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:

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

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*.

$\#D_k = k$ $\to$ ci serve la somma delle cardinalità delle $\to$ $\sum_{k=1}^{i+j-2} \#D_k = \frac{(i+j-2)\cdot(i+j-1)}{2}$
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:

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

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:

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

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:

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

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 $\{0, 1\}$:

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

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

$$\bar{S} = \bar{S_1},\ \bar{S_2},\ \bar{S_3},\ ...,\ \bar{S_j},\ ...\ ||\ \text{dove } \bar{S_j} \neq S_{jj}$$

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

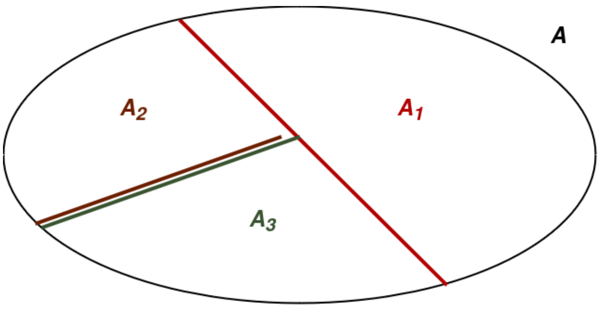


Figura 1.1: **Partizionamento**

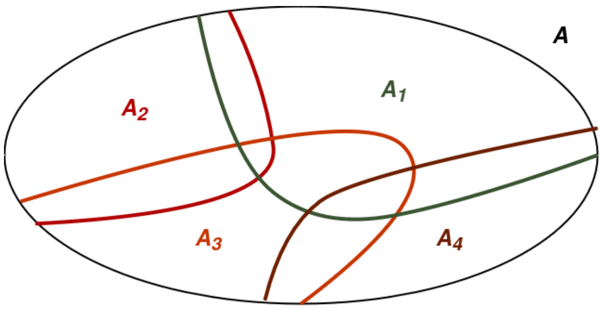


Figura 1.2: **Ricoprimento**

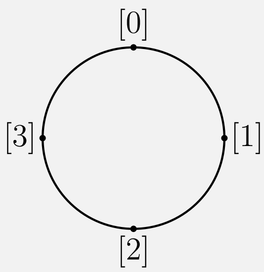
Sia A un insieme; un sottoinsieme $\mathcal{B} \subseteq \mathcal{P}(A)$ è detto **partizione** di A se $\emptyset \notin \mathcal{B}$ e $\forall c \in A,\ \exists! B \in \mathcal{B} \mid x \in B$. Ovvero ogni sottoinsieme non ha intersezione con gli altri.

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

$$* \ : \ G \times G \to G$$

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**:

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

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:

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

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

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

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.

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

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:

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

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:

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

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:

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

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

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

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

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

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

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

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

$$\ldots$$

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

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 $\mathbb{Z}_n$

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

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 $\mathbb{Z}_n$

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

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:

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

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: $\exists q, r \in \mathbb{Z}, 0 \leq r \leq d - 1$ 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 $\mathbb{Z}_7$:

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

3.3 Sistemi di Congruenze Lineari

Lemma: ogni sistema di congruenze lineari del tipo:

$$\begin{cases} a_1 \cdot x \equiv b_1 & \bmod n_1 \\ a_2 \cdot x \equiv b_2 & \bmod n_2 \\ \vdots \\ a_r \cdot x \equiv b_r & \bmod n_r \end{cases}$$

con $\gcd(n_i, n_j) = 1 \ \forall i \neq j$ e $\gcd(a_i, n_i) = d_i | b_i \ \forall i \in \mathbb{N}$, è equivalente ad un sistema del tipo:

$$\begin{cases} x \equiv c_1 & \bmod n'_1 \\ x \equiv c_2 & \bmod n'_2 \\ \vdots \\ x \equiv c_r & \bmod n'_r \end{cases}$$

in cui $\gcd(n'_i, n'_j) = 1 \ \forall i \neq j$

Dimostrazione: consideriamo la i-esima congruenza lineare del sistema $a_i \cdot x \equiv b_i \bmod n$ dividiamo entrambi i membri per il $\gcd(a_i, n_i) = d_i$. Per poterlo fare bisogna primi modificare in maniera opportuna anche il modulo $n'_i = \frac{n_i}{\gcd(d_i, n_i)}$ ottenendo:

$$\underbrace{\frac{a_i}{d_i}}_{\in \mathbb{Z}} \equiv \underbrace{\frac{b_i}{d_i}}_{\in \mathbb{Z}} \bmod \frac{n_i}{\gcd(d_i, n_i)} \Longrightarrow a'_i \cdot x \equiv b'_i \bmod n'_i$$

Osservo che $\gcd(a'_i, n'_i) = \gcd(\frac{a_i}{d_i}, \frac{n_i}{d_i}) = 1$ che comporta che a'_i e n'_i sono **coprimi** tra loro. Quindi la i-esima congruenza lineare avrà *una e una sola* soluzione in $\mathbb{Z}_{n'}$. Se chiamiamo c_i l'unica soluzione della congruenza lineare $a_i \cdot x \equiv_{n_i} b'_i$ allora posso riscriverla come $\boxed{x \equiv c_i \bmod n'_i}$ ottenendo così il sistema equivalente.

Teorema cinese del resto

dato un sistema di congruenze lineari del tipo:

$$\begin{cases} x \equiv c_1 \mod n_1 \\ x \equiv c_2 \mod n_2 \\ \vdots \\ x \equiv c_r \mod n_r \end{cases}$$

con $\gcd(n_i, n_j) = 1\ \forall i \neq j\ (i, j \in \{1, ..., r\})$ allora esiste sempre una ed una sola soluzione modulo $N = n_1 \cdot n_2 \cdot ... \cdot n_r$

Dimostrazione: **Th.** $\exists! Sol \mod N = n_1 \cdot n_2 \cdot ... \cdot n_r$ per farlo dobbiamo dimostrare che la soluzione $\boxed{\textbf{esiste}}$ ed è $\boxed{\textbf{unica}}$

esistenza: indico $N_k = \frac{N}{n_k}\ \forall k \in \mathbb{N}$ e considero una congruenza "fittizia" $N_k \cdot x \equiv c_k \mod n_k$ e osservo che il coefficienti della x e il modulo sono **coprimi** quindi $\gcd(N_k, n_k) = 1$ infatti N_k è il prodotto tra tutti i moduli escluso n_k. Quindi la k-esima congruenza "fittizia" ha una e una sola soluzione in $\mathbb{Z}_{nk}$ e lo indico con $\overline{x_k}$. Affermo che $\overline{x} = N_1 \cdot \overline{x_1} + N_2 \cdot \overline{x_2} + ... + N_r \cdot \overline{x_r}$ è la **soluzione** del sistema iniziale dato, per dimostrarlo sostituiamo $\overline{x}$ nella k-esima congruenza del sistema dato e dimostriamo che lo verifica. $\overline{x} \overset{?}{\equiv} c_k \mod n_k$.

$$N_1 \cdot \overline{x_1} + N_2 \cdot \overline{x_2} + ... + N_r \cdot \overline{x_r} \equiv N_k \cdot \overline{x_k} \bmod n_k$$

Questo semplificazione è possibile perché le varie coppie sono tutte multiple di N_k, quindi modulo n_k si annullano. Ma $\overline{x_k}$ è soluzione della k-esima congruenza "fittizia" $N_K \cdot x \equiv_{n_k} c_K \Rightarrow N_k \cdot \overline{x_k} \equiv_{n_k}$. Quindi $\boxed{\overline{x} \equiv_{n_k} c_k\ \forall k \in \mathbb{N}_r}$ con $\overline{x}$ soluzione del sistema.

unicità: bisogna ora dimostrare che la soluzione $\overline{x}$ è unica modulo N: suppongo che sia $\overline{x}$ che $\overline{y}$ siano soluzioni del sistema dato. Cioè $\boxed{\overline{x} \equiv_{n_k} c_k\ \forall k = 1, ..., r}$ e $\boxed{\overline{y} \equiv_{n_k}\ \ \forall k = 1, ..., r}$. Questo significa che $\overline{x} - \overline{y} \equiv_{n_k} 0\ \forall k = 1, ..., r$ cioè $(\overline{x} - \overline{y})$ è un multiplo intero di $n_k\ \forall k = 1, ..., r$, ma poiché i moduli $n_1, n_2, ..., n_r$ sono tutti mutualmente coprimi, segue che $(\overline{x} - \overline{y})$ è multiplo intero di $n_1 \cdot n_2 \cdot ... \cdot n_r = N$, ovvero $\boxed{\overline{x} \equiv \overline{y} \mod N}$

Esercizio:

Dato il sistema di congruenze lineari, risolverlo: $\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 1 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 1 \bmod 5 \\ x \equiv 0 \bmod 7 \end{cases}$

Dato che (mod 4) e (mod 2) sono congrui allo stesso valore, allora posso rimuovere (mod 2) in quanto viene incluso completamente da (mod 4). Ora tutti i moduli sono **coprimi** tra loro, in questo modo $\exists!\text{Sol} \bmod N,\ N = 3 \cdot 4 \cdot 5 \cdot 7 = 420$

Troviamo la soluzione applicando la dimostrazione:

$N_1 = \frac{420}{3} = 4 \cdot 5 \cdot 7 = 140$ || prima congruenza fittizia: $\boxed{140x \equiv 1 \bmod 3}$

$N_2 = \frac{420}{4} = 3 \cdot 5 \cdot 7 = 105$ || seconda congruenza fittizia: $\boxed{105x \equiv 1 \bmod 4}$

$N_3 = \frac{420}{5} = 3 \cdot 4 \cdot 7 = 84$ || terza congruenza fittizia: $\boxed{84x \equiv 1 \bmod 5}$

$N_4 = \frac{420}{7} = 3 \cdot 4 \cdot 5 = 60$ || quarta congruenza fittizia: $60x \equiv 0 \bmod 7 \Rightarrow \overline{x}_4 = 0 \bmod 7$

- $\boxed{104x - 3y \equiv 1}$, $\gcd(104, 3) = 1 = 140 \cdot (-1) + 3 \cdot (47)$ (**identità di bezout**)

  $\overline{x}_1 = -1 \bmod 3 \equiv_3 2$
- $\boxed{105x - 4y = 1}$, $\gcd(105, 4) = 1 = 105 \cdot (1) + 4 \cdot (-26)$ (**identità di bezout**)

  $\overline{x}_2 = 1 \bmod 4$
- $\boxed{84x - 5y = 1}$, $\gcd(84, 5) = 1 = 84 \cdot (-1) + 5 \cdot (17)$ (**identità di bezout**)

  $\overline{x}_3 = -1 \bmod 5 \equiv_5 4$

Allora l'unica soluzione del sistema è: $\overline{x} = N_1 \cdot \overline{x}_1 + N_2 \cdot \overline{x}_2 + N_3 \cdot \overline{x}_3 + N_4 \cdot \overline{x}_4 = 140 \cdot 2 + 105 \cdot 1 + 84 \cdot 4 + 60 \cdot 0 = 301 \bmod 420$

