Rigurgiti di Unicorno

di Valentino Bocchino

Parte di Teoria

Rigurgiti di unicorno

di Valentino Bocchino

08 febbraio 2026

Prefazione

Ho creato questo curioso formulario/dispensa per me stesso. Non credevo di riuscire a creare un documento così carino.
È la prima volta che mi affaccio al mondo di LaTeX, pertanto mi sono affidato a LyX.
Ho deciso di condividerlo con tutt* per una vasta serie di ragioni:

1. I formulari in circolazione sono di solito scritti a mano libera oppure al computer, con sistemi che non supportano l'inserimento di formule.

   1.1 Volevo offrire un'alternativa, proponendo un materiale elegante e che presentasse le formule in maniera conforme a come sono presentate nei materiali ufficiali del corso.

   1.2 Volevo anche offrire un'alternativa *accessibile* a molti student* come me[1], che hanno bisogno di una scrittura chiara e ben impostata. *Per chi non avesse esigenze particolari, è comunque bello avere un documento ben strutturato.*

2. Il materiale in circolazione è di solito estremamente condensato e focalizzato esclusivamente sulla risoluzione degli esercizi, trascurandone la comprensione.

   2.1 Volevo proporre un'alternativa flessibile e arricchente dal punto di vista didattico: potete modificare questo formulario, tagliando tutte le parti che non vi servono. Gli indici dinamici si aggiorneranno automaticamente.

      2.1.1 Il nostro corso ad oggi non impone un limite sulla quantità di materiale all'esame. Quindi (*nei limiti del ragionevole)*, *più volte*, mentre scrivevo questo formulario mi sono detto:
      "*Perché non metterlo?*"

[1] *Le neurodivergenze possono essere davvero toste. Tuttavia, alla fine sono una sfida come tante e magari si possono anche vincere a colpi di* LaTeX *e formulari.*
Prima dei ringraziamenti vorrei mettere mettere in luce le **caratteristiche principali** (*di cui vado fiero*) di questo formulario:

1. Possiede i riferimenti incrociati *dinamici*: Per intenderci: se si modificano l'ordine e/o i numeri dei vari titoli, *l'indice* assieme a tutti i riferimenti verso quel titolo, vengono *automaticamente* aggiornati. Inoltre, nella versione digitale, questi numeri sono cliccabili così come *l'indice*: rimandano direttamente al punto del documento a cui fanno riferimento.

2. Cerca di ridurre, con ogni mezzo possibile alcune ambiguità che possono insorgere durante la lettura, ad esempio, l'elemento neutro *e* viene colorato in arancione, per permettere di distinguerlo dalla congiunzione grammaticale.

3. Cerca di mantenere il più possibile uno stile coerente, per evitare fraintendimenti o brutte sorprese.

4. Nonostante si ispiri molto al libro del nostro corso, aggiunge anche parti in più e quasi sempre *commenta* le definizioni e i contenuti più *formali* per cercare di agevolare il più possibile una comprensione chiara e rapida.

5. Fa un uso massiccio dei **COLORI:** sono belli, e soprattutto sono utili per *enfatizzare trucchetti e relazioni.* Vengono spesso usati anche per evidenziare *collegamenti* tra sezioni diverse.

6. Ultimo ma non meno importante: **evita** *a tutti i costi* e con *ogni mezzo possibile* che un paragrafo venga troncato tra una pagina e l'altra. Ho sempre odiato profondamente tutti i libri che lo fanno. Sovente mi è capitato di arrivare alla fine della frase di un paragrafo credendo che fosse concluso insieme alla pagina, quando in realtà, proseguiva sul retro.

Ringraziamenti

Ringrazio la dott.ssa Vannini, che in veste di tutor mi ha aiutato tantissimo a trovare il coraggio di affrontare la vita universitaria. Ringrazio anche l* tutor Altair *(student* del nostro dipartimento)*, per avermi aiutato nella preparazione all'esame e per aver risposto a molti miei quesiti riguardanti i contenuti di questo documento.
Inoltre, ringrazio la mia famiglia per avermi aiutato a correggere le bozze di questo formulario.

Indice

Parte I
Formulario

1 Cose utili

1.1 Prodotti notevoli

1. Quadrato di un binomio con somma
   $(A+B)^2 = A^2 + 2AB + B^2$
2. Quadrato di un binomio con differenza
   $(A-B)^2 = A^2 - 2AB + B^2$
3. Prodotto tra la somma di due termini e la loro differenza
   $(A+B)\cdot(A-B) = A^2 - B^2$
4. Cubo di un binomio con somma
   $(A+B)^3 = A^3 + 3A^2B + 3AB^2 + B^3$
5. Cubo di un binomio con differenza
   $(A-B)^3 = A^3 - 3A^2B + 3AB^2 - B^3$
6. Quadrato di un trinomio con somma
   $(A+B+C)^2 = A^2 + B^2 + C^2 + 2AB + 2AC + 2BC$
7. Quadrato di un trinomio con differenza
   $(A-B+C)^2 = A^2 + B^2 + C^2 - 2AB + 2AC - 2BC$
8. Somma di due cubi
   $A^3 + B^3 = (A+B)(A^2 - AB + B^2)$
9. Differenza di due cubi
   $A^3 - B^3 = (A-B)(A^2 + AB + B^2)$
10. Trinomio speciale
    $x^2 + sx + p = (x+a)(x+b)$ *se e solo se*:
    $s = a+b, p = a\cdot b$

1.2 Equazioni di 2° grado

$$ax^2 + bx + c = 0$$
$$\Delta = b^2 - 4ac$$

$\Delta > 0 \to x_{1,2} = \dfrac{-b \pm \sqrt{\Delta}}{2a}$	$\Delta = 0 \to x = -\left(\dfrac{b}{2a}\right)$	$\Delta < 0 \to \nexists x \in \mathbb{R}$

1.3 Potenze

$a^0 = 1$	$a^{\frac{m}{n}} \cdot b^{\frac{m}{n}} = (a\cdot b)^{\frac{m}{n}}$
$a^{\frac{m}{n}} \cdot a^{\frac{p}{q}} = a^{\frac{m}{n}+\frac{p}{q}}$	$\dfrac{a^{\frac{m}{n}}}{b^{\frac{m}{n}}} = \left(\dfrac{a}{b}\right)^{\frac{m}{n}}$
$\dfrac{a^{\frac{m}{n}}}{a^{\frac{p}{q}}} = a^{\frac{m}{n}-\frac{p}{q}}$	$a^{-b} = \dfrac{1}{a^b}$
$\left(a^{\frac{m}{n}}\right)^{\frac{p}{q}} = a^{\frac{m}{n}\cdot\frac{p}{q}}$	

2 Insiemi

2.1 Definizioni generali

2.1.1 Definizione di insieme

Un insieme è una collezione ben definita di oggetti distinti, detti gli elementi dell'insieme.

2.1.2 Simboli

- $\in$ "appartiene"
- $\notin$ "**non** appartiene"
- $|$ "tale che" *Questa definizione può essere ambigua. Vedere "Definizione di divisione" (sezione 4).*
- $\forall$ "per ogni"
- $\exists$ "esiste"
- $\nexists$ "**non** esiste"
- $\exists!$ "esiste uno e uno solo", oppure "esiste un **unico**"
- $\neg$ negazione
- $\rightarrow$ implicazione
- $\mapsto$ "va in", oppure "viene mandato in"

Gli altri simboli verranno introdotti con le loro opportune definizioni.
Nel libro, tra una formula e l'altra vengono costantemente interscambiati i simboli con il loro equivalente in italiano.
In questo formulario ho scelto di mantenere le formule esattamente come compaiono nel libro dove possibile.

2.1.3 Insiemi uguali

Due insiemi si dicono uguali se hanno esattamente gli stessi elementi. $(A = B)$.

2.1.4 Appartenenza degli elementi ad un insieme: caso particolare

Se l'insieme A è un elemento dell'insieme B, gli elementi di A non sono, in generale, elementi di B. Ad esempio:
$A = \{1, -1\} \qquad B = \{0, A\}$
Allora $1 \in A$ e $A \in B$ ma $1 \notin B$.

2.1.5 Insieme vuoto

Si chiama insieme vuoto e si denota Ø l'insieme privo di elementi.
L'insieme vuoto è sempre un sottoinsieme banale di un insieme. Vedi il punto 2.2

2.1.6 Cardinalità

Si dice cardinalità di un insieme A, denotata $|A|$ il numero degli elementi di A.

2.2 Sottoinsiemi

2.2.1 Definizione di sottoinsieme

Un insieme B è un sottoinsieme *proprio* di A, denotato $B \subset A$, se ogni elemento di B è anche un elemento di A.
Vale anche la negazione, ovvero: $B \not\subset A$ dice che B ***non*** *è* un sottoinsieme di A.
Sottoinsiemi banali:

1. $A \subset A$, ovvero, A è sempre un sottoinsieme di se stesso.
2. $\emptyset \subset A$, ovvero, ogni insieme A ha come sottoinsieme l'insieme vuoto.

2.2.2 Insieme delle parti

Sia A un insieme.
Si dice insieme delle parti di A, denotato $P(A)$ l'insieme i cui elementi sono i sottoinsiemi di A:

$$P(A) = \{B | B \subset A\}$$

Include anche gli insiemi banali!

2.3 L'insieme $\mathbb{N}$ dei numeri naturali

2.3.1 Assiomi di Peano

1. $0 \in \mathbb{N}$
2. ogni $n \in \mathbb{N}$ ha un successore $s(n) \in \mathbb{N}$
3. se $m, n \in \mathbb{N}$e $m \neq n$ allora $s(m) \neq s(n)$
4. $\forall n \in \mathbb{N}$, $0 \neq s(n)$
5. Se $U \subset \mathbb{N}$ è tale che $0 \in U$ e $s(n) \in U$, $\forall n \in U$, allora $U = \mathbb{N}$

2.3.2 Teorema delle proprietà dei numeri naturali

Supponiamo assegnata per ogni $n \in \mathbb{N}$ una certa proprietà $P(n)$ e supponiamo che:

1. la proprietà $\mathcal{P}(0)$ è vera
2. $\forall n \in \mathbb{N}$ la verità di $\mathcal{P}(n)$ implica la verità di $\mathcal{P}(n+1)$.

Allora la proprietà $\mathcal{P}(n)$ è vera per ogni n.

2.4 Intersezione, unione, differenza, complementare e Leggi di De Morgan

2.4.1 Intersezione

Siano A e B insiemi. Si dice intersezione di A e B l'insieme:

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

Ovvero: tutti gli elementi che appartengono ad entrambi gli insiemi.
Due insiemi sono disgiunti se $A \cap B = \emptyset$

2.4.2 Unione

Siano A e B insiemi. Si dice insieme unione di A e B l'insieme:

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

L'insieme unione è l'insieme composto da tutti gli elementi di A *e tutti gli elementi di* B

2.4.3 Unione e intersezioni tra insiemi

Siano A B e C tre insiemi. Allora valgono le uguaglianze:

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \qquad (A \cap B) \cup C = (A \cup C) \cap (B \cup C)$$

2.4.4 Differenza tra insiemi

Siano A e X due insiemi.
Si dice differenza di X ed A e si denota $X \setminus A$ il sottoinsieme degli elementi di X non in A:

$$X \setminus A = \{x \in X | x \notin A\}$$

La differenza è composta da tutti gli elementi di X che **NON** sono presenti in A: *"sottrai a X gli elementi di A".*

2.4.5 Complementare tra insiemi

Sia A un **sottoinsieme** dell'insieme X. Si dice complementare di A in X e si denota $C_X(A)$ il sottoinsieme degli elementi di X non in A:

$$X \setminus A = \{x \in X | x \notin A\}$$

Il complementare funziona esattamente come la differenza (Punto 2.4.4), soltanto che A è un sottoinsieme di X. Il complementare è essenzialmente un "caso particolare di differenza tra insiemi".

2.4.6 Leggi di De Morgan (teorema)

Sia X un insieme e siano A e B sottoinsiemi di X. Allora:

$$C_X(A \cap B) = C_X(A) \cup C_X(B), \qquad C_X(A \cup B) = C_X(A) \cap C_X(B)$$

2.5 Partizioni e quozienti

Per i punti 1.4.x:
Sia X un insieme e sia $\mathcal{A} = \{A_i\}_{i \in \mathcal{I}}$ una famiglia di sottoinsiemi di X.

2.5.1 Ricoprimento

La famiglia $\mathcal{A} = \{A_i\}_{i \in \mathcal{I}}$ è detta un ricoprimento di X se:

$$\bigcup_{i \in \mathcal{I}} A_i = X$$

Se l'unione di tutti i sottoinsiemi della famiglia $\mathcal{A}$ genera l'insieme X, allora la famiglia $\mathcal{A}$ è un ricoprimento di X

2.5.2 Partizione

La famiglia $\mathcal{A} = \{A_i\}_{i \in \mathcal{I}}$è detta una partizione di X se:

1. è un **ricoprimento** di X
2. $\forall i \in \mathcal{I},\ A_i \neq \emptyset$ (la famiglia non ha insiemi vuoti)
3. $\forall i, j \in \mathcal{I} | i \neq j$ i sottoinsiemi A_i e A_j sono disgiunti, ovvero $A_i \cap A_j = \emptyset$ (tutti gli insiemi della famiglia sono disgiunti tra loro)

Pensa ad una partizione come alla suddivisione di una torta: l'insieme di tutte le fette (sottoinsiemi) genera l'intera torta. Non esistono fette "vuote" e tutte le fette sono disgiunte dalle altre.

2.5.3 Quoziente

Dato un insieme X con una partizione $\mathcal{A} = \{A_i\}_{i \in \mathcal{I}}$ l'insieme $Q = \{A_i\}$ i cui elementi sono i sottoinsiemi costituenti la partizione $\mathcal{A}$ si dice **insieme quoziente** di X (relativamente alla partizione $\mathcal{A}$). Dato un elemento $A \in Q$ ogni elemento $x \in X$ tale che $x \in A$ si dice **rappresentante** di A e a volte scriveremo $A = [x]$ oppure $A = \overline{x}$.
I sottoinsiemi costituenti la partizione sono proprio le classi di equivalenza di quella partizione!
Vedere il punto 2.7.3

2.6 Prodotto cartesiano

2.6.1 Definizione di prodotto cartesiano

Siano A e B insiemi. Si definisce prodotto cartesiano di A e B e si denota $A \times B$ l'insieme i cui elementi sono coppie di elementi con il primo elemento in A ed il secondo in B, ovvero:

$$A \times B = \{(a, b) | a \in A \text{ e } b \in B\}$$

La lettera e nella formula è il connettivo logico $\wedge$.
Vale la seguente: $\emptyset \times B = A \times \emptyset = \emptyset$
Per il prodotto tra più insiemi vale la seguente:

$$A_1 \times A_2 \times ... \times A_n = \{(a_1, a_2, ..., a_n) | a_i \in A_i, \forall i = 1, 2, ..., n\}$$

Il piano cartesiano π è definito dal prodotto $\mathbb{R} \times \mathbb{R}$, ovvero: $\pi = \mathbb{R} \times \mathbb{R}$
Esempio:
Siano $A = \{1, 2, 3\}$ e $B = \{6, 7\}$. Calcolare $A \times B$.
Dobbiamo trovare tutte le coppie possibili (a, b):

$$A \times B = \{(1, 6), (1, 7), (2, 6), (2, 7), (3, 6), (3, 7)\}$$

Per l'elemento $a = 1$ elenchiamo tutti i possibili elementi b di B e per ciascun b indichiamo una coppia. Una volta esaurito tutto B scegliamo il prossimo elemento di A, e ricominciamo, finché non esauriamo tutto l'insieme A.
Nota che l'ordine con cui si elencano le coppie (a, b) è indifferente, ma l'ordine all'interno della coppia lo è per definizione! Infatti:

$$(a, b) \neq (b, a)$$

2.6.2 Cardinalità del prodotto cartesiano

Siano A e B insiemi non vuoti. Se A e B sono finiti con $|A| = m$ e $|B| = n$ allora $|A \times B| = mn$. Se invece almeno uno tra A e B è infinito, allora anche $A \times B$ è infinito.

2.7 Relazioni

Per i punti 2.7.x:
A è un insieme non vuoto

2.7.1 Relazione binaria

Una relazione binaria *(o più semplicemente una **relazione** nell'insieme A)* è un sottoinsieme $\Gamma \subset A \times A$.
Data una relazione Γ nell'insieme A ed elementi $a, b \in A$ scriveremo alternativamente $a \Gamma b$ oppure "a è in relazione con b" per dire che $(a, b) \in \Gamma$.
*(il **prodotto cartesiano** elenca tutte le coppie possibili nell'insieme A. La relazione è semplicemente una scelta di alcune di queste coppie)*
Una relazione può godere delle seguenti **proprietà:**

1. **Proprietà riflessiva:** per ogni $a \in A$ si ha $a \Gamma a$.
2. **Proprietà simmetrica:** ogni qualvolta che a e b sono tali che $a \Gamma b$ allora anche $b \Gamma a$.
3. **Proprietà antisimmetrica:** se a e b sono tali che $a \Gamma b$ e $b \Gamma a$ allora $a = b$.
4. **Proprietà transitiva:** se a, b e c sono tali che $a \Gamma b$ e $b \Gamma c$ allora anche $a \Gamma c$.

Una relazione binaria è:

- una **relazione di equivalenza** se è **riflessiva, simmetrica** e **transitiva**
- una **relazione d'ordine** se è **riflessiva, antisimmetrica** e **transitiva**

2.7.2 Relazione di equivalenza

Sia Γ una relazione di equivalenza, tale che $\Gamma \subset A \times A$. Vale la seguente notazione:
Se $a\Gamma b$ diremo che a e b sono *equivalenti* e scriveremo: $a \sim b$.
Dato un elemento $a \in A$ possiamo considerare il *sottoinsieme* degli elementi ad esso *equivalenti*, ovvero:

$$C_a = \{x \in A | x \sim a\} = \{x \in A | a \sim x\}$$

Notiamo che le scritture $x \sim a$ e $a \sim x$ sono equivalenti perché Γ è *simmetrica*. L'insieme C_a è detto classe di equivalenza di a.
Vedere il punto 2.7.3

2.7.3 Teorema - Classi di equivalenza e partizioni

Vedere il punto 2.7.2
Sia A un insieme non vuoto e sia Γ una **relazione di equivalenza** in A. Allora le **classi di equivalenza** definiscono una **partizione** di A. Viceversa, data una partizione:

$$A = \bigcup_{i \in \mathcal{I}} C_i$$

esiste una **relazione di equivalenza** in A per cui i **sottoinsiemi** C_i **sono esattamente le classi di equivalenza.**
*Quindi, una **relazione di equivalenza** in A genera delle **classi di equivalenza** e pertanto le suddette classi definiscono una **partizione**.*
*Inoltre, ogni **partizione** ha origine dalle **classi di equivalenza** e un insieme di **classi di equivalenza** danno origine ad una **partizione**.*
Per capire meglio quanto appena detto vedere i punti 2.5.2 e 2.7.1
I colori usati qui verranno abbinati al punto 8.1.1 per facilitare la comprensione.

2.8 Insiemi numerici

- $\mathbb{N}$ insieme dei numeri **naturali** *(Vedere il punto 2.3)*
- $\mathbb{Z}$ insieme dei numeri **interi**: $\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ *Vedere il punto 5*
- $\mathbb{Q}$ insieme dei numeri **razionali**: $\{..., -3, -\frac{1}{2}, 0, 1, 2, \frac{10}{3}, ...\}$
  Sono tutti quei numeri esprimibili con il rapporto $\frac{a}{b}$, dove $a, b \in \mathbb{Z}$ e $b \neq 0$
- $\mathbb{R}$ insieme dei numeri **reali**: $\{..., 0, 1, \sqrt{2}, 2, \pi, ...\}$
- $\mathbb{C}$ insieme dei numeri **complessi**: *sono definiti mediante il prodotto cartesiano $\mathbb{R} \times \mathbb{R}$ e sono composti da una parte reale e una parte immaginaria.*

3 Funzioni

3.1 Definizioni generali

3.1.1 Definizione di funzione

Siano A e B insiemi non vuoti. Una funzione f con **dominio** A e **codominio** B è un sottoinsieme $\Gamma \subset A \times B$ tale che:
per ogni $a \in A$ esiste un unico elemento $b \in B$ tale che $(a, b) \in \Gamma$
Il sottoinsieme $\Gamma \subset A \times B$ è detto **grafico** della funzione.
Ne consegue che:

1. Dare una funzione f significa assegnare tre oggetti: il dominio A, il codominio B ed il grafico Γ. Usiamo le seguenti notazioni:

   1.1 $f : A \to B$

   1.2 $f(a) = b$ per intendere che $(a, b) \in \Gamma$

2. La condizione che per ogni $a \in A$ esista e sia unico $b \in B$ tale che $(a, b) \in \Gamma$ può essere riscritta dicendo che:
   "f deve essere definita per ogni $a \in A$ **e** in ogni $a \in A$ la funzione f può assumere un unico valore."

