

Rigurgiti di Unicorno

di Valentino Bocchino

Parte di Teoria

Rigurgiti di unicorno

di Valentino Bocchino

02 gennaio 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 L^AT_EX, 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 me¹, 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?”

¹Le neurodivergenze possono essere davvero toste. Tuttavia, alla fine sono una sfida come tante e magari si possono anche vincere a colpi di L^AT_EX e formulari.

Prima dei ringraziamenti vorrei 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 distinguere 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. Sovrte 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

I Formulario	6
1 Cose utili	6
1.1 Prodotti notevoli	6
1.2 Equazioni di 2° grado	6
1.3 Potenze	6
2 Insiemi	7
2.1 Definizioni generali	7
2.2 Sottoinsiemi	8
2.3 L'insieme \mathbb{N} dei numeri naturali	8
2.4 Intersezione, unione, differenza, complementare e Leggi di De Morgan	8
2.5 Partizioni e quoienti	9
2.6 Prodotto cartesiano	10
2.7 Relazioni	10
2.8 Insiemi numerici	11
3 Funzioni	12
3.1 Definizioni generali	12
3.2 Immagini e controimmagini	13
3.3 Composizione di funzioni	14
3.4 Funzioni invertibili	15
3.5 Operazioni	16
4 Combinatoria	18
4.1 Schemino rapido	18
4.2 Introduzione	18
4.3 Insiemi finiti	18
4.4 Principio di inclusione-esclusione	20
4.5 Metodo delle scelte successive	20
4.6 Ordinamenti	21
4.7 Disposizioni	22
4.8 Combinazioni	24
5 I numeri interi	27
5.1 Operazioni e divisibilità	27
5.2 La divisione euclidea (Algoritmo di Euclide)	28
5.3 Teorema fondamentale dell'aritmetica	31
5.4 Extra: mcm e tabella dei numeri primi	32
6 Permutazioni	33
6.1 Definizione e notazioni	33
6.2 Cicli	35
6.3 Scambi e parità	39
6.4 Periodi	40
7 Gruppi	41
7.1 Definizioni	41
7.2 Sottogruppi	43
7.3 Teorema di Lagrange	44
7.4 Omomorfismi	45
7.5 Gruppi e sottogruppi ciclici	47
8 Aritmetica Modulare	49
8.1 Classi resto e loro operazioni	49
8.2 Il gruppo moltiplicativo	50
8.3 Congruenze	52
8.4 Applicazioni dell'aritmetica modulare	54

II Esercizi	56
9 Esercizi sugli insiemi (sezione 2)	56
9.1 Appartenenza, insiemi, sottoinsiemi, insieme vuoto	56
9.2 Insieme delle parti di A (Punto 2.2.2)	56
9.3 Intersezione, unione, prodotto cartesiano e complementare.	57
10 Esercizi sulle funzioni (sezione 3)	58
10.1 Immagine e controimmagine	58
10.2 Funzioni iniettive e suriettive	59
11 Esercizi sulla combinatorica (sezione 4)	62
11.1 Principio di inclusione-esclusione	62
11.2 Ordinamenti	65
11.3 Esercizi misti	66
11.4 Principio delle gabbie e dei piccioni	77
11.5 Anagrammi	78
12 Esercizi sui numeri interi (sezione 5)	79
12.1 Divisione euclidea	79
12.2 MCD e Identità di Bézout	79
12.3 Basi numeriche	82
12.4 Numeri primi	85
13 Esercizi sulle permutazioni (sezione 6)	86
13.1 Composizioni e cicli	86
13.2 Scrittura in cicli disgiunti, tipo, parità e periodo	87
13.3 Numero di cicli, numero di permutazioni (cardinalità)	89
14 Esercizi sui gruppi (sezione 7)	91
14.1 Verifica di sottogruppi	91
14.2 Dimostrazione sui sottogruppi delle permutazioni.	94
14.3 Verifica di omomorfismi	95
15 Esercizi sull'aritmetica modulare (sezione 8)	98
15.1 Inverso di una classe di resto	98
15.2 Funzione φ di Eulero	102
15.3 Congruenze lineari	103
15.4 Applicazioni pratiche	106

Parte I

Formulario

1 Cose utili

1.1 Prodotti notevoli

1. Quadrato di un binomio con somma

$$(A + B)^2 = A^2 + 2AB + B^2$$

6. Quadrato di un trinomio con somma

$$(A + B + C)^2 = A^2 + B^2 + C^2 + 2AB + 2AC + 2BC$$

2. Quadrato di un binomio con differenza

$$(A - B)^2 = A^2 - 2AB + B^2$$

7. Quadrato di un trinomio con differenza

$$(A - B + C)^2 = A^2 + B^2 + C^2 - 2AB + 2AC + 2BC$$

3. Prodotto tra la somma di due termini e la loro differenza

$$(A + B) \cdot (A - B) = A^2 - B^2$$

8. Somma di due cubi

$$A^3 + B^3 = (A + B)(A^2 - AB + B^2)$$

4. Cubo di un binomio con somma

$$(A + B)^3 = A^3 + 3A^2B + 3AB^2 + B^3$$

9. Differenza di due cubi

$$A^3 - B^3 = (A - B)(A^2 + AB + B^2)$$

5. Cubo di un binomio con differenza

$$(A - B)^3 = A^3 - 3A^2B + 3AB^2 - B^3$$

10. Trinomio speciale

$$\begin{aligned} x^2 + sx + p &= (x + a)(x + b) \text{ se e solo se:} \\ s &= a + b, p = a \cdot b \end{aligned}$$

1.2 Equazioni di 2° grado

$$\begin{aligned} ax^2 + bx + c &= 0 \\ \Delta &= b^2 - 4ac \end{aligned}$$

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

1.3 Potenze

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

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:
 $A = \{1, -1\}$ $B = \{0, A\}$

Allora $1 \in A$ e $A \in B$ ma $1 \notin B$.

2.1.5 Insieme vuoto

Si chiama insieme vuoto e si denota \emptyset 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 $P(0)$ è vera
2. $\forall n \in \mathbb{N}$ la verità di $P(n)$ implica la verità di $P(n+1)$.

Allora la proprietà $P(n)$ 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:

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

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:

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

2.5 Partizioni e quoziendi

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 quoziende** 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:

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

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: $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ Vedere il punto 5
- \mathbb{Q} insieme dei numeri razionali: $\{\dots, -3, -\frac{1}{2}, 0, 1, 2, \frac{10}{3}, \dots\}$
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: $\{\dots, 0, 1, \sqrt{2}, 2, \pi, \dots\}$
- \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 $f : A \rightarrow B$
 - 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 $\text{id}_A : A \rightarrow A$, definita come $\text{id}_A(a) = a$ per ogni $a \in A$.
Il grafico è $\Gamma = \{(a, a) \in A \times A \mid a \in A\}$. (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:
 $F_\beta : A \rightarrow B, \quad F_\beta(a) = \beta, \forall a \in A$.
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:
 $p_1 : A \times B \rightarrow A, \quad p_2 : A \times B \rightarrow B, \quad p_1(a, b) = a, \quad p_2(a, b) = b$
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, \dots in un insieme B è una funzione $s : \mathbb{N} \rightarrow B$, tale che:
 $s(0) = b_0, s(1) = b_1, s(2) = b_2$
L'esempio più comune di successione è la successione $s : \mathbb{N} \rightarrow B$, con $B \subset \mathbb{N}$, tale che $s(x) = \{y \mid y = x + 1\}$
(*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 $f : A \rightarrow X$ e $g : B \rightarrow Y$ resta definita una funzione:
 $f \times g : A \times B \rightarrow X \times Y,$
ponendo $(f \times g)((a, b)) = (f(a), g(b))$.

3.1.3 Restrizione

Sia $f : A \rightarrow B$ una funzione e sia $S \subset A$ un sottoinsieme di A . Si dice restrizione di f ad S la funzione $f|_S : S \rightarrow B$, 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 quoziante. Capita sovente di definire una funzione:

$$f : Q \rightarrow B$$

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 $f : A \rightarrow B$ 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 $f : A \rightarrow B$ una funzione e sia $S \subset A$ un sottoinsieme del dominio A .

Si dice immagine di S tramite f il sottoinsieme $f(S)$ del codominio B costituito dalle immagini degli elementi di S , cioè:

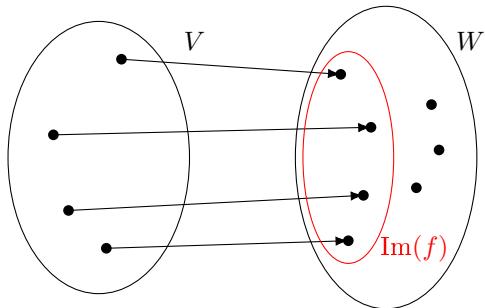
$$f(S) = \{f(s) | s \in S\} \subset B$$

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

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

La definizione generale dice che per l'insieme di partenza corrisponde un insieme delle immagini di destinazione.

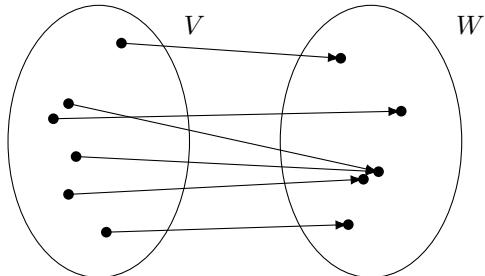
La definizione fa la distinzione tra il caso in cui l'insieme di partenza è un sottoinsieme S di A , ed il caso in cui invece il sottoinsieme S è tutto A ($S = A$).



3.2.2 Funzione suriettiva

Una funzione $f : A \rightarrow B$ si dice suriettiva se $\text{Im}(f) = B$, 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 $f : A \rightarrow B$ 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**.

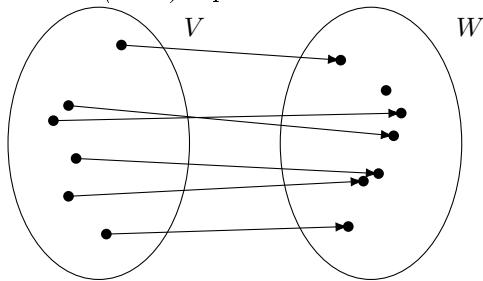
Invece se $T \subset B$ è un sottoinsieme **non vuoto** del codominio, la controimmagine $f^{-1}(T)$ **può anche essere vuota**.

3.2.5 Funzione iniettiva

Una funzione $f : A \rightarrow B$ 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 **restruzione** (3.1.3) è possibile rendere iniettiva una funzione che non lo è.



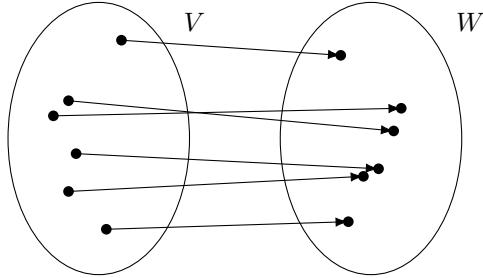
3.2.6 Proposizione sulle funzioni iniettive e suriettive

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 $f : A \rightarrow B$ 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.



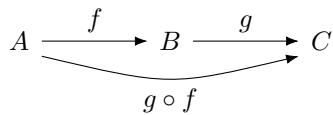
3.3 Composizione di funzioni

3.3.1 Definizione

Siano $f : A \rightarrow B$ e $g : B \rightarrow C$ due funzioni. La composizione di f e g , denotata $g \circ f$ è la funzione $g \circ f : A \rightarrow C$, 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 $f : A \rightarrow B$, $g : B \rightarrow C$ e $h : C \rightarrow D$ 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: $A \rightarrow D$ 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 $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$.

Con id si intende la **funzione identità** (3.1.2), che è sempre biettiva.

Ad esempio, consideriamo due funzioni $f : A \rightarrow B$ e $g : B \rightarrow A$. Applicando la definizione:

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

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 $f : A \rightarrow B$ una funzione **biettiva**. Allora *esiste ed è unica* una funzione $g : B \rightarrow A$ 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 $f : A \rightarrow B$ e $g : B \rightarrow C$ due funzioni biettive. Allora:

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

3.4.4 Proprietà di funzioni equivalenti

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

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**:

$$* : A \times A \rightarrow A$$

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*

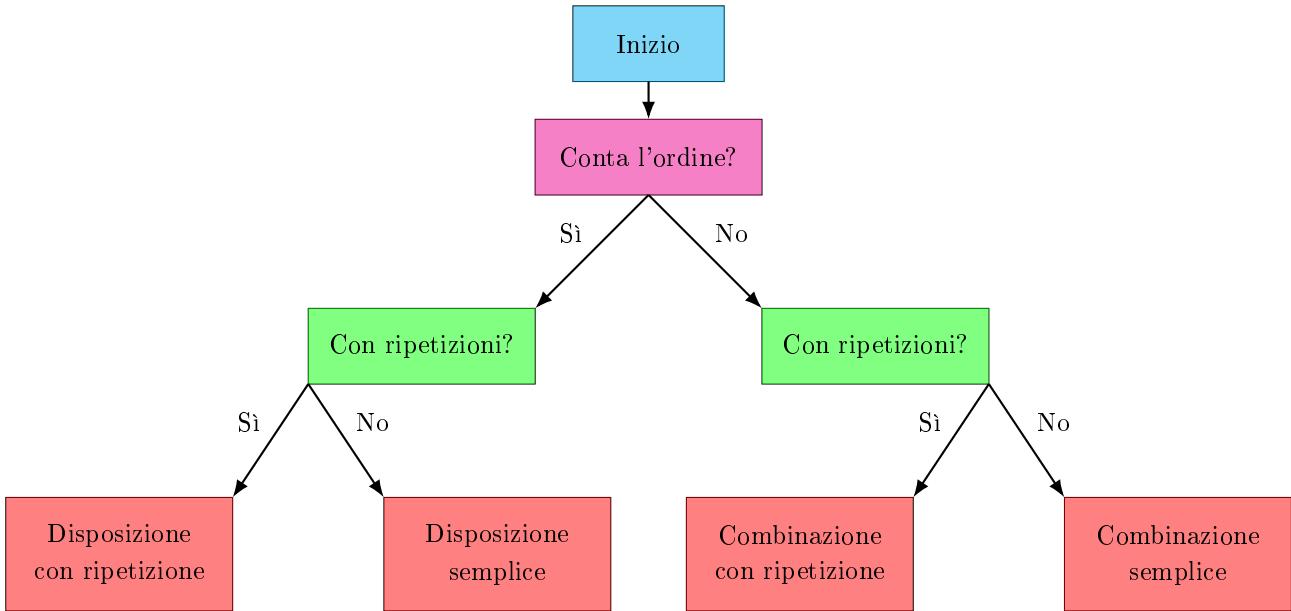
3.5.9 Il sottoinsieme degli elementi invertibili è chiuso rispetto all'operazione $*$

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 Combinatoria

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:

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

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** $f : A \rightarrow B$.

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** $f : A \rightarrow B$.
2. Esiste una funzione **suriettiva** $g : B \rightarrow A$.

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 $f : A \rightarrow A$ **iniettiva** ma *non suriettiva*.
2. Un insieme A si dice **finito** se non è infinito, cioè se ogni funzione **iniettiva** $f : A \rightarrow A$ 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** $f : A \rightarrow B$.

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, \dots, A_r insiemi finiti a due a due **disgiunti**. Allora:

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

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:

$$|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n| - \text{l'intersezione (a coppie) di ogni insieme con ogni altro insieme}^* + |A_1 \cap \dots \cap A_n|$$

***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, \dots, A_k insiemi finiti con $|A_i| = n_i$ per ogni $i = 1, 2, \dots, k$. Allora:

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

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.

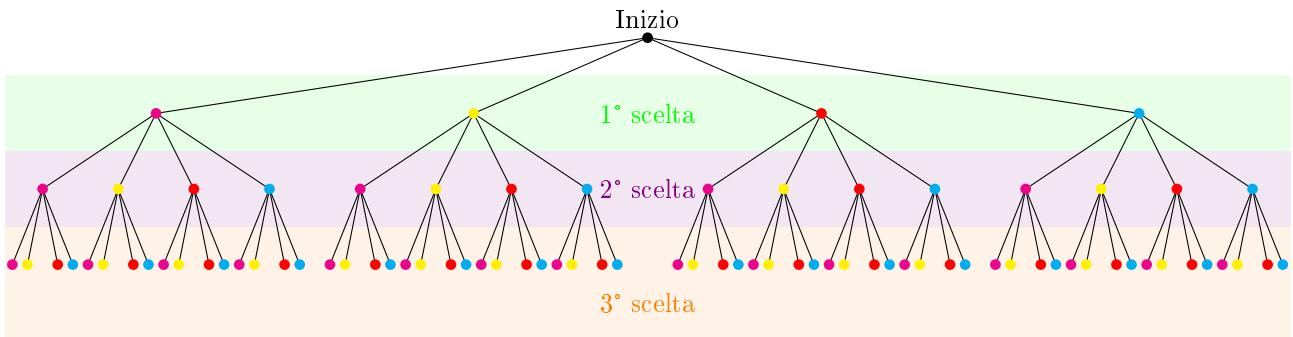
Il numero totale delle scelte possibili è dato da:

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

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) $I_n \rightarrow A$.

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:

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

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:

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

modi diversi.

4.6.4 Definizione di anagramma

Sia A un insieme non vuoto di simboli e sia $f : I_n \rightarrow A$ una lista in A di lunghezza n . Un anagramma di f è una lista $h : I_n \rightarrow A$ ottenuta come composizione $h = f \circ g$, dove $g : I_n \rightarrow I_n$ 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 $f : I_n \rightarrow A$ una lista di lunghezza n in A e supponiamo $\text{Im}(f) = \{a_1, \dots, a_k\}$ dove $a_i \in A$ compare $r_i \geq 1$ volte fra $f(1), \dots, f(n)$.

Allora il numero degli anagrammi di f è:

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

Ad esempio:

Gli anagrammi della parola MATEMATICA sono:

Le lettere di MATEMATICÀ 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. Scrivereemo quindi: 3! · 2! · 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, \dots, 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 $A \times \dots \times A$ (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 $I_k \rightarrow A$.

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, \dots, 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** $I_k \rightarrow A$. 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

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

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:*

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

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:

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

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

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 :

$$\begin{aligned} C''_{8,24} &= C_{24+8-1,8-1} = C_{31,7} = \frac{31!}{7!(31-7)!} = \frac{31!}{7! \cdot 24!} = \frac{25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30 \cdot 31}{7!} = \frac{25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30 \cdot 31}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7} = \frac{25 \cdot 13 \cdot 27 \cdot 28 \cdot 29 \cdot 30 \cdot 31}{3 \cdot 4 \cdot 5 \cdot 6 \cdot 7} = \\ &= \frac{25 \cdot 13 \cdot 9 \cdot 28 \cdot 29 \cdot 30 \cdot 31}{4 \cdot 5 \cdot 6 \cdot 7} = \frac{25 \cdot 13 \cdot 9 \cdot 7 \cdot 29 \cdot 30 \cdot 31}{5 \cdot 6 \cdot 7} = \frac{5 \cdot 13 \cdot 9 \cdot 7 \cdot 29 \cdot 30 \cdot 31}{5 \cdot 6 \cdot 7} = \frac{5 \cdot 13 \cdot 9 \cdot 7 \cdot 29 \cdot 5 \cdot 31}{7} = 5 \cdot 13 \cdot 9 \cdot 29 \cdot 5 \cdot 31 = 2.629.575 \end{aligned}$$

Questi passaggi sono del tutto opzionali: per numeri così grandi è più opportuno inserire $\frac{31!}{7! \cdot 24!}$ 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 convenzione** 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
:	:	:	:	:	:	:	:	:	:	:

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:

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

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

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

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

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:** $s : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, tale che $s(a, b) = a + b$
2. **La moltiplicazione:** $m : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, 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**:

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

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: $n : 0 = \emptyset$.
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 intuitibile 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:

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

La formula in magenta non è un prodotto.

Quando la base $b \leq 10$ si usano le cifre $\mathcal{C} = \{0, 1, 2, \dots, 9\}$. 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:

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

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: $53,1334\dots$
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 $56.773 : 5.761 = 9,854\dots$
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 $\text{MCD}(a, b) = \text{MCD}(b, r)$

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:

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

5.2.7 Calcolo del MCD

L'algoritmo è molto simile a quello visto nel punto 5.2.5.

Facciamo un esempio:

$$\text{MCD}(143.779, 2.706) = ?$$

$$143.779 = 53 \cdot 2.706 + 361$$

$$2.706 = 7 \cdot 361 + 179$$

$$361 = 2 \cdot 179 + 3$$

$$179 = 59 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

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:

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

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 scriviamo 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):

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

dove i p_i sono numeri primi positivi.