Corollario: dato un sistema di congruenze lineari del tipo:

$$\begin{cases} a_1 x \equiv b_1 \quad \bmod n_1 \\ a_2 x \equiv b_2 \quad \bmod n_2 \\ \vdots \\ a_r x \equiv b_r \quad \bmod n_r \end{cases}$$

con $\gcd(n_i, n_j) = 1\ \forall i \neq j$ e $\gcd(a_k, n_k) = 1\ \forall k \in \{1, ..., r\}$ allora la soluzione è:

$$\overline{x} = N_1 \cdot \overline{x}_1 + N_2 \cdot \overline{x}_2 + ... + N_r \cdot \overline{x}_r \bmod N$$

dove $N_k = \frac{N}{n_k}$ e $\overline{x}_k$ è soluzione della k-esima congruenza lineare fittizia: $(a_k \cdot N_k)x \equiv b_k \bmod n_k$

Teorema per la Risoluzione di Sistemi di due congruenze lineari: un sisteam di due congruenze lineari del tipo:

$$\begin{cases} x \equiv a \bmod n \\ x \equiv b \bmod m \end{cases}$$

ammette soluzioni **se e solo se** $\gcd(n,m)|(a-b)$ inoltre, se ammette soluzioni, la soluzione è unica modulo $M = mcm(m,n)$

Dimostrazione

Prima Parte "$\Rightarrow$"

Hp.: $\exists$Sol **Th.**: $\gcd(n,m)|(a-b)$

Per **Hp.** $\exists\overline{x}$ t.c. $\overline{x} \equiv a \bmod n$ e $\exists\overline{x}$ t.c. $\overline{x} \equiv b \bmod n$, ma queste due ugualianze significano rispettivamente che: $\exists h \in \mathbb{Z}$ t.c. $\overline{x} - a = k \cdot n$ e $\exists k \in \mathbb{Z}$ t.c. $\overline{x} - b = k \cdot m$ sottraendo membro per membro si ottiene:

$$\overline{x} - b - (\overline{x} - a) = k \cdot m - n \cdot h \Longrightarrow \boxed{a - b = km + hn}$$

Ponendo $\gcd(m,n) = d$ l'equazione è equivalente a: $k\alpha d - h\beta d = (k\alpha + h\beta) \cdot d \Rightarrow d|(a-b)$

Seconda Parte "$\Leftarrow$"

Th.: $\gcd(n,m)|(a-b)$ **Hp.**: $\exists$Sol

Se $d = \gcd(m,n)$, per l'**identità di bezout**: $\exists\alpha,\beta \in \mathbb{Z}$ t.c. $d = \alpha n + \beta m$ e per **Hp.** sappiamo che $d|(a-b)$ ovvero che $\exists h \in \mathbb{Z}$ t.c. $a - b = d \cdot h$ moltiplicando per l'**identità di bezout** otteniamo: $\boxed{a - b = h \cdot (\alpha n + \beta m) \Longrightarrow a - b = h\alpha n + h\beta m}$.

Posso riscrivere l'equazione come: $\underbrace{a - h\alpha n}_{\overline{x}} = \underbrace{b - h\beta m}_{\overline{x}}$, voglio provare che $\overline{x}$ è soluzione per il sistema dato.

- $\overline{x} = a - h\alpha n \Rightarrow \overline{x} - a = \underbrace{-h\alpha}_{\in\mathbb{Z}} \cdot n$ allora possiamo dire $\overline{x} - a$ è multiplo di n quindi $\overline{x} \equiv a \bmod n$
- $\overline{x} = b - h\beta m \Rightarrow \overline{x} - b = \underbrace{h\beta}_{\in\mathbb{Z}} \cdot m$ allora possiamo dire $\overline{x} - b$ è multiplo di m quindi $\overline{x} \equiv b \bmod m$

Esempio

Il sistema di congruenze lineari:

$$\begin{cases} x \equiv 7 \bmod 9 \\ x \equiv 3 \bmod 5 \end{cases}$$

$\gcd(9,5) = 1|(7-3)$ applico l'**identità di bezout**: $1 = 9(-1) + 5(2)$, moltiplico entrami i lati per $(7-3) = 4$ e otteniamo: $4 = 9(-4) + 5(8)$

La nostra soluzione $\overline{x}$ sarà $\underbrace{7 - 9(-4)}_{43} = \underbrace{3 + 5(8)}_{43}$, quindi $\overline{x} = 43$ sarà l'**unica soluzione** del sistema modulo $M = mcm(9,5) = \frac{9 \cdot 5}{\gcd(9,5)} = 45$ $\boxed{\overline{x} = 43 \bmod 45}$

3.4 Applicazioni dell'Aritmetica Modulare

Sull'insieme $\mathbb{Z}_r \times \mathbb{Z}_s \ \forall r, s \in \mathbb{Z}$ si definisce un'operazione logica di **somma** e di **prodotto**:

$$([a]_r, [b]_s) + ([a']_r, [b']_s) \stackrel{\text{def}}{=} ([a + a']_r, [b + b']_s)$$
$$([a]_r, [b]_s) \cdot ([a']_r, [b']_s) \stackrel{\text{def}}{=} ([a \cdot a']_r, [b \cdot b']_s)$$

Tali operazioni strutturano $\mathbb{Z}_r \times \mathbb{Z}_s$ come un **anello**.

Proprietà: se r e s sono **coprimi** allora la corrispondenza $f : \mathbb{Z}_{rs} \mapsto \mathbb{Z}_r \times \mathbb{Z}_s$ definita come $[x]_{rs} \mapsto ([x]_r, [x]_s)$ è un'applicazione **biunivoca** che conserva somma e prodotto (è un "**isomorfismo di anelli**").

Dimostrazione: bisogna provare che $\boxed{\forall([a]_r, [b]_s) \in \mathbb{Z}_r \times \mathbb{Z}_s \ \exists![x]_{rs} \text{ t.c. } f([x]_{rs}) = ([a]_r, [b]_s)}$ la condizione è però equivalente a dimostrare che il sistema di congruenze lineari:

$$\begin{cases} x \equiv_r a \\ x \equiv_s b \end{cases}$$

siccome il sistema ha $\gcd(r, s) = 1$ (per **Hp** sono coprimi) allora ammetterà una e una sola soluzione modulo $mcm(r, s) = r \cdot s$.

Esercizio

$\mathbb{Z}_{21} \to [17]_{21} \cdot [19]_{21} = ?$ 21 è pari a $3 \cdot 7$ che sono coprimi.

$[17]_{21} = ([2]_3, [3]_7)$ $\Rightarrow ([2 \cdot 1]_3, [3 \cdot 5]_7) = ([2]_3, [1]_7)$

$[19]_{21} = ([1]_3, [5]_7)$

Avremo il sistema associato:

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 7 \end{cases}$$

$\gcd(3, 7) = 1 = 3(-2) + 7(1) \quad \to \quad 2 - 3(-2) = 1 + 7(1) \quad \to \quad 8 = 8$

Quindi $\boxed{\mathbb{Z}_{21} \to [17]_{21} \cdot [19]_{21} = [8]_{21}}$

Piccolo Teorema di Fermat: sia p un numero **primo**, allora $\forall a \in \mathbb{Z}$ t.c. $\gcd(a, p) = 1$ si ha:

$$a^{p-1} \equiv 1 \bmod p$$

Dimostrazione (di Eulero): consideriamo i primi $p-1$ multipli di a: $a, 2a, 3a, ..., (p-1)a$ poiché il $\gcd(a, p) = 1$ nessuno di questi è multiplo di p, infatti, se $r \cdot a = h \cdot p$ con $1 \leq r \leq p-1$ allora seguirebbe che affinché p divida r, p non dovrebbe essere compreso tra 1 e r, il che ci porta all'**assurdo**.

Inoltre i $(p-1)$ multipli di a considerati sono mutualmente **non** congrui mod p, infatti se fosse $r \cdot a \equiv s \cdot a \bmod p$ con $1 \leq r < s \leq p-1$ si avrebbe che $(s-r) \cdot a = h \cdot p$ ma questo è **assurdo** perché r e s sono compresi tra 1 e r.

Segue che in $\mathbb{Z}_p$ $[a]_p, [2a]_p, ...[(p-1)a]_p$ non sono altro che $\mathbb{Z}_p = \{[1]_p, [2]_p, ..., [(p-1)]_p\}$ (a meno dell'ordine).

$$\begin{aligned}
a \cdot 2a \cdot ... \cdot (p-1)a &\equiv_p 1 \cdot 2 \cdot ...(p-1) \\
[1 \cdot 2 \cdot ... \cdot (p-1)] \cdot a^{p-1} &\equiv_p 1 \cdot 2 \cdot ...(p-1) \\
[1 \cdot 2 \cdot ... \cdot (p-1)] \cdot a^{p-1} &\equiv 1 \cdot 2 \cdot ...(p-1) \bmod \frac{p}{\gcd(p, (1, 2, ..., p-1))} \\
a^{p-1} &\equiv_p 1
\end{aligned}$$

Il $\gcd(p, (1, 2, ..., p-1))$ è pari a 1 in quanto se $1, 2, ..., p-1$ fosse multiplo di p, si avrebbe che p dividerebbe uno dei suoi fattori $\rightarrow$ **assurdo**

Corollario: sia p un numero **primo**. Allora, per ogni $a \in \mathbb{Z}$ si ha:

$$a^p \equiv a \bmod p$$

Test di Non Primalità: se, fissato $n \in \mathbb{Z}$, $\exists a \in \mathbb{Z} \mid a^n \not\equiv a \bmod n$, allora n non è primo.

Capitolo 4

Funzione di Eulero e RSA

4.1 Funzione di Eulero

Si dice **funzione di eulero** (o **toziente di eulero**) l'applicazione $\boxed{\phi : \mathbb{N} \mapsto \mathbb{N}}$ che associa ad ogni $n \in \mathbb{N}$ il numero di interi compresi fra 1 e n coprimi con n. Se n è **primo** allora si può dire che $\phi(n) = n - 1 \ \forall n$ primo.

Proprietà:

- Il numero di elementi invertibili in $\mathbb{Z}_n$ $(\forall n \geq 2)$ è esattamente $\phi(n)$.

  Dimostrazione: fissato $n \geq 2$, un elemento $x \in \mathbb{Z}$ è invertibile **se e solo se** $\exists y \in \mathbb{Z}$ t.c. $x \cdot y \equiv_n 1$ questa è una congruenza lineare che ammette soluzioni **se e solo se** $\gcd(x, y) = 1$ ovvero se x e y sono **coprimi**. Quindi il numero di elementi invertibili in $\mathbb{Z}_n$ è pari al numero di elementi coprimi ad n in $\mathbb{Z}_n$ che è la stessa definizione di $\phi(n)$

- $\forall n \in \mathbb{N}$, il numero di stelle (distinte) a n punte è:
  $$\frac{\phi(n)-2}{2}$$
- se $p \in \mathbb{Z}^+$ è un numero primo allora $\phi(p) = p - 1$.
- se $p \in \mathbb{Z}^+$ è un numero primo allora $\phi(p^h) = p^h - p^{h-1}$, $\forall h \geq 1$
- se $p, q \in \mathbb{Z}^+$ sono due numeri primi distinti allora $\phi(pq) = \phi(p) \cdot \phi(q)$

Corollario: se $n = p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_r^{h_r}$, con p_i **primi distinti** $(i \in \mathbb{N}_r)$ allora:

$$\phi(n) = \phi(p_1^{h_1}) \cdot \phi(p_2^{h_2}) \cdot ... \cdot \phi(p_r^{h_r})$$

ovvero posso calcolare il **toziente di eulero** per ogni $n \in \mathbb{Z}$ se conosco la sua **fattorizzazione**.