3. Due funzioni f e g **coincidono** se hanno dominio, codominio e grafico uguali

3.1.2 Funzioni particolari

1. **Funzione identità:** Dato un insieme A la funzione identità (su A) è la funzione $\mathrm{id}_A : A \to A$, definita come $\mathrm{id}_A(a) = a$ per ogni $a \in A$.
   Il grafico è $\Gamma = \{(a, a) \in A \times A | a \in A\}$. (restituisce sempre l'elemento in entrata.
   Una funzione identità è sempre biettiva)

2. **Funzione costante:** Dati gli insiemi A e B non necessariamente distinti, e fissato un elemento $\beta \in B$ la funzione costante con valore β è la funzione:
   $F_\beta : A \to B, \qquad F_\beta(a) = \beta, \forall a \in A.$
   Il grafico della funzione costante è: $\Gamma = A \times \{\beta\} \subset A \times B$.
   (restituisce sempre lo stesso valore)

3. **Proiezioni:** Dati due insiemi A e B non vuoti ed il loro prodotto cartesiano $A \times B$ le proiezioni sui singoli fattori sono:
   $p_1 : A \times B \to A, \qquad p_2 : A \times B \to B, \qquad p_1(a, b) = a, \qquad p_2(a, b) = b$
   per ogni $(a, b) \in A \times B$.
   (la proiezione è essenzialmente la rappresentazione, sull'insieme di destinazione, del prodotto cartesiano in ingresso. Ne consegue che su ogni prodotto cartesiano è possibile applicare infinite proiezioni.)

4. Una **successione** $b_0, b_1, b_2, ...$ in un insieme B è una funzione $s : \mathbb{N} \to B$, tale che:
   $s(0) = b_0, s(1) = b_1, s(2) = b_2$
   L'esempio più comune di successione è la successione $s : \mathbb{N} \to B$, con $B \subset \mathbb{N}$, tale che $s(x) = \{y | y = x + 1\}$
   (*la successione nei numeri naturali, dove ad esempio il successore di 3 è 4*).
   Tuttavia sono definibili successioni qualunque con criteri arbitrari.
   L'insieme di destinazione di una funzione di successione deve essere ordinabile.

5. **Prodotto cartesiano:** date le funzioni $f : A \to X$ e $g : B \to Y$ resta definita una funzione:
   $f \times g : A \times B \to X \times Y$,
   ponendo $(f \times g)((a, b)) = (f(a), g(b))$.

3.1.3 Restrizione

Sia $f : A \to B$ una funzione e sia $S \subset A$ un sottoinsieme di A. Si dice restrizione di f ad S la funzione $f_{|S} : S \to B$, tale che:

$$f_{|S}(s) = f(s), \forall s \in S$$

se f vale per l'insieme A, allora vale per qualunque sottoinsieme di A

3.1.4 Problema della buona definizione

Vedere il punto 2.5.3
Sia X un insieme con una data partizione e Q il corrispondente insieme quoziente. Capita sovente di definire una funzione:

$$f : Q \to B$$

avente dominio Q specificando il valore $f(A)$ per $A \in Q$ in termini non di A direttamente ma di un suo rappresentante $x \in A$.
È estremamente importante controllare che il valore $f(x)$ non dipenda dalla rappresentazione $A = [x]$ scelta, ma solo da A.
In tal caso diremo che f è ben definita.
Il rappresentante x scelto deve essere un argomento valido per la funzione, ovvero $f(x)$ deve avere soluzione nell'insieme di destinazione B.

3.2 Immagini e controimmagini

3.2.1 Immagine

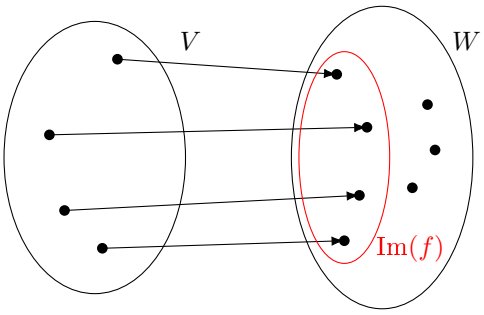
Sia $f : A \to B$ una funzione e sia $a \in A$.
Il valore della funzione in a, cioè l'elemento $b = f(a) \in B$ è anche detto immagine di a tramite f.
Questa terminologia si generalizza alla definizione seguente:
Sia $f : A \to B$ una funzione e sia $S \subset A$ un sottoinsieme del dominio A.
Si dice immagine di S tramite f il sottoinsieme $f(B)$ del codominio B costituito dalle immagini degli elementi di S,cioè:

$$f(S) = \{f(s) | s \in S\} \subset B$$

Quando $S = A$ l'immagine $f(S)$ si chiama semplicemente immagine di f e si denota $\mathrm{Im}(f)$, cioè:

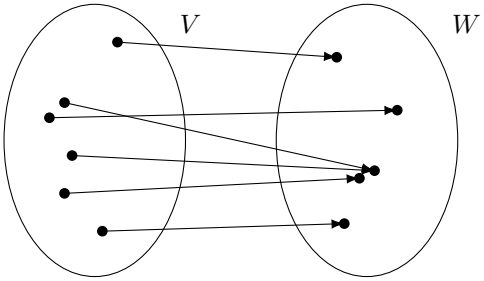
$$\mathrm{Im}(f) = f(A) = \{f(a) | a \in A\}$$

La definizione generale dice che per l'insieme di partenza corrisponde un insieme delle immagini di destinazione.
La definizione fa la distinzione tra il caso in cui l'insieme di partenza è un sottoinsieme S di A, ed il caso in cui invece il sottoinsieme S è tutto A ($S = A$).



3.2.2 Funzione suriettiva

Una funzione $f : A \to B$ si dice suriettiva se $\mathrm{Im}(f) = B$, ovvero se per ogni $b \in B$ esiste sempre $a \in A$ tale che $f(a) = b$.
L'insieme delle immagini coincide con l'insieme di destinazione.



3.2.3 Controimmagine

Sia $f : A \to B$ una funzione e sia $b \in B$. Si dice controimmagine di b tramite f il sottoinsieme $f^{-1}(b)$ degli elementi del dominio A che hanno b come immagine, ovvero:

$$f^{-1}(b) = \{a \in A | f(a) = b\}$$

In generale, dato un sottoinsieme $T \subset B$, si dice controimmagine di T tramite f il sottoinsieme $f^{-1}(T)$ del dominio costituito dalle controimmagini degli elementi di T, ovvero:

$$f^{-1}(T) = \{a \in A | f(a) \in T\}$$

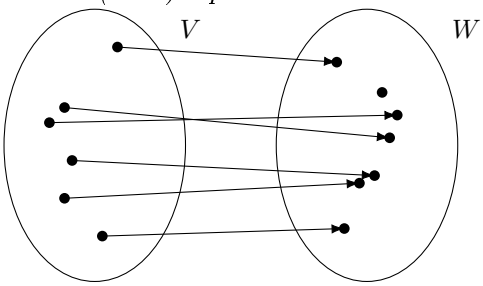
Attenzione a non confondere f^{-1} con il simbolo per la funzione inversa.

3.2.4 Differenze tra immagine e controimmagine

Se $S \subset A$ è un sottoinsieme **non vuoto** del dominio, l'immagine $f(S)$ **non è mai vuota**.
Invece se $T \subset B$ è un sottoinsieme **non vuoto** del codominio, la controimmagine $f^{-1}(T)$ **può anche essere vuota.**

3.2.5 Funzione iniettiva

Una funzione $f : A \to B$ si dice iniettiva se per ogni scelta di $a_1, a_2 \in A$, con $a_1 \neq a_2$ si ha $f(a_1) \neq f(a_2)$
Nessun elemento del dominio A ha la stessa immagine
Utilizzando la definizione di ***restrizione*** *(3.1.3) è possibile rendere iniettiva una funzione che non lo è.*

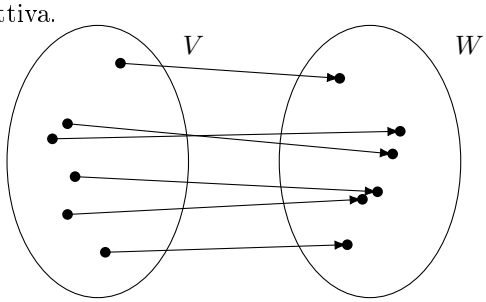


3.2.6 Proposizione sulle funzioni iniettive e suriettive

1. Una funzione è **iniettiva** *se e soltanto se* $|f^{-1}(b)| \leq 1$ per ogni b
2. Una funzione è **suriettiva** *se e soltanto se* $f^{-1}(b) \neq \emptyset$ per ogni $b \in B$

3.2.7 Funzione biettiva

Una funzione $f : A \to B$ si dice biettiva se è contemporaneamente **sia iniettiva che suriettiva**, ovvero se per ogni $b \in B$ *esiste ed è unico* un elemento $a \in A$ tale che $f(a) = b$.
Una **biezione** è una funzione biettiva.



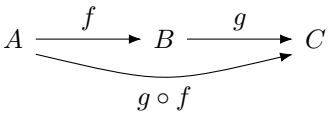
3.3 Composizione di funzioni

3.3.1 Definizione

Siano $f : A \to B$ e $g : B \to C$ due funzioni. La composizione di f e g, denotata $g \circ f$ è la funzione $g \circ f : A \to C$, ovvero:

$$(g \circ f)(a) = g(f(a)), \forall a \in A.$$

Quindi:



La composizione è definita soltanto se il codominio di f coincide con il dominio di g (nell'esempio sopra, il codominio B di f è infatti anche il dominio B di g).
ATTENZIONE: come puoi notare nell'esempio, nonostante "si parta da f e si arrivi a g", quando scrivi la composizione in simboli, l'ordine è invertito.

3.3.2 Proprietà associativa della composizione

Siano $f : A \to B$, $g : B \to C$ e $h : C \to D$ tre funzioni. Allora:

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

Ovvero:

$$A \xrightarrow{g \circ f} C \xrightarrow{h} D = A \xrightarrow{f} B \xrightarrow{h \circ g} D$$

entrambe le scritture hanno lo stesso effetto: $A \longrightarrow D$ e pertanto sono equivalenti.

3.3.3 Composizioni iniettive, suriettive e biettive

1. Se f e g sono **iniettive**, allora anche $g \circ f$ è **iniettiva**.
2. Se f e g sono **suriettive**, allora anche $g \circ f$ è **suriettiva**.
3. Se f e g sono **biettive**, allora anche $g \circ f$ è **biettiva**.

ATTENZIONE: NON vale il contrario: ad esempio con una composizione $g \circ f$ iniettiva *non è detto* che f e g siano entrambe iniettive, infatti:

3.3.4 Proprietà di funzioni derivate da composizioni

1. Se $g \circ f$ è **iniettiva**, allora f è **iniettiva**. *(come detto prima al punto 3.3.3, non è detto che lo siano entrambe, infatti, l'iniettività della composizione ci garantisce solo che f sia iniettiva, su g non possiamo dedurre nulla).*
2. Se $g \circ f$ è **suriettiva**, allora g è **suriettiva**.
3. Se $g \circ f$ è biettiva, allora f è **iniettiva** e g è **suriettiva**.
   *Questo è un **corollario**.*
   *Ricorda che una funzione per essere biettiva deve essere **sia suriettiva che iniettiva**.*
   *Il corollario ti dice che con una composizione biettiva, f è **sicuramente iniettiva** e g è **sicuramente suriettiva**. Quindi con la biettività della composizione non possiamo dire nulla sulla **suriettività** di f e sulla **iniettività** di g. (Infatti f e g potrebbero anche essere biettive).*
   Per riassumere la conseguenza di questo punto e di quello nel punto precedente (3.3.3):
   *Tutte le composizioni di funzioni biettive sono biettive, ma solo alcune composizioni con f soltanto iniettiva e g soltanto suriettiva sono biettive. L'iniettività di f e la suriettività di g sono condizioni entrambe **necessarie** ma **non sufficienti** affinché una composizione sia biettiva.*

3.4 Funzioni invertibili

3.4.1 Definizione

f e g sono funzioni inverse l'una dell'altra se $g \circ f = \mathrm{id}_A$ e $f \circ g = \mathrm{id}_B$.
Con id *si intende la **funzione identità** (3.1.2), che è sempre **biettiva**.*
Ad esempio, consideriamo due funzioni $f : A \to B$ e $g : B \to A$. Applicando la definizione:

$$g \circ f : A \to A \text{ e } f \circ g : B \to B$$

Quindi f e g sono funzioni inverse l'una dell'altra.
Pensa ad una funzione inversa come una funzione che ti permette, conoscendo un elemento dell'insieme di destinazione B, di ritornare all'elemento di origine nell'insieme A. Una funzione inversa "annulla" l'effetto della funzione originale.
Come conseguenza di tutto quello che è stato detto finora, se f e g sono inverse l'una dell'altra, allora sono anche entrambe **biettive**.

Se una funzione non è biettiva, allora non può avere un'inversa.
La funzione inversa si denota *per convenzione* con f^{-1}.
Attenzione perché la stessa notazione viene usata per indicare la controimmagine di f.
Invertendo la funzione inversa ottieni la funzione originale:

$$(f^{-1})^{-1} = f$$

3.4.2 Teorema sull'unicità della funzione inversa

Sia $f : A \to B$ una funzione **biettiva**. Allora *esiste ed è unica* una funzione $g : B \to A$ tale che f e g sono inverse l'una dell'altra.
(*Tutte le funzioni biettive hanno un'inversa, e questa inversa è unica, ovvero, non esistono funzioni che hanno più di una inversa.*)

3.4.3 Inversa della composizione di funzioni biettive

Siano $f : A \to B$ e $g : B \to C$ due funzioni biettive. Allora:

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

3.4.4 Proprietà di funzioni equivalenti

Sia $f : A \to B$ una funzione biettiva e supponiamo di avere funzioni $g_1, g_2 : B \to Y$ e $h_1, h_2 : X \to A$.

1. Se $g_1 \circ f = g_2 \circ f$, allora $g_1 = g_2$.
2. Se $f \circ h_1 = f \circ h_2$, allora $h_1 = h_2$.

3.5 Operazioni

3.5.1 Definizione di operazione binaria

Sia A un insieme non vuoto. Un'operazione binaria (*o più semplicemente, operazione*) su A è una **funzione**:

$$* : A \times A \to A$$

che associa a due elementi di un insieme un terzo elemento dello stesso insieme.
Il valore dell'operazione $*$ sulla coppia $(a_1, a_2) \in A \times A$ dovrebbe essere scritto come:

$$*((a_1, a_2))$$

Tuttavia, per praticità si adotta:

$$a_1 * a_2$$

Chiameremo l'operazione $*$ *"prodotto"* di a_1 e a_2 e dove non crea confusione, omettiamo il simbolo $*$ scrivendo:

$$a_1 a_2$$

3.5.2 Proprietà delle operazioni

Sia $*$ un'operazione su un insieme A. Diciamo che l'operazione $*$ è:

1. **associativa**: se $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$ per ogni $a_1, a_2, a_3 \in A$
2. **commutativa**: se $a_1 * a_2 = a_2 * a_1$ per ogni $a_1, a_2 \in A$

3.5.3 Elemento neutro

Sia $*$ un'operazione su un insieme A.
Un elemento $e \in A$ si dice **neutro** per $*$ se $a * e = e * a = a$, per ogni $a \in A$.
Se un elemento neutro per $*$ esiste, allora è **unico**.

3.5.4 Elemento inverso

Sia A un'insieme con un'operazione $*$ per cui esiste l'elemento neutro e. Diremo che un elemento $a \in A$ è invertibile, se esiste un elemento $b \in A$ tale che

$$a * b = b * a = e$$

b è quindi **l'inverso** di A.

3.5.5 Unicità dell'inverso nelle operazioni associative

Sia A un insieme con un'operazione **associativa** $*$ *per cui esiste l'elemento* ***neutro*** e. Sia $a \in A$ un elemento **invertibile** e siano $b, b' \in A$ tali che:

$$b * a = a * b' = e$$

Allora: $b = b'$

3.5.6 Potenze

Sia A un insieme dotato di un'operazione **associativa** $*$ e sia $a \in A$.

1. Se $n \geq 1$ diciamo n-esima potenza di a l'elemento definito *induttivamente* come:
   $a^1 = a$, e per ogni $n \geq 2$, $a^n = a^{n-1} * a$.
2. Se esiste l'elemento *neutro* e per $*$ poniamo $a^0 = e$.
3. Se $a \in A$ è *invertibile* e $n < 0$ poniamo $a^n = (a^{-1})^{|n|}$

Questa definizione e la proposizione seguente, stanno dicendo che, dove le potenze esistono, queste si comportano esattamente come ci si aspetta.

3.5.7 Legge delle potenze

Sia A un insieme con un'operazione **associativa** $*$ e sia $a \in A$. Allora per ogni $m, n \geq 1$ vale la formula:

$$a^m * a^n = a^{m+n}$$

Inoltre, se esiste l'elemento *neutro* per $*$ ed a è *invertibile*, la formula vale per ogni $m, n \in \mathbb{Z}$.

3.5.8 Sottoinsieme chiuso rispetto all'operazione $*$

Sia A un insieme con un'operazione $*$ e sia $S \subset A$ un sottoinsieme non vuoto. Diremo che S è **chiuso** rispetto all'operazione $*$ se:

$$s_1 * s_2 \in S, \forall s_1, s_2 \in S$$

Il risultato dell'operazione $*$ rimane nell'insieme di origine S

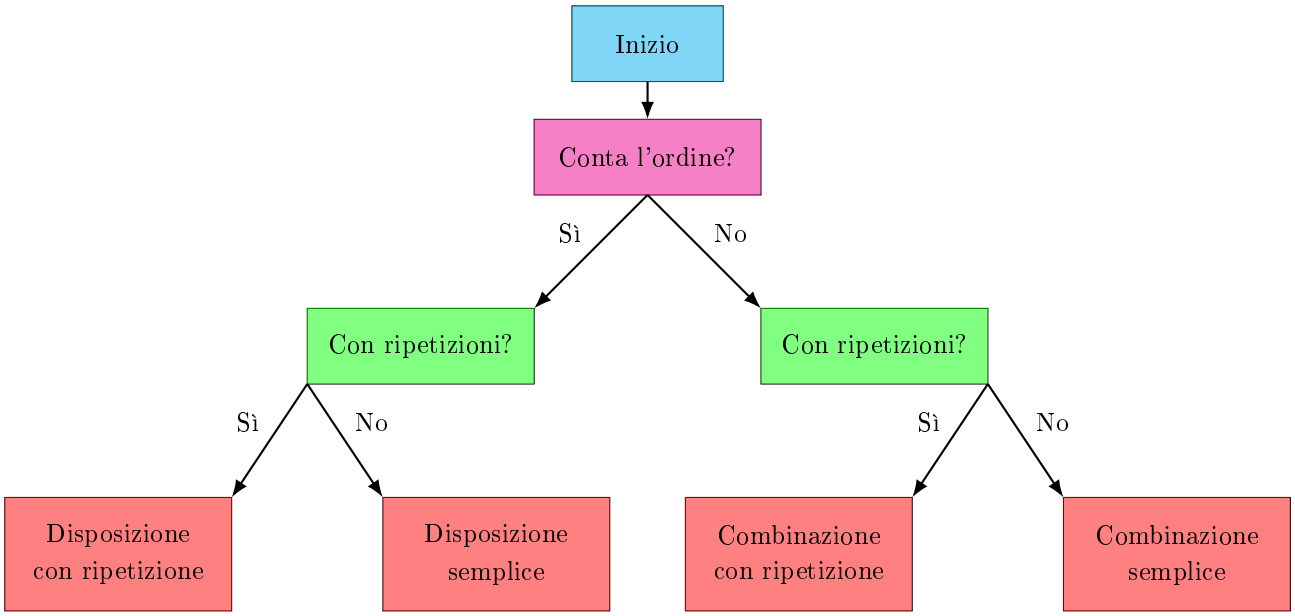
3.5.9 Il sottoinsieme degli elementi invertibili è chiuso rispetto all'operazione $*$

Sia A un insieme con un'operazione associativa $*$ per cui esiste l'elemento neutro e e sia $U \subset A$ il sottoinsieme degli elementi invertibili. Allora U è chiuso rispetto a $*$. Più precisamente, se $a, b \in A$ sono invertibili, allora:

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

4 Combinatorica

4.1 Schemino rapido



4.2 Introduzione

4.2.1 Introduzione alla combinatorica

Si tratta di tecniche per calcolare il numero di elementi in un insieme. In questo contesto ci occuperemo di insiemi finiti.
La situazione tipica è quella in cui è dato un insieme finito X e si vogliono calcolare quanti modi ci sono di scegliere un certo numero dei suoi elementi soddisfacenti alcune condizioni assegnate.

4.3 Insiemi finiti

4.3.1 Introduzione

Intuitivamente, contare gli elementi di un insieme A significa assegnare *un'etichetta* (ad. es. 1, 2, ecc.) ai suoi elementi, fino a quando non abbiamo *etichettato* tutti gli elementi di A.
Quindi, contare gli elementi di un insieme A vuol dire definire una funzione:

$$\alpha : A \to \mathbb{N}$$

α è **iniettiva** per costruzione *(nessun elemento di A ha la stessa etichetta di un altro elemento).*
Questo pone due problemi:

1. Il risultato finale dipende da quale funzione α viene scelta. *(come conti gli elementi)*
2. Non è detto che una funzione α esista.

Seguono a quanto appena scritto le definizioni necessarie per costruire l'approccio corretto al problema posto.

4.3.2 Insiemi equipollenti *(hanno lo stesso numero di elementi)*

Due insiemi A e B si dicono **equipollenti** se esiste una funzione **biettiva** $f : A \to B$.
Due insiemi A e B equipollenti hanno la stessa **cardinalità**, pertanto scriviamo $|A| = |B|$.
Siccome la composizione di biezioni è una biezione, se A, B e C sono insiemi, con $|A| = |B|$ e $|B| = |C|$, allora $|A| = |C|$.