5.3.3 Teorema: Esistono infiniti numeri primi.

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):

$$f : X \rightarrow X$$

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 $\mathcal{S}_X = \{\text{id}_X, \pi\}$ dove π è la funzione tale che $\pi(a) = b$ e $\pi(b) = a$.
Quindi:
 $\text{id}_X \circ \text{id}_X = \pi \circ \pi = \text{id}_X$ e $\pi \circ \text{id}_X = \text{id}_X \circ \pi = \pi$
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 $f : \mathcal{S}_X \rightarrow \mathcal{S}_n$ 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 \mathcal{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).

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

Ad esempio:

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

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 $\pi \in S_n$ sappiamo che esiste la permutazione inversa $\pi^{-1} \in S_n$.

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:

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

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

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

Per poi riscrivere la tabella finale omettendo la seconda riga:

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

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, \dots, t_ℓ 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:

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

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:

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

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:

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

Inverso di un ciclo

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

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

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

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

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 Comutazione 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 $\pi \neq \text{id}_{\mathcal{S}_n}$ 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 disgiunti 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 $\pi \in \mathcal{S}_{13}$:

$$\pi : \left(\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 5 & 11 & 4 & 7 & 10 & 9 & 2 & 1 & 3 & 6 & 13 & 12 \end{array} \right)$$

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 $\sigma \in S_9$:

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

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:

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

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

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

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 $\sigma!$: (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 $\pi \neq \text{id}_{\mathcal{S}_n}$ e sia

$$\pi = c_1 \circ c_2 \circ \dots \circ c_r$$

la sua scrittura in **cicli disgiunti**, con c_1, c_2, \dots, c_r di lunghezza $\ell_1 \geq \ell_2 \geq \dots \geq \ell_r$ rispettivamente.

Si dice **tipo** di π la r-pla di numeri interi:

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

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* $(\ell_1, \ell_2, \dots, \ell_r)$ deve risultare:
 $\ell_1 + \ell_2 + \dots + \ell_r \leq n$
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 $(\ell_1, \ell_2, \dots, \ell_r)$.

Dobbiamo innanzitutto controllare che la somma delle lunghezze del tipo $\ell_1 + \ell_2 + \dots + \ell_r$ 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:

$$(\ell_1^{\alpha_1} \cdot \ell_2^{\alpha_2} \cdot \dots \cdot \ell_r^{\alpha_r})$$

A questo punto, per conoscere il numero di permutazioni possiamo usare la formula:

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

6.2.10 Numero di tipi in \mathcal{S}_n

Vogliamo capire quanti tipi $(\ell_1, \ell_2, \dots, \ell_r)$ 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:

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

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 S_n generano tutte le permutazioni di 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 $\pi \in S_n$. 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 $\pi, \sigma \in S_n$. 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 $\pi \in S_n$ con tipo $(\ell_1, \ell_2, \dots, \ell_r)$, definiamo un numero P tale che:

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

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

6.3.8 Numero di permutazioni pari e dispari

In 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:

$$\pi^0 = \text{id}, \pi^1 = \pi, \pi^2 = \pi \circ \pi, \pi^3 = \pi \circ \pi \circ \pi, \dots$$

Iniziamo dicendo che:

Se un ciclo di lunghezza $\ell \geq 2$, allora:

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

Pertanto:

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

con $k = 1, \dots, \ell - 1$

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 $\pi^0 = \text{id}, \pi^1 = \pi, \pi^2, \pi^3, \dots$ 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:

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

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

6.4.3 Definizione di periodo

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

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 $p = \text{per}(\pi)$. 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:

$$\pi^m = \pi^{q \cdot p + r} = (\pi^p)^q \circ \pi^r = (\text{id})^q \circ \pi^r$$

Ricorda che $(\text{id})^q = \text{id}, \forall q \geq 1$ (*proprietà idempotente*)

Quindi, l'insieme delle potenze di una permutazione è:

$$\{\text{id}, \pi, \pi^2, \dots, \pi^{p-1}\}$$

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 $(\ell_1, \ell_2, \dots, \ell_r)$. Allora il periodo della permutazione è il *minimo comune multiplo* (Vedi punto 5.4.1) delle lunghezze nel tipo:

$$p = \text{per}(\pi) = \text{mcm}(\ell_1, \ell_2, \dots, \ell_r)$$

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:

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

Moltiplicazione \cdot :

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

$(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ sono *monoidi 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:

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

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* $\{\textcolor{orange}{e}\}$, 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*:

$$gH = \{gh \mid h \in H\} \subset G$$

Ovvero: $g * H = \{g * h \mid h \in H\} \subset G$. Se il gruppo fosse stato commutativo, allora avrei scritto + al posto di *

2. **Laterale destro** di H definito da g il *sottoinsieme*:

$$Hg = \{hg \mid h \in H\} \subset G$$

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:

$$n\mathbb{Z} + r = \{nk + r \mid k \in \mathbb{Z}\}$$

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* $H \rightarrow gH$
2. Si ha $g_1H = g_2H$ 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* $H \rightarrow Hg$
2. Si ha $Hg_1 = Hg_2$ se e solo se $g_2g_1^{-1} \in H$
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 codominio.

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

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

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 $\phi : (G, *) \rightarrow (H, \star)$ 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 codominio 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 $\phi : G \rightarrow H$ 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** $\phi : G \rightarrow H$ i due gruppi G e H si dicono essere **isomorfi** e si scrive simbolicamente come $G \cong H$.

7.4.5 Nucleo di un omomorfismo

Sia $\phi : G \rightarrow H$ 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 $\phi : G \rightarrow H$ 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 $\phi : G \rightarrow H$ 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** $\phi_h : G \rightarrow H$ 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:

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

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

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

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 $\text{id}(g) = g$ è un *omomorfismo*, in quanto:

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

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: $\mathcal{S}_n \rightarrow \{1, -1\}$ la funzione:

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

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:

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

4. Coniugio:

Sia G un gruppo qualunque e sia $x \in G$ un elemento fissato.

Definiremo una funzione $\varphi : G \rightarrow G$ 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:

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

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:

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

$\langle g \rangle$ è il *sottoinsieme* in G costituito da tutte le *potenze* di g .

Con la notazione *additiva*, scriviamo:

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

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 $\epsilon : \mathbb{Z} \rightarrow \langle g \rangle$, 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.
Ovvvero: 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:

$$\phi : G \rightarrow H$$

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:

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

Ricordiamo che \mathbb{Z} è un gruppo abeliano con l'operazione di somma, quindi in realtà stiamo considerando $\phi : G \rightarrow (\mathbb{Z}, +)$, 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:

$$m \equiv n \pmod{N} \quad \text{se } N \text{ divide } m - n$$

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: $m \equiv n \pmod{N}$

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 $m \equiv n \pmod{N}$
3. Le N classi $[0]_N, [1]_N, \dots, [N-1]_N$ 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 quoziante 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 \bar{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**: $\bar{a} + \bar{b} = \overline{a+b}$
- Di **moltiplicazione**: $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$

Per ogni $\bar{a}, \bar{b} \in \mathbb{Z}_N$

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. $\bar{0}$ è l'**elemento neutro**
3. Ogni elemento $\bar{a} \in \mathbb{Z}_N$ ammette il suo opposto: $-\bar{a} = \bar{-a}$
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: $G \cong (\mathbb{Z}_N, +)$

Quindi G e $(\mathbb{Z}_N, +)$ sono *isomorfi*, perché tra loro esiste un *isomorfismo* $\phi : G \rightarrow (\mathbb{Z}_N, +)$.

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:

$$\phi_{N,M} : \mathbb{Z}_N \rightarrow \mathbb{Z}_M, \quad \phi_{N,M}([\bar{n}]_N) = [\bar{n}]_M$$

8.1.9 Proprietà della moltiplicazione in \mathbb{Z}_N

1. La moltiplicazione in \mathbb{Z}_N è **associativa**
2. $\bar{1}$ 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 $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_N$ si ha:

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

8.2 Il gruppo moltiplicativo

8.2.1 Divisori dello zero

Sia $\bar{0} \neq \bar{a} \in \mathbb{Z}_N$ una classe resto modulo N non nulla (vedi il punto 8.1.3).

Diremo che \bar{a} è un divisore dello zero (oppure 0-divisore) se esiste una classe non nulla $\bar{b} \in \mathbb{Z}_N$ tale che $\bar{a} \cdot \bar{b} = \bar{0}$
Può anche succedere che $\bar{a} = \bar{b}$, tuttavia, un divisore dello zero **non** può essere *invertibile*.

8.2.2 Classe di resto invertibile, oppure divisore dello zero

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

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

\bar{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 $\text{MCD}(n, N)$ 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:

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

$$907 \cdot 143.779 - 48.192 \cdot 2.706 = 1$$

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. $\bar{1}$ 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 $\varphi : \mathbb{N}^{\geq 1} \rightarrow \mathbb{N}$ 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 $\text{MCD}(n, N) = 1$ 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: $|\mathbb{Z}_N^\times| = \varphi(N)$

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 $\text{MCD}(a, b) = 1$. 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 $\text{mcd}(a, b) = 1$ 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 $X \equiv n \pmod{10^2}$. Sappiamo che $10^2 = 2^2 \cdot 5^2$ entrambi coprimi tra loro. Il teorema cinese del resto dice che:

Risolvere $X \equiv n \pmod{10^2}$ equivale a risolvere il sistema di congruenze lineari:

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

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

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

Più precisamente, si riduce tutto ad una risoluzione di congruenze lineari.

La soluzione di $X \equiv n \pmod{10^2}$ si trova sommando con il loro relativo peso, tutti i valori X_k trovati. Nel caso del nostro esempio abbiamo:

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

Più in generale:

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

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 $\text{MCD}(a, b) = 1$. 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:

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

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

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

8.3.2 Risoluzione di congruenze lineari

Vogliamo risolvere congruenze lineari della forma:

$$mX \equiv n \pmod{N}$$

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:

$$b \cdot mX \equiv X \equiv b \cdot n \pmod{N}$$

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

$$\bar{1} \cdot m \cdot X \equiv X \equiv b \cdot n \pmod{N}$$

Ovvero: $X \equiv b \cdot n \pmod{N}$, quindi $X \equiv b \cdot n \pmod{N}$.

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 $mX \equiv n \pmod{N}$ e dividiamo tutti i termini per d :

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

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:

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

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 $mX \equiv n \pmod{N}$ 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:

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

8.3.5 Teorema di Fermat

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

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

8.4 Applicazioni dell'aritmetica modulare

8.4.1 Criteri di divisibilità

Siano c_n le cifre di un numero k positivo. Consideriamo $c_0 + c_1 + \dots + c_n$ 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:

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

Rigurgiti di Unicorno

di Valentino Bocchino

Esercizi svolti

Parte II

Esercizi

9 Esercizi sugli insiemi (sezione 2)

9.1 Appartenenza, insiemi, sottoinsiemi, insieme vuoto

Per risolvere questo esercizio, leggere nella teoria dal punto 2.1 fino al punto 2.2.2
Sia $A = \{a, b, c\}$. Dire quali delle seguenti affermazioni sono **vere** e quali **false**:

$$b \in A, \quad \emptyset \subset A, \quad \{\emptyset\} \subset A, \quad \{c, d\} \not\subset A, \quad \{a, \{c\}\} \subset A$$

1. $b \in A$ è **vera** poiché l'elemento b è effettivamente nell'insieme A .
2. $\emptyset \subset A$ è **vera** per il punto 2.2, ovvero: **ogni insieme ha come sottoinsieme \emptyset** . Questo è un **sottoinsieme banale**.
3. $\{\emptyset\} \subset A$ è **falsa** perché nonostante sia vero che A ha come sottoinsieme l'insieme vuoto, *non è corretto affermare* che contiene un insieme che a sua volta contiene l'insieme vuoto.
4. $\{c, d\} \not\subset A$ è **vera** perché è vero che A *non* contiene l'oggetto d .
5. $\{a, \{c\}\} \subset A$ è **falsa** perché A contiene l'oggetto a ma non contiene il sottoinsieme che a sua volta contiene l'oggetto c .

Per i punti 2,3,4,5 è utile ricordare che gli unici sottoinsiemi di A sono:

$$A = \{\emptyset, A, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}\}$$

Quello che ho appena descritto è l'insieme delle parti di A : $P(A)$

9.2 Insieme delle parti di A (Punto 2.2.2)

Sia $A = \{a, e, i, o, u\}$. Dire quali delle seguenti affermazioni sono vere e quali sono false:

$$\emptyset \in P(A), \quad a \in P(A), \quad \{i, u\} \subset P(A), \quad \{e, o\} \in P(A), \quad \{\{e\}, \{o\}\} \subset P(A)$$

Per vedere un esempio di $P(A)$ vedi il punto 9.1

1. $\emptyset \in P(A)$ è **vera**. Guarda i punti: 2.2.1 e 2.2.2
2. $a \in P(A)$ è **falsa**. Perché $\{a\}$ è un elemento di $P(A)$ ma a non lo è.
3. $\{i, u\} \subset P(A)$ è **falsa**. Perché $\{i, u\}$ non è un sottoinsieme di $P(A)$. *Da non confondere con un sottoinsieme di A.*
4. $\{e, o\} \in P(A)$ è **vera**. Perché $\{e, o\}$ è un sottoinsieme di A .
5. $\{\{e\}, \{o\}\} \subset P(A)$ è **vera**. Perché $\{\{e\}, \{o\}\}$ è un sottoinsieme di $P(A)$. *Da non confondere con un sottoinsieme di A.*

Nei punti 3 e 5 il trucco è quello di capire che stiamo considerando i sottoinsiemi dell'insieme delle parti di A , ovvero: $P(P(A))$.

Prestare **estrema attenzione** al simbolo utilizzato dal quesito. \in e \subset sono facilmente confondibili quando si legge velocemente, quindi è opportuno leggere con assoluta lentezza e svolgere l'esercizio per poi ricontraddirlo bene più tardi.

9.3 Intersezione, unione, prodotto cartesiano e complementare.

Si considerino gli insiemi:

$$\begin{array}{ll} A = \{a, g, h, i, p, u, v\} & B = \{b, g, l, m, n, q, v, z\} \\ C = \{d, e, f, m, n, o, q, r, s, v\} & D = \{c, d, e, h, i, p, r, t, u, z\} \end{array}$$

Dire quali delle seguenti affermazioni sono vere e quali sono false:

1. $A \cap B \subset C$
3. $\{d, e\} \in P(C \cap D)$
5. $(A \times B) \cap (C \times D) = \emptyset$
2. $(v, v) \in A \times B \setminus B \times C$
4. $(e, p) \in A \times D$
6. $\{b, l, u\} \subset P(B \cup D)$

Per i punti 1,3,5 vedere nella teoria il punto 2.4.1

Per il punto 6 vedere nella teoria il punto 2.4.2

Per i punti 2,4,5 vedere nella teoria il punto 2.6.1

Per il punto 2 vedere nella teoria il punto 2.4.4

1. **Falsa**, perché $A \cap B = \{g, v\}$, ma $\{g, v\}$ non può essere un sottoinsieme di C perché g non è un elemento di C .
2. **Falsa**:
Possiamo anche calcolare $A \times B$ e $B \times C$ per poi calcolare la differenza, ma sarebbe un'operazione estremamente dispendiosa.
Ragionando, possiamo dedurre che la coppia (v, v) può solo esistere nel prodotto $A \times B$ se sia A che B contengono v .
Con una rapida verifica, possiamo affermare che $(v, v) \in A \times B$.
Ora però, dobbiamo ricordare che la differenza *rimuove* tutti gli elementi di $B \times C$ presenti in $A \times B$.
Quindi dobbiamo verificare se la coppia (v, v) esiste in $B \times C$.
Con una rapida verifica, possiamo affermare che $(v, v) \in B \times C$.
Siccome (v, v) appare in entrambi i prodotti cartesiani, il complementare la rimuove e pertanto possiamo concludere che l'affermazione è **FALSA**.
3. **Vera**, perché $C \cap D = \{d, e, r\}$, quindi il suo insieme delle parti $P = \{\emptyset, \{d\}, \{e\}, \{r\}, \{d, e\}, \{d, r\}, \{e, r\}, \{d, e, r\}\}$, contiene $\{d, e\}$
4. **Falsa**, perché e non è un oggetto presente in A , e quindi per il prodotto non può esistere nessuna coppia che abbia come primo elemento e . Anche qui, non serve calcolare $A \times D$.
5. **Falsa**:
Anche qui non serve calcolare alcun prodotto.
Dobbiamo semplicemente trovare almeno una coppia che sia in comune ai due prodotti.
Ragionando, per avere due coppie in comune ai due prodotti, serve che A e C abbiano almeno un elemento in comune e che anche B e D abbiano almeno un elemento in comune.
Notiamo che A e C hanno in comune un solo elemento v .
Quindi un'eventuale coppia in comune ai due prodotti deve per forza essere del tipo $(v, ?)$.
Notiamo che B e D hanno in comune un solo elemento z .
Quindi la coppia in comune è proprio (v, z) e pertanto è **falso** dire che i due prodotti non hanno nessuna coppia in comune, e che quindi la loro intersezione è vuota.
6. **Falsa**: perché l'unione di B e D è l'insieme composto da tutti gli elementi di B e di D , e gli elementi b, l, u compaiono in B e D . L'insieme delle parti P ha come oggetto $\{b, l, u\}$, ma non ha certamente come sottoinsieme $\{b, l, u\}$.

10 Esercizi sulle funzioni (sezione 3)

10.1 Immagine e controimmagine

Per risolvere questo esercizio, vedere nella teoria il punto 3.2.3

Sia $f : \mathbb{Z} \rightarrow \mathbb{Z}$ la funzione definita da $f(n) = n^2 - 1$.

Calcolare: $f^{-1}(-5), f^{-1}(-1), f^{-1}(8), f^{-1}(12)$.

Qui notiamo subito che la notazione può essere confusa con la definizione di funzione inversa. Tuttavia, qui non ci è stato chiesto di trovare o definire una funzione inversa. Inoltre, l'esercizio non specifica tale funzione. Pertanto f^{-1} è da intendersi come il simbolo per indicare la controimmagine.

L'esercizio è molto banale e consiste nel trovare n per ognuno dei valori proposti. Quindi:

1. Per $f^{-1}(-5)$:

$$n^2 - 1 = -5$$

$$n^2 = -4$$

La soluzione di questa equazione non esiste in \mathbb{Z} , pertanto per $f^{-1}(-5)$ non esistono controimmagini ($f^{-1}(-5) = \emptyset$).

2. Per $f^{-1}(-1)$:

$$n^2 - 1 = -1$$

$$n^2 = 0$$

L'equazione è risolta per $n = 0$, pertanto $f^{-1}(-1) = \{0\}$

3. Per $f^{-1}(8)$:

$$n^2 - 1 = 8$$

$$n^2 = 9$$

L'equazione è risolta per $n = \pm 3$ (2 soluzioni), pertanto $f^{-1}(8) = \{-3, 3\}$.

4. Per $f^{-1}(12)$:

$$n^2 - 1 = 12$$

$$n^2 = 13$$

La soluzione di questa equazione non esiste in \mathbb{Z} , pertanto per $f^{-1}(12)$ non esistono controimmagini ($f^{-1}(12) = \emptyset$).

10.2 Funzioni iniettive e suriettive

Per risolvere questo esercizio, vedere nella teoria i punti 3.2.2 e 3.2.5

10.2.1 Verifica di una funzione

Sia $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ la funzione definita come $f((m, n)) = m^2 - n$.

1. Dire se f è iniettiva
2. Dire se f è suriettiva
3. Calcolare l'insieme $f^{-1}(0) \cap \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = 4 \cdot m\}$
4. Calcolare l'immagine $f(S)$ del sottoinsieme $S = \{(m, n) \in \mathbb{Z} \times \mathbb{Z} \mid n = 2m - 1\}$

Risolviamo:

1. Notiamo subito che non è iniettiva, perché per le coppie $(0, 0)$ e $(1, 1)$ abbiamo:

$$f((0, 0)) = 0^2 - 0 = 0 \text{ e } f((1, 1)) = 1^2 - 1 = 1 - 1 = 0$$

Per verificare l'iniettività, possiamo anche imporre che se $f((m, n)) = f((a, b))$, allora $(m, n) = (a, b)$ e vedere se funziona:

Quindi se $m^2 - n = a^2 - b$, allora $(m, n) = (a, b)$, ovvero $m = a$ e $n = b$

Partendo da $m^2 - n = a^2 - b$ proviamo ad arrivare alla forma $m = a$:

$$m = \pm \sqrt{a^2 - b + n}$$

è palese che, avendo 2 soluzioni, questo risultato non garantisce mai che $m = a$. Perché sia iniettiva, $m = a$ deve valere per ogni coppia $\mathbb{Z} \times \mathbb{Z}$.