Teorema di Eulero-Fermat

$\forall n \in \mathbb{N}$ e $\forall a \in \mathbb{Z}$ tale che $\gcd(a, n) = 1$, si ha:

$$a^{\phi(n)} \equiv_n 1$$

Dimostrazione: dimostriamo il teorema per **induzione** con $n = p^h$ con p **primo** e $h_i \in \mathbb{N}$, $\forall i \in \mathbb{N}$

Passo Iniziale

se $h = 1$, significa che $n = p^1 = p$ primo quindi la tesi non è altro che il **piccolo teorema di fermat**.

Passo Induttivo

Hp. $\forall a \in \mathbb{Z} \mid \gcd(a, p^h) = 1$
$\implies \quad a^{\phi(p^h)} \equiv 1 \bmod p^h$

Th. $\forall a \in \mathbb{Z} \mid \gcd(a, p^{h+1}) = 1$
$\implies \quad a^{\phi(p^{h+1})} \equiv 1 \bmod p^{h+1}$

Per la **proprietà** del *toziente di eulero* $\phi(p^h) = p^h - p^{h-1}$

$$\begin{aligned}\phi(p^{h+1}) &= p^{h+1} - p^h \\ &= p \cdot (p^h - p^{h-1}) \\ &= p \cdot \phi(p^h)\end{aligned}$$

Quindi $a^{\phi(p+1)} = a^{p \cdot \phi(p^h)}$ che si può rapprensentare anche come $\boxed{(a^{\phi(p^h)})^p}$. Per **Hp.** induttiva $a^{\phi(p^h)} \equiv 1 \bmod p^h$, ovvero $\exists k \in \mathbb{Z} \mid a^{\phi(p^h)} = 1 + k \cdot p^h$ andando a sostituire otteniamo:

$$(a^{\phi(p^h)})^p = (1 + k \cdot p^h)^p$$

che corrisponde alla **potenza di un binomio** (calcolabile con il **Binomio di Newton** $\rightarrow$ $(A + B)^n = \sum_{r=0}^{n} \binom{n}{r} A^{n-r} \cdot B^r$), quindi avremo:

$$(1 + k \cdot p^h)^p = 1 + \binom{p}{1}(k \cdot p^h)^1 + \binom{p}{2}(k \cdot p^h)^2 + ... + \binom{p}{p}(k \cdot p^h)^p$$

Ad eccezione del "1+" tutti gli altri membri sono multipli di p^{h+1}, infatti:

$\binom{p}{1}(k \cdot p^h)^1 = p \cdot kp^h = k \cdot \boxed{p^{h+1}}$

$\binom{p}{1}(k \cdot p^h)^2 = \frac{p(p-1)}{2} \cdot k^2 \cdot p^{2h} = \frac{p-1}{2} \cdot k^2 \cdot \boxed{p^{2h+1}}$

$\vdots$

$\binom{p}{p}(k \cdot p^h)^p$

Quindi tutti i fattori sono multipli di p^{h+1} quindi modp^{h+1} si annullano quindi avremo che:

$$\boxed{(1 + k \cdot p^h)^p \equiv 1 \bmod p^{h+1}}$$

Questo dimostra il passo induttivo e quindi la nostra **Th.**

Dimostrazione: ora dimostriamo il teorema (**caso generale**) con $n = p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_r^{h_r}$ con p_i **primi distinti** e $h_i \in \mathbb{N}$, $\forall i \in \mathbb{N}_r$. Voglio provare che $\forall a \in \mathbb{Z} \mid \gcd(a, n) = 1$ e che quindi $a^{\phi(n)} \equiv_n 1$ (è la nostra **Th.**)

- so che $a^{\phi(p_i^{h_i})} \equiv 1 \bmod p_i^{h_i}$ $\forall i \in \mathbb{N}_r$ dato che $\gcd(a, p_i^{h_i}) = 1$, perché se a è **coprimo** con n, allora è **coprimo** anche con i singoli fattori.
- d'altra parte so che $\phi(n) = \phi(p_1^{h_1}) \cdot \phi(p_2^{h_2}) \cdot ... \cdot \phi(p_r^{h_r})$, quindi $\phi(p_i^{h_i}) | \phi(n)$ $\forall i \in \mathbb{N}_r$, cioè $\boxed{\frac{\phi(n)}{\phi(p_i^{h_i})} \in \mathbb{Z}}$
- elevando entrambi i membri della prima equivalenza a tale esponente ottendo:

$$a^{\phi(p_i^{h_i})} \equiv 1 \bmod p_i^{h_i}$$
$$\left(a^{\phi(p_i^{h_i})}\right)^{\frac{\phi(n)}{\phi(p_i^{h_i})}} \equiv (1)^{\frac{\phi(n)}{\phi(p_i^{h_i})}} \bmod p_i^{h_i}$$
$$\left(a^{\cancel{\phi(p_i^{h_i})}}\right)^{\frac{\phi(n)}{\cancel{\phi(p_i^{h_i})}}} \equiv (1)^{\frac{\phi(n)}{\phi(p_i^{h_i})}} \bmod p_i^{h_i}$$
$$a^{\phi(n)} \equiv 1 \bmod p_i^{h_i} \ \forall i \in \mathbb{N}_r$$

Ciò significa che $a^{\phi(n)} - 1$ è multiplo di $p_i^{h_i}$ $\forall i \in \mathbb{N}_r$, ma poiché i p_i sono **primi distinti**, si ha $a^{\phi(n)} - 1$ multiplo di $p_1^{h_1} \cdot p_2^{h_2} \cdot ... \cdot p_r^{h_r} = n$ e quindi avremo che:

$$\boxed{a^{\phi(n)} \equiv_n 1}$$

Formulazione equivalente del Teorema di Eulero-Fermat

$\forall n \in \mathbb{N}$ e $\forall a \in \mathbb{Z}$ tale che $\gcd(a, n) = 1$, si ha:

$$a^{\phi(n)+1} \equiv a \bmod n$$

Inoltre $a^{h \cdot \phi(n)+1} \equiv a \bmod n$

N.B.: se n non è primo, in generale l'ipotesi $\gcd(a, n) = 1$ **non** può essere rimossa.

$\Longrightarrow$ **intero libero da quadrati**: un intero $n \in \mathbb{N}$ si dice **libero da quadrati** se la sua scomposizione è il prodotto di primi disgiunti: $\boxed{n = p_1 \cdot p_2 \cdot ... \cdot p_r}$

Teorema di Eulero-Fermat Generalizzato: se $n \in \mathbb{Z}$ è un *intero libero da quadrati*, allora:

$$a^{\phi(n)+1} \equiv a \bmod n \quad \forall a \in \mathbb{Z}$$

Inoltre $a^{h\cdot\phi(n)+1} \equiv a \bmod n \quad \forall a \in \mathbb{Z},\ \forall h \in \mathbb{Z}^+$

Dimostrazione: supponiamo $n = p_1 \cdot p_2 \cdot ... \cdot p_r$ con p_i **primo** $\forall i \in \mathbb{N}_r$ e $p_i \neq p_j,\ \forall i \neq j$ e consideriamo il sistema di congruenze lineari:

$$\begin{cases} x \equiv a \bmod p_1 \\ x \equiv a \bmod p_2 \\ \vdots \\ x \equiv a \bmod p_r \end{cases}$$

Per il **Teorema Cinese del Resto** $\exists!$Sol $\bmod(p_1 \cdot p_2 \cdot ... \cdot p_r)$ cioè n. Banalmente $\overline{x} = a$ è soluzione del sistema. Quindi per provare la **Th.** basta verificare che anche $a^{k\cdot\phi(n)+1}$ è soluzione del sistema. Sappiamo che $\phi(n) = \phi(p_1 \cdot ... \cdot p_r) = \phi(p_1) \cdot ...\phi(p_r)$. Quindi $\forall i \in \mathbb{N}_r$ avremo che $\phi(n) = \phi(p_i) \cdot [\prod_{j\neq i} \phi(p_j)]$, che rappresenta la produttoria degli altri numeri primi escluso p_i e la chiameremo $S_i \in \mathbb{Z}$. Allora:

$$\begin{aligned} a^{k\cdot\phi(n)+1} &= a^{k\cdot S_i\cdot\phi(p_i)+i} && \forall i \in \mathbb{N}_r \\ &= a^{k\cdot S_i\cdot(p_i-1)+1} && k \cdot S_i \in \mathbb{Z} \\ &= a^{k\cdot S_i\cdot(p_i-1)+1} \equiv a \bmod p_i && \forall a \in \mathbb{Z} \end{aligned}$$

L'ultimo passaggio è possibile per il **corollario derivante dal piccolo teorema di fermat**. Quindi $a^{k\cdot\phi(n)+1}$ verifica la i-esima congruenza del sistema, si può quindi dimostrare analogamente per le restanti $r-1$ congruenze lineari del sistema.

4.2 Codici Correttori e Rilevatori

Alfabeto: insieme finito $\mathbb{F}$, ad esempio nel caso dell'alfabeto binario avremo che $\mathbb{F} = \{0, 1\}$

Parole: Sequenze finite di elemnti di $\mathbb{F}$, ad esempio se consideriamo la parola binaria: $100100_{(2)}$ questa sarà una parola di lunghezza 6.

Codice (a blocchi): Un qualunque sottoinsieme non vuoto $\mathbb{C} \subseteq \mathbb{F}^n$, ad esempio $\mathbb{C} = \{00000, 01011, 10101, 11110\}$ è un codice binario di lunghezza 5.

N.B. nell'addizione binaria, la somma di m bit è 0 quando tra di essi vi è un numero pari di bit uguale 1.

Controllo di Parità: il controllo di parità è un bit che, aggiunto ad una parola binaria, è: **0** se la parola conteneva un numero pari di bit a 1, **1**, se la parola conteneva un numero dispari di bit a 1.

4.2.1 Sistemi di Comunicazione

Nei canali di comunicazione, sono presenti un codificatore (lato mittente) e un decodificatore (lato destinatario). Il compito del codificatore, conoscendo la regola di codificazione usata dal mittente, è di tentare di ricostruire, in caso di messaggio disturbato, la versione originale.

- **Decodificatore a controllo di parità**: Si limita a controllare se la somma dei bit fa 0 oppure no, in caso negativo, si limita a segnalare che nella trasmissione della parola, è avvenuto un errore. Questo codice rilevatore si chiama **codice 1-rilevatore**, perché si accore di un errore, ma non riesce a correggerlo, in quanto non riesce a stabilire quale bit è stato invertito.
- **Codice ripetitivo**: viene inviato lo stesso messaggio di lunghezza k più volte (ad esempio triplo $n = 3k$)
  1. suddivide la parola ottenuta in parole parziali.
  2. partendo dal primo, si controlla l'i-esimo caratterre di ogni parola e, se una maggioranza dei caratteri coincide, allora si considera tale carattere come quello corretto.
  3. se non c'è una maggioranza, il processo emette una comunicazione di errore e si ferma. Altrimenti, si itera il procedimento per tutti i caratteri.
  4. infine, emette la parola ottenuta.

