11 la somma a segni alterni delle sue cifre:

$$a_0 - a_1 + a_2 - ... + (-1)^k a_k \equiv 0 \bmod 11$$

> **Dimostrazione**: basta osservare che:
>
> $$10 \equiv -1 \bmod 11 \Rightarrow \begin{cases} 10^{2p} \equiv 1 \bmod 11 \\ 10^{2p+1} \equiv -1 \bmod 11 \end{cases}$$

3.2 Congruenze Lineari

Si chiama **congruenza lineare** un'equazione di primo grado in $\mathbb{Z}_n$ a coefficienti interi:

$$a \cdot x \equiv b \bmod n \qquad \text{con } a, b, n \in \mathbb{Z}, n \geq 2$$

Che equivale a $[a] \cdot [x] = [b]$

Teorema dell'Esistenza di Soluzioni: una congruenza lineare ammette soluzioni se e solo se $\gcd(a, n)|b$

> **Dimostrazione**: ad ogni **congruenza lineare** è possibile associare un'**equazione diofantea**. Infatti:
>
> $$ax \equiv b \bmod n \iff \exists h \in \mathbb{Z} \text{ t.c. } b - ax = hn \text{ ovvero } \boxed{ax + hn = b}$$
>
> Quindi come condizione necessaria e sufficiente per la risolubilità della congruenza lineare è verificare la risolubilità dell'equazione diofantea associata è $\gcd(a, n)|b$

Teorema per la Risoluzione di Congruenze Lineari: sia $ax \equiv b \bmod n$ una congruenza lineare tale che $d|b$ con $d = \gcd(a, n)$ e sia $\boxed{x_0}$ una sua particolare risoluzione. Allora:

- in $\mathbb{Z}$ le soluzioni sono tutti e soli gli interi del tipo:

$$x_0 + h \cdot \tfrac{n}{d},\ h \in \mathbb{Z}$$

- in $\mathbb{Z}_n$ le soluzioni sono tutti e soli li interi del tipo

$$x_0 + h \cdot \tfrac{n}{d},\ h \in \mathbb{Z}_n$$

Inoltre, ogni soluzione in $\mathbb{Z}$ è congrua modulo n ad una delle d soluzioni in $\mathbb{Z}_n$

> **Esempio**
>
> $12x = 15 \bmod 39 \ \rightarrow\ \gcd(12, 39) = 3|15 \Rightarrow \exists\text{Sol}$
>
> **id. di bezout**: $3 = 12(-3) + 39(1) \rightarrow 5 \cdot 3 = 12 \cdot (-3 \cdot 5) + 39 \cdot (1 \cdot 5) \Rightarrow (\boxed{-15}, 5)$ è soluzione
>
> In $\mathbb{Z}$: $\text{Sol} = \{(-15 + 13 \cdot h) \text{ t.c. } h \in \mathbb{Z}\}$
>
> In $\mathbb{Z}_n$: $\text{Sol} = \{(-15 + 13 \cdot h) \text{ t.c. } h \in \mathbb{Z}_3\} = \{[-15]_{39}, [-2]_{39}, [11]_{39}\} = \{[24]_{39}, [37]_{39}, [11]_{39}\}$

Dimostrazione

Prima Parte: dimostriamo l'esistenza di una soluzione.

Hp. $a \cdot x_0 = b \bmod n$ **Th.** $x_0 + h \cdot \frac{n}{d}$ è soluzione $\forall h \in \mathbb{Z}$

Consideriamo $a \cdot x_0 + a \cdot h\frac{n}{d}$ per **Hp** $\exists k \in \mathbb{Z}$ t.c. $a \cdot x_0 = b + k \cdot n$

$$a \cdot (x_0 + h\tfrac{n}{d}) = b + kn + h \cdot \underbrace{\boxed{\tfrac{an}{d}}}_{mcm(a,n)}$$

Quindi avremo che $\boxed{a(x_0 + h\frac{n}{d}) \equiv b \bmod n}$

Seconda Parte: cerchiamo di dimostrare che **ogni** soluzione della congruenza lineare è del tipo considerato.