4.3.3 Disuguaglianze tra cardinalità d'insiemi

Siano A e B due insiemi, diciamo che $|A| \leq |B|$ se: *(usiamo "diciamo che" perché questa è una **definizione**)*

1. Esiste una funzione **iniettiva** $f : A \to B$.
2. Esiste una funzione **suriettiva** $g : B \to A$.

Non devono valere entrambi i punti, basta che valga uno dei due.

4.3.4 Teorema di Schröder-Bernstein

Se $|A| \leq |B|$ *e* $|B| \leq |A|$, allora $|A| = |B|$.
Questo implica che in tutti gli altri casi si ha sempre $|A| \leq |B|$ *oppure* $|B| \leq |A|$.

4.3.5 Definizione di insiemi infiniti e finiti

1. Un insieme A si dice **infinito** se è ***equipollente*** ad un suo sottoinsieme *proprio*, cioè se esiste una funzione $f : A \to A$ **iniettiva** ma *non suriettiva.*
2. Un insieme A si dice **finito** *se non è infinito*, cioè se ogni funzione **iniettiva** $f : A \to A$ è una **biezione** (*è anche suriettiva*).
   Proposizione: f è **iniettiva**, **suriettiva** e **biettiva**.

4.3.6 Teorema sulla cardinalità degli insiemi

Valgono i fatti seguenti:

1. Per ogni $n \geq 1$ l'insieme I_n è **finito**.
2. Se $m \neq n$ gli insiemi I_m e I_n *non* sono **equipollenti** ($|I_m| \neq |I_n|$).
3. Se $m \leq n$ allora $|I_m| \leq |I_n|$.
4. Ogni insieme **finito** *non vuoto* è **equipollente** ad un I_n.
5. Per ogni insieme **infinito** X si ha $|\mathbb{N}| \leq |X|$.
   Fra tutti i possibili insiemi infiniti, $\mathbb{N}$ *è quello che ha cardinalità più piccola.*

4.3.7 *Principio delle gabbie di piccioni*

"Se abbiamo più piccioni che gabbie, c'è almeno una gabbia che contiene più di un piccione."
Se A e B sono insiemi finiti con $|A| > |B|$ *non* possono esserci funzioni **iniettive** $f : A \to B$.
Questo principio può essere usato in casi concreti per arrivare a conclusioni difficili da verificare. Ad esempio:
Su un corpo umano crescono circa *5 milioni* di peli. Ne consegue che in una metropoli con ben più di *5 milioni* di abitanti, anche escludendo le persone totalmente glabre, esistono almeno 2 persone con *lo stesso numero esatto di peli* (*limitandosi soltanto ai capelli* una coincidenza si ottiene tra gli abitanti di una città con una popolazione di oltre *200.000 unità).*
Inoltre questo principio è necessario per risolvere problemi simili. Ad esempio:
Una gelateria vende del gelato in confezioni sigillate. Purtroppo il gelataio ha scordato di mettere le etichette e quindi non sappiamo quali gusti ci siano in ogni confezione. Dalle dimensioni della vaschetta, il gelataio sa dirci quanti gusti contiene. Sappiamo che la gelateria vende 3 gusti di gelato (crema, fiori di sambuco e limone) e vogliamo acquistare una confezione dove siamo sicuri che almeno uno di questi gusti compaia 2 volte.
Per risolvere questo problema usiamo la formula:

$$n \cdot (k-1) + 1 = p$$

dove n rappresenta i gusti di gelato e k rappresenta il numero *minimo* di volte che desideriamo che un gusto qualunque si ripeta.
La formula restituisce p, che rappresenta il numero *minimo* di gusti all'interno della confezione, affinché la condizione sia soddisfatta.
Abbiamo quindi:

$$3 \cdot (2-1) + 1 = 4$$

Dal **quarto** gusto di gelato in poi, abbiamo la garanzia che *almeno uno* dei gusti sia *presente*, *almeno 2 volte*, nella confezione.

4.3.8 Insiemi infiniti numerabili

Un insieme infinito X si dice numerabile se è *equipollente* ad $\mathbb{N}$.
Valgono i seguenti fatti dimostrati da G. Cantor nel 1880. Le dimostrazioni di tali fatti esulano dai requisiti del corso (e probabilmente anche dalle mie competenze):

1. Esistono insiemi **infiniti non numerabili.**
2. $\mathbb{R}$ **non è numerabile.**
3. Per ogni insieme X, l'insieme delle parti $P(X)$ ha *cardinalità* **strettamente maggiore** a quella di X.

4.4 Principio di inclusione-esclusione

Questa sezione si occuperà come contare gli elementi di un'unione di due o più insiemi finiti di cui conosciamo separatamente il numero di elementi.

4.4.1 Cardinalità dell'unione di insiemi finiti disgiunti

Siano $A_1, ..., A_r$ insiemi *finiti* a due a due **disgiunti**. Allora:

$$\left|\bigcup_{i=1}^{r} A_i\right| = \sum_{i=1}^{r} |A_i| = |A_1| + ... + |A_n|$$

Se conosciamo la cardinalità di ogni insieme A_n e ognuno di questi insiemi è disgiunto da ogni altro insieme A_n (non hanno elementi in comune tra di loro), allora la cardinalità della loro unione è semplicemente la somma delle loro cardinalità.

4.4.2 Cardinalità dell'unione di due insiemi non disgiunti

Siano A e B insiemi finiti. Allora:

$$|A \cup B| = |A| + |B| - |A \cap B| \text{ oppure } |A \cup B| + |A \cap B| = |A| + |B|$$

La cardinalità dell'unione di due insiemi si ottiene sommando le loro singole cardinalità e sottraendo a tale somma, la cardinalità della loro intersezione.
Se hanno elementi in comune, questi compariranno in $A \cap B$ (impedendo che vengano contati due volte), altrimenti (come nel punto (4.4.1)), $A \cap B = \emptyset$, quindi $|A \cap B| = 0$.
Se si hanno più insiemi, si possono usare i metodi al punto 4.4.3, oppure si può usare ricorsivamente la formula sopra:
ad esempio per gli insiemi A, B, C possiamo prima considerare la cardinalità $|A \cup B|$, e successivamente definire un insieme $D = A \cup B$, che quindi avrà $|D| = |A \cup B|$, quindi possiamo poi considerare $|D \cup C|$. Abbiamo quindi che $|D \cup C| = |A \cup B \cup C|$.
Ecco un esempio di un problema risolvibile con questo principio:
Alla fine delle sessioni d'esame di un certo corso universitario, *152* matricole hanno superato l'esame di matematica e *144* matricole hanno superato l'esame di fisica. Sapendo che *89* matricole hanno superato entrambi gli esami, quante sono le matricole che hanno superato almeno uno dei due esami?
Dobbiamo contare tutti quelli che hanno superato matematica e tutti quelli che hanno superato fisica, escludendo coloro che hanno superato entrambi (Calcolo di $|F \cup M|$). Indichiamo con F l'insieme di chi ha superato fisica e con M l'insieme di chi ha superato matematica. Chi ha superato entrambi è di fatto nell'intersezione $F \cap M$. Sapendo che $|F| = 144$, $|M| = 152$ e $|F \cap M| = 89$, possiamo applicare la formula:

$$|F \cup M| = |F| + |M| - |F \cap M| = 144 + 152 - 89 = 207$$

4.4.3 Principio di inclusione-esclusione generale

Viene mostrato per 3 insiemi per comodità:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

In forma generale:

$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$ − l'intersezione (a coppie) di ogni insieme con ogni altro insieme* + $|A_1 \cap \cdots \cap A_n|$

*__Attenzione__ *a non prendere più volte la stessa intersezione ($A \cap B = B \cap A$).*
Vengono sommate tutte le cardinalità e poi vengono sottratte tutte le cardinalità delle intersezioni tra singoli insiemi.
*Tuttavia, così facendo, gli eventuali elementi in comune a tutti gli insiemi vengono sottratti al punto da essere conteggiati **0 volte**.*
La somma alla fine corregge il conteggio.

4.5 Metodo delle scelte successive

4.5.1 Cardinalità del prodotto cartesiano

Questa è una generalizzazione di quanto detto nella sezione del prodotto cartesiano (capitolo 1).
Siano $A_1, A_2, ..., A_k$ insiemi finiti con $|A_i| = n_i$ per ogni $i = 1, 2, ..., k$. Allora:

$$|A_1 \times A_2 \times ... \times A_k| = n_1 \cdot n_2 \cdot ... \cdot n_k$$

4.5.2 Metodo delle scelte successive

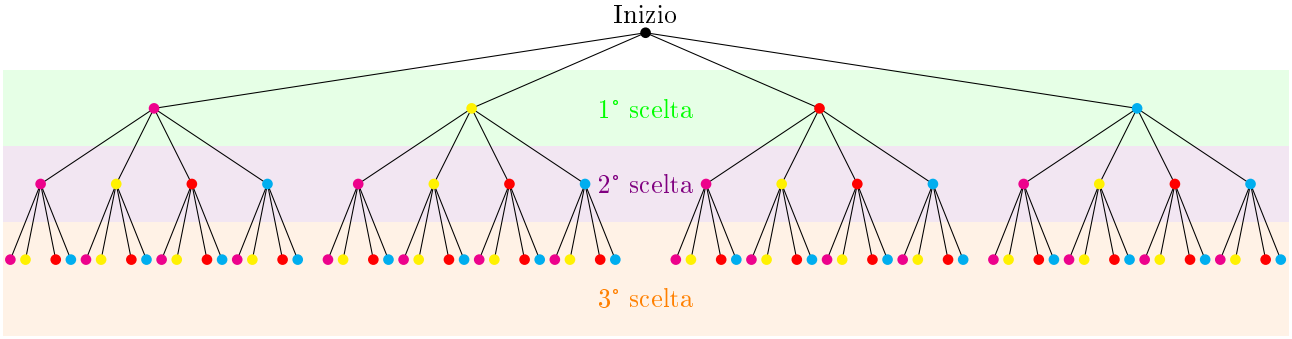
Se una certa situazione si ottiene con una successione di k scelte **indipendenti** e per la prima scelta ci sono n_1 possibilità, n_2 per la seconda, n_3 per la terza e così via, il numero totale delle situazioni è:

$$n = \prod_{i=1}^{k} n_i$$

Si applica quanto detto al punto (4.5.1). Le possibili scelte della prima scelta sono nell'insieme A_1 con $|A_1| = n_1$, e così via.
Il numero totale delle scelte possibili è dato da:

$$|A_1 \times A_2 \times ... \times A_k| = n_1 \cdot n_2 \cdot ... \cdot n_k$$

È anche possibile rappresentare questa struttura di scelte possibili in un diagramma ad albero. Facciamo un esempio:
Abbiamo un numero illimitato di sfere, di colore magenta, giallo, rosso e ciano.
Mettendo in fila 3 sfere, ammettendo anche più volte una sfera dello stesso colore, in quanti modi possibili, possiamo scegliere una fila di 3 sfere?



In questo caso particolare, tutti e tre gli insiemi hanno la stessa cardinalità.
Esempio di applicazione del metodo (senza diagramma):
Il codice PIN di uno smartphone è una sequenza di 4 cifre. Poiché per ogni cifra sono disponibili 10 scelte (0-9) e possono essere ripetute per ogni cifra, il totale dei PIN possibili è:
(Insiemi delle scelte, al pedice il numero della cifra del PIN). In questo caso particolare, tutti e quattro gli insiemi hanno la stessa cardinalità.

$$|A_1| = |A_2| = |A_3| = |A_4|$$

$$|A_1 \times A_2 \times A_3 \times A_4| = 10 \cdot 10 \cdot 10 \cdot 10 = 10.000$$

Ricordando il principio delle gabbie e dei piccioni (4.3.7): Se avessimo 10.001 smartphone, tutti con un PIN a 4 cifre, almeno 2 smartphone avranno lo stesso PIN.

4.6 Ordinamenti

4.6.1 Definizione di ordinamento

In quanti modi possibili possiamo ordinare un insieme?
Sia A un insieme finito con $|A| = n$. Un ordinamento di A è una funzione **biettiva (3.2.7)** $I_n \to A$.
Denotiamo con $\mathcal{O}_A$ *l'insieme degli ordinamenti* di A.

4.6.2 Definizione del fattoriale

Sia $n \in \mathbb{N}$. Si dice fattoriale di n e si denota $n!$ il numero così definito:

$$n! = \begin{cases} 1 & \text{se } n = 0 \\ 1 \cdot 2 \cdot 3 \cdot ... \cdot n & \text{se } n \geq 1 \end{cases}$$

La posizione $0! = 1$ è puramente convenzionale, tuttavia è necessaria (obbligatoria) per quello che facciamo qui.

4.6.3 Cardinalità dell'insieme degli ordinamenti

Sia A un insieme finito con $|A| = n$. Allora gli ordinamenti di A sono $n!$, ovvero:

$$|\mathcal{O}_A| = n!$$

Esempio di applicazione:
Uno youtuber vuole produrre una compilation con 12 brani. Una volta scelti i 12 brani avrà la scelta di ordinarli in:

$$12! = 1 \cdot 2 \cdot ... \cdot 12 = 479.001.600$$

modi diversi.

4.6.4 Definizione di anagramma

Sia A un insieme non vuoto di simboli e sia $f : I_n \to A$ una lista in A di lunghezza n. Un anagramma di f è una lista $h : I_n \to A$ ottenuta come composizione $h = f \circ g$, dove $g : I_n \to I_n$ è una biezione qualunque.
Gli anagrammi di una parola sono un elenco di tutte le parole possibili che si possono formare con le lettere della parola di partenza. Non viene richiesto che le parole generate abbiano senso compiuto. A noi interessa il numero di anagrammi che ha una parola. Tale calcolo necessita di una formula a parte poiché le lettere ripetute di una parola vanno conteggiate in modo diverso.

4.6.5 Calcolo del numero di anagrammi di una parola

Sia $f : I_n \to A$ una lista di lunghezza n in A e supponiamo $\mathrm{Im}(f) = \{a_1, ..., a_k\}$ dove $a_i \in A$ compare $r_i \geq 1$ volte fra $f(1), ..., f(n)$.
Allora il numero degli anagrammi di f è:

$$\frac{n!}{r_1! \cdot ... \cdot r_k!}$$

Ad esempio:
Gli anagrammi della parola MATEMATICA sono:
Le lettere di $MATEMATICA$ *sono 10, quindi a numeratore abbiamo* $10!$.
Per il denominatore, notiamo che A *compare* 3 *volte,* M *compare* 2 *volte e* T *compare* 2 *volte. Scriveremo quindi:* $3! \cdot 2! \cdot 2!$.

$$\frac{10!}{3! \cdot 2! \cdot 2!} = 151.200$$

Se nessuna lettera si ripete, al denominatore abbiamo 1: per parole con nessuna lettera che si ripete, è sufficiente calcolare il fattoriale del numero di lettere.

4.7 Disposizioni

L'ordine conta

4.7.1 Introduzione

Esistono situazioni in cui il problema non consiste nell'ottenere un elenco totale degli elementi di un insieme.
Distinguiamo ***due casi diversi:***

1. Quando ammettiamo ripetizioni tra gli elementi: **disposizione con ripetizione**
2. Quando **non** ammettiamo ripetizioni: **disposizione semplice**

Una disposizione produce una sequenza di elementi ***ordinati****.*

4.7.2 Definizione di disposizione con ripetizione

Sia A un insieme finito e $k \geq 1$ un numero intero. Una *disposizione con ripetizione di ordine k in A* è una *sequenza* di k elementi di A ***non necessariamente a due a due distinti***.
Una disposizione con ripetizione di ordine k è quindi un *sequenza di elementi* ***ordinati*** di A:
$a_1, ..., a_k$ con $a_i \in A$ che ammette $a_i = a_j$ $(i \neq j)$.
Può essere quindi vista come:

1. Una k-pla ordinata di elementi di A, cioè come un elemento arbitrario nel prodotto cartesiano $A \times ... \times A$ (k fattori)
   Ad esempio:
   Sia $A = \{1, 2\}$ un insieme e $k = 3$.
   Per la proposizione successiva, possiamo dedurre che il prodotto cartesiano sarà composto da $|A|^k = 2^3 = 8$ terne *(3 elementi)*.
   Quindi $A^3 = \{(1,1,1), (1,1,2), (1,2,1), (1,2,2), (2,1,1), (2,1,2), (2,2,1), (2,2,2)\}$.
   Ognuna di queste terne rappresenta una disposizione.
   L'ordine con cui vengono elencate le terne è irrilevante, invece è fondamentale ***l'ordine all'interno della stessa****, infatti ad esempio:*
   $(1,2,2) \neq (2,2,1)$
   Nelle disposizioni, conta l'ordine!
   Notiamo inoltre che siccome si tratta di disposizioni ***con ripetizioni*** *gli elementi 1 e 2 possono essere ripetuti all'interno della stessa disposizione (terna).*

2. Una funzione arbitraria $I_k \to A$.

4.7.3 Numero di disposizioni con ripetizioni in un insieme

Sia A un insieme finito con $|A| = n$ e sia $k \geq 1$ un intero.
Allora ci sono n^k disposizioni con ripetizione di ordine k in A.

4.7.4 Definizione di disposizione semplice

Sia A un insieme finito e $k \geq 1$ un numero intero. Una *disposizione semplice* di ordine k in A è una sequenza di k elementi di A ***a due a due distinti.***
Una disposizione semplice di ordine k è quindi un *sequenza di elementi* ***ordinati*** di A:
$a_1, ..., a_k$ con $a_i \in A$ che impone $a_i \neq a_j$ $(i \neq j)$.
Può essere quindi vista come una funzione **iniettiva** $I_k \to A$. A tal proposito, vanno considerati due **casi speciali**:
Sia $n = |A|$, allora:

1. Se $k > n$ *il principio delle gabbie e dei piccioni* ci dice che **non** ci sono funzioni **iniettive** e pertanto nemmeno disposizioni semplici di ordine k.

2. Se $k = n$ allora una disposizione semplice non è altro che un **ordinamento** di A. *Vedere il punto 4.6.3*

4.7.5 Numero di disposizioni semplici in un insieme

Sia A un insieme finito con $|A| = n$ e sia k un intero tra 1 e n. Allora il numero delle disposizioni semplici di ordine k in A è:

$$D_{n,k} = \frac{n!}{(n-k)!}$$

4.7.6 Esempi di problemi risolvibili con le disposizioni

1. Un artigiano ha prodotto *7 oggetti* di legno *diversi* l'uno dall'altro che ora vuole colorare avendo a disposizione smalti di *4 colori diversi. Quante sono le possibili colorazioni di questi oggetti*?
   Si tratta di assegnare un colore ad ogni oggetto e ovviamente possono esserci *oggetti diversi colorati col medesimo colore*. Dunque la soluzione è data dal numero delle *disposizioni con ripetizione* di ordine 7 *(k=7)* nell'insieme di 4 colori *(n=4), cioè* $4^7 = 16384$.

2. Ad una finale olimpica partecipano *12 atleti. Quanti sono i possibili podi?*
   Alle Olimpiadi un podio è costituito dai primi 3 classificati, nell'ordine a cui vengono assegnate le medaglie. Nella stessa gara, non vengono attribuite *più medaglie allo stesso atleta.* La soluzione è quindi data dal numero di *disposizioni semplici* di ordine 3 nell'insieme dei 12 atleti:
   $D_{12,3} = \frac{12!}{(12-3)!} = \frac{12!}{9!} = 10 \cdot 11 \cdot 12 = 1320$.

4.8 Combinazioni

L'ordine non conta!