Nell'ipotetico caso in cui fossimo riusciti ad arrivare ad $m = a$, serve comunque che anche $n = b$.

Possiamo quindi concludere che **non** è iniettiva.

2. Si verifica banalmente che la funzione è *suriettiva* poiché non esistono elementi in \mathbb{Z} che $m^2 - n$ non può rappresentare.

In maniera più formale, si può dire che, per ogni $x \in \mathbb{Z}$ arbitrario, se consideriamo tutte le coppie del dominio del tipo:

$(0, n)$ allora $m^2 - n = x$ diventa:

$$-n = x$$

Siccome $n, x \in \mathbb{Z}$ possiamo tranquillamente imporre $n = -x$

e quindi ottenere: $-(-x) = x$ e quindi $x = x$ il che conferma che per ogni $x \in \mathbb{Z}$ arbitrario esiste una *controimmagine*.

3. Possiamo calcolare $f^{-1}(0)$, oppure possiamo direttamente impostare l'equazione:

$$m^2 - 4m = 0$$

che con $= 0$ impone la condizione di $f^{-1}(0)$ e con $-4m$ impone la condizione dell'insieme.

Otteniamo quindi:

$$m^2 = 4 \cdot m$$

$$m^2 - 4 \cdot m = 0$$

$$\Delta = (-4)^2 - 4 \cdot 1 \cdot 0 = 16$$

$$m = \frac{-(-4) \pm \sqrt{16}}{2 \cdot 1} = \frac{4 \pm 4}{2}$$

$$m_1 = 0, m_2 = 4$$

Con i valori ottenuti, sostituendo nella coppia $(m, 4 \cdot m)$ i valori ottenuti, abbiamo le coppie che formano l'insieme cercato:

$$\{(0, 0), (4, 16)\}$$

4. Per ogni $m \in \mathbb{Z}$, l'immagine è data da:

$$m^2 - (2 \cdot m - 1) = m^2 - 2 \cdot m + 1, \text{ ovvero: } (m - 1)^2, \text{ quindi:}$$

$$f(S) = \{(m - 1)^2 \mid m \in \mathbb{Z}\}$$

10.2.2 Iniettività/suriettività di una funzione - caso particolare

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Sia $f : \mathbb{N} \rightarrow \mathbb{N}$ la funzione definita come:

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ 3 \cdot n + 1 & \text{se } n \text{ è dispari} \end{cases}$$

Dimostrare o confutare le affermazioni seguenti:

1. f è iniettiva
2. f è suriettiva
3. L'immagine $f(2\mathbb{N})$ dell'insieme dei numeri pari è contenuta nell'insieme dei numeri dispari.
4. La controimmagine $f^{-1}(3\mathbb{N})$ dell'insieme dei numeri divisibili per 3 è contenuta nell'insieme dei numeri pari.

Dopodiché, calcolare esplicitamente:

$$f(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}) \quad \text{e} \quad f^{-1}(\{1, 2, 7, 9, 10, 13\})$$

1. Usiamo la tecnica vista nel punto 10.2.1:

Ricordiamo che la funzione è iniettiva se $f(a) = f(b)$, solo quando $a = b$, per ogni a, b nel dominio.

Analizziamo tutti i casi possibili:

1.1 Primo caso: a e b sono uguali e sono entrambi pari: allora $\frac{a}{2} = \frac{b}{2}$, quindi $a = b$

1.2 Secondo caso: a e b sono uguali e sono entrambi dispari: allora $3 \cdot a + 1 = 3 \cdot b + 1$, quindi $a = b$

1.3 Terzo caso: a e b sono diversi ma sono anche pari e dispari rispettivamente. In questo caso non devono avere la stessa immagine. Quindi deve valere:

$$\frac{a}{2} \neq 3 \cdot b + 1$$

Notiamo tuttavia, che l'equazione $\frac{a}{2} = 3 \cdot b + 1$ ha soluzione sia per a che per b e che tali soluzioni sono distinte ($a \neq b$). Questo significa che, scelti valori opportuni di a e b , possiamo ottenere la stessa immagine con entrambi.

Pertanto la funzione *non* è iniettiva.

Non serve verificare il caso in cui a e b siano diversi ma entrambi con la stessa parità, poiché il primo e il secondo caso dimostrano che due numeri con la stessa parità non possono produrre la stessa immagine.

2. Dobbiamo capire se l'immagine di f copre tutto \mathbb{N} : Prendiamo un $a \in \mathbb{N}$ qualunque e iniziamo a vedere cosa succede quando n è pari:

Dobbiamo partire da $\frac{n}{2} = a$ ed arrivare a: $a = a$.

Se a è pari, allora con $n = 2 \cdot a$, otteniamo:

$$\frac{2 \cdot a}{2} = a.$$

Sé a è dispari, con $n = 2 \cdot a$, abbiamo comunque n pari e pertanto riotteniamo:

$$\frac{2 \cdot a}{2} = a$$

Questo funziona perché $2\mathbb{N}$ è l'insieme dei numeri pari, quindi $2 \cdot a$ è sempre pari.

Quindi f è suriettiva.

3. Falso perché come abbiamo visto nel punto 2, l'immagine dei numeri pari è mappata su tutto \mathbb{N} . Inoltre, non è vero che siccome un numero del tipo $2 \cdot a$ è sempre pari, allora un numero a sia sempre dispari. A titolo esemplificativo:

Prendiamo $2 \in \mathbb{N}$, e valutiamo $f(2\mathbb{N})$:

$$f(4) = \frac{4}{2} = 2 \text{ ma } 2 \text{ è pari.}$$

4. Vero. Iniziamo dicendo che tutti i numeri pari sono mappati in \mathbb{N} , quindi sicuramente $f^{-1}(3\mathbb{N})$ è contenuta nei numeri pari, tuttavia, viene da chiedersi se un n dispari sia in grado di generare $f^{-1}(3\mathbb{N})$, perché in tal caso sarebbe mappata sia nei pari che nei dispari. Tuttavia, notiamo che se n è dispari, allora: $f(n) = 3 \cdot n + 1$, quindi con n dispari non si avrà mai un divisore di 3 ma semmai un successore di un divisore di 3.

Quindi $f^{-1}(3\mathbb{N})$ è contenuta solo nei numeri pari.

Calcoliamo le immagini

$$f(1) = 3 \cdot 1 + 1 = 4, f(2) = \frac{2}{2} = 1, f(3) = 3 \cdot 3 + 1 = 10, f(4) = \frac{4}{2} = 2, f(5) = 3 \cdot 5 + 1 = 16$$

$$f(6) = \frac{6}{2} = 3, f(7) = 3 \cdot 7 + 1 = 22, f(8) = \frac{8}{2} = 4, f(9) = 3 \cdot 9 + 1 = 28, f(10) = \frac{10}{2} = 5$$

Per le controimmagini, verifichiamo entrambe le condizioni:

1. $f^{-1}(1)$:

$3 \cdot n + 1 = 1 \rightarrow n = 0$ quindi è impossibile perché n dovrebbe essere dispari.

$\frac{n}{2} = 1 \rightarrow n = 2$ quindi $\{2\}$ è l'insieme delle controimmagini per $f^{-1}(1)$.

2. $f^{-1}(2)$:

$3 \cdot n + 1 = 2 \rightarrow n \notin \mathbb{N}$ quindi è impossibile

$\frac{n}{2} = 2 \rightarrow n = 4$ quindi $\{4\}$ è l'insieme delle controimmagini per $f^{-1}(2)$.

3. $f^{-1}(7)$:

$3 \cdot n + 1 = 7 \rightarrow n = 2$ quindi è impossibile perché n dovrebbe essere dispari.

$\frac{n}{2} = 7 \rightarrow n = 14$ quindi $\{14\}$ è l'insieme delle controimmagini per $f^{-1}(7)$.

4. $f^{-1}(9)$:

$3 \cdot n + 1 = 9 \rightarrow n \notin \mathbb{N}$ quindi è impossibile

$\frac{n}{2} = 9 \rightarrow n = 18$ quindi $\{18\}$ è l'insieme delle controimmagini per $f^{-1}(9)$.

5. $f^{-1}(10)$:

$3 \cdot n + 1 = 10 \rightarrow n = 3$ quindi 3 è una controimmagine.

$\frac{n}{2} = 10 \rightarrow n = 20$ quindi 20 è una controimmagine. L'insieme delle controimmagini è $\{3, 20\}$ per $f^{-1}(10)$

6. $f^{-1}(13)$:

$3 \cdot n + 1 = 13 \rightarrow n = 4$ quindi è impossibile perché n dovrebbe essere dispari.

$\frac{n}{2} = 13 \rightarrow n = 26$ quindi $\{26\}$ è l'insieme delle controimmagini per $f^{-1}(13)$.

Per risolvere questo esercizio è molto utile svolgere prima l'ultima parte dove è necessario calcolare esplicitamente i valori di f e f^{-1} .

Infatti, nelle immagini, si notava subito che $f(1) = f(8)$ e quindi si aveva già la risposta al primo quesito. Inoltre, il calcolo di $f^{-1}(10)$ avrebbe anche risolto immediatamente il primo quesito.

11 Esercizi sulla combinatorica (sezione 4)

11.1 Principio di inclusione-esclusione

Per risolvere questi esercizi, vedere i punti 4.4.2 e 4.4.3

11.1.1 Numero di multipli

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Calcolare quanti sono i numeri interi

1. Da 1 a 1.680 che sono divisibili per almeno uno tra 2, 6 e 7.
2. Da 1 a 2.160 che sono divisibili né per 5, né per 9, né per 12.

Soluzione:

1. Analizzando bene la richiesta, possiamo impostare il problema in questo modo:

Definiamo 3 insiemi A, B, C che contengono i multipli di 2, 6 e 7 rispettivamente. Ovviamente consideriamo solo i multipli tra 1 e 1680 come da richiesta.

Notiamo immediatamente che questi insiemi non sono disgiunti e che l'esercizio richiede di contare un qualunque numero tra 1 e 1680 che sia almeno multiplo di 2, 6 e 7. Infatti ad esempio 6 è multiplo di 2 e di 6

Per risolvere questo quesito dobbiamo quindi fare riferimento al principio di inclusione-esclusione, ed in particolare usare la formula per più di due insiemi (in alternativa si può applicare ricorsivamente la formula del punto 4.4.2).

La formula $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ richiede la conoscenza di $|A|, |B|, |C|$ e inoltre richiede la conoscenza delle varie intersezioni.

Nonostante queste conoscenze non vengano fornite esplicitamente, è comunque possibile ricavarle attraverso il ragionamento:

Ad esempio, facciamo finta di dover trovare il numero di multipli di 5 tra 1 e 50.

Quindi abbiamo 5, 10, 15, 20, ...

Quindi i multipli si ottengono come $5 \cdot 1, 5 \cdot 2, \dots, 5 \cdot k$. Quindi per ottenere il valore di k basta prendere un multiplo e dividerlo per 5.

Siccome k cresce di +1 per ogni nuovo multiplo, per ottenere il numero di multipli tra 1 e 50, è sufficiente calcolare $\frac{50}{5} = 10$. Infatti i multipli tra 1 e 50 di 5 sono proprio la tabellina del 5: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50.

Ovviamente se avessimo dovuto trovare i multipli di 3 avremmo avuto $\frac{50}{3} = 16, \overline{6}$. In questo caso si troncano i decimali (NON si approssima) e si conserva 16. Infatti i multipli di 3 tra 1 e 50 sono 16.

Quindi abbiamo per $|A| = \frac{1.680}{2} = 840$ per $|B| = \frac{1.680}{6} = 280$ e per $|C| = \frac{1.680}{7} = 240$.

Ora dobbiamo trovare le cardinalità delle intersezioni tra due insiemi.

Per trovare i multipli in comune tra due insiemi, possiamo usare l'mcm (vedi il punto 5.4.1). Il minimo comune multiplo infatti ci dà il numero più piccolo che è il multiplo di tutti i numeri per cui stiamo calcolando l'mcm. Dopodiché se dividiamo 1680 per questo numero, otteniamo il numero di multipli di questo multiplo, e quindi otteniamo il numero di elementi che sono multipli di entrambi gli insiemi.

Quindi abbiamo per $|A \cap B| = \frac{1.680}{\text{mcm}(2, 6)}$, per $|A \cap C| = \frac{1.680}{\text{mcm}(2, 7)}$, per $|B \cap C| = \frac{1.680}{\text{mcm}(6, 7)}$.

Calcoliamo gli mcm:

$\text{mcm}(2, 6)$: abbiamo $2 = 2 \cdot 1$ e $6 = 2 \cdot 3$, quindi $\text{mcm}(2, 6) = 2 \cdot 3 = 6$

$\text{mcm}(2, 7)$: abbiamo $2 = 2 \cdot 1$ e $7 = 7$, quindi $\text{mcm}(2, 7) = 2 \cdot 7 = 14$

$\text{mcm}(6, 7)$: abbiamo $6 = 2 \cdot 3$ e $7 = 7$, quindi $\text{mcm}(2, 7) = 2 \cdot 3 \cdot 7 = 42$

Quindi per $|A \cap B| = \frac{1.680}{6} = 280$, per $|A \cap C| = \frac{1.680}{14} = 120$, per $|B \cap C| = \frac{1.680}{42} = 40$.

Con lo stesso metodo calcoliamo $|A \cap B \cap C| = \frac{1.680}{\text{mcm}(2, 6, 7)}$

$\text{mcm}(2, 6, 7)$: abbiamo $2 = 2$, $6 = 2 \cdot 3$ e $7 = 7$, quindi $\text{mcm}(2, 6, 7) = 2 \cdot 3 \cdot 7 = 42$

Quindi $|A \cap B \cap C| = \frac{1.680}{42} = 40$

Quindi la soluzione è data da: $|A \cup B \cup C| = 840 + 280 + 240 - 280 - 120 - 40 + 40 = 960$

2. Qui il ragionamento è il medesimo ma con un "tocco finale". Dobbiamo contare tutti i numeri tra 1 e 2160 che sono multipli di 5, 9 oppure 12. Una volta trovato questo numero, dobbiamo sottrarlo a

2160, che rappresenta il totale di tutti i numeri, ovvero, quelli che rispettano il criterio e quelli che non lo rispettano. Definiamo quindi gli insiemi A, B, C come contenenti i multipli (da 1 a 2160) di 5, 9 e 12 rispettivamente. Quindi dobbiamo risolvere:

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

Abbiamo quindi:

$$|A| = \frac{2.160}{5} = 432, |B| = \frac{2.160}{9} = 240, |C| = \frac{2.160}{12} = 180$$

$$|A \cap B| = \frac{2.160}{\text{mcm}(5, 9)} = \frac{2.160}{45} = 48, |A \cap C| = \frac{2.160}{\text{mcm}(5, 12)} = \frac{2.160}{60} = 36, |B \cap C| = \frac{2.160}{\text{mcm}(9, 12)} = \frac{2.160}{36} = 60$$

inoltre:

$$|A \cap B \cap C| = \frac{2.160}{\text{mcm}(5, 9, 12)} = \frac{2.160}{180} = 12$$

quindi:

$$|A \cup B \cup C| = 432 + 240 + 180 - 48 - 36 - 60 + 12 = 720$$

L'esercizio è quindi risolto con: $2.160 - 720 = 1.440$

11.1.2 Numero di monete

Un numismatico possiede una collezione che include 25 monete d'argento, 170 monete europee e 415 monete di formato rotondo. Sappiamo che ogni sua moneta possiede almeno una delle caratteristiche suddette. Sappiamo anche che: le monete d'argento tonde sono 22, le monete europee tonde sono 152 e le monete europee d'argento sono tutte tonde. Quante monete ci sono nella collezione?

Anche qui per risolvere l'esercizio si usa il principio di esclusione-inclusione. In particolare, se definiamo tre insiemi A, B, C dove A contiene le monete di argento, B contiene le monete europee e C contiene le monete di formato rotondo, allora l'esercizio si risolve cercando: $|A \cup B \cup C|$.

$$\text{Quindi: } |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$|A|, |B|, |C|, |A \cap C|, |B \cap C|$ sono già noti. Infatti: $|A| = 25, |B| = 170, |C| = 415, |A \cap C| = 22, |B \cap C| = 152$.

Sappiamo anche che $A \cap B \subset C$ il che significa che $|A \cap B \cap C| = |A \cap B|$

Riscriviamo la formula:

$$|A \cup B \cup C| = 25 + 170 + 415 - |A \cap B| - 22 - 152 + |A \cap B|$$

Abbiamo quindi:

$$|A \cup B \cup C| = 25 + 170 + 415 - |A \cap B| - 22 - 152 + |A \cap B|$$

$$|A \cup B \cup C| = 25 + 170 + 415 - 22 - 152 = 436$$

11.1.3 Numero di presenti alla festa

Ad una festa c'erano 20 persone con i capelli biondi, 18 con i capelli neri, 15 con gli occhi azzurri e 12 con gli occhi verdi e ogni invitato aveva almeno una di queste caratteristiche. Sappiamo che delle persone bionde 12 avevano gli occhi azzurri e 4 gli occhi verdi mentre tra coloro che avevano i capelli neri 1 aveva gli occhi azzurri e 7 gli occhi verdi. Quante persone erano presenti alla festa?

Definiamo gli insiemi A, B, C, D per le persone con i capelli biondi, neri e gli occhi azzurri, verdi rispettivamente.

Stiamo cercando $|A \cup B \cup C \cup D|$. Usando quanto detto al punto 4.4.3 otteniamo:

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

Sostituiamo con quello che conosciamo:

$$|A \cup B \cup C \cup D| = 20 + 18 + 15 + 12 - |A \cap B| - 12 - 4 - 1 - 7 - |C \cap D| + |A \cap B \cap C \cap D|$$

Inoltre, vale per forza la seguente:

$$|A \cap B| = |C \cap D| = |A \cap B \cap C \cap D| = 0, \text{ ovvero:}$$

Nessuna persona ha i capelli biondi e neri allo stesso tempo, nessuna persona ha gli occhi azzurri e verdi e nessuno ha i capelli biondi e neri e gli occhi azzurri e verdi.

Abbiamo quindi:

$$|A \cup B \cup C \cup D| = 20 + 18 + 15 + 12 - 0 - 12 - 4 - 1 - 7 - 0 + 0 = 41$$

11.2 Ordinamenti

Per risolvere questo esercizio, vedere il punto 4.6.3

11.2.1 Ordinare gli elementi di un insieme rispettando particolari vincoli

Sia $S = \{a, b, c, d, e, f, 1, 2, 3, 4\}$. Calcolare il numero degli ordinamenti di S tali che:

1. Il primo e l'ultimo simbolo siano una lettera ed una cifra
2. Il primo e l'ultimo simbolo siano due lettere oppure due cifre

Ci sta chiedendo di calcolare un ordinamento, quindi sappiamo già cosa fare:

1. Abbiamo 10 scelte per 10 posizioni da popolare e non possiamo considerare ripetizioni. Quindi per ogni scelta che facciamo, abbiamo 10 - 1 scelte rimanenti. Se non avessimo vincoli, per le 10 scelte potremmo usare $10!$ per calcolare tutte le scelte possibili. Tuttavia il vincolo ci impone un massimo di 6 scelte per la prima posizione e un massimo di 4 scelte per l'ultima posizione. Quindi, per i restanti 8 elementi abbiamo solo più $8!$ scelte restanti. Pertanto abbiamo:

$$6 \cdot 8! \cdot 4 = 967.680$$

Dobbiamo ancora considerare il caso dove si inizia con una cifra e si finisce con una lettera: il caso è identico al precedente:

$$4 \cdot 8! \cdot 6 = 967.680$$

Tuttavia queste scelte vanno sommate tra loro, quindi abbiamo:

$$967.680 + 967.680 = 1.935.360$$

possibili scelte.

Nota: il testo è poco chiaro perché può anche essere interpretato pensando di dover considerare solo il caso in cui si inizi con una lettera e si finisca con una cifra. In questo caso, potrebbe essere opportuno chiedere chiarimenti, oppure svolgerlo considerando tutti i casi possibili, ovvero tutti i casi non esplicitamente vietati, per poi magari aggiungere un commento, spiegando la situazione e motivando il proprio ragionamento.

2. Qui facciamo lo stesso ragionamento. Dividiamo lo studio in 2 casi:

2.1 Iniziamo e terminiamo con una lettera:

Qui dobbiamo fare particolarmente attenzione perché siccome il primo e l'ultimo elemento sono della stessa tipologia, una volta scelto uno di loro, abbiamo esaurito una scelta nel sottoinsieme delle lettere. Quindi per l'ultima posizione, possiamo solo più considerare 5 lettere, in quanto una di queste è già stata usata. Pertanto abbiamo

Abbiamo in questo caso: $6 \cdot 8! \cdot 5$ possibili scelte.