Hp. x_0, x_0' soluzioni di $a \cdot x = b \bmod n$ **Th.** $x_0' \equiv x_0 + h\frac{n}{d},\ h \in \mathbb{Z}$

Sappiamo per **Hp** che $\exists k \in \mathbb{Z}$ t.c. $a \cdot x_0 = b + k \cdot n$ e $\exists k' \in \mathbb{Z}$ t.c. $a \cdot x_0' = b + k' \cdot n$ andando a eseguire la differenza membro per membro si ottiene:

$$a(x_0 - x_0') = n(k - k') \rightarrow \tfrac{1}{d} \cdot a(x_0 - x_0') = \tfrac{1}{d} \cdot n(k - k') \mid\mid \text{divido per } \gcd(a, n) = d$$

Andando ad ottenere $\boxed{\frac{a}{d}(x_0 - x_0') = \frac{n}{d}(k - k')}$ in questo modo $\frac{n}{d}$ divide il primo membro dell'equazione, ma poiché $\frac{n}{d}$ è coprimo con $\frac{a}{d}$, per il **lemma di euclide** $\frac{n}{d}$ divide anche $(x_0 - x_0')$ e quindi avremo che

$$\exists h \in \mathbb{Z} \text{ t.c. } x_0 - x_0' = h \cdot \tfrac{n}{d}$$

In questo modo abbiamo dimostrato l'esistenza di infinite soluzioni in $\mathbb{Z}$, bisogna fare la stessa cosa per $\mathbb{Z}_n$

Terza Parte: dimostriamo che le soluzioni siano distinte in $\mathbb{Z}_n$, supponiamo per **assurdo** che:

$$\exists h, h' \in \mathbb{Z}_d \text{ t.c. } x_0 + h\tfrac{n}{d} = x_0 + h'\tfrac{n}{d} \bmod n$$

$$\cancel{x_0} + h\tfrac{n}{d} = \cancel{x_0} + h'\tfrac{n}{d} \bmod n$$

Per dividere entrambi i lati per $\frac{n}{d}$ dobbiamo anche dividere anche il modulo per per il $\gcd(\frac{n}{d}, n) = \frac{n}{d} \Rightarrow h \equiv h' \bmod (\frac{n}{n/d}) \Rightarrow \boxed{h \equiv h' \bmod d}$ questo rappresenta che h e h' sono la stessa classe, quindi abbiamo raggiunto l'*assurdo*.

Quarta Parte: manca solo da dimostrare che ogni soluzione intera è congrua mod n ad una delle d soluzioni scritte:

$$\{x_0, x_0 + \tfrac{n}{d}, ..., x_0 + (d-1)\tfrac{n}{d}\}$$

Consideriamo la generica soluzione intera $x_0 + h\frac{n}{d}, h \in \mathbb{Z}$. Per la divisione euclidea tra h e d: $\exists q, r \in \mathbb{Z}, 0 \le r \le d - 1$ t.c. $h = qd + r$ avremo che:

$$x_0 + h\tfrac{n}{d} = x_0(dq + r)\tfrac{n}{d} = x_0 + q\cancel{d}\tfrac{n}{\cancel{d}} + r\tfrac{n}{d} = x_0 + \underbrace{\boxed{\cancel{qn}}}_{\text{multiplo di } n} + r\tfrac{d}{n}$$

Quindi avremo che $\boxed{x_0 + h\frac{n}{d} = x_0 + r\frac{n}{d}}$, dove il resto r varia tra 1 e $d - 1$.

Corollario: se $\gcd(a, n) = 1$ allora la congruenza lineare $\boxed{ax \equiv b \bmod n}$ ammette una ed una sola soluzione in $\mathbb{Z}_n$

Esempio

$$5x \equiv 3 \bmod 7$$

Calcoliamo il *massimo comun divisore*: $\gcd(5,7) = 1$, allora esiste una sola soluzione in $\mathbb{Z}_7$, infatti troviamo i parametri dell'*identità di bezout*: $1 = 5 \cdot (3) + 7 \cdot (-2)$

$$3 \cdot 1 = 5 \cdot (3 \cdot 3) + 7 \cdot (-2 \cdot 3) \Rightarrow (9, -6) \text{ è soluzione della diofantea}$$

In particolare a noi interessa $\boxed{x = 9}$ è soluzione della congruenza. In $\mathbb{Z}$: $\text{Sol} = \{9 + k \cdot 7 \text{ t.c. } k \in \mathbb{Z}\} = \{9 + 7k\}$, mentre in $\mathbb{Z}_7$:

$$\mathbb{Z}_7 : \text{ Sol} = \{9 + k \cdot 7 \text{ t.c. } k \in \mathbb{Z}_1\} = \{[9]_7\} = \{[2]_7\}$$