4.8.1 Definizione di combinazione semplice

Sia A un insieme finito con $|A| = n$ e sia k un intero compreso tra 0 e n. Si dice *combinazione semplice di ordine k* in A la scelta di un sottoinsieme C con $|C| = k$.
L'ordine non conta e in accordo col risultato seguente, gli elementi ***non*** *si ripetono!*

4.8.2 Calcolo del numero di combinazioni semplici

Sia A un insieme finito con $|A| = n$ e sia k un intero compreso tra 1 e n. Il numero dei sottoinsiemi $C \subset A$ con $|C| = k$ (cioè il numero delle combinazioni di ordine k in A) è

$$C_{n,k} = \frac{1}{k!} D_{n,k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n \cdot (n-1) \cdot ... \cdot (n-k+1)}{k!}$$

Questa formula lega il fatto che ogni combinazione semplice C può essere ottenuta da $k!$ disposizioni semplici D. Questo è dovuto al fatto che nelle combinazioni non conta l'ordine, pertanto le disposizioni semplici con ordine diverso ma con gli stessi elementi, generano una singola combinazione.
Valgono i fatti seguenti:

1. $C_{n,0} = C_{n,n} = 1$
2. $C_{n,1} = n$

Esempio di applicazione:
Un fioraio vende piante di 14 specie diverse. Una cliente vuole comprare 3 piante di specie diverse da regalare ad un'amica. Quante scelte ha? *Dovendo scegliere 3 piante su 14 il numero delle possibilità è:*

$$C_{14,3} = \frac{14!}{3! \cdot (14-3)!} = \frac{\cancel{14!}}{3! \cdot \cancel{11!}} = \frac{12 \cdot 13 \cdot 14}{3!} = \frac{\cancel{12} \cdot 13 \cdot 14}{2 \cdot \cancel{3}} = \frac{\cancel{4} \cdot 13 \cdot 14}{\cancel{2}} = 2 \cdot 13 \cdot 14 = 364$$

4.8.3 Semplificazione del calcolo di combinazioni semplici

Siano n e k due numeri interi con $0 \leq k \leq n$. Allora $C_{n,k} = C_{n,n-k}$

4.8.4 Risoluzione di problemi con combinazioni insieme ad altre tecniche

Ad esempio:
Ad una scuola di ballo partecipano 11 ballerine e 9 ballerini.
Per realizzare una coreografia, i maestri di hanno bisogno di scegliere 5 ballerini e 3 ballerine.
Quante sono, in totale le scelte possibili?
La soluzione comporta 2 scelte separate.
Per il gruppo dei ballerini e delle ballerine è necessario calcolare il numero di combinazioni semplici:

$$C_{9,5} = C_{9,9-5} = C_{9,4} = \frac{9!}{4! \cdot (9-4)!} = \frac{\cancel{9!}}{4! \cdot \cancel{5!}} = \frac{6 \cdot 7 \cdot 8 \cdot 9}{4!} = \frac{\cancel{6} \cdot 7 \cdot 8 \cdot 9}{\cancel{2} \cdot 3 \cdot 4} = \frac{\cancel{3} \cdot 7 \cdot 8 \cdot 9}{\cancel{3} \cdot 4} = \frac{7 \cdot \cancel{8} \cdot 9}{\cancel{4}} = 7 \cdot 2 \cdot 9 = 126$$

$$C_{11,3} = \frac{11!}{3! \cdot (11-3)!} = \frac{\cancel{11!}}{3! \cdot \cancel{8!}} = \frac{9 \cdot 10 \cdot 11}{3!} = \frac{9 \cdot \cancel{10} \cdot 11}{\cancel{2} \cdot 3} = \frac{\cancel{9} \cdot 5 \cdot 11}{\cancel{3}} = 3 \cdot 5 \cdot 11 = 165$$

Le 2 scelte sono indipendenti tra loro, ovvero: un qualunque gruppo di ballerine può ballare con un qualsiasi gruppo di ballerini.
Applicando il metodo delle scelte successive:

$$C_{9,5} \cdot C_{11,3} = 126 \cdot 165 = 20.790$$

4.8.5 Definizione di combinazione con ripetizione

Sia A un insieme finito con $|A| = n$ e sia k un intero non negativo. Si dice combinazione con ripetizione di ordine k in A una scelta di k elementi in A in cui *ciascun elemento può essere scelto più volte.*
Indichiamo con C' le combinazioni con ripetizione.

4.8.6 Calcolo del numero di combinazioni con ripetizione

Sia A un insieme finito con $|A| = n$ e sia k un intero positivo. Allora il numero delle combinazioni con ripetizione di ordine k in A è:

$$C'_{n,k} = C_{k+n-1,n-1} = \frac{(k+n-1)!}{(n-1)! \cdot k!}$$

Esempio di applicazione:
Una pasticceria produce cioccolatini di 8 tipi diversi e permette di far decidere ai clienti la composizione delle scatole.
Quanti modi ha un cliente di comporre una scatola di 24 cioccolatini?
Siccome un cliente può scegliere più cioccolatini dello stesso tipo, è necessario calcolare il numero di combinazioni con ripetizione di ordine 24 nell'insieme A:

$$C'_{8,24} = C_{24+8-1,8-1} = C_{31,7} = \frac{31!}{7!\cdot(31-7)!} = \frac{\cancel{31!}}{7!\cdot\cancel{24!}} = \frac{25\cdot26\cdot27\cdot28\cdot29\cdot30\cdot31}{7!} = \frac{25\cdot\cancel{26}\cdot27\cdot28\cdot29\cdot30\cdot31}{\cancel{2}\cdot3\cdot4\cdot5\cdot6\cdot7} = \frac{25\cdot13\cdot\cancel{27}\cdot28\cdot29\cdot30\cdot31}{\cancel{3}\cdot4\cdot5\cdot6\cdot7} =$$
$$= \frac{25\cdot13\cdot9\cdot\cancel{28}\cdot29\cdot30\cdot31}{\cancel{4}\cdot5\cdot6\cdot7} = \frac{\cancel{25}\cdot13\cdot9\cdot7\cdot29\cdot30\cdot31}{\cancel{5}\cdot6\cdot7} = \frac{5\cdot13\cdot9\cdot7\cdot29\cdot\cancel{30}\cdot31}{\cancel{6}\cdot7} = \frac{5\cdot13\cdot9\cdot\cancel{7}\cdot29\cdot5\cdot31}{\cancel{7}} = 5\cdot13\cdot9\cdot29\cdot5\cdot31 = 2.629.575$$

Questi passaggi sono del tutto opzionali: per numeri così grandi è più opportuno inserire $\frac{31!}{7!\cdot24!}$ direttamente nella calcolatrice.

4.8.7 Coefficienti binomiali

4.8.8 Definizione di coefficiente binomiale

Siano k ed n due numeri interi, con $0 \leq k \leq n$. Usiamo la notazione $\binom{n}{k}$ per indicare il numero:

$$\frac{n!}{k! \cdot (n-k)!}$$

Quindi:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Pertanto:

$$C_{n,k} = \binom{n}{k}$$

4.8.9 Formula di Stiefel e altre formule

Valgono le seguenti formule:

1. Per ogni $n \geq 0$, $\binom{n}{0} = \binom{n}{n} = 1$. *Come già visto al punto 4.8.2".*
2. Per ogni coppia di numeri interi k ed n tali che $n \geq 0$ e $0 \leq k \leq n$, vale:

   $$\binom{n}{k} = \binom{n}{n-k}$$

   Come già visto al punto 4.8.2.
3. **Formula di Stiefel**: Per ogni coppia di numeri interi k ed n tali che $n \geq 1$ e $1 \leq k \leq n$ vale la seguente:

   $$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

   Per farla valere per ogni k possiamo per convezione imporre $\binom{n}{k} = 0$ quando $k < 0$ oppure $k > n$.
   Questa convenzione è in accordo col fatto che ***la formula di Stiefel vale sempre e solo per le disposizioni semplici****.*

4.8.10 Triangolo di Pascal-Tartaglia

La **formula di Stiefel** suggerisce un metodo ricorsivo, che permette di produrre una tabella. Per le sue caratteristiche questa tabella è nota come triangolo di Pascal-Tartaglia.
Per costruire la tabella:
La posizione $(0,0)$ *contiene per convenzione il valore 1. Tale convenzione è coerente con le precedenti.*

1. Per ogni riga $n \geq 1$ e colonna $k \geq 1$ la posizione (n,k) è data da $(n-1,k-1)+(n-1,k)$.

Ripetere il punto 1 per tutte le righe che si vogliono calcolare.

	$k=0$	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	Somma della riga	2^n
$n=0$	**1**	0	0	0	0	0	0	0	1	1
$n=1$	**1**	**1**	0	0	0	0	0	0	2	2
$n=2$	**1**	2	**1**	0	0	0	0	0	4	4
$n=3$	**1**	3	3	**1**	0	0	0	0	8	8
$n=4$	**1**	4	6	4	**1**	0	0	0	16	16
$n=5$	**1**	5	10	10	5	**1**	0	0	32	32
$n=6$	**1**	6	15	20	15	6	**1**	0	64	64
$n=7$	**1**	7	21	35	35	21	7	**1**	128	128
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Se applichiamo ***la convenzione*** *nel punto 3 nel paragrafo 4.8.9 per cui* $\binom{n}{k}=0$ *quando* $k<0$ *oppure* $k>n$*, allora tecnicamente compaiono gli* 0 *in grigio, anche se nella definizione standard, questi non esistono. Questo è utile per validare le somme al punto 1.*
La parte in violetto della tabella non fa parte del triangolo di tartaglia, ma serve come rappresentazione visiva di una proposizione che verrà enunciata in un secondo momento.

4.8.11 Formula del binomio di Newton

Per ogni numero intero $n \geq 1$ vale la formula:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + y^n$$

4.8.12 Proposizione: calcolo una somma di coefficienti binomiali con n costante

Per ogni numero intero $n \geq 0$ vale la formula:

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n$$

Vedere la parte in violetto nella tabella del triangolo di Tartaglia (4.8.10).

5 I numeri interi

5.1 Operazioni e divisibilità

5.1.1 Operazioni naturali in $\mathbb{Z}$

$\mathbb{Z}$ possiede:

1. **L'addizione**: $s : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tale che $s(a, b) = a + b$
2. **La moltiplicazione**: $m : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, tale che $m(a, b) = a \cdot b$

Entrambe *godono delle proprietà* **commutative** e **associative**.
Entrambe *possiedono* **l'elemento neutro** che vale:

1. 0 per **l'addizione**
2. 1 per **la moltiplicazione**.

Elementi **invertibili**:

1. *Tutti gli elementi di* $\mathbb{Z}$ sono invertibili per **l'addizione**.
2. *Solo gli elementi 1 e -1* sono invertibili per **la moltiplicazione**.

Vale anche la proprietà **distributiva**:

$$\forall a, x, y \in \mathbb{Z} \qquad a(x + y) = ax + ay$$

Questa proprietà rende "compatibili" somma e moltiplicazione.
Inoltre, **nell'addizione** il numero 1 ha la seguente proprietà: *tutti i suoi* ***multipli****, insieme ai loro* ***inversi****,* ***esauriscono*** $\mathbb{Z}$.
Infatti tutti i multipli di 1 esauriscono $\mathbb{N}$. *Siccome* $\mathbb{Z}$ *è composto da* $\mathbb{N}$ *e gli inversi di* $\mathbb{N}$*, i multipli di 1 e gli inversi dei multipli di 1 esauriscono* $\mathbb{Z}$.
Più avanti vedremo che il termine corretto per l'addizione è in realtà "opposto" anziché "inverso". Ho lasciato "inverso" per rendere chiaro il concetto rispetto alla definizione di "Elemento inverso" al punto 3.5.4.

5.1.2 Definizione di divisione

Siano a e b due numeri interi. Diciamo che a divide b (oppure che a è un **divisore** di b, oppure che b è **divisibile** per a), talvolta simbolicamente scritta come $a|b$, se esiste un numero intero k tale che $b = k \cdot a$.
La scrittura $a|b$ *può essere ambigua. Vedere "Simboli" (2.1.2).*
La definizione appena data può dare luogo a confusione.
Questo perché tendenzialmente noi scriviamo le divisioni come $b : a$*, ovvero con il divisore (che in questo caso è a) sempre a destra rispetto al dividendo (che in questo caso è b). Tuttavia l'intera definizione è formulata "all'inverso".*
Inoltre, questo fatto è da ricordare soprattutto se si usa una scrittura come $a|b$.
Valgono le seguenti, con $n \in \mathbb{Z}$*:*

1. *La divisione per 0* ***non è definita****, infatti:* $n : 0 = \nexists$.
   Mentre invece la divisione che ha 0 come dividendo è sempre definita e ha sempre lo stesso risultato: $0 : n = 0$.
2. I numeri invertibili *(nel caso della moltiplicazione: 1 e -1, quindi valgono anche qui)* dividono ogni n. Infatti:

   $$n : 1 = n, \quad -n : (-1) = n$$

   Questo è banalmente dimostrabile dal fatto che 1 e -1 sono divisibili soltanto per se stessi, quindi nessun altro numero ha la capacità di dividere ogni n.

5.1.3 Divisibilità della somma

Siano a e b numeri interi e sia $s = a + b$. Allora:

1. Un **divisore** di a e b è anche un **divisore** di s.
2. Un **divisore** di s e di uno degli *addendi* è un **divisore** anche dell'altro *addendo*.

5.1.4 (*Ir*)riducibilità di un intero e numeri primi

Sempre in riferimento alla moltiplicazione, gli *invertibili* sono 1 e -1.
Siano n, a, b numeri interi.
Sia $n \notin \{0, 1, -1\}$.

1. n è **irriducibile** se ogni qualvolta $n = a \cdot b$ allora a e/o b è *invertibile*
   Ad esempio: 7 è *irriducibile* perché in tutti i modi che ci sono per scrivere 7 come prodotto di a e b, almeno a o b è un *inverso*.

2. n è **riducibile** se *non è irriducibile*, ovvero, esistono modi di scrivere $n = a \cdot b$ dove né a né b sono *invertibili*.

3. n è **primo** se ogni qualvolta $ab : n$, n è anche un *divisore* di a oppure b.
   n è primo se ogni qualvolta che n si può scrivere come prodotto di a e b, n è divisore di a oppure b.

n viene imposto come diverso da 0, 1, -1 perché valutare queste condizioni per tali numeri produce contraddizioni logiche e va contro a convenzioni.
Nota: *Assicurati di leggere anche quanto detto nel "Teorema fondamentale dell'aritmetica" (5.3) per avere un quadro completo.*

5.1.5 MCD: *Massimo Comun Divisore*

Siano a e b due numeri interi non entrambi nulli. Si definisce **massimo comun divisore** di a e b il divisore comune più grande di a e b.

5.2 La divisione euclidea (Algoritmo di Euclide)

5.2.1 Teorema: Unicità del risultato della divisione

Siano a e b numeri interi con $b \neq 0$. Allora *esistono e sono unici* i numeri interi q e r con $0 \leq r < |b|$ tali che:

$$a = q \cdot b + r$$

Quando esegui $a : b$ ottieni un quoziente q ed un resto r ($a : b = q + r$). Nelle divisioni "senza resto" $r = 0$. La formula sopra indica che moltiplicando il divisore b con il quoziente q e sommando l'eventuale resto r si riottiene a.
La stessa divisione non produce più quozienti e/o resti, quindi è intuibile che q ed r sono unici ed esistono per una qualunque divisione in $\mathbb{Z}$.
ATTENZIONE!! *a questo fatto: $0 \leq r < |b|$*
NON *puoi mai avere un resto negativo!* Vedi il punto 5.2.4

5.2.2 Notazione posizionale

Sia $b \geq 2$ un numero intero *(detto **base**)* e sia $\mathcal{C}$ un insieme di b *simboli (detti **cifre**)* che rappresentano i numeri interi *da 0 a $b-1$ inclusi.*
Si dice *notazione posizionale* di un numero intero $N \geq 0$ *in base b*, la successione di cifre:

$$N = c_n ... c_2 c_1 c_0, \qquad \text{dove} \qquad N = c_0 b^0 + c_1 b + c_2 b^2 + ... + c_n b^n$$

La formula in magenta non è un prodotto.
Quando la base $b \leq 10$ si usano le cifre $\mathcal{C} = \{0, 1, 2, ..., 9\}$. Invece quando $b \geq 11$ le *10 cifre* non bastano più, quindi si usano le lettere.
Indicherò nella tabella seguente le lettere fino alla base 16, per rendere più immediate le operazioni di calcolo per la quasi totalità degli esercizi proposti:

Lettera	Valore
A	10
B	11
C	12
D	13
E	14
F	15
⋮	⋮

Al pedice destro di un elenco di cifre (numero), possiamo indicare la base racchiusa in parentesi quadre, per evitare ambiguità:
$11101_{[2]}$ rappresenta un numero in base 2 mentre le stesse cifre così indicate: $11101_{[10]}$ indicano lo stesso numero ma in base 10 (undicimilacentouno).

5.2.3 Da una base b alla base 10

È sufficiente osservare quanto detto al punto 5.2.2:

$$N = c_0 b^0 + c_1 b + c_2 b^2 + ... + c_n b^n$$

Facciamo 2 esempi:

1. Base $b < 10$: Per convertire $17627_{[8]}$ calcoliamo: $7 \cdot 8^0 + 2 \cdot 8^1 + 6 \cdot 8^2 + 7 \cdot 8^3 + 1 \cdot 8^4$
   Prima di continuare, per chiarezza non ho messo i pedici che indicavano le posizioni delle cifre, ma ho usato i colori.
   Importante notare come la posizione della cifra determini l'esponente della base.
   Continuando il calcolo... $7 \cdot 1 + 2 \cdot 8 + 6 \cdot 64 + 7 \cdot 512 + 1 \cdot 4096 = 7 + 16 + 384 + 3584 + 4096 = 8087_{[10]}$

2. Base $b > 10$: Per convertire $E1C45_{[16]}$, ricordiamo grazie alla tabella che $C = 12$ ed $E = 14$.
   Calcoliamo: $5_0 \cdot 16^0 + 4_1 \cdot 16^1 + 12_2 \cdot 16^2 + 1_3 \cdot 16^3 + 14_4 \cdot 16^4 = 5_0 \cdot 1 + 4_1 \cdot 16 + 12_2 \cdot 256 + 1_3 \cdot 4096 + 14_4 \cdot 65536 =$
   $= 5 + 64 + 3072 + 4096 + 917.504 = 924.741_{[10]}$

Per calcoli così lunghi (soprattutto il punto 2) è utile utilizzare una calcolatrice scientifica. Permette di avere il risultato inserendo solo il primo passaggio.

5.2.4 Divisioni intere con resto

Distinguiamo due casi:
Primo caso: la divisione ha divisore e dividendo **positivi**:
Vogliamo risolvere la prima divisione (143.779 : 2706) dell'esercizio sull'MCD (5.2.7):

1. *Eseguiamo la divisione, notando che la calcolatrice restituirà:* 53,1334....
2. ***Tronchiamo** i decimali (quindi **non approssimiamo** altrimenti sarebbe arrotondare)*
   Otteniamo quindi 53 che è il nostro quoziente q.
3. *Moltiplichiamo il nostro **quoziente** 53 per il divisore 2.706. Otteniamo* 143.418
4. *Al nostro dividendo* 143.779 *sottraiamo il numero ottenuto al punto 3.*
   Otteniamo quindi: $143.779 - 143.418 = 361$
   *361 è il nostro **resto** r.*

Secondo caso: il **dividendo** è **negativo**:
Per calcolare $-56.773 : 5.761$ procediamo in questo modo:

1. Prendiamo $|-56.773|$ e nella calcolatrice calcoliamo $56.773 : 5.761 = 9,854...$
2. ***Tronchiamo** i decimali* e aggiungiamo 1, quindi abbiamo $9 + 1 = 10$.
3. Moltiplichiamo 10 con 5.761 e otteniamo 57.610.
4. Sottraiamo al nostro dividendo 56.773 il numero appena ottenuto: $56.773 - 57.610 = -837$
5. Prendiamo $|-837|$ e otteniamo $+837$ che è il nostro **resto** (non puoi **mai** avere un resto negativo).
6. Prendiamo il numero che abbiamo ottenuto al punto 2 e lo moltiplichiamo per -1. Otteniamo quindi: $10 \cdot (-1) = -10$ che sarà il nostro **quoziente**.
   Infatti: $-56.773 = -10 \cdot 5.761 + 837$

Per tutti gli altri casi ricorda che:
Se dividendo e divisore sono negativi, il segno si semplifica e quindi si applica il primo caso.
Se solo il divisore è negativo, si può comunque applicare il primo caso poiché il prodotto al punto 3 del primo caso è tra due numeri negativi, quindi il risultato è positivo e pertanto, procedendo con i calcoli si rispetta il requisito che il resto sia sempre positivo.

5.2.5 Dalla base 10 alla base b

Anche qui si tratta di un calcolo abbastanza banale: ricorsione di divisioni con resto.
Facciamo 2 esempi:

1. Base $b < 10$: Per convertire $249.368_{[10]}$ in base $b = 5$:
   $249.368 = 49.873 \cdot 5 + 3_0$
   Prima di continuare, preciso che 49.873 *è il quoziente (risultato) della divisione* $249.368:5$ *e che* 3 *è il resto. Continuando:*
   $49.873 = 9.974 \cdot 5 + 3_1$
   $9.974 = 1.994 \cdot 5 + 4_2$
   $1.994 = 398 \cdot 5 + 4_3$
   $398 = 79 \cdot 5 + 3_4$
   $79 = 15 \cdot 5 + 4_5$
   $15 = 3 \cdot 5 + 0_6$
   $3 = 0 \cdot 5 + 3_7$
   Quando il quoziente è uguale a 0*, l'algoritmo termina.*
   Utilizzando i resti calcolati in rosso, possiamo comporre il nostro numero in base 5*.*
   $3_7 0_6 4_5 3_4 4_3 4_2 3_1 3_0 = 30434433_{[5]}$
   Abbiamo quindi: $249.368_{[10]} = 30434433_{[5]}$
   Volendo fare una verifica rapida: $3_0 \cdot 5^0 + 3_1 \cdot 5^1 + 4_2 \cdot 5^2 + 4_3 \cdot 5^3 + 3_4 \cdot 5^4 + 4_5 \cdot 5^5 + 0_6 \cdot 5^6 + 3_7 \cdot 5^7 =$
   $= 3 + 15 + 100 + 500 + 1875 + 12.500 + 0 + 234.375 = 249.368$
   Il risultato è quindi corretto.