2.2 Iniziamo e terminiamo con una cifra:

Anche qui, dobbiamo considerare il discorso per il caso precedente e quindi ricordarci che per l'ultima posizione possiamo solo più scegliere tra 3 cifre, poiché una è già stata utilizzata:

Abbiamo in questo caso: $4 \cdot 8! \cdot 3$ possibili scelte.

Anche qui eseguiamo la somma dei casi per ottenere il totale delle scelte possibili quando sono imposti i vincoli della richiesta:

$$6 \cdot 8! \cdot 5 + 4 \cdot 8! \cdot 3 = 1.693.440$$

11.3 Esercizi misti

Per risolvere questi esercizi, vedere i punti 4.5.2, 4.7.4, 4.8.2, 4.8.6, 4.8.8

11.3.1 6 amici e 6 sedie (Ordinamenti, disposizioni semplici)

6 amici, Alessandro, Bruno, Carlo, Daniele, Enrico e Franco prendono posto su una fila di 6 sedie. Calcolare in quanti modi i 6 possono sedersi:

1. Senza restrizioni
2. In modo che Carlo e Franco siedano sulle 2 sedie centrali
3. In modo che Bruno e Carlo siedano vicini

Soluzione:

Indichiamo Alessandro, Bruno, Carlo, Daniele, Enrico e Franco con le lettere a, b, c, d, e ed f rispettivamente. Inoltre chiamiamo M l'insieme degli amici

1. Per sedersi senza restrizione, sicuramente dobbiamo considerare un metodo di calcolo che escluda le ripetizioni. Siccome a noi interessa che ad esempio le coppie (a, b, c, d, e, f) e (a, b, d, c, f, e) vengano contate entrambe, l'ordine conta. Quindi sceglieremo la disposizione semplice:

$$\mathcal{O}_M = D_{6,6} = \frac{6!}{(6-6)!} = \frac{6!}{1} = 6! = 720$$

Ricordando la convenzione che $0! = 1$ Vedere 4.6.2

Inoltre, per chi si ricorda, in questo caso si poteva applicare: $\mathcal{O}_M = 6!$ Per chi non si ricorda, la disposizione fa lo stesso lavoro, niente panico!

2. Per questo caso, c ed f si possono sedere sulle due sedie centrali, ma non abbiamo nessun vincolo in merito al loro ordine, quindi possiamo considerare ??cf?? e ??fc?? come 2 ordinamenti possibili. Dopodiché, gli altri possono sedersi nei restanti sedili, quindi dobbiamo chiederci in quanti modi possiamo ordinare 4 persone distinte sulle restanti 4 sedie. Anche qui possiamo scrivere una disposizione semplice che alla fine non sarà niente meno che un ordinamento del sottoinsieme di M che chiameremo $S = \{a, b, d, e\}$:

$$\mathcal{O}_S = 4! = 24$$

Per considerare tutte le scelte possibili tra loro, consideriamo 24 possibili scelte per ??cf?? e altre 24 per ??fc??, in altre parole, le due scelte sono indipendenti. Abbiamo quindi:

$$2 \cdot 24 = 48$$

modi diversi di sedersi.

3. Qui si applica un discorso simile, ma non uguale al punto precedente. Infatti b e d possono sedersi in posti diversi, che non sono per forza al centro. Per questo problema, non esistono formule nella teoria, quindi serve ragionare. Se consideriamo un *array* di 6 sedie, possiamo prendere la coppia dei 2 e vedere in quanti modi distinti possiamo farli sedere. Otteniamo 5 modi possibili.

In realtà la formula per queste situazioni esiste: chiamiamo il numero di sedie (dim. array) con la variabile d . Chiamiamo la dimensione della coppia c .

La formula è: $d - c + 1$. Infatti $6 - 2 + 1 = 5$. (non confondere d e c con Daniele e Carlo del problema!)

Questo problema capita spesso in programmazione quando abbiamo a che fare con pattern matching, sottosequenze, ecc.ecc.... Per ricordare questo concetto si può pensare al concetto delle "sliding windows".

Dopodiché consideriamo come nel punto precedente che la coppia b e c può anche configurarsi come c e b . Infine, considera nell'esercizio precedente come gli altri possono disporsi, ovvero in 24 modi possibili.

Siccome questi tre casi sono completamente indipendenti tra loro, abbiamo:

$$5 \cdot 2 \cdot 24 = 240$$

modi possibili di sedersi.

11.3.2 Gli outfit di Anna (Scelte successive, disposizioni semplici, combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Anna possiede 11 magliette, 5 paia di pantaloni, 6 paia di scarpe e 2 borsette.

1. In quanti modi diversi Anna può scegliere maglietta, pantaloni, scarpe e borsetta per vestirsi?
2. Anna ha comprato una scarpiera che ha 14 scomparti. In quanti modi diversi Anna può riporre le sue scarpe mettendo ogni paio di scarpe in un diverso scomparto nella scarpiera?
3. Anna parte per 1 weekend al mare e decide di portare con sé 4 magliette, 2 paia di pantaloni, 2 paia di scarpe e 1 borsetta. Quante sono le possibili scelte di questi capi?

Soluzione:

1. Dobbiamo escludere le ripetizioni, assumendo che Anna non indossa 2 scarpe contemporaneamente, oppure ad esempio, che non si metta più di una borsetta per compensare il fatto che non si è messa una maglietta. Per ogni outfit, abbiamo 4 oggetti e per ciascuno di questi oggetti abbiamo 11, 5, 6 e 2 scelte possibili. Possiamo usare il metodo delle scelte successive:

$$11 \cdot 5 \cdot 6 \cdot 2 = 660$$

poiché ogni scelta è indipendente dalle altre.

2. Dobbiamo anche qui escludere le ripetizioni per quanto riguarda le scarpe poiché un ordine che conta due volte lo stesso paio non è valido. Tuttavia, siccome stiamo contando i modi di ordinare le scarpe, dobbiamo avvalerci di una disposizione, per la quale appunto, conta l'ordine. Per questo dobbiamo usare le disposizioni semplici (ovvero senza elementi ripetuti). Infatti ci stiamo chiedendo quanti modi esistono, per disporre 6 paia di scarpe in 14 scomparti, ovvero, stiamo considerando la disposizione semplice di ordine 6 nell'insieme dei 14 scomparti. Consideriamo quindi la formula:

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

dove n rappresenta la cardinalità dell'insieme degli scomparti, ovvero: $n = 14$ e k rappresenta l'ordine, ovvero $k = 6$.

Abbiamo quindi:

$$D_{14,6} = \frac{14!}{(14-6)!} = \frac{14!}{8!} = 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 = 2.162.160$$

possibili ordinamenti. Anna può scegliere tra 2.162.160 modi diversi di riordinare le sue scarpe nella scarpiera.

Quindi, nessun oggetto si ripete (non prendiamo in considerazione una singola disposizione che abbia in 2 scomparti lo stesso paio), ma prendiamo certamente in considerazione tutte le disposizioni che considerano le 6 paia (che infatti saranno sempre le stesse paia di scarpe tra una disposizione e l'altra).

3. Concentriamoci sul primo oggetto: le magliette. Anche qui dobbiamo calcolare quanti modi esistono di scegliere 4 magliette da un insieme più grande di 11 magliette (senza ripetizioni), tuttavia, non possiamo considerare le disposizioni, perché per questo problema, ad esempio, gli insiemi delle magliette (gialla, verde, blu, rosa) e (verde, blu, rosa, gialla) andrebbero conteggiati una sola volta perché sono lo stesso insieme, mentre con una disposizione, questi verrebbero entrambi conteggiati! Per questa ragione ci avvaliamo delle combinazioni semplici, che denotiamo col coefficiente binomiale.

Quindi per le magliette abbiamo:

$$\binom{11}{4} = \frac{11!}{4! \cdot (11-4)!} = \frac{11!}{4! \cdot 7!} = \frac{8 \cdot 9 \cdot 10 \cdot 11}{4!} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

Per i pantaloni abbiamo:

$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{5!}{2! \cdot 3!} = \frac{4 \cdot 5}{2!} = 2 \cdot 5 = 10$$

Per le scarpe:

$$\binom{6}{2} = \frac{6!}{2! \cdot (6-2)!} = \frac{6!}{2! \cdot 4!} = \frac{5 \cdot 6}{2!} = 5 \cdot 3 = 15$$

Per le borsette:

$$\binom{2}{1} = \frac{2!}{1! \cdot (2-1)!} = \frac{2}{1} = 2$$

Il quesito ci chiede essenzialmente in quanti modi diversi possiamo comporre la nostra valigia. Quindi anche qui si tratta di escludere le ripetizioni, perché una valigia con le stesse scelte non costituisce una nuova scelta. Inoltre, anche qui notiamo che basta anche solo che un singolo oggetto (ad esempio una maglietta) sia diversa tra una valigia e un'altra per poter dire che si tratta di due modi diversi di comporre la valigia. Le scelte sono quindi indipendenti tra loro, e pertanto Anna ha:

$$330 \cdot 10 \cdot 15 \cdot 2 = 99.000$$

modi diversi di comporre la sua valigia.

Attenzione: Anche qui, la domanda “*Quante sono le possibili scelte di questi capi?*” è estremamente ambigua perché ammette più risposte, ad esempio si potrebbe pensare che vengano richieste solo le singole disposizioni, oppure che venga richiesto il totale delle scelte possibili, oppure (come nel caso specifico) che chieda quanti modi ci sono di scegliere un set completo composto da 4 magliette, 2 paia di pantaloni, 2 paia di scarpe ed 1 borsetta. Se capitasse una roba del genere in sede d'esame, suggerisco di argomentare la risposta ed eventualmente di chiedere chiarimenti.

11.3.3 PIN degli impiegati (Disposizioni e combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Una ditta associa ad ogni impiegato un codice numerico di 6 cifre. Calcolare il numero dei codici possibili in ciascuno dei casi seguenti.

1. Un codice deve alternare cifre pari a cifre dispari e non può contenere cifre ripetute.
2. Un codice non può cominciare con la cifra 0 ed inoltre la somma delle cifre che lo compongono deve essere pari.
3. Un codice non può contenere la cifra 0 più di due volte.

Soluzione:

1. Per alternare le cifre pari con quelle dispari esistono 2 modi (indichiamo con P le cifre pari e con D le cifre dispari):

1.1 $PDPDPD$:

Qui possiamo usare il metodo delle scelte successive, considerando che per 10 cifre, 5 sono pari e 5 sono dispari. Dobbiamo capire quanti modi possibili ci sono di scegliere 6 cifre da un insieme di 10 cifre, considerando anche il fatto che non possono esserci ripetizioni. Abbiamo quindi:

$$5 \cdot 5 \cdot 4 \cdot 4 \cdot 3 \cdot 3 = 3.600$$

Se invece vogliamo usare una disposizione semplice, possiamo considerare che un numero a 6 cifre con ogni cifra che si alterna tra pari e dispari, avrà sempre 3 cifre pari e 3 cifre dispari. Possiamo quindi considerare quanti modi ci sono di scegliere 3 cifre pari da un insieme di 5 cifre pari:

$$D_{5,3} = \frac{5!}{(5-3)!} = \frac{5!}{2!} = 3 \cdot 4 \cdot 5 = 60$$

Qui usiamo una disposizione e non una combinazione perché ad esempio le coppie (3,5,7) e (3,7,5) andrebbero contate entrambe, ma la combinazione semplice ne conterebbe solo una.

Per le cifre dispari vale lo stesso ragionamento, ovvero $D_{5,3} = 60$. Siccome la scelta delle cifre pari è indipendente dalla scelta delle cifre dispari abbiamo:

$$D_{5,3} \cdot D_{5,3} = 60 \cdot 60 = 3.600$$

1.2 $DPDPDP$:

è identico al primo.

Abbiamo quindi la somma dei due casi: $3.600 + 3.600 = 7.200$ casi possibili.

2. Il trucco qui è notare che la richiesta non impone vincoli sugli elementi ripetuti, e quindi dà per scontato che in un codice le cifre possono ripetersi:

Intanto ragioniamo sul fatto che una somma di numeri pari è sempre pari, mentre una somma di numeri dispari è pari solo se il numero degli addendi dispari è pari. Quindi una somma con numeri pari e dispari è pari solo se il numero di elementi dispari è pari.

Questo ci permette di arrivare ad un vincolo隐含的, ovvero che l'ultima cifra (o comunque una delle 6 cifre) dovrà essere pari oppure dispari, per permettere di avere una somma pari. Quindi per l'ultima cifra possiamo solo avere 5 scelte possibili.

Inoltre per la prima cifra, non possiamo scegliere lo 0, quindi abbiamo solo 9 scelte possibili.

Per le altre cifre invece, non abbiamo il vincolo dello 0, quindi abbiamo 10 scelte possibili, visto che consideriamo anche le ripetizioni: Quindi abbiamo:

$$9 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 5 = 450.000$$

codici possibili.

3. Anche qui consideriamo i codici con ripetizione. Per trovare tutti i codici, dobbiamo prima considerare tutti i codici che non contengono lo 0. Abbiamo quindi:

$$9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 \cdot 9 = 9^6 = 531.441$$

Dobbiamo poi considerare tutti i codici che hanno un solo 0. Quindi dobbiamo innanzitutto chiederci, quanti modi ci sono per mettere una cifra nulla in un insieme di 6 cifre. Anche qui usiamo una combinazione semplice perché in realtà l'ordine in cui viene messa la cifra non conta.

$$\binom{6}{1} = \frac{6!}{1! \cdot (6-1)!} = \frac{6!}{1! \cdot 5!} = 6$$

Dopodiché calcoliamo:

$$9^5 = 59.049$$

Moltiplichiamo il risultato per tutti i modi possibili:

$$59.049 \cdot 6 = 354.294$$

Consideriamo anche il caso con 2 cifre che hanno uno 0. Anche qui, proprio perché l'ordine delle due cifre non conta, la combinazione semplice è il metodo adatto:

$$\binom{6}{2} = \frac{6!}{2! \cdot (6-2)!} = \frac{6!}{2! \cdot 4!} = \frac{5 \cdot 6}{2!} = \frac{30}{2} = 15$$

Infatti non ci interessa contare ad esempio le disposizioni distinte 001234 e 001234 perché sono equivalenti ma una disposizione semplice le conterebbe entrambi. Quindi vanno considerate appunto le combinazioni e non le disposizioni.

Dopodiché calcoliamo:

$$9^4 = 6.561$$

Moltiplichiamo il risultato per tutti i modi possibili:

$$15 \cdot 6.561 = 98.415$$

Per ottenere il risultato sommiamo i tre casi:

$$531.441 + 354.294 + 98.415 = 984.150$$

11.3.4 Scuola di ballo (interessante per il principio di inclusione-esclusione)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Ad un corso di ballo sono iscritti 11 uomini e 9 donne. Si tengono 2 lezioni a settimana, il lunedì ed il giovedì.

1. Se ad una lezione tutti gli studenti sono presenti, quante sono le possibili coppie (uomo-donna) che si possono formare durante la lezione?
2. Per uno spettacolo alla fine del corso i maestri scelgono fra gli studenti 5 uomini e 5 donne per una certa coreografia. Quante sono le scelte possibili di quei 10 studenti?
3. La scorsa settimana ogni studente era presente ad almeno una lezione: al lunedì erano presenti 8 donne e 7 uomini mentre al giovedì erano presenti 7 donne e 9 uomini. Quanti dei 20 studenti erano presenti ad entrambe le lezioni?

Soluzione:

1. Dobbiamo fare estremamente attenzione perché con coppie possibili, l'esercizio ci chiede quante coppie si possono formare, e non quante coppie possono coesistere, andando quindi a discutere il fatto che se tutti ballano in coppia, 2 uomini rimarranno senza una donna. Quindi in questo caso la risposta corretta sarebbe:

$$11 \cdot 9 = 99$$

ovvero, *ogni ballerina può ballare con ogni ballerino* quindi le coppie sono 99.

2. La scelta dei 10 studenti è in realtà composta da 2 scelte indipendenti. Per ciascuna di queste scelte, l'ordine non conta e vale sempre il vincolo sulle ripetizioni. Quindi per gli uomini consideriamo la combinazione semplice:

$$\binom{11}{5} = \frac{11!}{5! \cdot (11-5)!} = \frac{11!}{5! \cdot 6!} = \frac{7 \cdot 8 \cdot 9 \cdot 10 \cdot 11}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = \frac{7 \cdot 2 \cdot 3 \cdot 2 \cdot 11}{2} = 7 \cdot 2 \cdot 3 \cdot 11 = 462$$

Per le donne:

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

Quindi ci sono $462 \cdot 126 = 58.212$ modi di scegliere i 10 studenti.

3. Qui dobbiamo fare un ragionamento profondo per sfruttare la formula di unione tra insiemi. Innanzitutto, consideriamo gli uomini e le donne separatamente. Consideriamo ora il principio di inclusione-esclusione:

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

Quando l'esercizio dice: "ogni studente era presente ad almeno una lezione" ci sta essenzialmente rivelando $|A \cup B|$, il che ci permette di ricavare $|A \cap B|$ dalla formula, ovvero il numero di coloro che hanno partecipato *ad entrambe* le lezioni.

Impostiamo il problema per gli uomini:

definiamo con M_ℓ l'insieme gli uomini presenti il lunedì e con M_g gli uomini presenti il giovedì. Abbiamo quindi:

$|M_\ell| = 7$ e $|M_g| = 9$. Inoltre sappiamo che gli uomini nel corso sono 11 e che tutti erano presenti almeno una volta nella settimana, pertanto: $|M_\ell \cup M_g| = 11$. Possiamo quindi trovare la soluzione:

$$11 = 7 + 9 - |M_\ell \cap M_g|$$

$$11 + |M_\ell \cap M_g| = 7 + 9$$

$$|M_\ell \cap M_g| = 7 + 9 - 11 = 5$$

Per le donne definiamo con D_ℓ e D_g gli insiemi delle donne presenti il lunedì e il giovedì rispettivamente. Abbiamo quindi: $|D_\ell| = 8$, $|D_g| = 7$ e $|D_\ell \cup D_g| = 9$. Pertanto abbiamo come soluzione:

$$|D_\ell \cap D_g| = 8 + 7 - 9 = 6$$

Pertanto gli studenti presenti ad entrambe le lezioni sono $5 + 6 = 11$.

11.3.5 Match di tennis (combinazioni semplici, ordinamenti)

I circoli di tennis “Laver” e “Rosewall” si sfidano su un match di 7 incontri: 4 singolari maschili, 2 singolari femminili ed un doppio misto. Il doppio misto è giocato da tennisti e tenniste già selezionate per i singoli.

1. Il circolo “Laver” ha 8 tennisti e 5 tenniste di buon livello tra cui selezionare la squadra. Quante sono le squadre possibili che il “Laver” può scegliere?
2. Formate le squadre, i partecipanti verranno accoppiati casualmente (tennisti con tennisti e tenniste con tenniste) per i 6 singolari ed un tennista ed una tennista per squadra verranno sorteggiati per il doppio misto. Quanti sono teoricamente i possibili accoppiamenti fra le squadre?
3. I 7 incontri vengono disputati consecutivamente: prima i 4 singoli singoli maschili, poi i 2 singoli femminili, poi il doppio. Quanti sono i possibili ordinamenti dei 7 incontri?

Soluzione:

Non conosco il tennis, ma per fortuna esiste Google!

1. Per giocare agli incontri è necessaria una squadra composta da 4 tennisti e 2 tenniste (1 giocatore per ogni singolo). Come già detto nel testo, per il doppio misto vengono utilizzati giocatori già presenti nella squadra. La scelta della squadra si scomponete in 2 scelte indipendenti, una riguarda la scelta dei tennisti e l'altra riguarda la scelta delle tenniste. Per ognuna di queste scelte, non possiamo avere ripetizioni (i giocatori non si clonano) e non ci interessa l'ordine. Pertanto, per i tennisti, calcoliamo la disposizione semplice:

$$\binom{8}{4} = \frac{8!}{4! \cdot (8-4)!} = \frac{8!}{4! \cdot 4!} = \frac{5 \cdot 6 \cdot 7 \cdot 8}{2 \cdot 3 \cdot 4} = \frac{5 \cdot 2 \cdot 7 \cdot 2}{2} = 5 \cdot 2 \cdot 7 = 70$$

Per le tenniste:

$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{5!}{2 \cdot 3!} = \frac{4 \cdot 5}{2} = 2 \cdot 5 = 10$$

Abbiamo quindi: $70 \cdot 10 = 700$ possibili squadre.

2. Qui chiede essenzialmente di calcolare tutti i possibili accoppiamenti tra squadre, che sono a loro volta composti da scelte indipendenti (i singoli accoppiamenti per ogni match).

Tenendo a mente che le 2 squadre sono composte da 4 tennisti e 2 tenniste, *Google ci conferma* che un giocatore può essere scelto per un solo singolare, quindi non sono ammesse ripetizioni.