  Problema: se i caratteri errati compongono la maggioranza, allora il codice ripetitivo considera il bit errato come corretto, per ovviare a questo problema bisogna avere una probabilità di errore dei singoli bit bassa. **Tasso di informazione**: $\frac{1}{d}$, dove d è il numero di ripetizioni del messaggio.
- **Codice binario di Hamming**: il codificatore aggiunge al blocco di k bit, $k-1$ bit di controllo secondo la seguente regola:

$$\begin{array}{ccccccccc} & x_2+ & x_3+ & x_4+ & y_1 & & & =0 \\ x_1+ & & x_3+ & x_4+ & & y_2 & & =0 \\ x_1+ & x_2+ & & x_4+ & & & y_3 & =0 \end{array}$$

Figura 4.1: Esempio con $k = 4$

  Verrà poi inviata la sequenza $M = x_1x_2x_3x_4y_1y_2y_3$, il decodificatore calcolerà le 3 somme di controllo:

  - se sono tutte e tre uguali a 0, allora il decodificatore assume che non ci siano stati errori di comunicazione.

- se una somma è diversa da 0, allora il decodificatore assume che l'errore sia avvenuto sul bit di controllo.
- se 2 su 3 sono diverse da 0, allora il decodificatore assume che il bit scambiato è quello non presente nella terza somma.
- se sono tutti e tre diversi da 0, allora l'errore è nel quarto bit (presente in tutte le somme)

In questo caso avremo un **Tasso di informazione**: $\frac{k}{n} = \frac{k}{k+(k-1)}$, solitamente migliore del codice ripetitivo.

- **Codice ISBM**:

John H. Conway, Richard K. Guy
Il libro dei Numeri
Hoepli, Milano 1999
ISBN 88 – 203 – 2519 – 5

Figura 4.2: International Standard Book Number

- 88: indica che il libro è stato pubblicato in Italia.
- 203: indica l'editore.
- 2519: identificativo di quel libro, dalla casa editrice.
- 5: cifra di controllo

Il numero complessivo è ammissibile come numero **ISBM** se la somma pesata $10 \cdot Y_10 + 9 \cdot Y_9 + ... + 1 \cdot Y_1$ da un risultato divisibile per 11. La cifra di controllo serve quindi per riconoscere errori di trasmissione, dovuti ad errori di scrittura o di comunicazione del numero ISBM.

Canale di Trasmissione: Il canale binario simmetrico è uno dei modelli di trasmissione più utilizzati: accetta in ingresso e trasmette in usicta solo i caratteri $\mathbb{F} = \{0, 1\}$. **Probabilità cruda di errore** (**p**): è la probabilità con la quale, un bit entrato nel canale viene trasformato dal rumore nel bit complementare. Quindi, in una parola $x_1x_2...x_m$ avvengono t errori con una probabilità pari:

$$\boxed{(1-p)^{m-t} \cdot p^t}.$$

4.2.2 Interleaving

Si è supposto che i disturbi coinvolgano i caratteri in maniera indipendente, tuttavia, in realtà se un carattere viene alterato, allora è più facile che anche quelli vicini a lui vengano alterati. Il metodo di *interleaving* è efficace control scrosci di errori (**burst errors**), che non siano troppo lunghi.

Esempi

Data la sequenza da trasmettere: 10 00 01 11 11 11 01 10 00 00 10 10 ... Adottando il codice binario di lunghezza 5:$x_1x_2y_1y_2y_3$, dove $y_1 = x_1$, $y_2 = x_2$ e $y_3 = x_1 + x_2$, otteniamo delle parole che, memorizzate a gruppi di 4 creano delle matrici:

$$\begin{array}{ccccc} \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array} \quad \begin{array}{ccccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{array} \quad \begin{array}{ccccc} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{array}$$

Il contenuto di tali matrici viene inviato colonna per colonna. Supponiamo che avvengano dei disturbi ai bit: 3, 5, 6, 39, 40, 41, 42, 59 e 60. Quindi il messaggio letto dal decodificatore sarà:

$$\begin{array}{ccccc} \mathbf{1} & \mathit{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathit{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathit{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \end{array} \quad \begin{array}{ccccc} \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathit{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathit{0} \end{array} \quad \begin{array}{ccccc} \mathit{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathit{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathit{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathit{0} \end{array}$$

Riesce a decodificare correttamente i bit, perchè ogni riga ha al massimo 1 errore. I vantaggi dell'interleaving, tuttavia, si pagano con una maggiore complessità per la comunicazione e con dei ritardi nella trasmission dei dati.

Conclusioni: un buon algoritmo di decodificazione, oltre a correggere un alto numeri di errori di trasmissione, deve essere facile da implementare. Una regola aurea adottata è quella di cercare codici con un alto grado di simmetria (ovver che abbiamo un **gruppo di automorfismi** molto ricco).

Capitolo 5

Calcolo Combinatorio

Per scegliere le strutture combinatorie elementari coinvolte in un problema, occorre rispondere a due domande:

- l'**ordine** degli elementi è rilevante oppure no?
- gli elementi si possono **ripetere** oppure no?

5.1 Strutture Combinatorie Elementari

1. una **disposizione semplice** di n oggetti a k a k con $k \leq n$ è una k-upla ordinata di k oggetti distinti scelti tra gli n dati (**non** si tiene conto dell'**ordine**, **non** si **ripetono** gli elementi).

   Il numero di disposizioni semplici è $\boxed{D(n;k) = n \cdot (n-1) \cdot ... \cdot (n-k+1)}$

   Esempio: In un collegio ci sono 10 professori, in quanti modi possono essere scelti *presidente*, *vicepresidente* e *segretario*

   $$D_{10,3} = 10 \cdot 9 \cdot 8$$

2. una **disposizione con ripetizione** di n oggetti a k a k è una k-upla ordinata di k (non necessariamente distinti) scelti tra n dati (si tiene conto dell'**ordine**, si possono **ripetere** gli elementi).

   Il numero di disposizioni con ripetizioni di n oggetti a k a k è: $\boxed{D^R(n;k) = n^k}$

   Esempio: In un collegio ci sono 10 professori, in quanti modi posso scegliere i tutor per i 3 vincitori (un professore può essere tutor di più professori)

   $$D^R_{10,3} = 10^3$$

3. una **permutazione** di n oggetti è una n-upla ordinata i cui elementi sono tutti gli n oggetti (è una disposizione semplice di n oggetti a n a n). Il numero di permutazioni di n oggetti è:
$$\boxed{P(n) = n!}$$
4. una **combinazione semplice** di n oggetti a k a k (con $k \leq n$) è un sottoinsieme di k oggetti distinti scelti tra gli n dati (in questo caso **non** conta l'**ordine** e **non** posso ripetere gli elementi).

Il numero di combinazioni semplici di n oggetti a k a k è il "*coefficiente binomiale*" di n su k: $\boxed{C(n;k) = \binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}}$

Esempio: In un collegio di sono 10 professori, in quanti modi posso scegliere 3 professori per la commissione

$$C_{10,3} = \binom{10}{3} = \frac{10!}{3!\cdot(10-3)!} = \frac{10!}{3!\cdot 7!} = \frac{10\cdot 9\cdot 8\cdot \cancel{7!}}{3!\cdot \cancel{7!}} = \frac{10\cdot 9\cdot 8}{3!}$$

Definizione: un **Multinsieme** di cardinalità k è una collezione di oggetti, ciascuno ripetuto con una data molteplicità, in modo che la somma delle molteplicità sia pari a k.

Definizione: una **combinazione con ripetizione** di n oggetti a k a k è una collezione di k oggetti (non necessariamente distinti) scelti tra gli n oggetti dati (ovvero: è un *sotto-insieme* di cardinalità k dell'insieme di n oggetti dati). Il numero di combinazioni con ripetizioni di n oggetti a k a k è:

$$\boxed{C^R(n;k) = \binom{n+k-1}{k}}$$

N.B.: la differenza tra **insieme** e **multinsieme** è che un insieme a tutti gli elementi distinti, mentre un multinsieme ammette anche elementi ripetuti.

Dimostrazione: consideriamo $\mathbb{N}_n = \{1, 2, ..., n-1\}$, per avere una combinazione con ripetizione di k elementi in $\mathbb{N}_n$, devo scegliere:

$$1 \leq a_1 \leq a_2 \leq ... \leq a_{k-1} \leq a_k \leq n$$

Osservando le combinazioni semplici, cioè con elementi tutti distinti:

$1 \leq a_1 < a_2 + 1 \leq a_3 + 1 \leq ... \leq n + 1$

$1 \leq a_1 < a_2 + 1 < a_3 + 1 + 1 \leq ... \leq n + 1 + 1$

$\dots$

$1 \leq a_1 < a_2 + 1 < a_3 + 2 < ... < a_{k-1} + (k-2) < a_k + (k-1) \leq n + (k-1)$

Questo implica che, svegliere k elementi con ripetizione tra 1 e n, è come scegliere k elementi distinti tra 1 e $n + (k-1)$, quindi il numero di combinazioni con ripetinizioni di n elementi a k a k è: $C^R(n;k) = C^R(n+k-1;k) = \binom{n+k-1}{k}$

Esempi

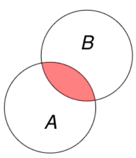
1. consideriamo la parola "discreta", quanti sono gli anagrammi (anche senza senso). Consideriamo che l'insieme $\mathbb{S} = \{d, i, s, c, r, e, t, a\}$ ogni suo elemento ha **molteplicità** uno, quindi l'esercizio si risolve con una **permutazione**:
$$P_3 = 8!$$
2. consideriamo la parola "matematica", quanti sono gli anagrammi (anche senza senso). Consideriamo l'insieme $\mathbb{S} = \{m, a, t, e, i, c\}$ in questo caso non tutti gli elementi dell'insieme hanno molteplicità uno, ad esempio, a ha molteplicità tre. Quindi dobbiamo utilizzare una **Permutazione su un multinsieme**.