2. Base $b > 10$: Per convertire $257.842_{[10]}$ in base $b = 14$:
   Usare il colore è estenuante quindi ne farò a meno. Abbiate pietà di me.
   La base $b = 14$ *ha 14 cifre, quindi le prime 10 saranno da 0 a 9 estremi inclusi, mentre le ultime 4 saranno le lettere dalla A alla D estremi inclusi.*
   Grazie alla tabella (5.2.2) ricordiamo che $A = 10$*,* $B = 11$*,* $C = 12$ *e* $D = 13$*. Calcoliamo:*
   $257.842 = 18.417 \cdot 14 + 4_0$
   $18.417 = 1315 \cdot 14 + 7_1$
   $1315 = 93 \cdot 14 + 13_2$
   $93 = 6 \cdot 14 + 9_3$
   $6 = 0 \cdot 14 + 6_4$
   Convertiamo il resto della posizione 2: $13_2 = D_2$
   Abbiamo quindi: $6_4 9_3 D_2 7_1 4_0 = 69D74_{[14]}$
   Il problema è risolto: $257.842_{[10]} = 69D74_{[14]}$

5.2.6 $\mathbf{MCD}(a, b) = \mathbf{MCD}(b, r)$

Siano a e b due numeri interi con $b \neq 0$ e tali che $a = q \cdot b + r$. Allora l'insieme dei *divisori comuni* di a e b coincide con l'insieme dei *divisori comuni* di b e r, ovvero:

$$\mathrm{MCD}(a, b) = \mathrm{MCD}(b, r)$$

5.2.7 Calcolo del MCD

L'algoritmo è molto simile a quello visto nel punto 5.2.5.
Facciamo un esempio:
$\mathrm{MCD}(143.779, 2.706) = ?$
$143.779 = 53 \cdot 2.706 + 361$
$2.706 = 7 \cdot 361 + 179$
$361 = 2 \cdot 179 + 3$
$179 = 59 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$
Quando il resto è 0 *l'algoritmo si ferma. Il resto prima dello* 0 *(che in questo caso è* 1*) è il risultato. Abbiamo quindi:*

$$\mathrm{MCD}(143.779, 2.706) = 1$$

5.2.8 Teorema: Identità di Bézout (Algoritmo di Euclide esteso)

Siano a e b due numeri interi e sia $d = \text{MCD}(a, b)$. Allora esistono numeri interi A e B tali che:

$$d = a \cdot A + b \cdot B$$

In realtà, l'identità di Bézout in generale *non è unica*: possono esistere più coppie possibili di A e B, che soddisfano la richiesta.
Tuttavia, l'algoritmo qui sotto, fornisce una coppia di valori di A e B ben specifica.
Calcolare l'identità di Bézout partendo dall'MCD calcolato con l'algoritmo di Euclide:
Prendiamo la coppia appena calcolata nel punto 5.2.7: $\text{MCD}(143.779, 2.706) = 1$

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= (361 - 2 \cdot 179) - 1 \cdot (179 - 59 \cdot 3) = \\
&= 361 - 2 \cdot 179 - 1 \cdot 179 + 59 \cdot 3 = \\
&= 361 - 3 \cdot 179 + 59 \cdot 3 = \\
&= 361 - 3 \cdot 179 + 59 \cdot (361 - 2 \cdot 179) = \\
&= 361 - 3 \cdot 179 + 59 \cdot 361 - 118 \cdot 179 = \\
&= 60 \cdot 361 - 121 \cdot 179 = \\
&= 60 \cdot (143.779 - 53 \cdot 2.706) - 121 \cdot 179 = \\
&= 60 \cdot 143.779 - 3.180 \cdot 2.706 - 121 \cdot 179 = \\
&= 60 \cdot 143.779 - 3.180 \cdot 2.706 - 121 \cdot (2.706 - 7 \cdot 361) = \\
&= 60 \cdot 143.779 - 3.180 \cdot 2.706 - 121 \cdot 2.706 + 847 \cdot 361 = \\
&= 60 \cdot 143.779 - 3.301 \cdot 2.706 + 847 \cdot 361 = \\
&= 60 \cdot 143.779 - 3.301 \cdot 2.706 + 847 \cdot (143.779 - 53 \cdot 2.706) = \\
&= 60 \cdot 143.779 - 3.301 \cdot 2.706 + 847 \cdot 143.779 - 44.891 \cdot 2.706 = \\
&= 907 \cdot 143.779 - 48.192 \cdot 2.706 = 1
\end{aligned}$$

Nella procedura, sostituiamo progressivamente i resti fino a quando non otteniamo soltanto le coppie originali (con i loro coefficienti).
All'inizio scriviamo infatti 3 come differenza tra 361 e 2·179. Scriviamo anche 2 come differenza.
Successivamente scriveremo 361 e 179 come differenze delle cifre originali.
Soprattutto per calcoli così grandi e complessi, è buona norma, tra un passaggio e l'altro verificare con la calcolatrice che quanto scritto rispetti sempre l'equivalenza: in questo caso, ogni riga deve equivalere a 1.
***Nota**: è possibile sostituire direttamente tutti i resti, ma verrebbe fuori, soprattutto in questo caso, un'equazione molto lunga, che porterebbe quindi a molti passaggi e pertanto a errori di calcolo/distrazione.*

5.3 Teorema fondamentale dell'aritmetica

5.3.1 Teorema dell'irriducibilità

Sia $n \notin \{0, 1, -1\}$ un numero intero. Allora n è **irriducibile** *se e soltanto se* n *è* **primo**.
Tutti i primi sono irriducibili e tutti gli irriducibili sono primi. (doppia implicazione)

5.3.2 Teorema fondamentale dell'aritmetica

Sia $n \notin \{0, 1, -1\}$ un numero intero. Allora *esiste un'unica* fattorizzazione *(scomposizione in fattori primi)*:

$$n = \pm p_1 \cdot p_2 \cdot ... \cdot p_i$$

dove i p_i sono *numeri primi positivi.*

5.3.3 Teorema: Esistono infiniti numeri primi.

5.4 Extra: mcm e tabella dei numeri primi

5.4.1 Extra: Calcolo del *minimo comun divisore*

Per questo è utile una tabella con i numeri primi. Vedi il punto 5.4.2
Supponiamo di dover calcolare $\text{mcm}(a, b, c, d, ...)$:

1. Scomponiamo in *fattori primi* i numeri $a, b, c, d, ...$
2. Annotiamo *una sola volta*, tutti i numeri primi che compaiono nelle scomposizioni dei numeri $a, b, c, d, ...$, scegliendo la versione con esponente maggiore.
3. Moltiplichiamo quindi tra loro, tutti i numeri primi, comuni e non comuni, presi una sola volta, con l'esponente maggiore.

Facciamo un esempio:
Calcolare: $\text{mcm}(2.530, 3.432, 6.460, 840)$
Scomponiamo in fattori primi:

2.530	2	3.432	2	6.460	2	840	2
1.265	5	1.716	2	3.230	2	420	2
253	11	858	2	1.615	5	210	2
23	23	429	3	323	17	105	3
1		143	11	19	19	35	5
		13	13	1		7	7
		1				1	

Abbiamo quindi:
$2.530 = 2 \cdot 5 \cdot 11 \cdot 23$
$3.432 = 2^3 \cdot 3 \cdot 11 \cdot 13$
$6.460 = 2^2 \cdot 5 \cdot 17 \cdot 19$
$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$
Ad esempio: 3 non compare in tutte le scomposizioni, ma lo prendiamo perché dobbiamo prenderli tutti, comuni e non comuni.
La versione con esponente maggiore è 3, quindi prendiamo, una volta sola 3 e con il 3 abbiamo finito.
Abbiamo quindi:

$$\text{mcm}(2.530, 3.432, 6.460, 840) = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 892.371.480$$

Infatti 892.371.480 è il numero più piccolo che 2.530, 3.432, 6.460 e 840 possono dividere.
Nota: questo è un esempio di un caso molto difficile, che coinvolge numeri enormi. Normalmente gli esercizi sono molto più semplici.

5.4.2 Tabella dei numeri primi da 1 a 1.000

2	41	97	157	227	283	367	439	509	599	661	751	829	919
3	43	101	163	229	293	373	443	521	601	673	757	839	929
5	47	103	167	233	307	379	449	523	607	677	761	853	937
7	53	107	173	239	311	383	457	541	613	683	769	857	941
11	59	109	179	241	313	389	461	547	617	691	773	859	947
13	61	113	181	251	317	397	463	557	619	701	787	863	953
17	67	127	191	257	331	401	467	563	631	709	797	877	967
19	71	131	193	263	337	409	479	569	641	719	809	881	971
23	73	137	197	269	347	419	487	571	643	727	811	883	977
29	79	139	199	271	349	421	491	577	647	733	821	887	983
31	83	149	211	277	353	431	499	587	653	739	823	907	991
37	89	151	223	281	359	433	503	593	659	743	827	911	997

6 Permutazioni

Non soddisfano la proprietà commutativa ($a_1 * a_2 \neq a_2 * a_1$)

6.1 Definizione e notazioni

6.1.1 Definizione di permutazione

Sia X un insieme non vuoto. Si dice permutazione di X una *funzione biettiva* (3.2.7):
$f : X \to X$
L'insieme di tutte le permutazioni di X si denota con $\mathcal{S}_X$
Per qualunque X la *funzione identità(3.2.7)* id_X è una *biezione*, quindi l'insieme $\mathcal{S}_X \neq \emptyset$ *(ogni insieme ha almeno una permutazione).*
L'insieme $\mathcal{S}_X$ è dotato di una operazione: *la composizione.* Inoltre:

1. L'operazione di composizione in $\mathcal{S}_X$ è *associativa. (Vedi il punto 3.3.2)*
2. La *funzione identità* id_X è *l'elemento neutro* per l'operazione di composizione.
   Se vuoi vedere un bell'esempio di questo guarda l'esercizio al punto 14.1.2
3. Ogni permutazione in $\mathcal{S}_X$ è *invertibile* in quanto *funzione biettiva* e la sua *inversa* è ancora un'altra permutazione, nell'insieme $\mathcal{S}_X$

Ricordo la proprietà associativa: $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$.
In generale l'operazione di composizione **non** è *commutativa*, tuttavia:

1. Se $X = \{a\}$ (X ha un solo elemento) allora *l'unica* permutazione di X è la *funzione identità* e quindi l'operazione in $\mathcal{S}_X$ **è commutativa.**
2. Se $X = \{a, b\}$ (X ha due elementi) allora $\mathcal{S}_X = \{\mathrm{id}_X, \pi\}$ dove π è la funzione tale che $\pi(a) = b$ e $\pi(b) = a$.
   Quindi:
   $\mathrm{id}_X \circ \mathrm{id}_X = \pi \circ \pi = \mathrm{id}_X \qquad$ e $\qquad \pi \circ \mathrm{id}_X = \mathrm{id}_X \circ \pi = \pi$
   Pertanto, abbiamo che anche in questo caso l'operazione di composizione è commutativa.

Ci occuperemo esclusivamente di permutazioni con insiemi X **finiti**.
Vedi anche il punto 7.1.7 se hai già letto tutto e stai ripassando.

6.1.2 Cardinalità dell'insieme delle permutazioni

Sia X un insieme finito con $|X| = n$. Allora esiste una biezione $f : \mathcal{S}_X \to \mathcal{S}_n$ tale che:
per ogni $\pi, \sigma \in \mathcal{S}_X$, si ha:

$$f(\sigma \circ \pi) = f(\sigma) \circ f(\pi)$$

In particolare,

$$|\mathcal{S}_X| = n!$$

Per trovare il numero di permutazioni in S_n calcoliamo $n!$

6.1.3 Notazione per rappresentare una permutazione (tabella)

Per rappresentare una permutazione, scriviamo sulla prima riga gli elementi del dominio, e nella seconda riga, gli elementi corrispondenti del codominio.
Nella prima riga scriviamo i valori "in ingresso" e nella seconda riga scriviamo quelli in "uscita", ovvero il risultato della permutazione (che è una funzione biettiva).

$$\begin{pmatrix} 1 & 2 & 3 & ... & n \\ \pi(1) & \pi(2) & \pi(3) & ... & \pi(n) \end{pmatrix}$$

Ad esempio:

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 6 & 1 & 5 & 7 & 4 \end{pmatrix} \tag{1}$$

Rappresenta la permutazione $\pi \in \mathcal{S}_7$ tale che $\pi(1) = 3, \pi(2) = 2, \pi(3) = 6, \pi(4) = 1, \pi(5) = 5, \pi(6) = 7, \pi(7) = 4$,
Attenzione*: le permutazioni sono funzioni biettive: sulla seconda riga, devono apparire tutti i numeri del dominio, una e una sola volta!*

6.1.4 Calcolo della permutazione inversa

Data una permutazione $\pi \in \mathcal{S}_n$ sappiamo che esiste la permutazione inversa $\pi^{-1} \in \mathcal{S}_n$.
Quindi se $\pi(a) = b$, allora $\pi^{-1}(b) = a$. La tabella di π^{-1} è così composta:

$$\pi^{-1} : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \pi^{-1}(1) & \pi^{-1}(2) & \pi^{-1}(3) & \pi^{-1}(4) & \pi^{-1}(5) \end{pmatrix}$$

Facciamo un esempio di come costruire questa tabella avendo già a disposizione la tabella di π.
Userò la tabella (1) nel paragrafo 6.1.3 come tabella di π:
Per costruire la tabella è sufficiente scambiare le righe di π:

$$\begin{pmatrix} 3 & 2 & 6 & 1 & 5 & 7 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

e riordinare gli elementi del dominio in ordine crescente per rispettare la convenzione. Abbiamo quindi:

$$\pi^{-1} : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 1 & 7 & 5 & 3 & 6 \end{pmatrix}$$

6.1.5 Calcolo della composizione di permutazioni

Date due permutazioni:

$$\pi : \begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix}, \sigma : \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n) \end{pmatrix}$$

Possiamo rappresentare $\sigma \circ \pi$ in una tabella con 3 righe:

$$\begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \\ \sigma(\pi(1)) & \sigma(\pi(2)) & ... & \sigma(\pi(n)) \end{pmatrix}$$

Per poi riscrivere la tabella finale omettendo la seconda riga:

$$\sigma \circ \pi : \begin{pmatrix} 1 & 2 & ... & n \\ \sigma(\pi(1)) & \sigma(\pi(2)) & ... & \sigma(\pi(n)) \end{pmatrix}$$

Questa procedura può essere estesa nel caso in cui si voglia calcolare una composizione con più di due permutazioni (basta aggiungere righe).

6.2 Cicli

6.2.1 Definizione di ciclo

L'obiettivo è quello di isolare un particolare sottoinsieme $C \subset \mathcal{S}_n$ di permutazioni, avente le seguenti proprietà:

1. Ogni permutazione in $\mathcal{S}_n$ si può ricostruire usando elementi di C
2. Il calcolo della composizione di elementi in C è *semplice*.

Definiamo quindi le permutazioni che compongono C:
Sia ℓ un intero, tale che $2 \leq \ell \leq n$, e siano $t_1, t_2, ..., t_\ell$ elementi *a due a due distinti* di I_n. Si dice ciclo di $\mathcal{S}_n$ la *permutazione* $\pi \in \mathcal{S}_n$ tale che:

$$\pi(k) = \begin{cases} t_{i+i} & se\ k = t_i\ e\ i = 1, ..., \ell - 1 \\ t_1 & se\ k = t_\ell \\ k & se\ k \notin \{t_1, ..., t_\ell\} \end{cases}$$

L'intero ℓ è detto **lunghezza** *del ciclo* e talvolta un ciclo di lunghezza ℓ è detto ℓ-**ciclo**.
Un ciclo di **lunghezza 2** è detto **trasposizione** o **scambio**.
Ad esempio:

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 8 & 3 & 6 & 4 & 2 & 9 \end{pmatrix}$$

è un ciclo con $\ell = 6$, perché $2 \mapsto 5 \mapsto 3 \mapsto 7 \mapsto 4 \mapsto 8 \mapsto 2$.
Nota: il 2 alla fine si omette.
Ma questo da solo non basta, tuttavia π soddisfa la richiesta perché per tutti gli elementi che non fanno parte del ciclo, *ovvero per gli elementi diversi da* $2, 5, 3, 7, 4, 8$ la funzione π restituisce il numero fornito. Infatti:

$$\pi(1) = 1, \pi(6) = 6, \pi(9) = 9$$

Per convenzione, denotiamo i cicli con:

$$(t_1\ \ t_2\ \ t_3\ \ ...\ \ t_\ell)$$

Quindi il ciclo $2 \mapsto 5 \mapsto 3 \mapsto 7 \mapsto 4 \mapsto 8 \mapsto 2$ andrebbe scritto così:

$$(2\ \ 5\ \ 3\ \ 7\ \ 4\ \ 8)$$

Visto che i cicli sono *circolari*, l'elemento t_1 da cui si *inizia* può essere scelto *arbitrariamente*. Infatti:

$$(2\ \ 5\ \ 3\ \ 7\ \ 4\ \ 8) = (5\ \ 3\ \ 7\ \ 4\ \ 8\ \ 2) = ...$$

Inverso di un ciclo
L'inverso di un ciclo di lunghezza ℓ è ancora un ciclo di lunghezza ℓ, tale che:

$$(t_1\ \ t_2\ \ t_3\ \ ...\ \ t_\ell)^{-1} = (t_\ell\ \ ...\ \ t_3\ \ t_2\ \ t_1)$$

Nota che l'inverso di uno *scambio/trasposizione* è lo scambio stesso, ovvero:
Sia s una trasposizione, allora: $s^{-1} = s$
Infatti: $s = (a\ \ b)$ e $s^{-1} = (b\ \ a)$, ma per quanto abbiamo visto prima $(b\ \ a) = (a\ \ b)$, quindi: $s^{-1} = s$

6.2.2 Cicli disgiunti

Due cicli $\sigma = (s_1 ... s_\ell)$ e $\tau = (t_1 ... t_{\ell'})$ si dicono *disgiunti* se:

$$\{s_1, ..., s_\ell\} \cap \{t_1, ..., t_\ell\} = \emptyset$$

Vedere la definizione di insiemi disgiunti e di intersezione al punto 2.4.1. Due cicli sono disgiunti se non hanno elementi in comune.

6.2.3 Commutazione di cicli disgiunti

Siano σ e τ cicli *disgiunti*. Allora σ e τ *commutano*, ovvero:

$$\tau \circ \sigma = \sigma \circ \tau$$

6.2.4 Teorema: unicità della composizione di cicli disgiunti

Ogni permutazione $\pi \neq \mathrm{id}_{\mathcal{S}_n}$ si può scrivere in modo essenzialmente *unico* come *composizione di cicli disgiunti. Con questo non si intende che le scritture di tali cicli sono uniche, ma siccome la composizione di cicli disgiunta è commutativa, l'ordine con cui questi vengono scritti è ininfluente.*

6.2.5 Convertire una permutazione da tabella a composizione di cicli disgiunti

Come esempio, consideriamo la permutazione $\pi \in \mathcal{S}_{13}$*:*

$$\pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 5 & 11 & 4 & 7 & 10 & 9 & 2 & 1 & 3 & 6 & 13 & 12 \end{pmatrix}$$

Iniziamo notando che $4 \mapsto 4$ *quindi soddisfa* $\pi(k) = k$ *pertanto lo escludiamo.*
Possiamo iniziare da un punto arbitrario che rispetti $\pi(k) \neq k$ *ma per seguire il libro iniziamo da 1. Abbiamo quindi:*
$1 \mapsto 8 \mapsto 2 \mapsto 5 \mapsto 7 \mapsto 9 \mapsto 1$
Anche qui, possiamo scegliere una nuova posizione arbitraria non presente nel ciclo appena descritto, purché valga $\pi(k) \neq k$ *ma, sempre per seguire il libro scegliamo 3. Abbiamo quindi:*
$3 \mapsto 11 \mapsto 6 \mapsto 10 \mapsto 3$
Concludiamo con:
$12 \mapsto 13 \mapsto 12$
Utilizzando la notazione scriviamo:

$$(1\ 8\ 2\ 5\ 7\ 9)(3\ 11\ 6\ 10)(12\ 13)$$

Il simbolo $\circ$ *tra i cicli disgiunti viene omesso per convenzione.*

6.2.6 Convertire una permutazione da composizione di cicli non disgiunti a composizione di cicli disgiunti

Come esempio, consideriamo la permutazione $\sigma \in \mathcal{S}_9$*:*
$\sigma = (1\ 5\ 8)(2\ 8\ 9\ 6)(9\ 7\ 4\ 1)(2\ 3)$
È importante ricordare che:

1. Capire chi soddisfa $\sigma(k) = k$ non è immediato in questo contesto.
2. I cicli non sono disgiunti, quindi *non commutano*, pertanto va rispettato *l'ordine di composizione*:
   $(1\ 5\ 8)(2\ 8\ 9\ 6)(9\ 7\ 4\ 1)(2\ 3) \neq (1\ 5\ 8)(2\ 8\ 9\ 6)(2\ 3)(9\ 7\ 4\ 1)$
   Inoltre, nella composizione, si va da destra a sinistra: *vedere nella sezione funzioni il punto 3.3.1* . Pertanto abbiamo:
$$\sigma = \underbrace{(1\ 5\ 8)}_{c_4}\underbrace{(2\ 8\ 9\ 6)}_{c_3}\underbrace{(9\ 7\ 4\ 1)}_{c_2}\underbrace{(2\ 3)}_{c_1}$$

Il metodo con cui mi trovo meglio riprende quanto detto nel "Calcolo della composizione di permutazioni" (6.1.5): Costruirò una tabella così composta:

$$\sigma : \begin{pmatrix} 1 & 2 & ... & 9 \\ c_1(1) & c_1(2) & ... & c_1(9) \\ c_2(c_1(1)) & c_2(c_1(2)) & ... & c_2(c_1(9)) \\ c_3(c_2(c_1(1))) & c_3(c_2(c_1(2))) & ... & c_3(c_2(c_1(9))) \\ c_4(c_3(c_2(c_1(1)))) & c_4(c_3(c_2(c_1(2)))) & ... & c_4(c_3(c_2(c_1(9)))) \end{pmatrix}$$

Consideriamo $c_1 : (2\ 3)$*. Tutti i numeri che non compaiono soddisferanno* $c_1(k) = k$*. Scriviamo quindi:*

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 9 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \end{pmatrix}$$

Continuiamo applicando lo stesso criterio per tutti gli altri cicli. Ricordiamo che "l'input" (k) per c_3 *saranno i valori sulla riga* c_2 *(seconda riga) e così via...:*

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \\ 6 & 3 & 8 & 1 & 5 & 2 & 4 & 9 & 7 \\ 6 & 3 & 1 & 5 & 8 & 2 & 4 & 9 & 7 \end{pmatrix}$$

Come illustrato in "Calcolo della composizione di permutazioni" (6.1.5), omettiamo le righe tra la prima e l'ultima. Abbiamo quindi a tutti gli effetti la tabella di σ*!: (il ! non è il fattoriale ma sono io che sono felice)*

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 1 & 5 & 8 & 2 & 4 & 9 & 7 \end{pmatrix}$$

Possiamo quindi usare quanto visto nel punto 6.2.5 per scrivere questa tabella come composizione di cicli disgiunti:
Partiamo da 1: $1 \mapsto 6 \mapsto 2 \mapsto 3 \mapsto 1$
Scegliamo 4: $4 \mapsto 5 \mapsto 8 \mapsto 9 \mapsto 7 \mapsto 4$
Scriviamo i cicli trovati con la corretta notazione:

$$(1\ 6\ 2\ 3)(4\ 5\ 8\ 9\ 7)$$

Abbiamo finito!
Nota: esistono metodi più efficienti, ma io mi distraggo molto e sbaglio tantissimo, quindi mi trovo bene con questo.