Per i tennisti: abbiamo per i singolari $4!$ possibili scelte. L'altra squadra ha a sua volta $4!$ possibili scelte, quindi abbiamo: $4! \cdot 4!$ possibili accoppiamenti

Per le tenniste: abbiamo $2!$ possibili accoppiamenti per i singolari, così come l'altra squadra. Abbiamo quindi $2! \cdot 2!$ possibili accoppiamenti:

Per il doppio misto: abbiamo $4 \cdot 2$ possibili scelte nella prima squadra per sorteggiare i due giocatori per il doppio misto, e l'altra squadra avrà a sua volta $4 \cdot 2$ possibili scelte. Quindi ci sono $4 \cdot 2 \cdot 4 \cdot 2$ possibili accoppiamenti.

Per il totale di tutti gli accoppiamenti:

$$4! \cdot 4! \cdot 2! \cdot 2! \cdot 4 \cdot 2 \cdot 4 \cdot 2 = (4!)^2 \cdot 4^2 \cdot 2^4 = (4!)^2 \cdot 4^2 \cdot 2^2 \cdot 2^2 = (4! \cdot 4 \cdot 4)^2 = (4! \cdot 4^2)^2 = 147.456$$

3. Qui viene richiesto di calcolare quanti modi possibili ci sono di giocare le dispute dei singolari maschili, femminili e i doppi misti. Per calcolare i modi possibili è necessario considerare come scelte indipendenti i singolari maschili, i singolari femminili e i doppi misti. Dobbiamo innanzitutto imporre che non ci siano ripetizioni, perché non si gioca 2 volte lo stesso match, tuttavia qui conta l'ordine. Pertanto, abbiamo per i singolari maschili, il numero di disposizioni semplici: $D_{4,4} = 4! = 24$ possibili modi di organizzare le dispute.

Per i singolari femminili abbiamo $2! = 2$ possibili modi.

Il caso del doppio misto è banale perché ammette 1 solo modo possibile.

Il totale dei modi possibili è quindi: $4! \cdot 2! = 24 \cdot 2 = 48$.

11.3.6 I 16 informatici (combinazioni semplici e con ripetizioni)

Viene formato un gruppo di lavoro costituito da 16 informatici per un progetto europeo a cui partecipano Italia, Francia, Belgio e Spagna.

1. Il gruppo di lavoro sarà denominato con una sigla formata dalle 4 iniziali I, F, B, S delle nazioni coinvolte. Quante sono le possibili sigle?
2. Quante diverse distribuzioni per nazionalità può avere un tale gruppo se si richiede che sia presente almeno 1 membro per ciascuna nazione partecipante?
3. Una volta scelto il gruppo dei 16 informatici, si provvede ad attribuire i compiti: 7 di loro lavoreranno al sottoprogetto 1, 6 al sottoprogetto 2, ed i 3 rimanenti ricopriranno il ruolo di coordinatore tra i 2 progetti, responsabile del budget e responsabile della presentazione dei risultati. In quanti modi in totale si possono attribuire i compiti?

Soluzione:

1. Le possibili sigle, date dall'ordinamento dell'insieme delle lettere I, F, B, S è: $4! = 24$
2. Siccome deve essere presente almeno 1 membro per ognuna delle 4 nazioni partecipanti, per le diverse distribuzioni dobbiamo solo considerare solo 12 persone, perché 4 sono già vincolate. Siccome stiamo cercando le possibili distribuzioni in riferimento alla nazione, l'ordine in cui queste persone compaiono nelle distribuzioni non conta, ma conta soltanto il numero di persone per nazioni. Inoltre, siccome dobbiamo occupare tutte e 12 le posizioni nel gruppo, dobbiamo avere anche più di un informatico per ogni nazione, pertanto il calcolo corretto è quello di una combinazione con ripetizione, ovvero:

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

dove $k = 12$ sono le persone da scegliere, da un insieme $n = 4$ di 4 nazioni. Quindi abbiamo:

$$C'_{4,12} = C_{12+4-1,4-1} = C_{15,3} = \frac{15!}{3! \cdot 12!} = \frac{13 \cdot 14 \cdot 15}{3!} = 13 \cdot 7 \cdot 5 = 455$$

distribuzioni possibili.

3. Il problema chiede di calcolare il prodotto tra più scelte indipendenti tra loro. Calcoliamo ciascuna di queste scelte:

Per decidere in quanti modi possiamo scegliere il gruppo per il sottoprogetto 1, facciamo attenzione a non ragionare come prima, perché qui non possiamo considerare un caso con ripetizioni, perché nessuna persona è clone di un'altra persona. Inoltre, non consideriamo l'ordine con cui vengono disposte le persone, ovvero, un gruppo con 7 persone del tipo $\{1, 2, 3, 4, 5, 6, 7\}$ e un gruppo del tipo $\{1, 2, 4, 5, 7, 6, 3\}$ sono lo stesso gruppo. Quindi applichiamo la formula della combinazione semplice:

$$C_{16,7} = \frac{16!}{7! \cdot (16-7)!} = \frac{16!}{7! \cdot 9!} = \frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = \frac{5 \cdot 11 \cdot 2 \cdot 13 \cdot 2 \cdot 3 \cdot 4}{3!} = 5 \cdot 11 \cdot 2 \cdot 13 \cdot 2 \cdot 4 = 11.440$$

Siccome non ammettiamo ripetizioni, per il prossimo caso dobbiamo considerare solo più $16 - 7 = 9$ persone. Consideriamo i modi possibili di formare il gruppo del sottoprogetto 2 composto da 6 persone. Applichiamo lo stesso metodo per il sottoprogetto 1:

$$C_{9,6} = \frac{9!}{6! \cdot (9-6)!} = \frac{9!}{6! \cdot 3!} = \frac{7 \cdot 8 \cdot 9}{2 \cdot 3} = 7 \cdot 4 \cdot 3 = 84$$

Per il coordinatore tra i 2 progetti abbiamo solo più $9 - 6 = 3$ persone rimanenti da cui scegliere:

$$C_{3,1} = \frac{3!}{1! \cdot (3-1)!} = \frac{3!}{2!} = 3$$

Per il responsabile del budget possiamo solo più scegliere tra 2 persone, quindi ci restano 2 scelte possibili. Per il responsabile della presentazione dei risultati ci resta solamente una scelta.

Abbiamo quindi:

$$11.440 \cdot 84 \cdot 3 \cdot 2 \cdot 1 = 5.765.760$$

modi possibili di organizzare i 16 informatici nei gruppi descritti.

11.3.7 Il chimico profumiere (combinazioni semplici e con ripetizioni)

Un chimico vuole preparare un profumo miscelando in parti uguali, 8 essenze base a sua disposizione.

1. Quante sono in totale le miscele possibili usando 2, 3 o 4 essenze?
2. Una volta scelta la miscela, questa viene commercializzata in scatolette contenenti 6 boccette ciascuna, ognuna delle quali può essere di 4 colori diversi. Quante sono le confezioni possibili se le 6 boccette sono prese a caso?
3. Quante invece sono le confezioni possibili se ogni scatola contiene 3 coppie di boccette dello stesso colore?

Soluzione:

1. Non dobbiamo considerare l'ordine, e inoltre, non possiamo considerare le ripetizioni. Il motivo per cui si scartano le ripetizioni è molto sottile, ma se riflettiamo sulla parte in cui dice “*in parti uguali*” e poi consideriamo una combinazione con ripetizione, allora potremmo avere ad esempio 2 parti di lavanda e 1 di bergamotto, il che violerebbe la richiesta “*in parti uguali*”. Quindi se uno considera il quesito come “...2, 3 o 4 essenze *in parti uguali*” in realtà risulta chiara l'esigenza di evitare ripetizioni. Impostiamo quindi una combinazione semplice per le 2 essenze:

$$\binom{8}{2} = \frac{8!}{2! \cdot (8-2)!} = \frac{8!}{2 \cdot 6!} = \frac{7 \cdot 8}{2} = 7 \cdot 4 = 28$$

per 3 essenze abbiamo:

$$\binom{8}{3} = \frac{8!}{3! \cdot (8-3)!} = \frac{8!}{3! \cdot 5!} = \frac{6 \cdot 7 \cdot 8}{3 \cdot 2 \cdot 1} = 2 \cdot 7 \cdot 4 = 56$$

per 4 essenze:

$$\binom{8}{4} = \frac{8!}{4! \cdot (8-4)!} = \frac{8!}{4! \cdot 4!} = \frac{5 \cdot 6 \cdot 7 \cdot 8}{4 \cdot 3 \cdot 2 \cdot 1} = \frac{5 \cdot 2 \cdot 7 \cdot 4}{2} = 5 \cdot 2 \cdot 7 = 70$$

Notiamo inoltre che il quesito non chiede quante miscele possiamo preparare usando 2, 3 e 4 essenze. Ma piuttosto chiede la somma delle singole casistiche. Quindi nonostante siano scelte indipendenti, anziché calcolare il prodotto calcoleremo la somma:

$$28 + 56 + 70 = 154$$

2. Ci stiamo chiedendo quanti modi possibili ci sono di scegliere 6 boccette di 4 colori diversi. Ovviamente dobbiamo considerare le ripetizioni. L'ordine in questo caso non conta perché 2 scatole aventi le stesse boccette sono considerate identiche, a prescindere da come queste boccette sono disposte al suo interno. Consideriamo quindi la combinazione con ripetizione:

$$C'_{4,6} = C_{6+4-1,4-1} = \frac{(6+4-1)!}{(4-1)! \cdot 6!} = \frac{9!}{3! \cdot 6!} = \frac{7 \cdot 8 \cdot 9}{3!} = \frac{7 \cdot 8 \cdot 9}{3 \cdot 2 \cdot 1} = 7 \cdot 4 \cdot 3 = 84$$

Possiamo quindi produrre fino ad 84 scatole distinte con boccette prese a caso.

3. Anche qui la consegna è **ambigua**: nonostante la soluzione di questo esercizio si aspetti il calcolo di una combinazione senza ripetizioni, nulla nella consegna vieta di considerare scatole che abbiano più coppie dello stesso colore. D'altronde il vincolo è imposto sulle boccette nelle coppie e non sulle coppie nella scatola. Inoltre, non è nemmeno un ragionamento assurdo, visto che nel mondo reale, dei prodotti simili sono ampiamente commercializzati. All'esame, di fronte ad un quesito del genere, è bene chiedere chiarimenti. Ci stiamo chiedendo quante scatole distinte da 3 coppie ciascuna possiamo generare, se abbiamo a disposizione 4 coppie (4 colori) da cui scegliere. Come al punto precedente, l'ordine non conta. Calcoliamo quindi il numero di combinazioni senza ripetizioni:

$$\binom{4}{3} = \frac{4!}{3! \cdot (4-3)!} = \frac{4!}{3!} = 4$$

Possiamo quindi comporre solamente 4 scatole distinte, senza ripetizioni, con i vincoli imposti dal quesito.

11.3.8 Semifinali olimpiche (casi particolari di combinazioni semplici)

ATTENZIONE: QUESTO ESERCIZIO È SU DUE PAGINE

(è troppo grande per una sola pagina)

Alle semifinali olimpiche della gara dei 100 metri piani sono ammessi i 16 tempi migliori delle qualificazioni. I 16 atleti sono poi distribuiti in 2 semifinali di 8 atleti ciascuna. Determinare il numero delle possibili distribuzioni dei 16 atleti nelle 2 semifinali nei casi seguenti:

1. Non si richiede nessuna condizione: tutte le possibilità sono ammesse.
2. I 4 atleti con i tempi migliori devono essere distribuiti equamente nelle 2 semifinali (2 per ciascuna)
3. 9 atleti in semifinale sono europei ed in ciascuna semifinale devono essere presenti non più di 6 atleti europei.

Soluzione:

1. Per calcolare il numero delle possibili distribuzioni dei 16 atleti dobbiamo valutare due scelte. Ognuna di queste scelte rappresenta una semifinale da 8 atleti ciascuna. Per ognuna di queste scelte l'ordine non conta, tuttavia non possiamo ammettere ripetizioni, perché gli umani non sono ancora clonabili. Tenendo conto del metodo delle scelte successive, per la prima semifinale abbiamo 16 atleti da cui scegliere mentre per la seconda ne avremo $16 - 8 = 8$. Per la prima scelta:

$$\binom{16}{8} = \frac{16!}{8! \cdot (16-8)!} = \frac{16!}{8! \cdot 8!} = \frac{9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} = \frac{9 \cdot 5 \cdot 11 \cdot 2 \cdot 13 \cdot 2 \cdot 3 \cdot 2}{3 \cdot 4} = 9 \cdot 5 \cdot 11 \cdot 2 \cdot 13 = 12.870$$

Per la seconda scelta abbiamo: $\binom{8}{8} = 1$

Abbiamo quindi 12.870 possibili distribuzioni.

2. Per tutte le casistiche consideriamo sempre delle combinazioni semplici.

Attenzione a non fare l'errore di scegliere i 4 migliori. Quelli sono già fissati dal quesito, che infatti non ci chiede i modi possibili per individuarli.

Per questi 4 atleti, consideriamo tutti i modi possibili per scegliere una coppia:

$$\binom{4}{2} = \frac{4!}{2! \cdot (4-2)!} = \frac{4!}{2! \cdot 2!} = \frac{2 \cdot 3 \cdot 4}{4} = 6$$

Quindi per la prima semifinale, consideriamo tutti i modi possibili per scegliere $8 - 2 = 6$ atleti dai $16 - 4 = 12$ concorrenti:

$$\binom{12}{6} = \frac{12!}{6! \cdot (12-6)!} = \frac{12!}{6! \cdot 6!} = 924$$

Come per il primo punto, alla seconda semifinale rimangono $\binom{6}{6} = 1$ scelte per gli atleti e $\binom{2}{2} = 1$ scelte per la coppia di atleti coi tempi migliori.

Abbiamo quindi 6 modi per accoppiarli tra di loro e 924 modi per scegliere i restanti 6. Pertanto:

$$6 \cdot 924 = 5.544$$

3. Consideriamo la prima semifinale:

Visto il vincolo, deve avere almeno 3 europei, e al massimo 6. Studiamo i vari casi:

Ricordo che $16 - 9 = 7$

Quando ha 3 europei, allora ha:

$$\binom{9}{3} = \frac{9!}{3! \cdot (9-3)!} = 84$$

scelte possibili tra gli europei e

$$\binom{7}{5} = \frac{7!}{5! \cdot (7-5)!} = 21$$

scelte possibili tra i non europei.

La seconda semifinale raccoglie tutti gli altri quindi non ha scelte.

Quando ha 4 europei, allora ha:

$$\binom{9}{4} = \frac{9!}{4! \cdot (9-4)!} = 126$$

scelte possibili tra gli europei e

$$\binom{7}{4} = \frac{7!}{4! \cdot (7-4)!} = 35$$

scelte possibili tra i non europei.
Quando ha 5 europei, allora ha:

$$\binom{9}{5} = \frac{9!}{5! \cdot (9-5)!} = 126$$

scelte possibili tra gli europei e

$$\binom{7}{3} = \frac{7!}{3! \cdot (7-3)!} = 35$$

scelte possibili tra i non europei.
Quando ha 6 europei, allora ha:

$$\binom{9}{6} = \frac{9!}{6! \cdot (9-6)!} = 84$$

scelte possibili tra gli europei e

$$\binom{7}{2} = \frac{7!}{2! \cdot (7-2)!} = 21$$

scelte possibili tra i non europei.
Quindi abbiamo in realtà

$$2 \cdot (84 \cdot 21) + 2 \cdot (126 \cdot 35) = 12.348$$

Sommiamo i casi perché appunto abbiamo 4 casi distinti, ma non è applicabile il metodo delle scelte successive poiché il numero di scelte possibili per ogni singolo evento è legato all'evento stesso, in particolare, è in funzione del numero di europei. Insomma, non sono scelte collegate l'una con l'altra. A questo punto diventa chiara la richiesta del quesito, ovvero: calcolare la sommatoria di tutte le possibili scelte per ogni caso possibile.

11.4 Principio delle gabbie e dei piccioni

Per risolvere questo esercizio, vedere il punto 4.3.7

11.4.1 Fioraio (principio delle gabbie e dei piccioni, combinazioni semplici e con ripetizioni)

Un fiorista vende rose di 5 colori diversi (rosa, rosse, gialle, bianche e azzurre)

1. Volendo acquistare un mazzo bicolore, quanti sono i possibili abbinamenti di colore?
2. Di quante rose deve essere costituito il mazzo per essere sicuri che ve ne siano almeno 5 dello stesso colore?
3. Quanti mazzi distinti di 12 rose si possono formare se si vuole che tutti i colori siano presenti?

Soluzione:

1. Vogliamo calcolare quanti modi possibili abbiamo per abbinare 2 colori diversi tra loro. Quindi non ammettiamo ripetizioni e non ci interessa l'ordine perché ad esempio un mazzo "rosso-rosa" è uguale ad un mazzo "rosa-rosso". I colori da cui possiamo scegliere sono 5. Calcoliamo quindi la combinazione semplice:

$$\binom{5}{2} = \frac{5!}{2! \cdot (5-2)!} = \frac{5!}{2! \cdot 3!} = \frac{4 \cdot 5}{2} = 2 \cdot 5 = 10$$

Si sottintende un mazzo formato da 2 rose. Se avessimo un mazzo formato da un numero pari di rose, il calcolo cambierebbe.

2. Qui possiamo usare il principio delle gabbie e dei piccioni. Assumendo il caso peggiore in cui il fioraio faccia di tutto per darci tutte le rose di un colore diverso, sappiamo per certo che dalla 6° rosa in poi sarà costretto a darcene una che abbia un colore uguale a una di quelle che ci ha già dato. Usando la formula $n \cdot (k-1) + 1$ abbiamo:

$$5 \cdot (5-1) + 1 = 21$$

Qualunque mazzo con un numero di rose ≥ 21 ha almeno 5 rose dello stesso colore.

3. Qui non conta l'ordine, ma possono esserci ripetizioni. Infatti non possiamo avere mazzi con tutte le rose dello stesso colore, ma dobbiamo avere più rose dello stesso colore nello stesso mazzo.

Dalle 12 rose su cui dobbiamo operare una scelta, dobbiamo sottrarre 5, perché su ognuna di queste 5 rose sarà assegnato un colore diverso così che queste 5 rappresentino tutti e 5 i colori, rispettando così il vincolo della richiesta. Sulle restanti 7 rose, dobbiamo trascurare l'ordine ma imporre ripetizioni. Calcoliamo quindi una combinazione con ripetizione:

$$C'_{5,7} = C_{7+5-1,5-1} = \frac{(7+5-1)!}{(5-1)! \cdot 7!} = \frac{11!}{4! \cdot 7!} = \frac{8 \cdot 9 \cdot 10 \cdot 11}{2 \cdot 3 \cdot 4} = 2 \cdot 3 \cdot 5 \cdot 11 = 330$$

Possiamo quindi comporre 330 mazzi diversi.

11.5 Anagrammi

Per risolvere questo esercizio vedere il punto 4.6.5

11.5.1 Anagrammi con lettere ripetute.

Calcolare il numero degli anagrammi delle parole seguenti:

1. ALGORITMO
2. INFORMATICA
3. TORINO
4. DISPOSIZIONI
5. COROLLARIO

Soluzione:

Questi sono tutti anagrammi con parole ripetute.