Una **Permutazione su un Multinsieme** di cardinalità n, i cui elementi hanno rispettivamente molteplicità $k_1, ..., k_r$ (con $r \geq 1,\ k_1 \geq 1\ \forall i \in \{1, ..., r\}$ e tali che $\sum_{i=1}^{r} k_i = n$) è una n-upla ordinata i cui elementi sono tutti gli n oggetti (non tutti distinti) del multinsieme. Il numero di permutazioni su un multinsieme è pari:

$$\boxed{P^R(n; k_1, k_2, ..., k_r) = \frac{n!}{k_1 \cdot k_2 \cdot ... \cdot k_r}}$$

5.2 Principi Fondanti del Calcolo Combinatorio

- **Principio della Somma**: dati due insiemi finiti e disgiunti A e B, allora: $\boxed{\#(A \cup B) = \#A + \#B}$
- **Principio Generalizzato della Somma**: dati n insimi finiti $A_1, A_2, ..., A_n$ con $A_i \cap A_j = \emptyset\ \forall i \neq j\ i, j \in \mathbb{N}_n$, allora: $\boxed{\#(\bigcup\limits_{i \in \mathbb{N}_n} A_i) = \sum\limits_{i \in \mathbb{N}_n} \#A_i}$
- **Principio del Prodotto**: dati due insiemi finiti A e B, allora: $\boxed{\#(A \times B) = \#A \cdot \#B}$
- **Principio Generalizzato del Prodotto**: dati n insimei finiti $A_1, A_2, ..., A_n$ allora: $\boxed{\#(A_1 \times A_2 \times ... \times A_n) = \prod\limits_{i \in \mathbb{N}_n} \#A_i}$
- **Principio di Inclusione/Esclusione**: siano A e B insiemi finiti, con $\#A = n$ e $\#B = m$, allora: $\boxed{\#(A \cup B) = \#A + \#B - \#(A \cap B)}$

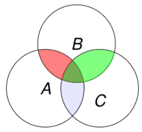


Dimostrazione: consideriamo l'unione disgiunta: $A \cup B = A \cup (B - A)$ $\Rightarrow \#(A \cup B) = \#A + \boxed{\#(B - A)}$, mentre B lo posso vedere come: $B = (B - A) \cup (A \cap B) \rightarrow \#B = \#(B - A) + \#(A \cap B)$ Quindi avremo $\boxed{\#(B - A)} = \#B - \#(A \cap B)$, sostituendo

$$\boxed{\#(A \cup B) = \#A + \#B - \#(A \cap B)}$$

- **Principio di Inclusione/Esclusione con tre Insiemi**: se A, B e C sono insiemi finiti, allora:

  $$\boxed{\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)}$$



Dimostrazione

$$\begin{aligned}
\#(A \cup B \cup C) &= \#[(A \cup B) \cup C] = \#(A \cup B) + \#C - \#[(A \cup B) \cap C] \\
&= \#(A \cup B) + \#C - \#[(A \cap C) \cup (B \cap C)] \\
&= \#A + \#B - \#(A \cap B) + \#C - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C) \\
&= \underline{\#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C)}
\end{aligned}$$

Formula di Da Silva: Se $A_1, A_2, ..., A_n$ sono insiemi finiti, allora:

$$\#(\bigcup_{i \in \mathbb{N}_n} A_i) = \sum_{I \subseteq \mathbb{N}_n,\, I \neq \emptyset} (-1)^{\#I-1} \cdot \#(\bigcap_{i \in I} A_i)$$

Generalizzando per n insiemi finiti: vengono aggiunte le cardinalità singole, si tolgono quelle a due a due, si aggiungono quelle a tre a tre, si tolgono quelle a quattro a quattro, e via dicendo. In questo modo avremo $2^n - 1$ addendi.

Capitolo 6

Relazioni Ricorsive

Una successione $\{a_n\}_{n\in\mathbb{N}}$ a valori interi può essere data in due forme differenti:

- per **elencazione**: $\{a_0, a_1, ..., a_i, ...\}$, con $a_i \in mathbbZ\ \forall i \in \mathbb{N}_0$
- in **forma chiusa**: $a_n = f(n)$, con $f : \mathbb{N}_0 \mapsto \mathbb{Z}$, f è un'**applicazione**

Successioni Definite per Ricorsione: una successione è definita **ricorsivamente** (ovvero tramite una **relazione ricorsiva**) se ogni termine della successione è espresso in funzione dei termini precedenti, e se sono noti un certo numero di termini iniziali che permettano di individuare univocamente la successione.

Risolvere una *relazione ricorsiva* significa ottenere una definizione in forma chiusa della successione stessa.

Esempio

$$\begin{cases} a_n = 3 \cdot a_{n-1} & n > 1 \text{ (relazione ricorsiva)} \\ a_1 = 3 & \text{(condizione iniziale)} \end{cases}$$

definisce univocamente la successione $\boxed{\{a_n\}_{n\in\mathbb{N}} = \{3, 3^2, 3^3, ...\}}$ che si può rappresentare in forma chiusa come:

$$a_n = 3^n\ \forall n \in \mathbb{N}$$

Una relazione ricorsiva si dice di **ordine *k*** se il generico elemento a_n della successione è dato in funzione di k elementi che lo precedono. La relazione ricorsiva determinerà univocamente una successione, noti i k elementi iniziali della successione

Una relazione ricorsiva di ordine k si dice **lineare** se viene rappresentata come:

$$a_n = b_{n-1}(n) \cdot a_{n-1} + b_{n-2}(n) \cdot a_{n-2} + ... + b_{n-k}(n) \cdot a_{n-k} + d(n)$$

dove i $b_{n-i}(n)$ $i \in \mathbb{N}$ sono delle funzioni (non necessariamente lineari) che determinano i coefficienti a_{n-i} $i \in \mathbb{N}$ mentre $d(n)$ è il termine noto (può non essere lineare).

Una relazione ricorsiva *lineare* si dice **omogenea** se il termine noto è nullo, ovvero $d(n) = 0$

Una relazione ricorsiva *lineare* si dice a **coefficienti costanti** se le funzioni coefficienti $[b_{n-i}(n)\ i \in \mathbb{N}]$ sono funzioni costanti, ovvero $b_{n-i}(n) = \alpha_i$, con α_i costante $\forall i$ e viene rappresentata:

$$a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} + ... + \alpha_k \cdot a_{n-k} + d(n)$$

6.1 Relazioni Ricorsive Lineari del 1° Ordine

Relazioni ricorsive lineari omogenee del I ordine a coefficienti costanti: la successione definita da:

$$\begin{cases} a_n = b \cdot a_{n-1} & \forall n > m \\ a_m = c \end{cases}$$

ha come forma chiusa: $\boxed{a_n = c \cdot b^{n-m}\ \forall n \geq m}$

Dimostrazione: si dimostra per **induzione**

Passo Iniziale: poniamo $n = m$ allora avremo che:

$$a_n = c \cdot b^{m-m} = c \cdot b^0 = c$$

abbiamo dimostrato le condizioni di partenza della relazione ricorsiva.

Passo Induttivo

Hp. $a_{n-1} = c \cdot b^{n-1-m}$ **Th.** $a_n = c \cdot b^{n-m}$

$$a_n = b \cdot a_{n-1} = b \cdot c \cdot b^{n-1-m} = c \cdot b^{n-m}$$

Esempio

$$\begin{cases} a_n = 3a_{a-1} \\ a_0 = 2 \end{cases} \Rightarrow a_n = 2 \cdot 3^{n-0} = 2 \cdot 3^n$$

Relazioni ricorsive lineari omogenee del I ordine a coefficienti non costanti: la successione definita da:

$$\begin{cases} a_n = b(n) \cdot a_{n-1} & \forall n > m \\ a_m = c \end{cases}$$

ha come forma chiusa $\boxed{a_n = c \cdot \prod_{i=1}^{n-m} b(m+i)\ \forall n \geq m}$. La forma chiusa può essere dimostrata per **induzione**, in perfetta analogia al caso precedente:

Relazioni ricorsive lineari del I ordine non omogenee a coefficienti costanti: la successione definita da:

$$\begin{cases} a_n = b \cdot a_{n-1} + d(n) \quad \forall n > m \\ a_m = c \end{cases}$$

ha come forma chiusa: $\boxed{a_n = b^{n-m} \cdot [c + \sum_{i=1}^{n-m} d(m+i) \cdot b^{-i}] \; \forall n \geq m}$

Dimostrazione: la forma chiusa viene dimostrata sempre per **induzione**

Passo Iniziale: poniamo $n = m$

$$a_n = b^{m-m} \cdot [c + \sum_{i=1}^{m-m} d(m+i) \cdot b^{-i}] = [c + \cancel{\sum_{i=1}^{0} d(m+i) \cdot b^{-1}}] = c$$

Passo Induttivo

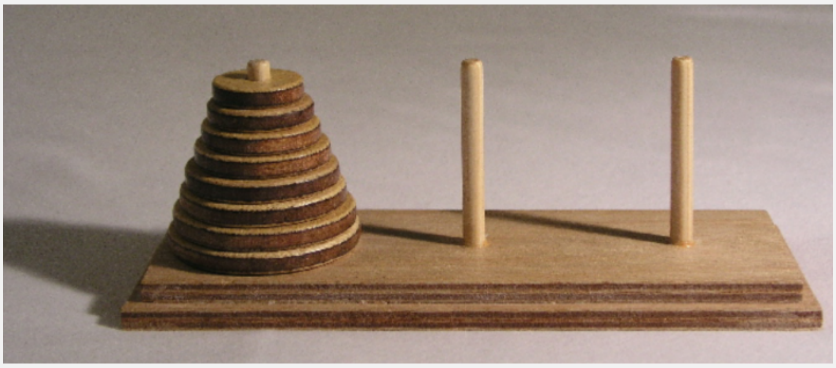
Hp.	**Th.**
$a_{n-1} = b^{n-1-m} \cdot [c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-i}]$	$a_n = b^{n-m} \cdot [c + \sum_{i=1}^{n-m} d(m+i) \cdot b^{-i}]$

$a_n = b \cdot a_{n-1} + d(n) = b \cdot b^{n-1-m}[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-1}] + d(n) \cdot \boxed{(b^{n-m} \cdot b^{-(n-m)})}$ moltiplico e divido per b^{n-m} in modo da poter raccogliere al primo addendo.

$$\begin{aligned} a_n &= b \cdot b^{n-1-m}[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-1}] + d(n) \cdot (b^{n-m} \cdot b^{-(n-m)}) \\ &= b^{n-m}[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-1}] + d(n) \cdot (b^{n-m} \cdot b^{-(n-m)}) \\ &= b^{n-m} \cdot \{[c + \sum_{i=1}^{n-1-m} d(m+i) \cdot b^{-1}] + \boxed{d(n) \cdot b^{-(n-m)}}\} \\ &= b^{n-m} \cdot [c + \sum_{i=1}^{n-m} d(m+i) \cdot b^{-i}] \end{aligned}$$

Il valore $\boxed{d(n) \cdot b^{-(n-m)}}$ posso portarlo dentro alla sommatoria in modo da poter ottenere e dimostrare la tesi.

Esempio - Torre di Hanoi: bisogna spostare n dischi di diametro crescente, in modo da riottenere la torre sull'ultima colonna. **Regole**: ad ogni passo si può spostare un solo disco, un disco non può mai essere spostato sopra ad uno di diametro inferiore.



Per spostare il generico n-esimo disco: $H_n = H_{n-1} + 1 + H_{n-1} = 2 \cdot H_{n-1} + 1$. Quindi la nostra relazione ricorsiva sarà: $H(n) = \begin{cases} H_n = 2 \cdot H_{n-1} + 1 \\ H_1 = 1 \end{cases}$

$$\begin{aligned} H(n) &= 2^{n-1}[1 + \sum_{i=1}^{n-1} 1 \cdot 2^{-i}] \\ &= 2^{n-1}[\sum_{i=0}^{n-1} 1 \cdot 2^{-i}] \\ &= 2^{n-1} \cdot \frac{1 - (\frac{1}{2})^n}{1 - \frac{1}{2}} \\ &= 2^n \cdot (1 - \frac{1}{2^n}) = 2^n - 1 \text{ mosse} \end{aligned}$$

Relazioni ricorsive lineri non omogenee del I ordine a coefficienti non costanti: la successione definita da:

$$\begin{cases} a_n = b(n) \cdot a_{n-1} + d(n) \quad \forall n > m \\ a_m = c \end{cases}$$

ha come forma chiusa: $\boxed{a_n = \prod_{i=1}^{n-m} b(m+i) \cdot [c + \sum_{i=1}^{n-m} d(m+i) \cdot \prod_{j=1}^{i} \frac{1}{b(m+j)}]\ \forall n \geq m}$. La forma chiusa può essere verificata per **induzione** come il caso a *coefficienti costanti*.