6.2.7 Definizione di tipo

Sia $\pi \in \mathcal{S}_n$ una permutazione, tale che $\pi \neq \mathrm{id}_{\mathcal{S}_n}$ e sia
$\pi = c_1 \circ c_2 \circ ... \circ c_r$
la sua scrittura in **cicli disgiunti**, con $c_1, c_2, ..., c_r$ di *lunghezza* $\ell_1 \geq \ell_2 \geq ... \geq \ell_r$ rispettivamente.
Si dice **tipo** di π la r-pla di numeri interi:

$$(\ell_1, \ell_2, ..., \ell_r)$$

Facciamo alcune osservazioni:

1. Per ordinare in ordine decrescente gli elementi nel *tipo*, è sufficiente scambiare di posto i cicli, cosa ammessa visto che si tratta di cicli disgiunti.

2. In un *tipo* le lunghezze possono essere ripetute. Ad esempio:
   $\pi = (1\ \ 4\ \ 6)(2\ \ 10\ \ 9)(5\ \ 7)(7\ \ 8) \in \mathcal{S}_{10}$
   ha *tipo* $(3, 3, 2, 2)$

3. Poiché si tratta di cicli disgiunti, la quantità di elementi coinvolti non può essere maggiore di n. Quindi se $\pi \in \mathcal{S}_n$ ha *tipo* $(\ell_1, \ell_2, ..., \ell_r)$ deve risultare:
   $\ell_1 + \ell_2 + ... + \ell_r \leq n$

4. Viceversa, assegnata una r-pla di numeri interi, è sempre possibile trovare una permutazione $\pi \in \mathcal{S}_n$ che ha come tipo la r-pla assegnata.

5. Se π è composta da un singolo ciclo di lunghezza ℓ, allora il suo tipo è semplicemente ℓ.

È importante ricordare che il tipo è definito solo per le scritture a cicli disgiunti.

6.2.8 Numero di cicli di lunghezza ℓ

Il numero di cicli di lunghezza ℓ in $\mathcal{S}_n$ è:

$$\frac{1}{\ell} D_{n,\ell} = \frac{1}{\ell} \cdot \frac{n!}{(n-\ell)!}$$

6.2.9 Numero di permutazioni possibili con un determinato tipo

Dato un tipo, vogliamo sapere quante permutazioni in $\mathcal{S}_n$ hanno quel tipo.
Consideriamo un tipo $(\ell_1, \ell_2, ..., \ell_r)$.
Dobbiamo innanzitutto controllare che la somma delle lunghezze del tipo $\ell_1 + \ell_2 + ... + \ell_r$ sia uguale ad n.
Se invece è minore di n, allora aggiungiamo al tipo dei cicli di lunghezza 1 finché la somma delle lunghezze non raggiunge n.
Riscriviamo il tipo, come prodotto delle singole lunghezze. In questo modo, gli elementi ripetuti possono essere scritti in forma esponenziale. Otteniamo una notazione del tipo:
$(\ell_1^{\alpha_1} \cdot \ell_2^{\alpha_2} \cdot ... \cdot \ell_r^{\alpha_r})$
A questo punto, per conoscere il numero di permutazioni possiamo usare la formula:

$$\frac{n!}{\ell_1^{\alpha_1} \cdot \ell_2^{\alpha_2} \cdot ... \cdot \ell_r^{\alpha_r} \cdot \alpha_1! \cdot \alpha_2! \cdot ... \cdot \alpha_n!}$$

6.2.10 Numero di tipi in $\mathcal{S}_n$

Vogliamo capire quanti tipi $(\ell_1, \ell_2, ..., \ell_r)$ esistono in $\mathcal{S}_n$.
Si ottiene quindi una *partizione* di n: $p(n)$, ovvero, tutte le possibili scritture di n come somma di interi positivi.
I primi valori di $p(n)$ sono:

n	$p(n)$ *(numero di partizioni)*	partizioni *(separate da =)*
1	1	1
2	2	2=1 + 1
3	3	3=2 + 1=1 + 1 + 1
4	5	4=3 + 1=2 + 2=2 + 1 + 1=1 + 1 + 1 + 1
5	7	5=4 + 1=3 + 2=3 + 1 + 1=2 + 2 + 1=2 + 1 + 1 + 1=1 + 1 + 1 + 1 + 1

I colori non indicano eventuali relazioni tra numeri ma servono solo per distinguere bene una partizione dall'altra.
Siccome non ho abbastanza colori, ho usato anche il nero e le scale di grigi.

6.3 Scambi e parità

6.3.1 Scrivere cicli come composizione di scambi.

Ogni ciclo di lunghezza ℓ è scrivibile come *composizione* di $\ell - 1$ *scambi*. Pertanto, vale l'identità:

$$(m_1 \ m_2 \ ...m_\ell) = (m_1 \ m_\ell)(m_1 \ m_{\ell-1})...(m_1 \ m_3)(m_1 \ m_2)$$

Tale scrittura **non** è *unica* e **non** è *commutativa, perché in generale una composizione di scambi (come appena visto) non è disgiunta.*
Pertanto, otteniamo il teorema 6.3.2:

6.3.2 Teorema: Ogni *permutazione* è una composizione di scambi

Questo significa che tutte le composizioni di tutti gli scambi in $\mathcal{S}_n$ generano tutte le permutazioni di $\mathcal{S}_n$.

6.3.3 Teorema: Parità di composizioni di scambi

Due composizioni di scambi (*che indichiamo con s)*, composte da p e q scambi, hanno *la stessa parità* se p e q sono entrambi *pari*, oppure se sono entrambi *dispari*. Ovvero:
Se $[(p:2) \in \mathbb{Z} \wedge (q:2) \in \mathbb{Z}] \vee [(p:2) \notin \mathbb{Z} \wedge (q:2) \notin \mathbb{Z}]$, allora le due composizioni hanno stessa parità.
Essenzialmente, due composizioni di scambi hanno stessa parità se sono entrambe composte da un numero pari, oppure da un numero dispari di scambi. Il punto 6.3.4 chiarisce ed integra quanto appena detto.

6.3.4 Determinare la parità di una permutazione con gli scambi

Sia $\pi \in \mathcal{S}_n$. Diremo che la permutazione π è:

1. **Pari**: se π si scrive come composizione di un numero *pari* di scambi
2. **Dispari**: se π si scrive come composizione di un numero *dispari* di scambi

Questo implica che nonostante le scritture di una permutazione come composizione di scambi non siano uniche, tutte le scritture di una medesima permutazione condividono la stessa parità.
Tuttavia, nonostante possa essere controintuitivo, è importante ricordare che siccome non tutte le scritture di composizione di scambi sono "essenziali" e pertanto tutte le possibili scritture di una permutazione non condividono lo stesso numero di scambi.

6.3.5 Parità di un ciclo

Sia c un ciclo di lunghezza ℓ. Allora:

1. c è **pari** se ℓ è *dispari*
2. c è **dispari** se ℓ è *pari*

6.3.6 Parità di una composizione

Siano $\pi, \sigma \in \mathcal{S}_n$. Allora la composizione $\sigma \circ \pi$ è:

1. **Pari**: se π e σ hanno *stessa parità.*
2. **Dispari**: se π e σ hanno *diversa parità.*

ATTENZIONE: Non la puoi concatenare!! Per calcolare la parità di composizioni con un numero arbitrario di permutazioni, vai al punto 6.3.7

6.3.7 Determinare la parità di una permutazione con il tipo

Data una permutazione $\pi \in \mathcal{S}_n$ con tipo $(\ell_1, \ell_2, ..., \ell_r)$, definiamo un numero P tale che:

$$P = (\ell_1 - 1) + (\ell_2 - 1) + ... + (\ell_r - 1) = \ell_1 + \ell_2 + ... + \ell_r - r$$

Allora, la permutazione π è *pari se e soltanto se* P è *pari.*

6.3.8 Numero di permutazioni pari e dispari

In $\mathcal{S}_n$ ci sono $\frac{1}{2} \cdot n!$ permutazioni *pari* e $\frac{1}{2} \cdot n!$ permutazioni *dispari.*

6.4 Periodi

6.4.1 Potenze di cicli

Vogliamo studiare le potenze di cicli, ovvero:
$\pi^0 = \mathrm{id}, \pi^1 = \pi, \pi^2 = \pi \circ \pi, \pi^3 = \pi \circ \pi \circ \pi, ...$
Iniziamo dicendo che:
Se un ciclo di lunghezza $\ell \geq 2$, allora:

$$\pi^\ell = \mathrm{id}$$

Pertanto:

$$\pi^k \neq \mathrm{id}$$

con $k = 1, ..., \ell - 1$
In generale, le potenze di un singolo ciclo, non sono a loro volta singoli cicli. Ad esempio:

$$\pi = (1\ \ 2\ \ 3\ \ 4) \in \mathcal{S}_4$$

$$\pi^2 = (1\ \ 3)(2\ \ 4)$$

6.4.2 Potenze ennesime di cicli

Siccome il totale delle permutazioni in $\mathcal{S}_n$ è finito, nella successione $\pi^0 = \mathrm{id}, \pi^1 = \pi, \pi^2, \pi^3, ...$ devono esserci ripetizioni.
Pertanto esistono due numeri interi $0 \leq r < s$ tali che:

$$\pi^r = \pi^s$$

Componendo entrambi i membri di questa uguaglianza con $(\pi^r)^{-1} = \pi^{-r}$ e usando le regole delle potenze otteniamo:

$$\mathrm{id} = \pi^r \circ \pi^{-r} = \pi^s \circ \pi^{-r} = \pi^{s-r}$$

Siccome $0 < s - r < s$, la prima potenza che si ripete è proprio $\pi^0 = \mathrm{id}$.

6.4.3 Definizione di periodo

Data una permutazione $\pi \in \mathcal{S}_n$ si dice periodo di π, denotato $\mathrm{per}(\pi)$, il più piccolo intero positivo k nell'insieme $\{k \in \mathbb{Z} | \pi^k = \mathrm{id}\}$.
Valgono le seguenti:

1. Il periodo di una permutazione *esiste sempre*
2. Il periodo di un ciclo è uguale alla sua lunghezza ℓ *(Punto 6.4.1)*
3. Sia $p = \mathrm{per}(\pi)$. Per ogni $m \in \mathbb{Z}$ usiamo la divisione euclidea *(5.2)* per scrivere $m = q \cdot p + r$ (con $0 \leq r < p$).
   Per la regola delle potenze:
   $\pi^m = \pi^{q \cdot p + r} = (\pi^p)^q \circ \pi^r = (\mathrm{id})^q \circ \pi^r$
   Ricorda che $(\mathrm{id})^q = \mathrm{id}, \forall q \geq 1$ *(proprietà* ***idempotente****)*
   Quindi, l'insieme delle potenze di una permutazione è:
   $\{\mathrm{id}, \pi, \pi^2, ..., \pi^{p-1}\}$
   Per calcolare m calcoliamo $m : q$. Questo ci dà il nostro quoziente q insieme al nostro resto r.

6.4.4 Ottenere il periodo di una composizione con il tipo

Sia $\pi \in \mathcal{S}_n$ una permutazione di tipo $(\ell_1, \ell_2, ..., \ell_r)$. Allora il periodo della permutazione è il *minimo comune multiplo (Vedi punto 5.4.1)* delle lunghezze nel tipo:

$$p = \mathrm{per}(\pi) = \mathrm{mcm}(\ell_1, \ell_2, ..., \ell_r)$$

7 Gruppi

7.1 Definizioni

7.1.1 Definizione di semigruppo, monoide e gruppo

Sia $(A, *)$ una *coppia* formata da un insieme A non vuoto e un'operazione binaria $*$ su A. Diremo:

1. Che $(A, *)$ è un *semigruppo* se $*$ è *associativa*
2. Che $(A, *)$ è un *monoide* se $*$ è *associativa* e se esiste un *elemento neutro* $e \in A$ per $*$
3. Che $(A, *)$ è un *gruppo* se $*$ è *associativa*, se esiste un elemento neutro $e \in A$ per $*$ e se ogni elemento $a \in A$ è *invertibile*

Vedi: Proprietà associativa (Punto 3.5.2), elemento neutro (Punto 3.5.3) e l'elemento inverso (Punto 3.5.4).
Ricordo la proprietà associativa: $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$.
Nota: vista la natura delle richieste, un *gruppo* è anche un *monoide* e un *semigruppo*.
Inoltre, un *monoide* è anche un *semigruppo*.
Nel caso in cui valga anche la *proprietà commutativa* per $*$, allora aggiungiamo l'aggettivo ***commutativo*** o ***abeliano*** ai termini *semigruppo, monoide* e *gruppo*, appena definiti.

7.1.2 Ordine (cardinalità) di $(A, *)$

Sia $(G, *)$ un *gruppo (o monoide, o semigruppo)*. Chiamiamo ordine di $(G, *)$ la cardinalità di $|G|$.
Il *gruppo/monoide/semigruppo* $(G, *)$ si dirà *finito* oppure *infinito* se G è *finito* oppure *infinito* rispettivamente.

7.1.3 Gruppi e monoidi negli insiemi $\mathbb{Z}$, $\mathbb{Q}$ ed $\mathbb{R}$

Addizione $+$:
Con l'operazione di *addizione* $+$, soddisfiamo la richiesta di *gruppo*, pertanto:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +) \text{ sono } \textit{gruppi commutativi.}$$

Moltiplicazione $\cdot$:
Siccome $\cdot$ è *associativa, commutativa* e ha 1 come *elemento neutro*:

$$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot) \text{ sono } \textbf{\textit{monoidi}} \textit{ commutativi.}$$

Per quanto riguarda $\mathbb{Q}$ ed $\mathbb{R}$, se *escludiamo* lo 0, allora diventano **gruppi** *commutativi*.
Mettendo come *esponente* alla lettera di un insieme il simbolo $\times$, stiamo dicendo che consideriamo l'insieme moltiplicativo. Quindi:

$$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}, \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}, \text{ ecc.ecc....}$$

Questa notazione viene usata nel corso di algebra lineare e rimanda al concetto di differenza tra insiemi (Vedi il punto 2.4.4*)*
Quindi, tornando a noi:
$(\mathbb{Q}^\times, \cdot), (\mathbb{R}^\times, \cdot)$ sono *gruppi commutativi.*
Precisamente, vengono chiamati il *gruppo moltiplicativo dei razionali* $(\mathbb{Q})$ e il *gruppo moltiplicativo dei reali* $(\mathbb{R})$.
$(\mathbb{Z}, \cdot)$ anche se escludessimo lo 0, non è un *gruppo* perché, *come visto nel punto* 5.1.1, ha come invertibili soltanto 1 e -1.
Nota: Se creassimo un sottoinsieme di $\mathbb{Z}$ con solo 1 e -1, allora questo sottoinsieme sarebbe un gruppo commutativo.
In simboli $\mathbb{Z}^\times = \{1, -1\}$

7.1.4 Notazione convenzionale

Per un *gruppo, monoide o semigruppo,* dove non è ambiguo, anziché usare $(G, *)$ usiamo direttamente G, sottintendendo l'operazione $*$, quindi diremo anche cose come, *"il gruppo G", "sia G un gruppo"*, ecc.ecc...
Questo perché nella maggior parte degli casi, esiste una sola operazione che rende G un gruppo.
Viene comunque riservata per enfasi o in caso di ambiguità, la notazione completa $(G, *)$.
Inoltre:

1. *Come visto in precedenza*, si adotta per un gruppo G una terminologia "*moltiplicativa*", quindi scriviamo gh anziché $g * h$, usiamo g^n per le *potenze* e g^{-1} per *l'inverso* di g.
2. Se invece il gruppo G è *commutativo*, si usa una terminologia "*additiva*", quindi scriviamo $g + h$ per l'operazione di "somma" tra g e h, e parliamo di *multipli* $n \cdot g$, anziché di *potenze* di g. Inoltre, parleremo di *opposto* $-g$ anziché di *inverso* di g.

Al punto 2 fanno eccezione i casi visti al punto 7.1.3 dove nonostante $\mathbb{Q}^\times$ ed $\mathbb{R}^\times$ siano *gruppi commutativi*, continueremo ad usare la notazione moltiplicativa (come nel punto 1).
Questo vale anche per il sottoinsieme di $\mathbb{Z}$ composto esclusivamente da $\{1, -1\}$, poiché anche lui è un *gruppo commutativo* rispetto alla *moltiplicazione*.

7.1.5 Neutro, inverso e legge di cancellazione per un gruppo

Sia $(G, *)$ un gruppo. Valgono i fatti seguenti:

1. *G ammette un unico* elemento **neutro** e
   Nel caso si abbia a che fare con più gruppi contemporaneamente, l'elemento neutro di G può essere denotato come e_G.
2. Ogni elemento $g \in G$ ammette *un unico* **inverso** g^{-1}
3. Per ogni $g, h \in G$ si ha $(g * h)^{-1} = h^{-1} * g^{-1}$
4. **Legge di cancellazione**: Se per $g, g', h \in G$ vale l'uguaglianza:
   $g * h = g' * h$ (oppure $h * g = h * g'$)
   Allora: $g = g'$

7.1.6 Gruppo prodotto

Siano $(G_1, *)$ e $(G_2, \star)$ due gruppi. Nell'insieme *prodotto cartesiano* $G_1 \times G_2$ consideriamo l'operazione $\bullet$ definita come segue:
$(g_1, g_2) \bullet (g_1', g_2') = (g_1 * g_1', g_2 \star g_2')$
L'operazione $\bullet$ avviene "*componente per componente*", nel senso che su ciascuna componente della coppia si opera con l'operazione corrispondente.
In altre parole, l'operazione $\bullet$ esegue sugli elementi forniti appartenenti a G_1 (g_1, g_1'), l'operazione del gruppo G_1 $(*)$, e sugli elementi forniti appartenenti al gruppo G_2 (g_2, g_2'), esegue l'operazione del gruppo G_2 $(\star)$.
Dopodiché restituisce una coppia, che ha come elementi il risultato delle operazioni $*$ e $\star$, dei gruppi G_1 e G_2 rispettivamente.
L'insieme $(G_1 \times G_2)$ è un *gruppo (rispetto all'operazione $\bullet$: $(G_1 \times G_2, \bullet)$ è un gruppo)* perché:

1. L'operazione $\bullet$ è *associativa per ipotesi.*
   Con questo si intende che $*$ e $\star$ sono associative, e siccome $\bullet$ opera "componente per componente" (non fa rimescolamenti strani), $\bullet$ "preserva" la proprietà associativa di $*$ e $\star$.
2. Per gli elementi neutri e_{G_1}, e_{G_2} la coppia $(e_{G_1}, e_{G_2}) \in G_1 \times G_2$ è un *elemento neutro* per $\bullet$.
3. La coppia (g_1, g_2) ha *inverso* (g_1^{-1}, g_2^{-1})

In modo analogo si possono costruire *gruppi prodotto* di tre o più gruppi.
Nel caso in cui il *gruppo prodotto* sia definito per due o più gruppi che sono lo stesso gruppo, allora si usa lo stesso simbolo per le per l'operazione nelle componenti e tra le coppie. Ad esempio usiamo il simbolo $+$ e parliamo di "somma" in:

$$\mathbb{Z} \times \mathbb{Z}, \mathbb{R} \times \mathbb{R}, \mathbb{R} \times \mathbb{R} \times \mathbb{R}, \ldots$$

I gruppi $\mathbb{R} \times \mathbb{R}$ e $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ non sono altro che il gruppo dei vettori nel piano $(\mathbb{R}^2)$ e nello spazio $(\mathbb{R}^3)$ rispettivamente. L'operazione "somma" $(+)$ è di fatto la somma vettoriale (vedi algebra lineare).
Ad esempio, se abbiamo due vettori (coppie) $(3, 4), (2, 6) \in \mathbb{R}$, allora $(3, 4) \times (2, 6) = (5, 10)$

7.1.7 Insieme delle permutazioni

Per ogni n l'insieme delle permutazioni $\mathcal{S}_n$ con l'operazione di composizione $\circ$ è sempre un gruppo *finito*.
Inoltre, $(\mathcal{S}_n, \circ)$ è:

- **Commutativo (*abeliano*)**: quando $n = 1$, oppure quando $n = 2$
- ***non* commutativo**: per tutti gli altri n, ovvero quando $n \geq 3$

7.2 Sottogruppi

7.2.1 Definizione di sottogruppo

Sia $(G, *)$ un gruppo. Un sottogruppo H di G è un *sottoinsieme* di G tale che $(H, *)$ è anch'esso un gruppo.
Per indicare che H è un sottogruppo di G scriviamo:
$H < G$
Da non confondere (concettualmente) con una cosa come: $|H| < |G|$.
Per verificare che un *sottoinsieme* $H \subset G$ sia un sottogruppo, vai al punto 7.2.2. Dal punto di vista teorico, occorre verificare che:

1. H sia chiuso rispetto a $*$: per ogni $h, h' \in H$ si ha $h * h' \in H$
2. H contiene *l'elemento neutro* per l'operazione $*$
3. H contiene *l'inverso* di ogni suo elemento: se $h \in H$, allora $h^{-1} \in H$

Non è necessario verificare che l'operazione $*$ sia associativa, perché siccome G è già un gruppo con l'operazione $*$, tale richiesta è già soddisfatta.
Se invece vogliamo verificare che un insieme sia un gruppo (e non un sottogruppo), allora tale verifica è opportuna.
Tornando ai *sottogruppi*, consideriamo un caso particolare e un esempio:

1. **Caso particolare**: Per *qualunque* gruppo G esistono sempre:

   1.1 il sottoinsieme $S = G$, ovvero il *sottoinsieme* S che comprende tutto G.