1. Per ALGORITMO abbiamo:

$$\frac{9!}{2!} = \frac{9!}{2} = 181.440$$

dove 9 è il numero di lettere e 2 rappresenta la lettera O, ripetuta 2 volte.

$$2. \frac{11!}{2! \cdot 2!} = 9.979.200 \quad 3. \frac{6!}{2!} = 360 \quad 4. \frac{12!}{4! \cdot 2! \cdot 2!} = 4.989.600 \quad 5. \frac{10!}{3! \cdot 2! \cdot 2!} = 151.200$$

12 Esercizi sui numeri interi (sezione 5)

12.1 Divisione euclidea

Per risolvere questo esercizio vai ai punti 5.2 e 5.2.4

12.1.1 Divisione euclidea

Calcolare la divisione euclidea per le seguenti coppie di dividendo a e divisore b :

1. $a = 26.754, b = -307$

2. $a = -29.244, b = 289$

3. $a = 781.116, b = 1.101$

Soluzione (q è il quoziente ed r è il resto) :

1. $q = -87, r = 45$ 2. $q = -102, r = 234$ 3. $q = 709, r = 507$

12.2 MCD e Identità di Bézout

Per risolvere questi esercizi, guarda i punti 5.2.7 e 5.2.8

12.2.1 MCD e identità di Bézout

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Calcolare i seguenti massimi comuni denominatori (*anche detti massimi comuni divisori o più semplicemente MCD*) e realizzare l'identità di Bézout:

- | | |
|----------------------|-------------------------|
| 1. MCD(1.156, 75) | 4. MCD(26.125, 17.043) |
| 2. MCD(1.377, 1.071) | 5. MCD(40.257, 5.439) |
| 3. MCD(3.973, 1.853) | 6. MCD(153.664, 24.321) |

1. MCD(1.156, 75):

$$1.156 = 15 \cdot 75 + 31$$

$$75 = 2 \cdot 31 + 13$$

$$31 = 2 \cdot 13 + 5$$

$$13 = 2 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 = \\ &= (13 - 2 \cdot 5) - 1 \cdot (5 - 1 \cdot 3) = \\ &= (75 - 2 \cdot 31) - 2 \cdot 5 - 1 \cdot 5 + 1 \cdot (13 - 2 \cdot 5) = \\ &= 75 - 2 \cdot 31 - 2 \cdot 5 - 1 \cdot 5 + 13 - 2 \cdot 5 = \\ &= 75 - 2 \cdot 31 - 2 \cdot (31 - 2 \cdot 13) - 1 \cdot (31 - 2 \cdot 13) + 13 - 2 \cdot 5 = \\ &= 75 - 2 \cdot 31 - 2 \cdot 31 + 4 \cdot 13 - 1 \cdot 31 + 2 \cdot 13 + 13 - 2 \cdot 5 = \\ &= 75 - 5 \cdot 31 + 7 \cdot 13 - 2 \cdot 5 = \\ &= 75 - 5 \cdot 31 + 7 \cdot 13 - 2 \cdot (31 - 2 \cdot 13) = \\ &= 75 - 5 \cdot 31 + 7 \cdot 13 - 2 \cdot 31 + 4 \cdot 13 = \\ &= 75 - 7 \cdot 31 + 11 \cdot 13 = \\ &= 75 - 7 \cdot 31 + 11 \cdot (75 - 2 \cdot 31) = \\ &= 75 - 7 \cdot 31 + 11 \cdot 75 - 22 \cdot 31 = \\ &= 75 - 29 \cdot 31 + 11 \cdot 75 = \\ &= 75 - 29 \cdot (1.156 - 15 \cdot 75) + 11 \cdot 75 = \\ &= 75 - 29 \cdot 1.156 + 435 \cdot 75 + 11 \cdot 75 = \\ &= 447 \cdot 75 - 29 \cdot 1.156 = 1 \end{aligned}$$

2. MCD(1.377, 1.071):

$$1.377 = 1 \cdot 1.071 + 306$$

$$1.071 = 3 \cdot 306 + 153$$

$$306 = 2 \cdot 153 + 0$$

$$\begin{aligned} 153 &= 1071 - 3 \cdot 306 = \\ &= 1071 - 3 \cdot (1.377 - 1 \cdot 1.071) = \\ &= 1071 - 3 \cdot 1.377 + 3 \cdot 1.071 = \\ &= 4 \cdot 1.071 - 3 \cdot 1.377 = 153 \end{aligned}$$

3. MCD(3.973,1.853):

$$\begin{aligned}3.973 &= 2 \cdot 1.853 + 267 \\1.853 &= 6 \cdot 267 + 251 \\267 &= 1 \cdot 251 + 16 \\251 &= 15 \cdot 16 + 11 \\16 &= 1 \cdot 11 + 5 \\11 &= 2 \cdot 5 + 1 \\5 &= 5 \cdot 1 + 0\end{aligned}$$

$$\begin{aligned}1 &= 11 - 2 \cdot 5 = \\&= (251 - 15 \cdot 16) - 2 \cdot (16 - 1 \cdot 11) = \\&= 251 - 15 \cdot 16 - 2 \cdot 16 + 2 \cdot 11 = \\&= 251 - 17 \cdot 16 + 2 \cdot 11 = \\&= 251 - 17 \cdot 16 + 2 \cdot (251 - 15 \cdot 16) = \\&= 251 - 17 \cdot 16 + 2 \cdot 251 - 30 \cdot 16 = \\&= 3 \cdot 251 - 47 \cdot 16 = \\&= 3 \cdot 251 - 47 \cdot (267 - 1 \cdot 251) = \\&= 3 \cdot 251 - 47 \cdot 267 + 47 \cdot 251 = \\&= 50 \cdot 251 - 47 \cdot 267 = \\&= 50 \cdot 251 - 47 \cdot (3.973 - 2 \cdot 1.853) = \\&= 50 \cdot 251 - 47 \cdot 3.973 + 94 \cdot 1.853 = \\&= 50 \cdot (1.853 - 6 \cdot 267) - 47 \cdot 3.973 + 94 \cdot 1.853 = \\&= 50 \cdot 1.853 - 300 \cdot 267 - 47 \cdot 3.973 + 94 \cdot 1.853 = \\&= 144 \cdot 1.853 - 300 \cdot 267 - 47 \cdot 3.973 = \\&= 144 \cdot 1.853 - 300 \cdot (3.973 - 2 \cdot 1.853) - 47 \cdot 3.973 = \\&= 144 \cdot 1.853 - 300 \cdot 3.973 + 600 \cdot 1.853 - 47 \cdot 3.973 = \\&= 744 \cdot 1.853 - 347 \cdot 3.973 = 1\end{aligned}$$

4. MCD(26.125,17.043):

$$\begin{aligned}26.125 &= 1 \cdot 17.043 + 9.082 \\17.043 &= 1 \cdot 9.082 + 7.961 \\9.082 &= 1 \cdot 7.961 + 1.121 \\7.961 &= 7 \cdot 1.121 + 114 \\1.121 &= 9 \cdot 114 + 95 \\114 &= 1 \cdot 95 + 19 \\95 &= 5 \cdot 19 + 0\end{aligned}$$

$$\begin{aligned}19 &= 114 - 1 \cdot 95 = \\&= (7.961 - 7 \cdot 1.121) - 1 \cdot (1.121 - 9 \cdot 114) = \\&= 7.961 - 7 \cdot 1.121 - 1 \cdot 1.121 + 9 \cdot 114 = \\&= 7.961 - 8 \cdot 1.121 + 9 \cdot 114 = \\&= 7.961 - 8 \cdot 1.121 + 9 \cdot (7.961 - 7 \cdot 1.121) = \\&= 7.961 - 8 \cdot 1.121 + 9 \cdot 7.961 - 63 \cdot 1.121 = \\&= 10 \cdot 7.961 - 71 \cdot 1.121 = \\&= 10 \cdot (17.043 - 1 \cdot 9.082) - 71 \cdot (9.082 - 1 \cdot 7.961) = \\&= 10 \cdot 17.043 - 10 \cdot 9.082 - 71 \cdot 9.082 + 71 \cdot 7.961 = \\&= 10 \cdot 17.043 - 81 \cdot 9.082 + 71 \cdot 7.961 = \\&= 10 \cdot 17.043 - 81 \cdot 9.082 + 71 \cdot (17.043 - 1 \cdot 9.082) = \\&= 10 \cdot 17.043 - 81 \cdot 9.082 + 71 \cdot 17.043 - 71 \cdot 9.082 = \\&= 81 \cdot 17.043 - 152 \cdot 9.082 = \\&= 81 \cdot 17.043 - 152 \cdot (26.125 - 1 \cdot 17.043) = \\&= 81 \cdot 17.043 - 152 \cdot 26.125 + 152 \cdot 17.043 = \\&= 233 \cdot 17.043 - 152 \cdot 26.125 = 19\end{aligned}$$

5. MCD(40.257,5.439):

$$\begin{aligned}40.257 &= 7 \cdot 5.439 + 2.184 \\5.439 &= 2 \cdot 2.184 + 1.071 \\2.184 &= 2 \cdot 1.071 + 42 \\1.071 &= 25 \cdot 42 + 21 \\42 &= 2 \cdot 21 + 0\end{aligned}$$

$$\begin{aligned}21 &= 1.071 - 25 \cdot 42 = \\&= (5.439 - 2 \cdot 2.184) - 25 \cdot (2.184 - 2 \cdot 1.071) = \\&= 5.439 - 2 \cdot 2.184 - 25 \cdot 2.184 + 50 \cdot 1.071 = \\&= 5.439 - 27 \cdot 2.184 + 50 \cdot 1.071 = \\&= 5.439 - 27 \cdot 2.184 + 50 \cdot (5.439 - 2 \cdot 2.184) = \\&= 5.439 - 27 \cdot 2.184 + 50 \cdot 5.439 - 100 \cdot 2.184 = \\&= 51 \cdot 5.439 - 127 \cdot 2.184 = \\&= 51 \cdot 5.439 - 127 \cdot (40.257 - 7 \cdot 5.439) = \\&= 51 \cdot 5.439 - 127 \cdot 40.257 + 889 \cdot 5.439 = \\&= 940 \cdot 5.439 - 127 \cdot 40.257 = 21\end{aligned}$$

6. MCD($153.664, 24.321$):
 $153.664 = 6 \cdot 24.321 + 7.738$
 $24.321 = 3 \cdot 7.738 + 1.107$
 $7.738 = 6 \cdot 1.107 + 1.096$
 $1.107 = 1 \cdot 1.096 + 11$
 $1.096 = 99 \cdot 11 + 7$
 $11 = 1 \cdot 7 + 4$
 $7 = 1 \cdot 4 + 3$
 $4 = 1 \cdot 3 + 1$
 $3 = 3 \cdot 1 + 0$

$$\begin{aligned}
& 1 = 4 - 1 \cdot 3 = \\
& = (11 - 1 \cdot 7) - 1 \cdot (7 - 1 \cdot 4) = \\
& = 11 - 1 \cdot 7 - 1 \cdot 7 + 1 \cdot 4 = \\
& = 11 - 2 \cdot 7 + 1 \cdot 4 = \\
& = 11 - 2 \cdot 7 + 1 \cdot (11 - 1 \cdot 7) = \\
& = 11 - 2 \cdot 7 + 1 \cdot 11 - 1 \cdot 7 = \\
& = 2 \cdot 11 - 3 \cdot 7 = \\
& = 2 \cdot (1.107 - 1 \cdot 1.096) - 3 \cdot (1.096 - 99 \cdot 11) = \\
& = 2 \cdot 1.107 - 2 \cdot 1.096 - 3 \cdot 1.096 + 297 \cdot 11 = \\
& = 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot 11 = \\
& = 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot (1.107 - 1 \cdot 1.096) = \\
& = 2 \cdot 1.107 - 5 \cdot 1.096 + 297 \cdot 1.107 - 297 \cdot 1.096 = \\
& = 299 \cdot 1.107 - 302 \cdot 1.096 = \\
& = 299 \cdot (24.321 - 3 \cdot 7.738) - 302 \cdot (7.738 - 6 \cdot 1.107) = \\
& = 299 \cdot 24.321 - 897 \cdot 7.738 - 302 \cdot 7.738 + 1.812 \cdot 1.107 = \\
& = 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot 1.107 = \\
& = 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot (24.321 - 3 \cdot 7.738) = \\
& = 299 \cdot 24.321 - 1.199 \cdot 7.738 + 1.812 \cdot 24.321 - 5.436 \cdot 7.738 = \\
& = 2.111 \cdot 24.321 - 6.635 \cdot 7.738 = \\
& = 2.111 \cdot 24.321 - 6.635 \cdot (153.664 - 6 \cdot 24.321) = \\
& = 2.111 \cdot 24.321 - 6.635 \cdot 153.664 + 39.810 \cdot 24.321 = \\
& = 41.921 \cdot 24.321 - 6.635 \cdot 153.664 = 1
\end{aligned}$$

12.2.2 Identità di Bézout

Dire se le seguenti equazioni lineari in 2 variabili ammettono soluzioni in $\mathbb{Z} \times \mathbb{Z}$:

$$\begin{array}{ll} 1. \quad 8X - 11Y = 6 & 3. \quad 9X - 12 = 22 \\ 2. \quad 15X - 6Y = 42 & 4. \quad 28X + 49Y = 91 \end{array}$$

Per risolvere questo esercizio, è sufficiente calcolare l'MCD. Se l'MCD divide il termine noto, allora l'equazione ammette soluzioni.

1. MCD(11,8):

$$11 = 1 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$6 : 1 = 6$$

l'equazione ammette soluzioni.

2. MCD(15,6):

$$15 = 2 \cdot 6 + 3$$

$$6 = 2 \cdot 3 + 0$$

$$42 : 3 = 14$$

l'equazione ammette soluzioni.

3. MCD(12,9):

$$12 = 1 \cdot 9 + 3$$

$$9 = 3 \cdot 3 + 0$$

$$22 : 3 = 7, \bar{3}$$

l'equazione **non** ammette soluzioni.

4. MCD(49,28):

$$49 = 1 \cdot 28 + 21$$

$$28 = 1 \cdot 21 + 7$$

$$21 = 3 \cdot 7 + 0$$

$$91 : 7 = 13$$

l'equazione ammette soluzioni.

12.3 Basi numeriche

Per risolvere questi esercizi vedere nella teoria i punti 5.2.2, 5.2.3 e 5.2.5

12.3.1 Da una base n alla base 10

Convertire in base 10 i seguenti numeri scritti nelle basi indicate:

Per gli ultimi 2 possiamo usare la tabella nel punto 5.2.2

Quindi abbiamo $A = 10$, $B = 11$, $C = 12$ ed $E = 14$.

$$11001_{[2]}, 20110_{[3]}, 13203_{[4]}, 14403_{[5]}, 25034_{[6]}, 57704_{[8]}, 1BA8_{[12]}, E1C45_{[16]}$$

$$\begin{aligned} 11001_{[2]} &= 1_0 \cdot 2^0 + 0_1 \cdot 2^1 + 0_2 \cdot 2^2 + 1_3 \cdot 2^3 + 1_4 \cdot 2^4 = \\ &= 1 + 2^3 + 2^4 = 25_{[10]} \end{aligned} \quad \begin{aligned} 20110_{[3]} &= 0_0 \cdot 3^0 + 1_1 \cdot 3^1 + 1_2 \cdot 3^2 + 0_3 \cdot 3^3 + 2_4 \cdot 3^4 = \\ &= 3 + 3^2 + 2 \cdot 3^4 = 174_{[10]} \end{aligned}$$

$$\begin{aligned} 13203_{[4]} &= 3_0 \cdot 4^0 + 0_1 \cdot 4^1 + 2_2 \cdot 4^2 + 3_3 \cdot 4^3 + 1_4 \cdot 4^4 = \\ &= 3 + 2 \cdot 4^2 + 3 \cdot 4^3 + 4^4 = 483_{[10]} \end{aligned} \quad \begin{aligned} 14403_{[5]} &= 3_0 \cdot 5^0 + 0_1 \cdot 5^1 + 4_2 \cdot 5^2 + 4_3 \cdot 5^3 + 1_4 \cdot 5^4 = \\ &= 3 \cdot 1 + 4 \cdot 5^2 + 4 \cdot 5^3 + 5^4 = 1.228_{[10]} \end{aligned}$$

$$\begin{aligned} 25034_{[6]} &= 4_0 \cdot 6^0 + 3_1 \cdot 6^1 + 0_2 \cdot 6^2 + 5_3 \cdot 6^3 + 2_4 \cdot 6^4 = \\ &= 4 + 3 \cdot 6 + 5 \cdot 6^3 + 2 \cdot 6^4 = 3.694_{[10]} \end{aligned} \quad \begin{aligned} 57704_{[8]} &= 4_0 \cdot 8^0 + 0_1 \cdot 8^1 + 7_2 \cdot 8^2 + 7_3 \cdot 8^3 + 5_4 \cdot 8^4 = \\ &= 4 + 7 \cdot 8^2 + 7 \cdot 8^3 + 5 \cdot 8^4 = 24.516_{[10]} \end{aligned}$$

$$\begin{aligned} 1BA8_{[12]} &= 8_0 \cdot 12^0 + 10_1 \cdot 12^1 + 11_2 \cdot 12^2 + 1_3 \cdot 12^3 = \\ &= 8 + 10 \cdot 12 + 11 \cdot 12^2 + 12^3 = 3.440_{[10]} \end{aligned}$$

$$\begin{aligned} E1C45_{[16]} &= 5_0 \cdot 16^0 + 4_1 \cdot 16^1 + 12_2 \cdot 16^2 + 1_3 \cdot 16^3 + 14_4 \cdot 16^4 = \\ &= 5 + 4 \cdot 16 + 12 \cdot 16^2 + 1 \cdot 16^3 + 14 \cdot 16^4 = 924.741_{[10]} \end{aligned}$$

12.3.2 Dalla base 10 ad una base n

Convertire nelle basi indicate, i numeri scritti in base 10

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE
(è troppo grande per una sola pagina)

- | | |
|-------------------------------|--------------------------------|
| 1. Base 2: 570, 2.095, 11.003 | 4. Base 8: 617, 4.038, 21.639 |
| 2. Base 3: 198, 1.532, 10.707 | 5. Base 12: 455, 6.169, 37.093 |
| 3. Base 4: 221, 3.037, 17.627 | 6. Base 16: 331, 4.773, 35 |

$$\begin{array}{lll}
 \text{1. } 570=285\cdot 2+0_0 & 2.095=1.047\cdot 2+1_0 & 11.003=5.501\cdot 2+1_0 \\
 285=142\cdot 2+1_1 & 1.047=523\cdot 2+1_1 & 5.501=2.750\cdot 2+1_1 \\
 142=71\cdot 2+0_2 & 523=261\cdot 2+1_2 & 2.750=1.375\cdot 2+0_2 \\
 71=35\cdot 2+1_3 & 261=130\cdot 2+1_3 & 1.375=687\cdot 2+1_3 \\
 35=17\cdot 2+1_4 & 130=65\cdot 2+0_4 & 687=343\cdot 2+1_4 \\
 17=8\cdot 2+1_5 & 65=32\cdot 2+1_5 & 343=171\cdot 2+1_5 \\
 8=4\cdot 2+0_6 & 32=16\cdot 2+0_6 & 171=85\cdot 2+1_6 \\
 4=2\cdot 2+0_7 & 16=8\cdot 2+0_7 & 85=42\cdot 2+1_7 \\
 2=1\cdot 2+0_8 & 8=4\cdot 2+0_8 & 42=21\cdot 2+0_8 \\
 1=0\cdot 2+1_9 & 4=2\cdot 2+0_9 & 21=10\cdot 2+1_9 \\
 1000111010 & 2=1\cdot 2+0_{10} & 10=5\cdot 2+0_{10} \\
 & 1=0\cdot 2+1_{11} & 5=2\cdot 2+1_{11} \\
 & 100000101111 & 2=1\cdot 2+0_{12} \\
 & & 1=0\cdot 2+1_{13} \\
 & & 10101011111011
 \end{array}$$

$$\begin{array}{lll}
 \text{2. } 198=66\cdot 3+0_0 & 1.532=510\cdot 3+2_0 & 10.707=3.569\cdot 3+0_0 \\
 66=22\cdot 3+0_1 & 510=170\cdot 3+0_1 & 3.569=1.189\cdot 3+2_1 \\
 22=7\cdot 3+1_2 & 170=56\cdot 3+2_2 & 1.189=396\cdot 3+1_2 \\
 7=2\cdot 3+1_3 & 56=18\cdot 3+2_3 & 396=132\cdot 3+0_3 \\
 2=0\cdot 3+2_4 & 18=6\cdot 3+0_4 & 132=44\cdot 3+0_4 \\
 21100 & 6=2\cdot 3+0_5 & 44=14\cdot 3+2_5 \\
 & 2=0\cdot 3+2_6 & 14=4\cdot 3+2_6 \\
 & 2002202 & 4=1\cdot 3+1_7 \\
 & & 1=0\cdot 3+1_8 \\
 & & 112200120
 \end{array}$$

$$\begin{array}{lll}
 \text{3. } 221=55\cdot 4+1_0 & 3.037=759\cdot 4+1_0 & 17.627=4.406\cdot 4+3_0 \\
 55=13\cdot 4+3_1 & 759=189\cdot 4+3_1 & 4.406=1.101\cdot 4+2_1 \\
 13=3\cdot 4+1_2 & 189=47\cdot 4+1_2 & 1.101=275\cdot 4+1_2 \\
 3=0\cdot 4+3_3 & 47=11\cdot 4+3_3 & 275=68\cdot 4+3_3 \\
 3131 & 11=2\cdot 4+3_4 & 68=17\cdot 4+0_4 \\
 & 2=0\cdot 4+2_5 & 17=4\cdot 4+1_5 \\
 & 233131 & 4=1\cdot 4+0_6 \\
 & & 1=0\cdot 4+1_7 \\
 & & 10103123
 \end{array}$$

$$\begin{array}{lll}
 \text{4. } 617=77\cdot 8+1_0 & 4.038=504\cdot 8+6_0 & 21.639=2.704\cdot 8+7_0 \\
 77=9\cdot 8+5_1 & 504=63\cdot 8+0_1 & 2.704=338\cdot 8+0_1 \\
 9=1\cdot 8+1_2 & 63=7\cdot 8+7_2 & 338=42\cdot 8+2_2 \\
 1=0\cdot 8+1_3 & 7=0\cdot 8+7_3 & 42=5\cdot 8+2_3 \\
 1151 & 7706 & 5=0\cdot 8+5_4 \\
 & & 52207
 \end{array}$$

5. $455 = 37 \cdot 12 + 11_0 \rightarrow B_0$ $37 = 3 \cdot 12 + 1_1$ $3 = 0 \cdot 12 + 3_2$ $31B$	$6.169 = 514 \cdot 12 + 1_0$ $514 = 42 \cdot 12 + 10_1 \rightarrow A_1$ $42 = 3 \cdot 12 + 6_2$ $3 = 0 \cdot 12 + 3_3$ $36A1$	$37.093 = 3.091 \cdot 12 + 1_0$ $3.091 = 257 \cdot 12 + 7_1$ $257 = 21 \cdot 12 + 5_2$ $21 = 1 \cdot 12 + 9_3$ $1 = 0 \cdot 12 + 1_4$ 19571
6. $331 = 20 \cdot 16 + 11_0 \rightarrow B_0$ $20 = 1 \cdot 16 + 4_1$ $1 = 0 \cdot 16 + 1_2$ $14B$	$4.773 = 298 \cdot 16 + 5_0$ $298 = 18 \cdot 16 + 10_1 \rightarrow A_1$ $18 = 1 \cdot 16 + 2_2$ $1 = 0 \cdot 16 + 1_3$ $12A5$	$35.916 = 2.244 \cdot 16 + 12_0 \rightarrow C_0$ $2.244 = 140 \cdot 16 + 4_1$ $140 = 8 \cdot 16 + 12_2 \rightarrow C_2$ $8 = 0 \cdot 16 + 8_3$ $8C4C$

12.4 Numeri primi

Per risolvere questo esercizio, utilizza la tabella al punto: 5.4.2

12.4.1 Scomposizione in fattori primi

Trovare la fattorizzazione come prodotto di primi dei seguenti numeri interi:

224, 1.584, 6.125, 11.343, 17.901, 37.422, 40.033, 69.629, 81.191

224	2	1.584	2	6.125	5	11.343	3	17.901	3
111	2		792	2	1.225	5	3.781	19	5.967
56	2		396	2	245	5	199	199	1.989
28	2		198	2	49	7	1		663
14	2		99	3	7	7		221	13
7	7		33	3	1			17	17
1			11	11				1	
			1						

37.422	2	40.033	7	69.629	7	81.191	11
18.711	3		5.719	7	9.947	7	7.381
6.237	3			817	19	1.421	7
2.079	3			43	43	203	7
693	3					29	29
231	3					1	
77	7						
11	11						
1							

13 Esercizi sulle permutazioni (sezione 6)

13.1 Composizioni e cicli

13.1.1 Composizione di permutazioni

Per risolvere questo esercizio vedere il punto 6.1.5 nella teoria.