6.2 Relazioni Ricorsive Lineari del 2 Ordine

Algoritmi "dividi et impera" La decomposizione di un problema complesso in due o più sottoproblemi ricorsivi rappresenta un approccio molto efficace per la risoluzione di vari problemi computazionali, in informatica, permettendo di parallelizzare la computazione.

Relazioni ricorsive del tipo *divide et impera*

La generica relazione ricorsiva che divide il problema in k sottoproblemi (con $k \in \mathbb{N}$) è:

$$\begin{cases} s_n = b \cdot s_{\frac{n}{k}} + d(n) \quad \forall n > m \\ s_m = c \end{cases}$$

Si può supporre che $\exists z \in \mathbb{N}$ tale che $n = k^z$, ovvero $\log_k n = z$, possiamo esprimere la relazione ricorsiva come:

$$s_{k^z} = b \cdot s_{\frac{k^z}{k}} + d(k^z) = b \cdot s_{k^z-1} + d(k^z)$$

Definiamo $s_{k^z} = r_z$, poniamo $d(k^z) = d'(z)$ e $\log_k m = m'$ otteniamo la relazione ricorsiva del tipo:

$$\begin{cases} r_z = b \cdot r_{z-1} + d'(z) \quad \forall z > m' \\ r_{m'} = c \end{cases}$$

Dalla soluzione in forma chiusa di tale *relazione ricorsiva lineare non omogenea del I ordine*, si ricava infine la forma chiusa di s_n, applicando ad r_z la sostituzione inversa: $r_z = s_n$ e $z = \log_k n$.

Esempio: Ricerca Binaria

Data una lista ordinata di n elementi, per cercarne uno non è necessario dover scorrere tutta la lista, basta confrontare l'elemento a metà, dividendo quindi il problema in due sotto-problemi.

$$\begin{cases} c_n = 1 + c_{\frac{n}{2}} \quad \forall n > 1 \\ c_1 = 1 \qquad \text{se ho solo un elemento dovrò fare un solo confronto} \end{cases}$$

Supponendo $n = 2^z$ (ovvero $z = \log_2 n$) e ponenedo $c_n = c_{2^z} = r_z$ otteniamo:

$$\begin{cases} r_z = 1 + r_{z-1} \quad \forall n > m \\ r_{\log_2 1} = r_0 = 1 \end{cases}$$

Allora la soluzione di questa relazione ricorsiva è:

$$\boxed{r_z = b^{z-m} \cdot [c + \sum_{i=1}^{z-m} d'(m+i) \cdot b^{-i}] = 1 + \sum_{i=1}^{z} \; = 1 + z}$$

Sostituendo $z = \log_2 n$ otteniamo il valore di $r_{\log_2 n} = c_{2^{\log_2 n}} = c_n$ quindi otteniamo:

$$\boxed{c_n = 1 + \log_2 n}$$

Relazioni ricorsive lineari omogenee del II ordine a coefficienti costanti: è univocamente determinata, $\forall n \geq m$, la successione a_n tale che:

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-1} \quad \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

Lemma A: data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$, se a'_n e a''_n sono due successione che la verificano, allora $\forall A, b \in \mathbb{C}$ andche la successione $a_n = A \cdot a'_n + B \cdot a''_n$ verifica la relazione ricorsiva data.

Dimostrazione

Hp.	**Th.**
$a'_n = \alpha_1 \cdot a'_{n-1} + \alpha_2 \cdot a'_{n-2}$	$a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$
$a''_n = \alpha_1 \cdot a''_{n-1} + \alpha_2 \cdot a''_{n-2}$	$\forall A, B \in \mathbb{C}$ t.c. $a_n = A \cdot a'_n + B \cdot a''_n$

$$\begin{aligned} \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} &= \alpha_1(A \cdot a'_{n-1} + B \cdot a''_{n-1}) + \alpha_2(A \cdot a'_{n-2} + B \cdot a''_{n-2}) \\ &= A(\alpha_1 \cdot a'_{n-1} + \alpha_2 \cdot a'_{n-2}) + B(\alpha_1 \cdot a''_{n-1} + \alpha_2 \cdot a''_{n-2}) \\ &= A \cdot a'_n + B \cdot a''_n \quad || \text{ è la nostra tesi} \end{aligned}$$

Lemma B: data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$, la successione $a_n = r^n$, $r \neq 0$ è soluzione di tale relazione ricorsiva se e solo se r è radice dell'equazione (**equazione caratteristica della rel. ric.**): $x^2 - \alpha_1 x - \alpha_2 = 0$

Dimostrazione: essendo un *se e solo se* bisogna dimostrare entrambi i casi.

Prima Parte: "$\Rightarrow$"

Hp. $r \neq 0$ è soluzione dell'equazione caratteristica $x^2 - \alpha_1 x - \alpha_2 = 0$	**Th.** $a_n = r^n$ verifica la relazione ricorsiva $a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2}$

Per **Hp.** abbiamo $r^2 - \alpha_1 r - \alpha_2 = 0$, moltiplico per r^{n-2} (siccome $r \neq 0$ posso farlo) e ottengo $r^n - \alpha_1 r^{n-1} - \alpha_2 r^{n-2} = 0$, ma a questo punto $a_n = r?n$ che verifica la relazione ricorsiva e quindi la nostra tesi.

Seconda Parte "$\Leftarrow$"

Th. $a_n = r^n$ verifica la relazione ricorsiva $a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2}$	**Hp.** r è soluzione dell'equazione caratteristica $x^2 - \alpha_1 x - \alpha_2 = 0$

Per **Hp.**: $r^n = \alpha_1 r^{n-1} + \alpha_2 r^{n-2}$ portando tutto al primo membro e dividendo per r^{n-2} ottengo $r^2 - \alpha_1 r - \alpha_2 = 0$ ovvero r è soluzione dell'equazione caratteristica.

Lemma C: data

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} \quad \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

se l'equazione caratteristica della relazione ricorsiva ammette due radici distinte $r_1, r_2 \neq 0$, allora l'unica soluzione della relazione ricorsiva che verifica le condizioni iniziali date è del tipo

$$\boxed{a_n = A \cdot r_1^n + B \cdot r_2^n \text{ con } A, B \in \mathbb{C}}$$

Dimostrazione

Hp. | l'equazione caratteristica $x^2 - \alpha_1 x - \alpha_2 = 0$ ha $\Delta \neq 0$ ($r_1, r_2 \neq$ distinte)

Th. | l'unica successione che verifica la relazione ricorsiva:

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} \quad \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

è del tipo $\boxed{a_n = \overline{A} \cdot r_1^n + \overline{B} \cdot r_2^n}$ con $\overline{A}, \overline{B} \in \mathbb{C}$

Per il lemma B, sia $a'_n = (r_1)^n$ che $a''_n = (r_2)^n$ verificano la relazione ricorsiva, ma allora, per il lemma A, ogni successione $a_n = A(r_1)^n \text{è} B(r_2)^n$ verifica la relazione ricorsiva.

Dobbiamo quindi cercare se una di queste successioni verifica anche le condizioni iniziali. Imponiamo quindi:

$$\begin{cases} (a_m =) A(r_1)^m + (r_2)^m = c_1 \\ (a_{m+1} =) A(r_1)^{m+1} + (r_2)^{m+1} = c_2 \end{cases}$$

Questo è un sistema di due equazioni a due incoglite con una matrice dei coefficenti:

$$M = \begin{pmatrix} (r_1)^m & (r_2)^m \\ (r_1)^{m+1} & (r_2)^{m+1} \end{pmatrix}$$

Andiamo a calcolarci ora il *determinante* $\det(M) = (r_1)^m \cdot (r_2)^{m+1} - (r_1)^{m+1} \cdot (r_2)^m$ ovvero:

$$\det(M) = (r_1 r_2)^m (r_2 - r_1) \neq 0 \;\Rightarrow\; \rho(M) = 2$$

Il sistema è un sistema di Cramer, quindi $\exists! Sol(\overline{A}, \overline{B})$.

Lemma D: data la relazione ricorsiva $a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2}$, se l'equazione caratteristica presenta due radici r coincidenti e non nulle, allora anche la successione $a''_n = n \cdot r^n$ verifica la relazione ricorsiva.

Dimostrazione

Hp. l'equazione caratteristica $x^2 - \alpha_1 x - \alpha_2 = 0$ ha $\Delta = 0$

Th. la successione $a_n = n \cdot r^n$ verifica la relazione ricorsiva $a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2}$

Per **Hp.** abbiamo che $x^2 - \alpha_1 x - \alpha_2 = (x-r)^2 = x^2 - 2rx + r^2$ quindi avremo che $\alpha_1 = 2r$ mentre $\alpha_2 = r^2$ e quindi la relazione ricorsiva sarà: $a_n = 2ra_{n-1} - r^2 a_{n-2}$.
Dobbiamo ora verificare che $a''_n = n \cdot r^n$ verifichi la relazione ricorsiva:

$$\begin{aligned} a''_n &= 2ra''_{n-1} - r^2 a''_{n-2} \\ &= 2r(n-1) \cdot r^{n-1} - r^2(n-2) \cdot r^{n-2} \\ &= r^n[2(n-1) - (n-2)] \\ &= r^n(2n - \cancel{2} - n + \cancel{2}) = n \cdot r^n \end{aligned}$$

Lemma E: data

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} & \forall n > m+1 \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$$

se l'equazione caratteristica della relazione ricorsiva ammette due radici r coincidenti e non nulle, allora l'unica soluzione della relazione ricorsiva che verifica le condizioni iniziali date è del tipo $a_n = A \cdot r^n + B \cdot n \cdot r^n$, con $A, B \in \mathbb{C}$

Dimostrazione:

Hp. l'eq. caratteristica $x^2 - \alpha_1 x - \alpha_2 = 0$ ha $\Delta = 0$

Th. l'unica successione che verifica $\begin{cases} a_n = \alpha_1 a_{n_1} + \alpha_2 a_{n-2} \\ a_m = c_1 \\ a_{m+1} = c_2 \end{cases}$ è del tipo $a_n = \overline{A} \cdot r^n + \overline{B} \cdot n \cdot r^n$ $(\overline{A}, \overline{B} \in \mathbb{C})$

Per il lemma B, $a'_n = r^n$ verifica la rel. ric., ma per il lemma D anche $a''_n = nr^2$ la verifica. Quindi per il lemma A, ogni successione $a_n = A \cdot r^n + B \cdot n \cdot r^n$ verifica la rel. ric. Imponiamo le confizioni iniziali:

$$\begin{cases} (a_m =) A \cdot r^m + B \cdot mr^m = c_1 \\ (a_{m+1} =) A \cdot r^{m+1} + B(m+1) \cdot r^{m+1} \end{cases} \rightarrow M = \begin{pmatrix} r^m & mr^m \\ r^{m+1} & (m+1)r^{m+1} \end{pmatrix}$$