   1.2 il sottoinsieme $\{e\}$, che contiene solo *l'elemento neutro*

   Questi *sottoinsiemi* sono entrambi *sottogruppi* e vengono detti **sottogruppi banali**.

2. **Esempio**: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono tutti *gruppi* rispetto all'operazione di somma.
   Per la teoria degli insiemi: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$
   Quindi in realtà, $\mathbb{Q}$ è un *sottogruppo* di $\mathbb{R}$. Pertanto, $\mathbb{Z}$ è un *sottogruppo* di $\mathbb{Q}$ e di $\mathbb{R}$.

7.2.2 Verifica di un sottogruppo

Sia $(G, *)$ un gruppo e sia $H \subset G$ un suo sottoinsieme *non vuoto*. Allora H è un *sottogruppo* di G se e solo se:

$$\text{per ogni } h_1, h_2 \in H \text{ si ha che } h_1 * h_2^{-1} \in H$$

Attenzione: Non dobbiamo solo verificare che per ogni elemento di H esista il suo inverso, ma dobbiamo anche verificare che l'elemento neutro, ovvero il risultato di $h_1 * h_2^{-1}$ sia effettivamente dentro H.
*Inoltre, verifichiamo **sempre** che l'operazione $*$ sia chiusa rispetto ad H.* Ovvero, se calcoliamo $*$ con degli elementi qualunque in H il risultato deve ***sempre*** rimanere in H.

7.2.3 Teorema: Sottogruppi di $(\mathbb{Z}, +)$

I sottogruppi di $(\mathbb{Z}, +)$ sono tutti e soli quelli della forma $n\mathbb{Z}$ con $n \in \mathbb{N}$.
Questo significa che i sottogruppi di $(\mathbb{Z}, +)$ sono solo i multipli di n in $\mathbb{Z}$.
*Per $n = 0$ e $n = 1$ si riottengono i **sottogruppi banali**: $0\mathbb{Z} = \{0\}$ e $1\mathbb{Z} = \mathbb{Z}$*
Vale anche la seguente: $n\mathbb{Z} = (-n)\mathbb{Z}$

7.2.4 Intersezione tra sottogruppi

Sia G un gruppo e siano H_1, H_2 sottogruppi di G, allora anche $H_1 \cap H_2$ *è un sottogruppo* di G.

7.2.5 Unione tra sottogruppi

In generale, l'unione tra sottogruppi **non** è un *sottogruppo*.

7.3 Teorema di Lagrange

7.3.1 Definizione di laterale destro e laterale sinistro

Sia G un gruppo e sia H un suo *sottogruppo*. Dato un elemento $g \in G$ si dice:

1. **Laterale sinistro** di H definito da g il *sottoinsieme:*
   $gH = \{gh | h \in H\} \subset G$
   Ovvero: $g * H = \{g * h | h \in H\} \subset G$. Se il gruppo fosse stato commutativo, allora avrei scritto $+$ al posto di $*$

2. **Laterale destro** di H definito da g il sottoinsieme:
   $Hg = \{hg | h \in H\} \subset G$
   Per la notazione vale sempre quanto detto prima. Vedere inoltre il punto 7.1.4

In entrambi i casi, g è detto ***rappresentante*** *del laterale.*
Inoltre:

1. Il *sottogruppo* H stesso è un *laterale, sia destro che sinistro, di se stesso. Quindi, preso un qualunque $h \in H$, allora:*
   $$H = hH = Hh$$
   Un esempio conveniente è quello dell'elemento neutro e, in quanto presente sia in H che in G:
   $$H = eH = He$$

2. Se G è un *gruppo commutativo,* abbiamo:
   $gh = hg$, per qualunque $h \in H$ e $g \in G$. Pertanto:
   $gH = Hg$, quindi i *laterali* sinistri e destri *coincidono*

3. Come visto prima, nel caso si utilizzi la notazione *additiva* per G si scrive

   3.1 $g + H$ per il *laterale* **destro**

   3.2 $H + g$ per il *laterale* **sinistro**

Nel caso di $G = \mathbb{Z}$ ad esempio, si usa la notazione *additiva*, infatti $n\mathbb{Z}$ denota un *sottogruppo* e **non** un *laterale.*
Un laterale del *sottogruppo* $n\mathbb{Z}$ ha questa forma:
$n\mathbb{Z} + r = \{nk + r | k \in \mathbb{Z}\}$

7.3.2 Proprietà dei laterali sinistri

Sia G un gruppo e H un suo sottogruppo. Valgono le seguenti proprietà per i laterali *sinistri* di H:

1. Per ogni $g \in G$ esiste una *biezione* $H \to gH$
2. Si ha $g_1 H = g_2 H$ *se e solo se* $g_1^{-1} g_2 \in H$
3. I laterali *sinistri* formano una *partizione* di G

7.3.3 Proprietà dei laterali destri

Sia G un gruppo e H un suo sottogruppo. Valgono le seguenti proprietà per i laterali destri di H:

1. Per ogni $g \in G$ esiste una *biezione* $H \to Hg$
2. Si ha $Hg_1 = Hg_2$ *se e solo se* $g_2 g_1^{-1} \in H$
3. I laterali *destri* formano una *partizione* di G

7.3.4 Teorema di Lagrange

Sia G un gruppo ***finito*** di ordine n e sia H un *sottogruppo* di G di *ordine* d. Allora d *divide* n.
Questo dice semplicemente che se in gruppo finito G di ordine n esiste un sottogruppo H con un ordine d, allora d deve essere un divisore di n. Questo però non implica che per tutti i divisori di n esistano altrettanti sottogruppi. Significa semplicemente che non esistono sottogruppi con un ordine che non divide n. ***Condizione necessaria ma non sufficiente****.*

7.4 Omomorfismi

7.4.1 Definizione di omomorfismo

Un omomorfismo è una funzione che ha due gruppi come dominio e codomino.
Siano $(G, *)$ e $(H, \star)$ due gruppi. Un omomorfismo da G ad H è una funzione $\phi : G \to H$ tale che:

$$\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2), \qquad \forall g_1, g_2 \in G$$

Provo a raccontarla con altre parole:
Fai finta di avere un numero g_k che hai ottenuto calcolando $g_1 * g_2$. Quindi:

$$g_k = g_1 * g_2$$

$\phi(g_k)$ ti restituisce *lo stesso valore* che otterresti prendendo $h_1 = \phi(g_1)$ e $h_2 = \phi(g_2)$ ed eseguendo su di loro l'operazione appartenente al loro gruppo: $h_1 \star h_2$.
Quindi abbiamo:
$\phi(g_k) = h_1 \star h_2$

7.4.2 Proprietà degli omomorfismi

Sia $\phi : (G, *) \to (H, \star)$ un omomorfismo di gruppi. Valgono i fatti seguenti:

1. $\phi(e_G) = e_H$
2. *Per ogni* $g \in G$, abbiamo: $\phi(g^{-1}) = \phi(g)^{-1}$, in notazione additiva: $\phi(-g) = -\phi(g)$
   *g è un elemento del dominio G. La funzione $\phi(g)$ restituisce un elemento h del codomino H. ($\phi(g) = h$). $\phi(g^{-1})$ **deve** restituire h^{-1} ($\phi(g^{-1}) = h^{-1}$)*
3. *Per ogni* $g \in G$ e *per ogni* $n \in \mathbb{Z}$ abbiamo: $\phi(g^n) = \phi(g)^n$, in notazione additiva: $\phi(n \cdot g) = n \cdot \phi(g)$
4. Se G_1 è un *sottogruppo* di G, allora *l'immagine* $\phi(G_1)$ è un *sottogruppo* di H.
5. Se H_1 è un *sottogruppo* di H, allora la *controimmagine* $\phi^{-1}(H_1)$ *è un sottogruppo di* G.

*Alcune delle proprietà appena descritte possono essere usate "in negativo" per dimostrare che certe funzioni tra gruppi **non** sono omomorfismi.*

7.4.3 Definizione di monomorfismo, epimorfismo, isomorfismo, endomorfismo

Sia $\phi : G \to H$ un omomorfismo, allora:

1. Se ϕ è *iniettivo* si dice **monomorfismo**
2. Se ϕ è *suriettivo* si dice **epimorfismo**
3. Se ϕ è *biettivo* si dice **isomorfismo/automorfismo**
4. Nel caso speciale in cui $G = H$, un *omomorfismo* si dice anche **endomorfismo**.

7.4.4 Gruppi isomorfi

Se G ed H sono due gruppi e se esiste un *isomorfismo* $\phi : G \to H$ i due gruppi G e H si dicono essere *isomorfi* e si scrive simbolicamente come $G \backsimeq H$.

7.4.5 Nucleo di un omomorfismo

Sia $\phi : G \to H$ un *omomorfismo* di gruppi. Si dice nucleo dell'omomorfismo G il sottoinsieme:

$$\ker(\phi) = \{g \in G | \phi(g) = e_H\} = \phi^{-1}(e_H)$$

Il nucleo di un omomorfismo $\phi : G \to H$ è un sottogruppo di G in quanto *controimmagine* del sottogruppo banale di H composto da $\{e_H\}$

7.4.6 Iniettività di un omomorfismo in base al suo nucleo

Sia $\phi : G \to H$ un *omomorfismo*. Allora:
ϕ è *iniettivo (monomorfismo) se e solo se* $\ker(\phi) = \{e_G\}$
Ovvero: l'unico modo per ottenere $\phi(g) = e_H$ è con $g = e_G$.
Quindi se ad esempio e_G fa parte dell'insieme delle soluzioni di $\ker(\phi)$, **ma** esiste anche solo un altro modo per ottenere e_H allora ϕ *non* è iniettivo.

7.4.7 Omomorfismi particolari

1. **Omomorfismo banale** (*funzione costante*):
   Sia $h \in H$, la **funzione costante** $\phi_h : G \to H$ *tale che* $\phi_h(g) = h$ per ogni $g \in G$.
   La funzione costante è un omomorfismo *se e solo se* $h = e_H$. Infatti l'uguaglianza:

   $$\phi_{e_H}(g_1 * g_2) = e_H = e_H \star e_H = \phi_{e_H}(g_1) \star \phi_{e_H}(g_2)$$

   è verificata. Invece se $h \neq e_H$, allora:

   $$\phi_h(g_1 * g_2) = h \neq h \star h = \phi_h(g_1) \star \phi_h(g_2)$$

   L'omomorfismo ϕ_{e_H} viene detto omomorfismo banale.
   La sua esistenza comporta che l'insieme degli omomorfismi da G ad H *non è mai vuoto.*
   L'omomorfismo banale è *iniettivo* (*monomorfismo*) *se e solo se* $|G| = 1$ ed è *suriettivo* (*epimorfismo*) *se e solo se* $|H| = 1$.
   Quindi se $|G| = |H| = 1$, allora l'omomorfismo banale è *biettivo* (*isomorfismo*).
   In ogni caso, $\phi_{e_H}(G) = \{e_H\}$ è un *sottogruppo banale* di H.

2. **Funzione identità**:
   Se $G = H$ allora la funzione identità $\mathrm{id}(g) = g$ è un *omomorfismo*, in quanto:

   $$\mathrm{id}(g * g) = g * g = \mathrm{id}(g) * \mathrm{id}(g)$$

   La funzione identità è sempre un **endomorfismo** e quindi ogni gruppo G è sempre isomorfo con se stesso.

3. **Funzione segno**:
   Ricordiamo che {1, -1} è un gruppo rispetto alla moltiplicazione. Vedere (7.1.3). Inoltre, $\mathcal{S}_n$ è l'insieme delle permutazioni
   Sia sg: $\mathcal{S}_n \to \{1, -1\}$ la funzione:

   $$\mathrm{sg}(\pi) = \begin{cases} 1 & \text{se } \pi \text{ è pari} \\ -1 & \text{se } \pi \text{ è dispari} \end{cases}$$

   La funzione sg così definita assegna -1 all'insieme delle permutazioni *dispari* e 1 all'insieme delle permutazioni *pari*. Vedere il punto (6.3)
   La funzione sg è detta funzione segno ed è un omomorfismo.
   La funzione segno è sempre *suriettiva*, quindi è un **epimorfismo**. Inoltre, è iniettiva *se e solo se* $n < 2$.
   Se è anche *iniettiva*, allora è un **isomorfismo**.
   sg ha come nucleo:

   $$\ker(\mathrm{sg}) = \{\pi \in \mathcal{S}_n | \mathrm{sg}(\pi) = 1\} = \{\pi \in \mathcal{S}_n | \pi \text{ è pari}\} = \mathcal{A}_n$$

4. **Coniugio**:
   Sia G un gruppo qualunque e sia $x \in G$ un elemento fissato.
   Definiremo una funzione $\varphi : G \to G$ ponendo $\varphi_x(g) = x \cdot g \cdot x^{-1}$
   La funzione φ_x è un *omomorfismo* detto coniugio per x in G.
   Il coniugio è *biettivo*, quindi è un **endomorfismo** per ogni x.
   Il coniugio ha come nucleo:

   $$\ker(\varphi_x) = \{g \in G | \varphi_x(g) = x \cdot g \cdot x^{-1} = e_G\}$$

7.5 Gruppi e sottogruppi ciclici

7.5.1 Sottogruppi delle potenze di un gruppo

Sia $(G, *)$ un gruppo e $g \in G$. Per costruire un sottogruppo di G, scriviamo:

$$\langle g \rangle = \{g^n \in G | n \in \mathbb{Z}\}$$

$\langle g \rangle$ è il *sottoinsieme* in G costituito da tutte le *potenze* di g.
Con la notazione *additiva*, scriviamo:

$$\langle g \rangle = \{n \cdot g \in G | n \in \mathbb{Z}\}$$

Il *sottoinsieme* $\langle g \rangle \subset G$ *è un sottogruppo* di G.

7.5.2 Gruppi e sottogruppi ciclici

Il sottogruppo $\langle g \rangle$ di G si dice *sottogruppo ciclico* di G generato da g.
Quindi, un sottogruppo $H < G$ per cui esiste un $g \in H$ tale che $H = \langle g \rangle$ si dice **generato** da g. L'elemento g si dice **generatore** di H.
Questo vale anche nei casi in cui $H = G$. Si ha quindi $g \in G$ tale che $G = \langle g \rangle$. In tal caso, il *gruppo* G stesso si dice *ciclico*.
Ad esempio, questo si applica con $G = \mathbb{Z}$: ogni intero è multiplo di 1, quindi possiamo scrivere $\mathbb{Z} = \langle 1 \rangle$, dicendo che $\mathbb{Z}$ è *ciclico*.
Inoltre, valgono le seguenti:

1. Siccome le potenze di un elemento *commutano* tra loro, $\langle g \rangle$ è **commutativo** (*abeliano*) anche se G non lo è.

2. Un gruppo G non *abeliano* **non** può essere *ciclico*. Questa è una condizione *necessaria ma non sufficiente*. Inoltre, questo implica che G può avere sottogruppi ciclici $\langle g \rangle$.

3. La condizione *necessaria ma non sufficiente* del punto 2 ci ricorda che *non tutti* i gruppi abeliani sono anche *ciclici*.

4. Un gruppo ciclico H può ammettere più di un *generatore* g.
   Ad esempio quando prima avevamo scritto $\mathbb{Z} = \langle 1 \rangle$ potevamo scrivere anche $\mathbb{Z} = \langle -1 \rangle$ perché ogni intero è anche multiplo di -1. Infatti i generatori di $\mathbb{Z}$ sono 1 e -1 (Vedere il punto 5.1.1 quando si dice che i multipli di 1 e -1 *esauriscono* $\mathbb{Z}$).

7.5.3 Potenze del generatore g

Consideriamo $\langle g \rangle$ come un sottogruppo ciclico di G. Inoltre, consideriamo la funzione $\epsilon : \mathbb{Z} \to \langle g \rangle$, con $\epsilon(k) = g^k$.
Infine, consideriamo $|\langle g \rangle| = n$ *(quando* $\langle g \rangle$ *è finito).*
Per la legge delle potenze ϵ è un *omomorfismo suriettivo.*
Distinguiamo due casi:

1. Se le potenze g^k sono tutte a due a due distinte, allora:
   ϵ è anche iniettivo, e quindi è un *isomorfismo.* Pertanto $\langle g \rangle$ e $\mathbb{Z}$ sono *isomorfi,* quindi $\langle g \rangle$ è **infinito**.

2. Se invece nelle potenze g^k ci sono delle ripetizioni, allora:
   $g^0 = e_G$ *(il primo elemento del periodo è per forza la potenza* g^0*)*, quindi $g^n = e_G$
   $\langle g \rangle$ è **finito** e ha esattamente n elementi. Inoltre, calcolare g^k vuol dire calcolare:
   $k : r = q \cdot n + r$ *(divisione con resto)*
   $g^k = g^r$
   Inoltre, $\ker(\epsilon) = n \cdot \mathbb{Z}$
   Per concludere questa voce dell'elenco, vedere il punto 7.5.4.

7.5.4 Periodo del generatore g

Sia G un gruppo e sia $g \in G$. Si dice periodo di g l'ordine $|\langle g \rangle|$ del sottogruppo ciclico generato da G.
Valgono le seguenti:

1. *L'elemento neutro* è l'unico elemento di un gruppo ad avere periodo 1.
   Ovvero: solo $\langle g \rangle = \{e_G\}$ ha periodo 1. Quindi solo il generatore g tale che $\langle g \rangle = \{e_G\}$ ha periodo 1.

2. Come visto nella voce 1 dell'elenco nel punto 7.5.3, tutti i gruppi ciclici infiniti sono *isomorfi* a $\mathbb{Z}$ e quindi *sono tutti isomorfi tra loro.*

3. Un gruppo *finito* G **non** può avere dei generatori g con periodo *infinito*. Tuttavia, un gruppo *infinito* **può** avere dei *generatori* g con periodo *finito* anche diversi dall'elemento neutro.

4. Se il generatore g ha periodo *infinito*, ogni potenza g^k è a sua volta un *generatore* con periodo *infinito*.
   Attenzione al particolare: definiamo con una lettera a caso: s il generatore g^k, quindi $s = g^k$. Allora s è generatore di un *sottogruppo* di $\langle g \rangle$, ovvero:
   $\langle s \rangle \subset \langle g \rangle$
   Qui arriva il punto importante: nonostante non sia sbagliato dire che $\langle s \rangle$ sia un *sottogruppo* di G, è più corretto dire che sia un *sottogruppo* di $\langle g \rangle$ visto che di fatto, $\langle s \rangle$ è sempre contenuto in $\langle g \rangle$ e non è mai più grande di $\langle g \rangle$.