Siano date le seguenti permutazioni in \mathcal{S}_7 :

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 1 & 7 & 5 & 6 \end{pmatrix}, \quad \tau : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 6 & 3 & 7 & 4 \end{pmatrix}$$

Calcolare $\sigma^2, \sigma\tau, \tau\sigma, \tau^2, \sigma\tau\sigma, \tau\sigma\tau$

Ricordiamoci che con $\sigma\tau$ si intende $\sigma \circ \tau$ e con σ^2 si intende $\sigma \circ \sigma$.

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

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

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

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

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

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

13.1.2 Da tabella a cicli disgiunti

Per risolvere questo esercizio, vedere il punto 6.2.5 nella teoria.

Determinare la decomposizione in cicli disgiunti delle seguenti permutazioni in \mathcal{S}_8 :

$$\pi_1 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 5 & 7 & 2 & 6 & 4 & 1 \end{pmatrix} \pi_2 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 6 & 2 & 8 & 3 & 5 & 1 & 7 \end{pmatrix}$$

$$\pi_3 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 2 & 7 & 1 & 8 & 4 & 6 \end{pmatrix} \pi_4 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 7 & 8 & 2 & 5 & 1 & 4 \end{pmatrix}$$

Per π_1 notiamo che 6 va in se stesso. Per tutti gli altri, scriviamo il loro percorso. Iniziamo per comodità da 1:

$$(1 \ 3 \ 5 \ 2 \ 8)$$

Notiamo che ci mancano ancora dei numeri. Ricominciamo da 4 (*anche qui si può ripartire da un qualunque numero mancante*):

$$(4 \ 7)$$

Abbiamo finito. Abbiamo quindi:

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

Per le altre permutazioni abbiamo $\pi_2 : (1 \ 4 \ 8 \ 7)(2 \ 6 \ 5 \ 3)$, $\pi_3 : (1 \ 5)(2 \ 3)(4 \ 7)(6 \ 8)$, $\pi_4 : (1 \ 3 \ 7)(2 \ 6 \ 5)(4 \ 8)$

13.2 Scrittura in cicli disgiunti, tipo, parità e periodo

13.2.1 Convertire cicli non disgiunti in cicli disgiunti, tipo e parità

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 6.2.6, 6.3.5, 6.3.6, 6.3.7

Per ciascuna coppia σ, τ di permutazioni in S_n , calcolare la decomposizione in cicli disgiunti, il tipo e la parità di $\sigma, \tau, \sigma\tau, \tau\sigma$

1. $n = 5 : \sigma = (2 \ 4 \ 5)(1 \ 4 \ 3), \tau = (1 \ 3)(2 \ 3 \ 5)$
2. $n = 6 : \sigma = (1 \ 6 \ 2 \ 4)(3 \ 4 \ 6 \ 5), \tau = (2 \ 5)(1 \ 2 \ 4 \ 6)$
3. $n = 7 : \sigma = (2 \ 4 \ 7 \ 1 \ 5 \ 3), \tau = (2 \ 5)(1 \ 5 \ 6 \ 4)(1 \ 2 \ 3 \ 7)$
4. $n = 9 : \sigma = (1 \ 4 \ 9 \ 5)(3 \ 4 \ 6 \ 7)(8 \ 7 \ 2), \tau = (2 \ 8)(3 \ 8 \ 9 \ 1 \ 4 \ 7 \ 6 \ 5)(2 \ 8)$

Soluzione:

1. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix} = (1 \ 5 \ 2 \ 4 \ 3) \\ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (1 \ 3 \ 5 \ 2) \\ \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix} = (2 \ 5 \ 4 \ 3) \\ \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} = (1 \ 2 \ 4 \ 5)\end{aligned}$$

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono (5), (4), (4), (4) rispettivamente.
 σ è pari mentre $\tau, \sigma\tau, \tau\sigma$ sono dispari.

2. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 4 & 6 & 3 & 5 \\ 6 & 4 & 1 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 3 & 5 \end{pmatrix} = (1 \ 6 \ 5 \ 3)(2 \ 4) \\ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 6 & 5 & 1 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix} = (1 \ 5 \ 2 \ 4 \ 6) \\ \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 2 & 1 \\ 3 & 2 & 1 & 5 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 5 & 4 & 6 \end{pmatrix} = (1 \ 3)(4 \ 5) \\ \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 3 & 5 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 5 & 4 & 3 & 2 \end{pmatrix} = (2 \ 6)(3 \ 5)\end{aligned}$$

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono (4, 2), (5), (2, 2), (2, 2) rispettivamente.
 σ è composto da due cicli con stessa parità, quindi è pari.
Per lo stesso motivo sono pari anche $\sigma\tau$ e $\tau\sigma$.
Inoltre τ ha lunghezza 5 quindi è pari.

3. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

σ è già espresso come composizione di cicli disgiunti. Scriviamo comunque la tabella di σ per facilitare i calcoli.

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

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 4 & 5 & 6 & 1 \\ 2 & 3 & 7 & 1 & 6 & 4 & 5 \\ 5 & 3 & 7 & 1 & 6 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 1 & 6 & 4 & 2 \end{pmatrix} = (1 \ 5 \ 6 \ 4)(2 \ 3 \ 7)$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 7 & 1 & 6 & 4 & 2 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 7 & 4 \end{pmatrix} = (1 \ 3)(4 \ 5 \ 6 \ 7)$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 2 & 7 & 3 & 6 & 1 \\ 6 & 1 & 3 & 2 & 7 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 3 & 2 & 7 & 4 & 5 \end{pmatrix} = (1 \ 6 \ 4 \ 2)(5 \ 7)$$

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono (6), (4,3), (2,4), (4,2) rispettivamente.

Quindi $\sigma\tau, \tau\sigma$ sono pari, mentre σ, τ sono dispari.

4. Scriviamo σ e τ in cicli disgiunti e calcoliamo $\sigma\tau$ e $\tau\sigma$:

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

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 3 & 4 & 5 & 6 & 7 & 2 & 9 \\ 4 & 9 & 8 & 7 & 3 & 5 & 6 & 2 & 1 \\ 4 & 9 & 2 & 7 & 3 & 5 & 6 & 8 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 7 & 3 & 5 & 6 & 8 & 1 \end{pmatrix} = (1 \ 4 \ 7 \ 6 \ 5 \ 3 \ 2 \ 9)$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 9 & 2 & 7 & 3 & 5 & 6 & 8 & 1 \\ 6 & 5 & 8 & 2 & 9 & 1 & 7 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 8 & 2 & 9 & 1 & 7 & 3 & 4 \end{pmatrix} = (1 \ 6)(2 \ 5 \ 9 \ 4)(3 \ 8)$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 8 & 9 & 6 & 1 & 7 & 2 & 3 & 5 \\ 7 & 8 & 1 & 5 & 4 & 6 & 9 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 1 & 5 & 4 & 6 & 9 & 2 & 3 \end{pmatrix} = (1 \ 7 \ 9 \ 3)(2 \ 8)(4 \ 5)$$

I tipi di $\sigma, \tau, \sigma\tau, \tau\sigma$ sono (9), (8), (2,4,2), (4,2,2) rispettivamente.

σ è pari, mentre τ è dispari.

Per $\sigma\tau$ calcoliamo: $P = (2 - 1) + (4 - 1) + (2 - 1) = 5$ quindi $\sigma\tau$ è dispari perché 5 è dispari.

Per $\tau\sigma$ P è sempre uguale a 5, quindi $\tau\sigma$ è dispari.

13.2.2 Parità e periodo di permutazioni

Per risolvere questo esercizio vedere i punti 6.3.7 e 6.4.4

Determinare la parità ed il periodo delle permutazioni in \mathcal{S}_n attraverso il loro tipo:

1. $n = 9$: tipo $(2, 3, 4)$, tipo $(3, 3, 3)$
2. $n = 10$: tipo $(3, 7)$, tipo $(2, 2, 2, 3)$
3. $n = 14$: tipo $(3, 11)$, tipo $(2, 4, 7)$, tipo $(4, 4, 6)$
4. $n = 20$: tipo $(3, 5, 6, 6)$, tipo $(8, 12)$, tipo $(2, 2, 2, 2, 2, 3, 4)$

Soluzione:

1. Le permutazioni con tipo $(2, 3, 4)$ hanno $P = (2 - 1) + (3 - 1) + (4 - 1) = 6$ e quindi sono pari.
Il loro periodo è: $\text{mcm}(2, 3, 4) = 12$
Le permutazioni con tipo $(3, 3, 3)$ hanno $P = (3 - 1) + (3 - 1) + (3 - 1) = 6$ e quindi sono pari.
Il loro periodo è: $\text{mcm}(3, 3, 3) = 3$
2. Le permutazioni con tipo $(3, 7)$ sono pari perché 3 e 7 hanno la stessa parità.
Il loro periodo è: $\text{mcm}(3, 7) = 21$
Le permutazioni con tipo $(2, 2, 2, 3)$ hanno $P = (2 - 1) + (2 - 1) + (2 - 1) + (3 - 1) = 5$ e quindi sono dispari.
Il loro periodo è: $\text{mcm}(2, 2, 2, 3) = 6$
3. Le permutazioni con tipo $(3, 11)$ sono pari perché 3 e 11 hanno la stessa parità.
Il loro periodo è: $\text{mcm}(3, 11) = 33$
Le permutazioni con tipo $(2, 4, 7)$ hanno $P = (2 - 1) + (4 - 1) + (7 - 1) = 10$ quindi sono pari.
Il loro periodo è: $\text{mcm}(2, 4, 7) = 28$
Le permutazioni con tipo $(4, 4, 6)$ hanno $P = (4 - 1) + (4 - 1) + (6 - 1) = 11$ quindi sono dispari.
Il loro periodo è: $\text{mcm}(4, 4, 6) = 12$
4. Le permutazioni con tipo $(3, 5, 6, 6)$ hanno $P = (3 - 1) + (5 - 1) + (6 - 1) + (6 - 1) = 16$ quindi sono pari.
Il loro periodo è: $\text{mcm}(3, 5, 6, 6) = 30$
Le permutazioni con tipo $(8, 12)$ sono pari perché 8 e 12 hanno la stessa parità.
Il loro periodo è: $\text{mcm}(8, 12) = 24$
Le permutazioni con tipo $(2, 2, 2, 2, 2, 2, 3, 4)$ hanno $P = 6 \cdot (2 - 1) + (3 - 1) + (4 - 1) = 11$ quindi sono dispari.
Il loro periodo è: $\text{mcm}(2, 2, 2, 2, 2, 2, 3, 4) = 12$

13.3 Numero di cicli, numero di permutazioni (cardinalità)

13.3.1 Numero di cicli nell'insieme delle permutazioni

Per risolvere questo esercizio, vedere nella teoria il punto 6.2.8

Calcolare il numero dei cicli:

1. Di lunghezza 4 in \mathcal{S}_7
2. Di lunghezza 6 in \mathcal{S}_8
3. Di lunghezza 10 in \mathcal{S}_{13}

Soluzione:

1. Abbiamo:

$$\frac{1}{4}D_{7,4} = \frac{1}{4} \cdot \frac{7!}{(7-4)!} = \frac{7!}{4 \cdot 3!} = 5 \cdot 6 \cdot 7 = 210$$

cicli di lunghezza 4 in \mathcal{S}_7 .

2. Abbiamo:

$$\frac{1}{6}D_{8,6} = \frac{1}{6} \cdot \frac{8!}{(8-6)!} = \frac{8!}{6 \cdot 2} = 3 \cdot 4 \cdot 5 \cdot 7 \cdot 8 = 3.360$$

cicli di lunghezza 6 in \mathcal{S}_8 .

3. Abbiamo:

$$\frac{1}{10}D_{13,10} = \frac{1}{10} \cdot \frac{13!}{(13-10)!} = \frac{13!}{10 \cdot 3!} = 103.783.680$$

cicli di lunghezza 10 in \mathcal{S}_{13} .

13.3.2 Numero di permutazioni in base al tipo

Per risolvere questo esercizio, vedere il punto 6.2.9

Calcolare il numero delle permutazioni:

1. Di tipo $(2, 3)$ in \mathcal{S}_6
2. Di tipo $(2, 2, 4)$ in \mathcal{S}_8
3. Di tipo $(3, 3)$ in \mathcal{S}_9
4. Di tipo $(2, 4, 5)$ in \mathcal{S}_{12}
5. Di tipo $(3, 3, 4, 4)$ in \mathcal{S}_{14}

Soluzione:

1. Per calcolare il numero di permutazioni di tipo $(2, 3)$ in \mathcal{S}_6 , riscriviamo il tipo come $(2, 3, 1)$ per ottenere $2 + 3 + 1 = 6$.

Dopodiché applichiamo la formula:

$$\frac{6!}{2 \cdot 3 \cdot 1} = 4 \cdot 5 \cdot 6 = 120$$

2. Il numero di permutazioni di tipo $(2, 2, 4)$ in \mathcal{S}_8 è:

$$\frac{8!}{2^2 \cdot 4 \cdot 2!} = 2 \cdot 3 \cdot 5 \cdot 6 \cdot 7 = 1.260$$

3. Per calcolare il numero di permutazioni di tipo $(3, 3)$ in \mathcal{S}_9 , riscriviamo il tipo come $(3, 3, 1, 1, 1)$.

Applichiamo la formula:

$$\frac{9!}{3^2 \cdot 2! \cdot 1^3 \cdot 3!} = 2 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 3.360$$

4. Per calcolare il numero di permutazioni di tipo $(2, 4, 5)$ in \mathcal{S}_{12} , riscriviamo il tipo come $(2, 4, 5, 1)$:

$$\frac{12!}{2 \cdot 4 \cdot 5 \cdot 1} = 11.975.040$$

5. Il numero di permutazioni di tipo $(3, 3, 4, 4)$ in \mathcal{S}_{14} è:

$$\frac{14!}{3^2 \cdot 4^2 \cdot 2! \cdot 2!} = 151.351.200$$

14 Esercizi sui gruppi (sezione 7)

14.1 Verifica di sottogruppi

14.1.1 Verifica dei sottogruppi del gruppo prodotto

Per risolvere questo esercizio, vedi i punti 3.5.4, 7.1.6 e 7.2.2

Nel gruppo prodotto $\mathbb{R} \times \mathbb{R}$ dire quali dei seguenti sottoinsiemi sono sottogruppi e quali no.

1. $A = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = 2 \cdot x\}$
2. $B = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = x^2\}$
3. $C = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y = x + 1\}$

Soluzione:

Innanzitutto, per quanto detto nella teoria, il gruppo prodotto $\mathbb{R} \times \mathbb{R}$ opera tra i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}, +)$.

Indico con $(\mathbb{R} \times \mathbb{R}, \bullet)$ il gruppo prodotto, con H invece indico un sottogruppo qualunque.

L'elemento neutro in $(\mathbb{R}, +)$ è 0, abbiamo quindi $(0, 0)$ come elemento neutro in $\mathbb{R} \times \mathbb{R}$.

Per ogni $(x, y) \in H$ deve esistere un $(x', y') \in H$ tale che:

$$(x, y) \bullet (x', y') = (0, 0) \in H$$

La condizione impone quindi di verificare che $(0, 0)$ sia presente in H .

Inoltre, controlliamo che per ogni $(x, y), (x', y') \in H$, $(x, y) \bullet (x', y')$ rimanga sempre in H .

1. Verifichiamo che $(0, 0) \in A$:

Ci stiamo chiedendo se $(x, 2 \cdot x) = (0, 0)$, ovvero, se fissato $x = 0$, vale $2 \cdot x = 0$.

La condizione è soddisfatta.

Dopodiché, per ogni $(x, 2 \cdot x) \in A$ deve esistere un $(x', 2 \cdot x') \in A$ tale che:

$$(x, 2 \cdot x) \bullet (x', 2 \cdot x') = (0, 0)$$

La condizione è rispettata per ogni coppia, perché siccome $2 \cdot x$ conserva il segno di x , per ogni x positivo, esiste un x negativo sempre nell'insieme A , ovvero:

$$(x, 2 \cdot x) \bullet (-x, -2 \cdot x) = (0, 0)$$

vale per ogni x . Quindi per ogni x esiste un $-x \in A$.

Inoltre, prese 2 coppie qualunque $(x, 2 \cdot x), (x', 2 \cdot x') \in A$ abbiamo:

$$(x, 2 \cdot x) \bullet (x', 2 \cdot x') = (x + x', 2 \cdot (x + x'))$$

$(x + x', 2 \cdot (x + x')) \in A$ vale sempre poiché $(x + x', 2 \cdot (x + x'))$ rispetta il vincolo imposto.

A è quindi un sottogruppo di $\mathbb{R} \times \mathbb{R}$.

2. $(0, 0)$ esiste in B , poiché la coppia (x, x^2) con $x = 0$ soddisfa la nostra richiesta.

Tuttavia, x^2 restituisce solo valori positivi o nulli, quindi non possiamo soddisfare:

$(x, x^2) \bullet (-x, (-x)^2) = (0, 0)$ per ogni $x \in B$ (infatti funziona solo con $x = 0$)

Quindi B non è un sottogruppo.

3. Verifichiamo che $(0, 0)$ esiste in C :

Siccome dobbiamo ottenere una coppia $(x, x + 1) = (0, 0)$ ci stiamo essenzialmente chiedendo se, fissato $x = 0$ sia vero che:

$x + 1 = 0$, ovvero $0 + 1 = 0$ che è ovviamente impossibile.

Siccome in C non esiste $(0, 0)$, C non è un sottogruppo.