Calcoliamo il determinante della matrice dei coefficenti:

$$\det(M) = r^m(m+1)r^{m+1} - r^{m+1}mr^m = r^{2m+1}(m+1) - r^{2m+1}m = r^{2m+1} \Rightarrow \exists! Sol(\overline{A}, \overline{B})$$

Esercizio: supponendo che al primo mese si formi una coppia di conigli, che nel secondo mese diventi adulta e che nel terzo mese si generi una nuova coppia avremmo:

$$\begin{cases} F_n = F_{n-1} + F_{n-1} \quad \forall n > 1 \ \rightarrow \ \textbf{successione di Fibonacci} \\ F_0 = 0 \\ F_1 = 1 \end{cases}$$

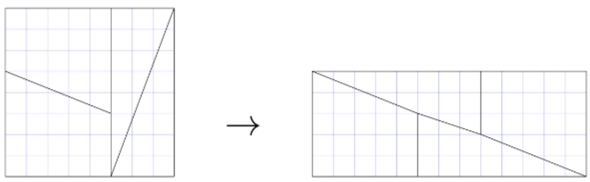
Ricaviamo l'equazione caratteristica della relazione ricorsiva: $x^2 - x - 1 = 0$ che avrà radici pari a $r_{1,2} = \frac{1 \pm \sqrt{5}}{2}$. Per il lemma C, la soluzione che verifica la relazione ricorsiva e le condizioni iniziali date è del tipo: $F_n = A \cdot r_1^n + B \cdot r_2^n$. Imponendo le condizioni iniziali avremmo:

$$\begin{cases} F_0 = 0 = A + B \\ F_1 = 1 = A \cdot \frac{1+\sqrt{5}}{2} + B \cdot \frac{1-\sqrt{5}}{2} \end{cases} \rightarrow \begin{cases} A = \frac{1}{\sqrt{5}} \\ B = -\frac{1}{\sqrt{5}} \end{cases}$$

La soluzione in forma chiusa è quindi: $\boxed{F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^2}$ In particolare, $r_1 = \frac{1+\sqrt{5}}{2} = \phi$ è detto **sezione aurea**. Questo numero è molto importante in quanto indica il rapporto tra i lati dei rettangoli "belli", viene infatti utilizzato nell'arte, nell'estetica, etc...

Dagli esempi di utilizzo della sezione aure sono le carte di credito, le proporzioni dell'uomo vitruviano o le colonne partenopee

Proprietà della successione di Fibonacci - Paradosso di Lewis Carrol: è possibile scomporre un quadrato di lato 8, per poi ricomporlo in un rettangolo di lati 5 e 13.



Identità di Cassini: se F_n denota l'n.esimo numeri di Fibonacci, allora:

$$F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$$

Dimostrazione: si procedeper **induzione**. Per $n = 1$ è banalmente vera, perché $1 \cdot 0 - (1)^2 = (-1)^1$. Supponiamo che l'identità valga per $n - 1$ ovvero: $F_n \cdot F_{n-1} - F_{n-1}^2 = (-1)^{n-1}$ [$F_n = F_{n-1} + F_{n-2} \ \rightarrow \ F_{n-2} = F_n - F_{n-1}$]

$$F_n \cdot (F_n - F_{n-1}) - F_{n-1}^2 = (-1)^{n-1}$$
$$(F_n)^2 - (F_n \cdot F_{n-1}) - F_{n-1}^2 = (-1)^{n-1}$$
$$(F_n)^2 - F_{n-1} \cdot (F_n + F_{n-1}) = (-1)^{n-1}$$

Poiche $F_n + F_{n-1} = F_{n+1}$ si ottiene l'identità di cassini per n: $F_n^2 - F_{n-1} \cdot F_{n+1} = (-1)^{n-1}$

6.3 Relazioni Ricorsive Lineari di Ordine Superiore al 2

Relazioni ricorsive lineari omogenee di ordin k a coefficienti costanti: è univocamente determinata, $\forall n \geq m$, la successione a_n tale che:

$$\begin{cases} a_n = \alpha_1 a_{n-1} + \alpha_2 a_{n-2} + ... + a_k a_{n-1} & \forall n \geq m+k \\ a_m = c_1 \\ a_{m+1} = c_2 \\ \vdots \\ a_{m+k+1} = c_k \end{cases}$$

Dividiamo il **procedimento risolutivo** in step:

1. si risolve l'*equazione caratteristica* (di grado k):
$$x^k - \alpha_1 x^{k-1} - \alpha_2 x^{k-2} - ... - \alpha_k = 0$$
questa soluzione ha sicuramente k radici complesse, se ogni radice si considera con la sua molteplicità.
2. per ogni radice r di molteplicità s, si considerano le successioni:
$a'_n = r^n$
$a''_n = n \cdot r^n$ $a'''_n = n^2 \cdot r^n$ $\vdots$
$a^{(s)}_n = n^{s-1} \cdot r^n$
3. tutte e k le successioni ottenute, sommate, verificheranno la relazione ricorsiva.
4. imponendo le condizioni iniziali si ottiene un sistema di Cramer da cui si ottiene l'unica soluzioni

N.B. il problema "grosso" in questi esercizi sarà il calcolo delle radici dell'equazione caratteristica (bisognerà utilizzare la scomposizione di **Ruffini**)

Esercizio

$$\begin{cases} a_n = 10a_{n-1} - 33a_{n-2} + 36a_{n-3} \quad \forall n \geq 3 \\ a_0 = 1 \\ a_1 = 5 \\ a_2 = 20 \end{cases}$$

1. eq. caratteristica: $x^3 - 10x^2 + 33x - 36 = 0$, devo trovare le sue radici: $(x-3)^2(x-4) = 0$
2. abbiamo trovato: $r_1 = 3$ con molteplicità 2, mentre $r_2 = 4$ con molteplicità 1
3. ottenendo: $A \cdot 3^n + B \cdot n \cdot 3^n + C \cdot 4^n$
4. impongo le condizion iniziali:

$$\begin{cases} (a_0 =) A \cdot 3^0 + B \cdot 0 \cdot 3^0 + C \cdot 4^0 = 1 \\ (a_1 =) A \cdot 3^1 + B \cdot 1 \cdot 3^1 + C \cdot 4^1 = 5 \\ (a_2 =) A \cdot 3^2 + B \cdot 2 \cdot 3^2 + C \cdot 4^2 = 20 \end{cases} \rightarrow \begin{cases} A + C = 1 \\ 3A + 3B + 4C = 5 \\ 9A + 18B + 16C = 20 \end{cases}$$

$$\begin{cases} A = 1 - C \\ 3 - 3C + 3B + 4C = 5 \\ 9 - 9C + 18B + 16C = 20 \end{cases} \rightarrow \begin{cases} A = 1 - C \\ 3B + C = 2 \\ 18B + 7C = 11 \end{cases} \rightarrow \begin{cases} A = 2 \\ C = -1 \\ B = 1 \end{cases}$$

Ottenendo $\boxed{a_n = 2 \cdot 3^n + n \cdot 3^n - 4^n}$

Relazioni ricorsive lineari non omogenee di ordine k: è univocamente determinata, $\forall n \geq m$, la successione a_n tale che:

$$\begin{cases} a_n = \alpha_1 \cdot a_{n-1} + \alpha_2 \cdot a_{n-2} + ... + \alpha_k \cdot a_{n-k} + d(n) \quad \forall n \geq m + k \\ a_m = c_1 \\ a_{m+1} = c_2 \\ \vdots \\ a_{m+k-1} = c_k \end{cases}$$

È possibile verificare che le **soluzioni** di una relazione lineare ricorsiva non omogenea si ottengano:

- una soluzione della relazione ricorsiva non omogenea.
- tutte le soluzioni della relazione ricorsiva omogenea associata.

Non ci sono metodi generali per il calcolo della soluzione particolare della non omogenea, abbiamo un teorema per 2 casi particolari:

Teorema: sia $d(n)$ il termine noto di una relazione ricorsiva lineare data.

- sia $d(n) = c \cdot q^n$, con c costante e $q \neq 0$. Se q non è radice dell'equazione caratteristica, allora esiste una soluzione particolare del tipo $a_n = \beta \cdot q^n$. Se q è radice dell'equazione caratteristica di molteplicità s, allora esiste una soluzione particolare del tipo $a_n = \beta \cdot n^s \cdot q^n$.
- sia $d(n)$ un polinomio in n di grado r. Se 1 non è radice dell'equazione caratteristica del tipo $a_n = \beta_0 + \beta_1 \cdot n + ... + \beta_r \cdot n^r$. Se 1 è radice dell'equazione caratteristica di molteplicità s, esiste una soluzione particolare del tipo: $a_n = n^s \cdot (\beta_0 + \beta_1 \cdot n + ... + \beta_r \cdot n^r)$

Corollario: se il termine noto di una relazione ricorsiva lineare data è costante, allora:

- se 1 non è radice dell'equazione caratteristica, esiste una soluzione particolare costante, ovvero del tipo $a_n = \beta$
- se 1 è radice dell'equazione caratteristica di molteplicità s, esiste una soluzione particolare del tipo $a_n = \beta \cdot n^s$

Capitolo 7

Funzioni Generatrici di una Successione

Una successione $\{a_n\}_{n\in\mathbb{N}_0}$ a volaroi interi può essere data:

- **per elencazione**: $\{a_0, a_1, ..., a_i, ...\}$, con $a_i \in \mathbb{Z}\ \forall i \in \mathbb{N}_0$
- **in forma chiusa**: $a_n = f(n)$, con $f : \mathbb{N}_0 \mapsto \mathbb{Z}$ applicazione
- **tramite una relazione ricorsiva**: ogni termine della successione è espresso in funzione dei termini precedenti, e la conoscenza di un certo numero di termini iniziali permettendo di individuare univocamente la successione.

Un altro modo per rappresentare una successione è attraverso una **Funzione Generatrice** di una successione, ovvero una serie formale di potenze i cui coefficienti coincidono con i termini della successione:

$$F(z) = \sum_{n=0}^{\infty} a_n z^n, \quad \text{con } z \in \mathbb{C}$$

Esempio

Alla successione $\{a_n\}_n = (1, 1, 1, 1, ...)$, ovvero $a_n = 1\ \forall n \in \mathbb{N}_0$, corrisponde la serie formale $\sum_{n\in\mathbb{N}_0} z^n$. Se si suppone $|z| < 1$ (quindi far convergere la serie) si ha $\sum_{n\in\mathbb{N}_0} z^n = \frac{1}{1-z}$; quindi la funzione generatrice è:

$$F(z) = \frac{1}{1-z}$$

Proprietà di Linearità: siano $F(z)$ e $G(z)$ le funzioni generatrici rispettivamente delle successioni: $\{f_n\}_n = (f_0, f_1, f_2, ..., f_n, ...)$ e $\{g_n\}_n = (g_0, g_1, g_2, ..., g_n, ...)$. Allora $\forall \alpha, \beta \in \mathbb{C}, \alpha \cdot F(z) + \beta \cdot G(z)$ è la funzione generatrice della successione:

$$\{\alpha f_n + \beta g_n\}_n = (\alpha f_0 + \beta g_0, \alpha f_1 + \beta g_1, ..., \alpha f_n + \beta g_n, ...)$$

Dimostrazione: consideriamo: $G(z) = \sum_n g_n z^n$ e $F(z) = \sum_n f_n z^n$ allora avremo che:

$$\alpha F(z) + \beta G(z) = \sum_n (\alpha f_n + \beta g_n) z^n$$

Esempio: data la successione $a_n = \{3, 0, 1, 0, 0, -2, 0, ...\}$, possiamo vedere la successione come combinazione lineare di 3 successione:

- $a'_n = (1, 0, 0, ...)$ e possiamo definirla come $F(z) = 1$
- $a''_n = (0, 0, 1, 0, 0, ...)$ definendola come $G(z) = z^2$
- $a'''_n = (0, 0, 0, 0, 0, 1, 0, ...)$ definendola come $H(z) = z^5$

Possiamo trovare un $\alpha, \beta, \gamma \in \mathbb{C}$ che ci permettano di ottenere la successione $F(z)$:

$$\overline{F}(z) = 3 \cdot F(z) + G(z) - 2 \cdot H(z) = 3 + z^2 - 2z^5$$

N.B. se una successione, da un certo punto in poi, ha tutti zeri, allora si può ricondurre ad una gunzione generatrice in forma polinomiale di grado pari all'ultimo elemento $\neq 0$ della successione.