5. Se G è un gruppo di ordine n il periodo di ogni generatore $g \in G$ deve essere un *divisore* di n. *(Vedere il teorema di Lagrange al punto 7.3.4)*

7.5.5 Omomorfismo del sottogruppo generato

Sia G un sottogruppo generato dall'elemento g, *(ovvero $G = \langle g \rangle$)*. Inoltre, sia H un gruppo qualunque.
Allora, un qualunque omomorfismo ϕ tale che:

$$\phi : G \to H$$

è completamente determinato dal valore di $\phi(g)$.
Siccome in un omomorfismo vale $\phi(g^k) = \phi(g)^k$, una volta che hai scelto dove mandare g in H, ovvero, una volta stabilito:
$\phi(g) = h$, con $h \in H$, allora tutti gli altri valori dipendono da $\phi(g)$, ovvero da h. Quindi:
$\phi(g) = h$
$\phi(g^k) = h^k$
Ovviamente vale sempre il discorso $\phi(g^0) = \phi(e_G) = e_H$
Quindi non tutti gli $h \in H$ possono soddisfare $\phi(g) = h$
Consideriamo il caso in cui G sia finito. Consideriamo n come il periodo di g. Vogliamo costruire un omomorfismo ϕ tale che:

$$\phi : G \to \mathbb{Z}$$

Ricordiamo che $\mathbb{Z}$ è un gruppo abeliano con l'operazione di somma, quindi in realtà stiamo considerando $\phi : G \to (\mathbb{Z}, +)$, quindi quando parliamo di quello che succede in $\mathbb{Z}$ usiamo la notazione additiva. Vedere il punto 7.1.3
Per G invece supponiamo sia un gruppo con l'operazione $*$, quindi usiamo la notazione moltiplicativa.
Se ϕ è un isomorfismo, deve valere:$\phi(g^k) = k \cdot \phi(g)$ con $k \in \mathbb{Z}$. In particolare:

$$0 = \phi(e_G) = \phi(g^n) = n \cdot \phi(g)$$

L'elemento neutro è nella parte in magenta (moltiplicativa) ma ho mantenuto il suo colore originale.
L'unico modo per soddisfare tale equivalenza è che $n \cdot \phi(g) = 0$. Quindi $\phi(g) = 0$. L'unico omomorfismo che soddisfa la richiesta è quello **costante**.
Attenzione *perché con $k \in \mathbb{Z}$ si potrebbe pensare che in generale $k \in H$.* ***Non è assolutamente vero****. k non appartiene né a G né ad H. k dice solo quante volte eseguire una determinata operazione in G oppure in H e quindi convenzionalmente per questo "contatore" si usa un intero e quindi si scrive $k \in \mathbb{Z}$, che per pura coincidenza, nell'esempio risulta essere anche l'insieme di destinazione.*

7.5.6 Elementi di G elevati all'ordine di G

Sia G un gruppo finito di ordine $|G| = n$ e sia $g \in G$ un suo elemento. Allora $g^n = e_G$
Attenzione perché con g non si intendono i generatori, ma **tutti** gli elementi di G.

8 Aritmetica Modulare

8.1 Classi resto e loro operazioni

8.1.1 Relazione di congruenza

Fissiamo un numero intero$N \geq 2$ detto **modulo**.
In realtà $N = 1$ è anche accettabile, tuttavia tale valore origina una situazione banale poco interessante e quindi per convenzione: $N \geq 2$.
Definiamo una relazione di congruenza in $\mathbb{Z}$ come segue:
Due numeri interi $m, n \in \mathbb{Z}$ si dicono *congruenti modulo N*. Scriveremo:

$$m \equiv n \bmod N \qquad \text{se } N \text{ divide } m - n$$

Ricordando la divisione euclidea dove$a : b = q + r$, qui m è la a, ovvero il dividendo. N è il divisore b ed n è il resto r.
Per capire quanto sto per dire, vedere il punto 2.7.3 dove ho avuto cura di abbinare i colori con questa definizione, per facilitare la comprensione.
La relazione di congruenza è una relazione di equivalenza.
Quindi, l'insieme $\mathbb{Z}$ può avere più partizioni. Ogni partizione è definita da un solo insieme di classi di equivalenza. Per ogni *modulo N* esiste una partizione, ovvero un insieme di classi di equivalenza di $\mathbb{Z}$. Ognuna di queste classi di equivalenza è detta **classe di congruenza modulo N**. Per ogni m, esiste una classe di equivalenza composta da tutti gli n, tali che: $m \equiv n \bmod N$
I termini "classe di congruenza modulo N", "classe di equivalenza modulo N" e "classe resto modulo N" sono equivalenti.

8.1.2 Teorema: proprietà delle classi di equivalenza modulo N

Fissiamo $N \geq 2$. Allora:

1. Per ogni $n \in \mathbb{Z}$ la classe di congruenza di n è $[n]_N$
2. Si ha $[m]_N = [n]_N$, *se e soltanto se* $m \equiv n \bmod N$
3. Le N classi $[0]_N, [1]_N, \ldots, [N-1]_N$ sono *distinte* ed *esauriscono* le classi di equivalenza modulo N

Inoltre, per la definizione di partizione, una classe di equivalenza modulo N *non è mai vuota.*

8.1.3 Classe di resto modulo N nulla

Con classe di resto modulo N *nulla* si intende quella classe di resto che ha $n = 0$, ovvero, quella che ha come resto 0 e che contiene quindi tutti i multipli di N.

8.1.4 L'insieme delle classi resto modulo N

Per capire cosa sto per dire, vedi il punto 2.5.3 assieme al punto 2.7.3 e segui bene i colori.
L'insieme delle classi resto modulo N è l'insieme quoziente per la *relazione di congruenza* corrispondente alla scelta del modulo N. Lo denoteremo $\mathbb{Z}_N$.
Quando non c'è rischio di confusione sul modulo N, useremo la notazione $\overline{n}$ per la classe di resto rappresentata da $n \in \mathbb{Z}$.

8.1.5 Operazioni nelle classi resto modulo N

Nell'insieme $\mathbb{Z}_N$ delle classi resto modulo N definiamo le operazioni:

- Di **addizione**: $\overline{a} + \overline{b} = \overline{a + b}$
- Di **moltiplicazione**: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Per ogni $\overline{a}, \overline{b} \in \mathbb{Z}_N$
Le operazioni in *rosso* definiscono la relativa operazione in $\mathbb{Z}_N$ che stiamo definendo, mentre le operazioni in *verde lime* sono le consuete operazioni in $\mathbb{Z}$.
Le operazioni di **addizione** e **moltiplicazione** in $\mathbb{Z}_N$ sono *sempre ben definite.*

8.1.6 Proprietà dell'addizione in $\mathbb{Z}_N$

Valgono le seguenti:

1. L'addizione in $\mathbb{Z}_N$ è **associativa**
2. $\overline{0}$ è l'elemento neutro
3. Ogni elemento $\overline{a} \in \mathbb{Z}_N$ ammette il suo opposto: $-\overline{a} = \overline{-a}$
4. Vale la proprietà **commutativa**

Ricordo la proprietà **associativa**: $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$
Ricordo che per definizione l'elemento neutro deve essere unico, quindi un'operazione può averne uno e uno soltanto.
Inoltre, $(\mathbb{Z}_N, +)$ è un **gruppo abeliano** (*commutativo*) **ciclico**. *Vedere il punto 7.5.2*

8.1.7 Isomorfismo tra G e $(\mathbb{Z}_N, +)$

Per comprendere la notazione, vedere il punto 7.4.4
Sia $G = \langle g \rangle$ un *gruppo ciclico* di ordine $|G| = N$.
Allora: $G \simeq (\mathbb{Z}_N, +)$
Quindi G e $(\mathbb{Z}_N, +)$ sono isomorfi, perché tra loro esiste un *isomorfismo* $\phi : G \to (\mathbb{Z}_N, +)$.

8.1.8 Omomorfismo suriettivo tra due moduli

Siano M ed N due numeri interi con M *che divide* N. Allora esiste un *omomorfismo suriettivo* tale che:

$$\phi_{N,M} : \mathbb{Z}_N \to \mathbb{Z}_M, \qquad \phi_{N,M}([n]_N) = [n]_M$$

8.1.9 Proprietà della moltiplicazione in $\mathbb{Z}_N$

1. La moltiplicazione in $\mathbb{Z}_N$ è **associativa**
2. $\overline{1}$ è l'elemento neutro
3. Vale la proprietà **commutativa**

8.1.10 Proprietà distributiva di $\mathbb{Z}_N$

In $\mathbb{Z}_N$ vale la proprietà **distributiva** *(vedi il punto 5.1.1)*:
Per ogni $a, b, c \in \mathbb{Z}_N$ si ha:

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$$

8.2 Il gruppo moltiplicativo

8.2.1 Divisori dello zero

Sia $\overline{0} \neq \overline{a} \in \mathbb{Z}_N$ una classe resto modulo N *non nulla (vedi il punto 8.1.3).*
Diremo che $\overline{a}$ è un divisore dello zero (*oppure 0-divisore*) se esiste una classe non nulla $\overline{b} \in \mathbb{Z}_N$ tale che $\overline{a} \cdot \overline{b} = \overline{0}$
Può anche succedere che $\overline{a} = \overline{b}$, tuttavia, un divisore dello zero **non** può essere *invertibile.*

8.2.2 Classe di resto invertibile, oppure divisore dello zero

Sia $\overline{0} \neq \overline{n} \in \mathbb{Z}_N$ una classe resto modulo N *non nulla.* Allora:

$$\overline{n} \begin{cases} \text{è invertibile} & \text{se MCD}(n, N) = 1 \\ \text{è uno zero divisore} & \text{se MCD}(n, N) > 1 \end{cases}$$

$\overline{n}$ può essere un qualsiasi rappresentante della sua classe di resto.

8.2.3 Calcolo dell'inverso $[n]_N^{-1}$

Per calcolare $[n]_N^{-1}$ è necessario calcolare MCD(n, N) con il metodo di Euclide (*Vedere il punto 5.2.7*) e verificare al punto 8.2.2 se è *invertibile*.
Se è invertibile, allora si calcola l'identità di Bézout *(Vedi il punto 5.2.8)*.
Copio i risultati ottenuti nei punti 5.2.7 e 5.2.8 per fare un esempio:

MCD(143.779,2.706) =1

907·143.779−48.192·2.706=1
In questo esempio$N = 2.706, n = 143.779, [n]_N^{-1} = [907]_N$
Attenzione! Bisogna prendere sempre il coefficiente (che chiamiamo c) di n nell'identità di Bézout e **non** quello di N.
Inoltre, **non si può usare sempre** c direttamente come il *rappresentante* r della classe di resto inversa tale che $[n]_N^{-1} = [r]_N$
In particolare, se c ***non*** è compreso tra $0 \leq c < N$, (*ovvero se è negativo oppure è uguale o maggiore di* N) allora calcoliamo la seguente divisione euclidea:

$$c : N$$

e utilizziamo il resto ottenuto come *rappresentante*.

8.2.4 Gruppo moltiplicativo di $\mathbb{Z}_N$

Si definisce come gruppo moltiplicativo di $\mathbb{Z}_N$, la restrizione della moltiplicazione in $\mathbb{Z}_N$ ai soli elementi *invertibili*.
Il gruppo moltiplicativo di $\mathbb{Z}_N$ si indica con $\mathbb{Z}_N^\times$ e viene anche detto **gruppo delle unità modulo** N e indicato con U_N.
Per $\mathbb{Z}_N^\times$ valgono le seguenti:

1. Il prodotto di *classi invertibili* è *invertibile*
2. $\overline{1}$ è *invertibile* con se stesso. *(invertibilità dell'elemento neutro)*
3. L'inversa di una classe *invertibile* è a sua volta *invertibile*

8.2.5 Funzione di Eulero

Si dice funzione φ di Eulero la funzione $\varphi : \mathbb{N}^{\geq 1} \to \mathbb{N}$ definita come:

$$\varphi(N) = |\{n \in \mathbb{N} | 1 \leq n \leq N \text{ e } \text{MCD}(n, N) = 1\}|$$

Quindi n deve sia rispettare $1 \leq n \leq N$ e deve anche rispettare MCD$(n, N) = 1$ per soddisfare la richiesta.
La e al centro della formula è il connettivo logico $\wedge$.
La funzione di Eulero restituisce la *cardinalità* dell'insieme $\mathbb{Z}_N^\times$. In formule: $\left|\mathbb{Z}_N^\times\right| = \varphi(N)$
I punti 8.2.7 e 8.2.8 spiegano come calcolare $\varphi(N)$ a patto di conoscere la scomposizione in fattori di N.

8.2.6 Isomorfismo tra $(\mathbb{Z}_N, +)$ e $(\mathbb{Z}_a, +) \times (\mathbb{Z}_b, +)$ - Teorema cinese del resto (CRT)

Per comprendere la notazione $\simeq$ vedere il punto 7.4.4
Sia N=$a \cdot b$ con a,$b \in \mathbb{Z}$ e sia MCD(a,b) = 1. Allora:$(\mathbb{Z}_N, +) \simeq (\mathbb{Z}_a, +) \times (\mathbb{Z}_b, +)$
Ovvero, se conosci N come prodotto di a e b e questi sono *coprimi, quindi mcd(a,b)=1* allora puoi applicare il teorema. In particolare, se conosci la scomposizione in fattori di N, allora puoi applicare il teorema esteso.
Ad esempio:
Dobbiamo calcolare $X \equiv n \bmod 10^2$. Sappiamo che $10^2 = 2^2 \cdot 5^2$ entrambi coprimi tra loro. Il teorema cinese del resto dice che:
Risolvere $X \equiv n \bmod 10^2$ equivale a risolvere il sistema di congruenze lineari:

$$\begin{cases} \frac{10^2}{2^2} X_1 \equiv r_1 \bmod & 2^2 \\ \frac{10^2}{5^2} X_2 \equiv r_2 \bmod & 5^2 \end{cases}$$

Inoltre, nel caso in cui avessimo una scomposizione con più fattori distinti, del tipo $= p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$ allora vale:

$$\begin{cases} \frac{N}{p_1} X_1 \equiv r_1 \bmod & p_1 \\ \frac{N}{p_2} X_2 \equiv r_2 \bmod & p_2 \\ \vdots & \vdots \\ \frac{N}{p_k} X_k \equiv r_k \bmod & p_k \end{cases}$$

Più precisamente, si riduce tutto ad una risoluzione di congruenze lineari.
La soluzione di $X \equiv n \bmod 10^2$ si trova sommando con il loro relativo peso, tutti i valori X_k trovati. Nel caso del nostro esempio abbiamo:

$$X = \frac{10^2}{2^2} \cdot X_1 + \frac{10^2}{5^2} X_2$$

Più in generale:

$$X = \frac{N}{p_1} \cdot X_1 + \frac{N}{p_2} \cdot X_2 + ... + \frac{N}{p_k} \cdot X_k$$

Il teorema garantisce che una soluzione per X esiste sempre ed è unica.

8.2.7 Prodotto della funzione di Eulero

Siano a e b numeri *interi positivi* con MCD$(a, b) = 1$. Allora:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

8.2.8 Funzione di Eulero avente come argomento un numero primo

Sia p un *numero primo* e sia $e \geq 1$ un esponente intero. Allora:

$$\varphi(p^e) = p^{e-1} \cdot (p - 1)$$

8.2.9 Ciclicità di $(\mathbb{Z}_a, +) \times (\mathbb{Z}_b, +)$

Distinguiamo due casi:

$$(\mathbb{Z}_a, +) \times (\mathbb{Z}_b, +) \begin{cases} \text{è cicliclo se} & \text{MCD}(a, b) = 1 \\ \text{non è ciclico se} & \text{MCD}(a, b) > 1 \end{cases}$$

Se è ciclico, allora è generato dalla coppia $([1]_a, [1]_b)$.

8.3 Congruenze

8.3.1 Proprietà delle congruenze

Fissiamo un intero $N \geq 2$. Allora valgono i fatti seguenti:

1. Per ogni $m, n \in \mathbb{Z}$ si ha $m \equiv n \bmod N$ se e soltanto se $n \equiv m \bmod N$
2. Per ogni $m, n, c \in \mathbb{Z}$, se $m \equiv n \bmod N$ e $n \equiv c \bmod N$, allora $m \equiv c \bmod N$

3. Per ogni $m, n, c, d \in \mathbb{Z}$, se $m \equiv n \mod N$ e $c \equiv d \mod N$, allora $m+c \equiv n+d \mod N$ e $m \cdot c \equiv n \cdot d \mod N$
4. Per ogni $m, n \in \mathbb{Z}$ e per ogni divisore M di N si ha che se $m \equiv n \mod N$, allora $m \equiv n \mod M$
5. Per ogni $a \in \mathbb{Z}$ esiste $b \in \mathbb{Z}$, tale che $a \cdot b \equiv 1 \mod N$ se e soltanto se $\text{MCD}(a, N) = 1$

8.3.2 Risoluzione di congruenze lineari

Vogliamo risolvere congruenze lineari della forma:

$$mX \equiv n \mod N$$

dove $m, X, n \in \mathbb{Z}$.
Con lineare si intende che X è di grado 1. La risoluzione di congruenze di grado superiore non ci interessa.
Per risolvere la congruenza, distinguiamo due casi:

1. $\text{MCD}(m, N) = 1$. In questo caso, per il punto 8.2.2 sappiamo che m ha l'inverso, e per il punto 8.2.3 sappiamo pure calcolarlo.
   Per convenienza indichiamo l'inverso con b, quindi: $b = [m]_N^{-1}$
   Moltiplicando per b entrambi i membri otteniamo:

   $$b \cdot mX \equiv X \equiv b \cdot n \mod N$$

   Ma per definizione $b \cdot m$ ci restituisce l'elemento neutro, quindi:

   $$\overline{1} \cdot m \cdot X \equiv X \equiv b \cdot n \mod N$$

   Ovvero: $X \equiv X \equiv b \cdot n \mod N$, quindi $X \equiv b \cdot n \mod N$.
   Abbiamo quindi trovato la classe di resto di $X \in [b \cdot n]_N$
   Se sei arrivato qui dal punto 2, ritorna alla fine del punto 2.
2. $\text{MCD}(m, N) = d$, con $d > 1$. Qui si aprono due strade *(il teorema al punto 8.3.3 definisce meglio quanto viene detto qui)*:

   2.1 Se d divide n, allora per X esistono esattamente d soluzioni:
   Per ottenerle, partiamo da $mX \equiv n \mod N$ e dividiamo tutti i termini per d:

   $$\frac{m}{d} \cdot X \equiv \frac{n}{d} \mod \frac{N}{d}$$

   A questo punto $\text{MCD}\left(\frac{m}{d}, \frac{N}{d}\right) = 1$ e quindi possiamo riutilizzare il punto 1 per trovare la classe di resto di X per poi *ripartire da qui*.
   Dopo aver trovato la classe di resto $[b \cdot n]_N$, tutte le d soluzioni di X, intese come tutti i valori che X può assumere sono:

   $$b \cdot n, b \cdot n + \frac{N}{d}, b \cdot n + 2 \cdot \frac{N}{d}, \ldots, b \cdot n + (d-1) \cdot \frac{N}{d}$$

   2.2 Se d **non** divide n, allora per X **non** esistono soluzioni.

8.3.3 Teorema sulla risoluzione di congruenze lineari

Sia $d = \text{MCD}(m, N)$. La congruenza lineare $mX \equiv n \mod N$ è risolvibile *se e soltanto se* d divide n. Se è risolvibile, allora esistono esattamente d soluzioni modulo N.

8.3.4 Teorema: Potenze con esponente $\varphi(N)$ (Teorema di Eulero)

Per la funzione di Eulero, vedere il punto 8.2.8
Sia $m \in \mathbb{Z}$ tale che $\text{MCD}(m, N) = 1$. Allora:

$$m^{\varphi(N)} \equiv 1 \mod N$$

8.3.5 Teorema di Fermat

Sia p un numero primo e sia $m \in \mathbb{Z}$ tale che p *non* divide m. Allora:

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

8.4 Applicazioni dell'aritmetica modulare

8.4.1 Criteri di divisibilità

Siano c_n le cifre di un numero k positivo. Consideriamo $c_0 + c_1 + ... + c_n$ la somma delle cifre di k, dove c_0 è l'ultima cifra a destra e c_n è l'ultima cifra a sinistra. Allora:

- k è divisibile per 2 se e soltanto se c_0 è *pari*
- k è divisibile per 3 se e soltanto se la somma delle sue cifre è divisibile per 3
- k è divisibile per 4 se e soltanto se le ultime due cifre (c_1 e c_0) formano un numero a sua volta divisibile per 4.
- k è divisibile per 5 se e soltanto se c_0 è uguale a 0 oppure 5.
- k è divisibile per 6 se e soltanto se è divisibile sia per 2 che per 3.
- k è divisibile per 7 se e soltanto se quando prendiamo il *doppio* di c_0, e lo *sottraiamo* al numero formato dalle restanti cifre (tutte le cifre, meno la cifra c_0), il risultato dell'operazione è un numero divisibile per 7. Tale operazione può essere reiterata finché non otteniamo un numero sufficientemente piccolo per cui verificare che sia divisibile per 7.
- k è divisibile per 8 se e soltanto se le ultime 3 cifre (c_2, c_1, c_0) formano un numero divisibile per 8.
- k è divisibile per 9 se e soltanto se la somma delle sue cifre è divisibile per 9.
- k è divisibile per 10 se e soltanto se $c_0 = 0$
- k è divisibile per 11 se e soltanto se la *differenza* tra la *somma* delle cifre in posizione pari e la *somma* delle cifre in posizione dispari è 0 oppure un numero divisibile per 11.
  Per questa valutazione si considera sempre il valore assoluto della differenza.
  A tal proposito, si può calcolare la differenza come sommaPari−sommaDispari*, oppure come* sommaDispari−sommaPari*, è indifferente.*

8.4.2 Calcolo del resto con dividendo in forma esponenziale avente esponente *enorme*

Supponiamo di voler determinare il resto della divisione $k^e : N$. Ovvero, vogliamo trovare r tale che: $k^e = q \cdot N + r$. Ma e è un esponente enorme. Abbiamo che:

$$k^e \equiv r \bmod N = k^{e \bmod \varphi(N)} \equiv r \bmod N$$