Proprietà di Shift "a destra": se $G(z)$ è una funzione generatrice della successione $\{g_n\}_n = (g_0, g_1, g_2, ..., g_n, ...)$, allora la funzione generatrice della successione $\{g_{n-m}\}_n = \{\underbrace{0, ..., 0}_{m}, g_0, g_1, g_2, ...\}$ è:

$$\overline{G}(z) = z^m G(z)$$

Dimostrazione

$\overline{G}(z) = 0 + 0z + ... + 0z^{m-1} + g_0 z^m + g_1 z^{m+1} + ... = z^m(g_0 + g_1 z + g_2 z^2 + ...) = z^m G(z)$

Esempio

La successione $(0, 0, 0, 1, 1, 1, 1, ...)$ ha come funzione generatrice $G(z) = z^3 \cdot \frac{1}{1-z} = \frac{z^3}{1-z}$

Proprietà di Shift "a sinistra": se $G(z)$ è la funzione generatrice della successione $\{g_n\}_n = (g_0, g_1, g_2, ..., g_n, ...)$, allora la funzione generatrice della successione $\{g_{n+m}\}_n = (g_m, g_{m+1}, g_{m+2}, ...)$ è:

$$\overline{G}(z) = \frac{G(z) - g_0 - g_1 z - ... - g_{m-1} z^{m-1}}{z^m}$$

Dimostrazione

$\overline{G}(z) = g_m + g_{m+1} z^{m+1} + g_{m+2} z^{m+2} + ... + g_{n+m} z^n + g_{n+m+1} z^{n+1} + ...$ quindi segue che:

$$z^m \cdot \overline{G}(z) = g_m z^m + g_{m+1} z^{m+1} + ... + g_{n+m} z^{m+n} + ... = G(z) - g_0 - g_1 z - ... - g_{m-1} z^{m-1}$$

In pratica "butto via" i primi m elementi e comincio da quello dopo.

Proprietà del Cambio di Variabile: sia data una generica successione $\{g_n\}_{n\in\mathbb{N}_0}$ con funzione generatrice $G(z) = g_0 + g_1 z + g_2 z^2 + ... + g_n z^n + ...$ allora $G(z)$ è la funzione generatrice della successione $\{g_n \cdot c^n\}_{n\in\mathbb{N}_0}$

Dimostrazione: applicando a $G(\overline{z}) = \sum_n g_n \overline{z}^n$ il cambiamento di veriabile $\overline{z} = cz$, si ottiene: $G(zc) = g_0 + g_1(cz) + g_2(cz)^2 + ... + g_n(cz)^n + ... = g_0 + (g_1 c)z + (g_2 c^2)z^2 + ... + (g_n c^n)z^n + ...$

Esempio: data la successione $(1, 3, 9, 27, 81, ..., 3^n, ...)$ la sua funzione generatrice è $G(z) = 1 + 3z + 9z^2 + ... + 3^m z^n + ... = G(3z)$, dove $G(z) = \frac{1}{1-z}$ è la funzione generatrice della successione di soli 1.

$$H(z) = G(3z) = \frac{1}{1-3z}$$

Proprietà di Derivazione: sia data una generica successione $\{g_n\}_{n\in\mathbb{N}_0}$ con funzione generatrice $G(z) = g_0 + g_1 z + g_2 z^2 + ... + g_n z^n + ...$ allora la funzione derivata della funzione genratrice $G(z)$ ovvero $G'(z)$ è la funzione generatrice della successione $\{(n+1)g_{n+1}\}_{n\in\mathbb{N}_0}$

Dimostrazione

$$\overline{G}(z) = g_1 + 2g_2 z + 3g_3 z^2 + ... + n g_n z^{n-1} + (n+1)g_{n+1} z^n + ... = \sum_{n\in\mathbb{N}_0} (n+1)g_{n+1} z^n$$

In pratica moltiplico per la posizione corrent e shifto a sinistra.

Proprietà di Convoluzione: siano $F(z)$ e $G(z)$ le funzioni generatrici rispettivamente delle successioni $\{f_n\}_n = (f_0, f_1, f_2, ..., f_n, ...)$ e $\{g_n\}_n = (g_0, g_1, g_2, ..., g_n, ...)$ allora, il prodotto delle due funzioni generatrici, $F(z)G(z)$, è la funzione generatrice della successione ottenuta per convoluzione da $\{f_n\}_n$ e $\{g_n\}_n$, ovvero della successione $\{\sum_{k=0}^{n} f_k \cdot g_{n-k}\}_n$

Dimostrazione: per la proprietà distributiva del prodotto si ha che:

$$F(z)G(z) = (f_0 g_0) + (f_0 g_1 + f_1 g_0)z + (f_0 g_2 + f_1 g_1 + f_2 g_0)z^2 + ... = \sum_{n\in\mathbb{N}_0} (\sum_{k=0}^{n} f_k \cdot g_{n-k}) z^n$$

Che corrisponde alla successione delle somme dei possibili prodotti con cui ottengo il grado z^n.

7.1 Da relazioni ricorsive a funzioni generatrici

Esempio: funzione generatrice della successione di Fibonacci:

$$\begin{cases} F_n = F_{n-1} + F_{n-2} \ \forall n \geq 2 \rightarrow F_n - F_{n-1} - F_{n-2} = 0 \ \forall n \geq 2 \\ F_0 = 0 \\ F_1 = 1 \end{cases}$$

Per prima cosa calcolo le $F(z)$ necessarie per la successione:

$$F(z) = F_0 + F_1 z + F_2 z^2 + ... + F_n z^n + ...$$
$$z \cdot F(z) = F_0 z + F_1 z^2 + F_2 z^3 + ...$$
$$z^2 \cdot F(z) = F_0 z^2 + F_1 z^3 + ...$$

Ora le applico alla successione di Fibonacci:

$$F(z)(1 - z - z^2) = F_0 + (F_1 - F_0)z + (F_2 - F_1 - F_0)z^2 + ... + (F_n - F_{n-1} - F_{n-2})z^n + ...$$

Possiamo applicare anche le condizioni iniziali; $F_n - F_{n-1} - F_{n-2} = 0 \ \forall n \geq 2$

$$F(z)(1 - z - z^2) = 0 + (1 - 0)z + 0 + 0 + ... = z \Rightarrow F(z) = \frac{z}{1-z-z^2}$$

Esempio:

$$\begin{cases} a_n = 7a_{n-1} - 12a_{n-2} \ \forall n \geq 2 \rightarrow a_n - 7a_{n-1} + 12a_{n-2} = 0 \ \forall n \geq 2 \\ a_0 = 1 \\ a_1 = 2 \end{cases}$$

calcolo le $F(z)$:

$$F(z) = a_0 + a_1 z + a_2 z^2 + ...$$
$$7z \cdot F(z) = 7a_0 z + 7a_1 z^2 + ...$$
$$12z^2 \cdot F(z) = 12a_0 z^2$$

E infine le applico alla successione:

$$F(z)(1 - 7z - 12z^2) = a_0 + (a_1 - 7a_0)z + \cancel{(a_2 - 7a_1 + 12a_0)z^2} + \cancel{...} + \cancel{(a_n - 7a_{n-1} + 12a_{n-2})z^n} + \cancel{...} =$$
$$1 + (2 - 7)z \quad \Rightarrow \quad F(z) = \frac{1-5z}{1-7z+12z^2}$$

7.2 Da funzioni Generatrici a Forma Chiusa

Proprietà:

- se la funzione generatrice di una successione è **polinomiale**, la linearità permette di derminare banalmente la forma chiusa.

  Esempio: $F(z) = 2 - 3z^2 + 5z^4$
  - $F'(z) = 1 \to (1, 0, 0, ..., 0, ...)$
  - $F''(z) = z^2 \to (0, 0, 1, 0, ..., 0, ...)$
  - $F'''(z) = z^4 \to (0, 0, 0, 0, 1, 0, ...)$

  $\Rightarrow \{a_n\}_n = (2, 0, -3, 0, 5, 0, ...)$

- se la funzione generatrice di una successione è **razionale fratta**, con grado del denominatore minore o uguale a due, è possibile passare dalla funzione generatrice alla forma chiusa della successione, attraverso al "decomposizione in fratte semplici" e la conoscenza della funzioni generatrici di alcune successioni "tipiche":
  - se il denominatore ha **grado uguale a uno**, o se ha **grado due con due radici distinte**, la decomposizione in fratte semplici coinvolge solo addendi del tipo $\frac{A}{1-cz}$; si ottiene pertanto la forma chiusa della successione utilizzando, inisieme alla *linearità*, la conoscenza delle funizoni generatrici per le successioni del tipo $\{c^n\}_n$

    Esempio:

    $F(z) = \frac{1-5z}{1-7z+12x^2} = \frac{A}{(1-3z)} + \frac{B}{1-4z} = \frac{A(1-4z)+B(1-3z)}{1-7z+12z^2} = \frac{(A+B)+(-4A-3B)}{1-7z+12z^2}$

    $$\begin{cases} A + B = 1 \\ -4A - 3B = -5 \end{cases} \to \begin{cases} A = 2 \\ B = -1 \end{cases}$$

    $\Rightarrow F(z) = \frac{1-5z}{1-7z+12z^3} = \frac{2}{1-3z} - \frac{1}{1-4z} = 2 \cdot \frac{1}{1-3z} - 1 \cdot \frac{1}{1-4z}$

    Dove $\frac{1}{1-3z} = 3^n$ e $\frac{1}{1-4z} = 4^n$ quindi la $F(z)$ è la funzione generatrice della successione

    $$a_n = 2 \cdot (3)^n - (4)^n$$

  - nel caso di un denominatore di secondo grado con **radice c coincidente**, la decomposizione in fratte semplici diventa del tipo $\frac{a}{1-cz} + \frac{Bz}{(1-cz)^2}$; si ottiene pertanto la forma chiusa della successione utilizzando, insieme alla linearità, la conoscenza delle funzioni generatrici sia per le successioni del tipo $\{c_n^\}$ che per le successioni del tipo $\{nc^n\}_n$