14.1.2 Verifica dei sottogruppi dei gruppi delle permutazioni

Per risolvere questo esercizio vedi i punti 7.1.7 e 6.1.1

Nel gruppo \mathcal{S}_7 delle permutazioni su 7 elementi, dire quali dei seguenti sottoinsiemi sono sottogruppi e quali no:

1. $A = \{\pi \in \mathcal{S}_7 | \pi(4) = 5\}$
2. $B = \{\pi \in \mathcal{S}_7 | \pi(6) = 6\}$
3. $C = \{\pi \in \mathcal{S}_7 | \pi^2 = \text{id}\}$

Soluzione:

Sappiamo che tutti gli S_n sono gruppi con l'operazione di *composizione*. Inoltre, siccome nei 3 quesiti, $n = 7$, sappiamo che il gruppo (S_7, \circ) non è commutativo.

Per l'operazione di composizione \circ in S_7 l'elemento neutro è la funzione identità id_7 .

La funzione identità è quella permutazione che manda tutto in se stesso.

Puoi pensarla come un ciclo vuoto () oppure, se vuoi esagerare, come ad una roba del genere:

$$\text{id}_7 = (1)(2)(3)(4)(5)(6)(7)$$

Indichiamo con H un sottogruppo di (S_7, \circ) .

Inoltre, sappiamo sempre che per ogni permutazione in S_n esiste sempre una sua inversa nello stesso insieme S_n , quindi non dobbiamo preoccuparci di capire se per una qualunque permutazione π l'inversa esiste, ma dobbiamo solo cercare di capire se questa appartiene all'insieme H .

Per ogni permutazione $\pi \in H$ deve esistere un'altra permutazione $\pi^{-1} \in H$, tale che: $\pi \circ \pi^{-1} = \text{id}_7$

Questo implica che id_7 deve esistere in H ($\text{id}_7 \in H$). In altre parole, per ogni:

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

deve esistere in H un π^{-1} tale che:

$$\pi^{-1} \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \pi(1) & \pi(2) & \pi(3) & \pi(4) & \pi(5) & \pi(6) & \pi(7) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \text{id}_7 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}$$

Se non hai capito quanto appena detto vai a vedere i punti 6.1.3 e 6.1.5

Inoltre, controlliamo che per ogni $\pi, \sigma \in H$, $\pi \circ \sigma$ rimanga sempre in H .

1. Il sottoinsieme A non è un sottogruppo perché non contiene id_7 in quanto id_7 non rispetta il criterio $\pi(4) = 5$.

2. In B esiste id_7 poiché id_7 rispetta il criterio $\pi(6) = 6$. Riflettiamo sull'esistenza della permutazione inversa:

L'unico vincolo è che tutte le permutazioni in B mandino 6 in se stesso, pertanto una qualunque permutazione inversa (*pensala come la permutazione che rimette tutto al suo posto*) non ha bisogno di *rimettere a posto* anche il 6 perché non è mai stato *toccato*.

Quindi possiamo dedurre che una qualunque inversa di una permutazione che manda un elemento in se stesso deve a sua volta mandare quell'elemento sempre in se stesso.

Concludiamo quindi che il vincolo $\pi(6) = 6$ non impedisce ad una qualunque inversa π^{-1} di far parte del sottoinsieme.

Inoltre, presi π_1 e π_2 qualunque, siccome né π_1 né π_2 toccano il 6, abbiamo la garanzia che:

$\pi_1 \circ \pi_2 \in B$ sia sempre vero.

B è quindi un sottogruppo.

3. In C esiste per forza id_7 poiché in C sono soltanto ammesse le permutazioni per cui vale $\pi \circ \pi = \text{id}_7$.

Inoltre, sempre per questo fatto, l'inversa di una qualunque permutazione in C è la permutazione stessa, ovvero: $\pi^{-1} = \pi$, quindi l'operazione $\pi \circ \pi^{-1}$ è sempre definita in C .

Tuttavia, se consideriamo due permutazioni π e σ in C con $\pi \neq \sigma$, notiamo che:

in generale $\pi \circ \sigma \notin C$ poiché non abbiamo alcuna garanzia del fatto che per la permutazione $\pi \circ \sigma$ valga: $(\pi \circ \sigma)^2 = \text{id}$

C non è un sottogruppo.

14.1.3 Verifica di sottogruppi astratti

Per risolvere questo esercizio, vedi il punto 3.5.4

Sia G un gruppo. Dire quali dei seguenti sottoinsiemi del gruppo prodotto $G \times G$ sono sottogruppi e quali no:

1. $A = \{(g, g) \in G \times G \mid g \in G\}$
2. $B = \{(g, g^{-1}) \in G \times G \mid g \in G\}$
3. $C = \{(g, e_G) \in G \times G \mid g \in G\}$

Soluzione:

Innanzitutto, per quanto detto nella teoria, il gruppo prodotto $G \times G$ opera tra i gruppi $(G, *)$ e $(G, *)$.

Indico con $(G \times G, \bullet)$ il gruppo prodotto. Con H invece indico un sottogruppo qualunque.

L'elemento neutro di $(G \times G, \bullet)$ è (e_G, e_G) .

Per ogni $(x, y) \in H$ deve esistere un $(x', y') \in H$ tale che: $(x, y) \bullet (x', y') = (e_G, e_G) \in H$.

La condizione impone quindi di verificare che (e_G, e_G) sia presente in H .

Inoltre, controlliamo che per ogni $(x, y), (x', y') \in H$, $(x, y) \bullet (x', y')$ rimanga sempre in H .

Ricordiamoci che $(G, *)$ è un gruppo e che quindi per definizione, ogni $g \in G$ ha un inverso $g^{-1} \in G$ rispetto all'operazione $*$.

1. $e_G \in G$ e quindi la coppia $(g, g) = (e_G, e_G)$ soddisfa il criterio $g \in G$, pertanto l'elemento neutro esiste in A .

L'operazione $(g, g) \bullet (g^{-1}, g^{-1}) = (g * g^{-1}, g * g^{-1}) = (e_G, e_G)$ è sempre definita, poiché la coppia (g^{-1}, g^{-1}) rispetta i criteri per A .

Inoltre, presi $(x, x), (y, y) \in A$ qualunque, abbiamo la garanzia che:

$$(g, g) \bullet (g', g') = (g * g', g * g') = (x, x)$$

con $x \in G$, quindi (x, x) rispetta i criteri per l'insieme A .

A è un sottogruppo.

2. $e_G \in G$ inoltre, e_G ha come inverso se stesso, quindi (e_G, e_G) appartiene ad B in quanto soddisfa i criteri. Nonostante non ci siano garanzie per il fatto che $(G, *)$ sia o meno abeliano, la definizione di elemento inverso ci rassicura sul fatto che se g ha come inverso g^{-1} , allora g^{-1} è unico e g^{-1} ha a sua volta come inverso g e g è unico. Vale quindi: $g * g^{-1} = g^{-1} * g$.

Pertanto l'identità: $(g, g^{-1}) \bullet (g^{-1}, g) = (e_G, e_G)$ è sempre definita in B in quanto (g^{-1}, g) rispetta il vincolo per l'insieme B in quanto g è l'inverso di g^{-1} .

Tuttavia, presi $a, b \in G$ qualunque, l'operazione:

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

non è definita in B , questo perché: $a * b * a^{-1} * b^{-1} \neq e_G$ in quanto non ci sono garanzie che $*$ sia commutativa. In generale:

$$a * b * a^{-1} * b^{-1} \neq a * a^{-1} * b * b^{-1}$$

Quindi B non è un sottogruppo.

3. Nulla vieta $g = e_G$, pertanto $(e_G, e_G) \in C$.

(g^{-1}, e_G) rispetta i criteri per C , pertanto l'operazione $(g, e_G) \bullet (g^{-1}, e_G) = (e_G, e_G)$ è definita in C .

Inoltre, presi $(g, e_G), (g', e_G) \in C$, allora: $(g, e_G) \bullet (g', e_G) = (g * g', e_G)$ e siccome $g * g' \in G$, risulta una chiusura di C rispetto all'operazione \bullet .

C è un sottogruppo.

Se G fosse stato abeliano, allora B sarebbe stato un sottogruppo, in quanto $a^{-1} + b^{-1}$ sarebbe stato un inverso di $a + b$.

14.2 Dimostrazione sui sottogruppi delle permutazioni.

14.2.1 Proprietà dei gruppi e sottogruppi delle permutazioni

Fissiamo $k \in I_{n+1} = \{1, \dots, n+1\}$ e sia $H_k = \{\pi \in S_{n+1} | \pi(k) = k\}$

1. Dimostrare che H_k è un sottogruppo di S_{n+1} ed è isomorfo a S_n
2. Dimostrare che S_{n+1} possiede almeno $n+1$ sottogruppi distinti ciascuno dei quali è isomorfo a S_n
3. Calcolare $H_1 \cap \dots \cap H_{n+1}$

Soluzione:

1. Dato l'insieme I_{n+1} , vogliamo studiare il suo insieme delle permutazioni S_{n+1} .

In particolare ci stiamo chiedendo se l'insieme H_k delle permutazioni, che raccoglie tutte le permutazioni di I_{n+1} , eccetto quelle che operano su k sia un sottogruppo dell'insieme di tutte le permutazioni di I_{n+1} . Siccome non consideriamo la cardinalità dell'insieme di tutte quelle permutazioni che operano su k , possiamo considerare H_k come l'insieme di tutte le permutazioni dell'insieme $I_{n+1} \setminus \{k\}$. La cardinalità di $I_{n+1} \setminus \{k\}$ è quindi:

$|I_{n+1} \setminus \{k\}| = n+1 - 1 = n$, pertanto H_k è a tutti gli effetti l'insieme delle permutazioni S_n , poiché per definizione, possiamo studiare le permutazioni di un insieme attraverso la sua cardinalità. In particolare, H_k e S_n sono legati da una biezione, e siccome H_k e S_n sono entrambi (per definizione) dotati dell'operazione associativa della composizione, tale biezione è a tutti gli effetti un isomorfismo.

S_n è un sottogruppo di S_{n+1} perché condivide lo stesso elemento neutro (*funzione identità*), è chiuso rispetto all'operazione \circ e per ogni permutazione, esiste la sua inversa.

2. I_{n+1} è composto da elementi distinti, pertanto, così come possiamo definire il sottogruppo H_k di tutte le permutazioni, eccetto per quelle che operano su k , possiamo definire altri sottogruppi con la stessa logica, che però anziché escludere k escludono un altro elemento distinto. Ci sono $n+1$ elementi distinti in I_{n+1} e per ciascuno di loro possiamo definire un sottogruppo H_k .
3. Per definizione ogni insieme delle permutazioni non è vuoto perché contiene la funzione identità, quindi l'intersezione tra tutti gli insiemi H , dove ciascuno di questi esclude le permutazioni che operano su un particolare oggetto di I hanno in comune (per definizione di permutazione e di sottogruppo) la funzione identità.

14.3 Verifica di omomorfismi

14.3.1 Verifica di monomorfismi, epimorfismi e isomorfismi I

Dire quali delle seguenti funzioni $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ sono omomorfismi e quali non lo sono.

Nei casi affermativi, discuterne l'iettività e la suriettività:

1. $f((m, n)) = m + n - 1$
2. $f((m, n)) = m^2 - n^2$
3. $f((m, n)) = 2m - 3n$

Soluzione:

Il gruppo $(\mathbb{Z}, +)$ è commutativo e ha come elemento neutro 0.

Il gruppo prodotto $(\mathbb{Z} \times \mathbb{Z}, \bullet)$ ha come elemento neutro $(0, 0)$.

Verifichiamo se $f((m, n) \bullet (a, b)) = f((m, n)) + f((a, b))$

Ricordiamoci che $(m, n) \bullet (a, b) = (m+a, n+b)$, quindi dobbiamo verificare $f((m+a, n+b)) = f((m, n)) + f((a, b))$

1. Abbiamo:

$$\begin{aligned} f((m+a, n+b)) &= m+a+n+b-1 \\ f((m, n)) + f((a, b)) &= m+n-1+a+b-1 = m+a+n+b-2 \\ f((m+a, n+b)) &\neq f((m, n)) + f((a, b)) \text{ quindi } f \text{ non è un isomorfismo.} \end{aligned}$$

2. Abbiamo:

$$\begin{aligned} f((m+a, n+b)) &= (m+a)^2 - (n+b)^2 \\ f((m, n)) + f((a, b)) &= m^2 - n^2 - a^2 - b^2 \\ m^2 + 2ma + a^2 - (n^2 + 2nb + b^2) &= m^2 + 2ma + a^2 - n^2 - 2nb - b^2 \\ m^2 + 2ma + a^2 - n^2 - 2nb - b^2 &\neq m^2 - n^2 - a^2 - b^2 \text{ quindi } f \text{ non è un isomorfismo.} \end{aligned}$$

3. Abbiamo:

$$f((m+a, n+b)) = 2(m+a) - 3(n+b) = 2m + 2a - 3n + 3b$$

$$f((m, n)) + f((a, b)) = 2m - 3n + 2a - 3b$$

$$2m + 2a - 3n + 3b = 2m - 3n + 2a - 3b$$

$$0 = 0$$

f è un isomorfismo. Verifichiamo se è iniettivo: Calcoliamo il nucleo:

Dobbiamo trovare quando $2m - 3n = 0$:

$$2m = 3n$$

Quindi, ognqualvolta la coppia (m, n) è tale per cui il doppio di m è uguale al triplo di n , allora $f((m, n)) = 0$

Pertanto, siccome 0 non è l'unica soluzione possibile, allora f non è iniettiva.

Verifichiamo se è suriettivo:

Ci stiamo chiedendo se un qualunque numero $a \in \mathbb{Z}$ può essere rappresentato come $2m - 3n$

$\text{MCD}(2, 3) = 1$ quindi tutti i multipli di 1 possono essere scritti come $2m - 3n$, pertanto f è suriettiva.

14.3.2 Verifica di monomorfismi, epimorfismi e isomorfismi II

Dire quali delle seguenti funzioni $f : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ sono omomorfismi e quali no.

Nei casi affermativi discuterne l'iniettività e la suriettività.

1. $f(n) = (n - 1, n + 1)$
2. $f(n) = (3n, 0)$
3. $f(n) = (1, 5n)$
4. $f(n) = (2n, -n)$

Soluzione:

Il gruppo $(\mathbb{Z}, +)$ è commutativo e ha come elemento neutro 0.

Il gruppo prodotto $(\mathbb{Z} \times \mathbb{Z}, \bullet)$ ha come elemento neutro $(0, 0)$.

Verifichiamo se $f(n+m) = f(n) \bullet f(m)$

1. Abbiamo:

$$f(n+m) = (n+m-1, n+m+1)$$

$$f(n) \bullet f(m) = (n-1, n+1) \bullet (m-1, m+1) = (n+m-2, n+m+2)$$

$(n+m-1, n+m+1) \neq (n+m-2, n+m+2)$ pertanto f non è un omomorfismo.

2. Abbiamo:

$$f(n+m) = (3(n+m), 0) = (3n+3m, 0)$$

$$f(n) \bullet f(m) = (3n, 0) \bullet (3m, 0) = (3n+3m, 0)$$

pertanto f è un omomorfismo. Vediamo se è iniettivo. Calcoliamo $\ker(f)$:

Dobbiamo trovare quando $f(n) = (0, 0)$. Per il secondo elemento della coppia questo è sempre soddisfatto.

Dobbiamo quindi vedere quando $3n = 0$. Otteniamo $n = 0$ come unica soluzione, pertanto $0 \in \mathbb{Z}$ è l'unica soluzione.

Quindi f è iniettiva. Verifichiamo se è suriettiva:

Ci stiamo chiedendo se con $(3n, 0)$ possiamo rappresentare una qualunque coppia in $\mathbb{Z} \times \mathbb{Z}$.

f non è suriettiva poiché è palese che qualunque coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ con $b \neq 0$ non sia rappresentabile.

3. Abbiamo:

$$f(n+m) = (1, 5(n+m)) = (1, 5n+5m)$$

$$f(n) \bullet f(m) = (1, 5n) \bullet (1, 5m) = (2, 5n+5m) \text{ quindi } f \text{ non è un omomorfismo.}$$

4. Abbiamo:

$$f(n+m) = (2(n+m), -(n+m))$$

$$f(n) \bullet f(m) = (2n, -n) \bullet (2m, -m) = (2n+2m, -n-m) = (2(n+m), -(n+m)) \text{ quindi } f \text{ è un omomorfismo.}$$

Vediamo se è iniettivo. Calcoliamo $\ker(f)$: dobbiamo trovare quando $f(n) = (0, 0)$:

Ci stiamo chiedendo quante (*e quali*) soluzioni ha il sistema:

$$\begin{cases} 2n = 0 \\ -n = 0 \end{cases}$$

$2n = 0$ solo quando $n = 0$, vale lo stesso per $-n$. Quindi f è iniettiva perché 0 è l'unica soluzione.

Vediamo se è suriettivo:

Ci stiamo chiedendo se con $(2n, -n)$ possiamo rappresentare una qualunque coppia in $\mathbb{Z} \times \mathbb{Z}$.

Anche qui ci accorgiamo subito che non è possibile, infatti:

una qualunque coppia $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ con a dispari non è rappresentabile.

14.3.3 Verifica di gruppi e isomorfismi

Sia $(G, *)$ un gruppo. Nell'insieme G si definisca una seconda operazione \circ definita da:

$$x \circ y = y * x \quad \text{per ogni } x, y \in G$$

1. Dimostrare che (G, \circ) è un gruppo.
2. Verificare che la funzione $\omega : (G, *) \rightarrow (G, \circ)$ definita da $\omega(g) = g^{-1}$ è un isomorfismo di gruppi.

Soluzione:

1. Dobbiamo verificare se \circ è associativa, ovvero, se

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

Sostituiamo $(g_1 \circ g_2)$ con $(g_2 * g_1)$ e $(g_2 \circ g_3)$ con $(g_3 * g_2)$ come da definizione di \circ :

$$(g_2 * g_1) \circ g_3 = g_1 \circ (g_3 * g_2)$$

Sostituiamo nuovamente, ovvero scriviamo $(g_2 * g_1) \circ g_3$ come $g_3 * (g_2 * g_1)$ e $g_1 \circ (g_3 * g_2)$ come $(g_3 * g_2) * g_1$:

$$g_3 * (g_2 * g_1) = (g_3 * g_2) * g_1$$

Sappiamo già che $(G, *)$ è un gruppo pertanto sappiamo che qui la proprietà associativa vale, e che quindi conta soltanto l'ordine degli elementi, in quanto fino a prova contraria, $*$ non è commutativa. L'ordine è preservato su entrambi i lati dell'uguaglianza, quindi \circ è associativa.

Dobbiamo inoltre verificare l'esistenza dell'elemento neutro e per \circ , ovvero, preso un $a \in (G, \circ)$ qualunque deve valere:

$$a \circ e = e \circ a = a$$

Siccome per definizione $*$ ha l'elemento neutro, anche se $*$ non è commutativa, per quanto appena visto, la posizione dell'elemento neutro non cambia l'esito dell'operazione.

Quindi di fatto, anche se \circ inverte la posizione degli elementi in $*$, \circ ha come elemento neutro, l'elemento neutro di $*$, ovvero:

$$e_* = e_\circ$$

A questo punto dobbiamo solo assicurarci che ogni elemento in G abbia un inverso rispetto all'operazione \circ , ovvero:

preso un $a \in G$ qualunque deve valere:

$$a^{-1} \circ a = a^{-1} \circ b = e \quad (\text{con } a^{-1} \in G)$$

Anche qui notiamo che l'ordine degli elementi non conta, pertanto ogni elemento di G ha lo stesso elemento neutro, sia per l'operazione $*$ che per l'operazione \circ .

2. Per ogni $g \in (G, *)$, ω deve restituire $g^{-1} \in (G, \circ)$. Come visto nella dimostrazione di (G, \circ) non solo $g_*^{-1} = g_\circ^{-1}$, ma l'ordine dell'inverso non conta, infatti: $g^{-1} * g = g * g^{-1} = g \circ g^{-1} = g^{-1} \circ g = e_G$. Perché ω sia un isomorfismo dev'essere sia iniettivo che suriettivo: calcoliamo il nucleo:
Ci stiamo chiedendo quale $g \in (G, *)$ abbia come inverso $g^{-1} = e_G$
Siccome devono valere:

$$g \circ e = e \circ g = g$$

$$g^{-1} \circ g = g \circ g^{-1} = e \quad (\text{con } g^{-1} \in G)$$

L'unico $g \in (G, *)$ che può soddisfare tali condizioni è $g = e_G$.

Quindi $\ker(\omega) = \{e_G\}$, pertanto ω è iniettivo.

Vogliamo ora verificare se ogniqualvolta $\omega(g) = \omega(a)$, con $g, a \in (G, *)$ allora $g = a$.

Questo fatto si verifica banalmente, dal momento in cui per la definizione di gruppo e più in generale, per la definizione di elemento inverso, se un inverso esiste allora è unico, pertanto due elementi non possono avere la stessa immagine in ω .

Pertanto, ω è un isomorfismo.

15 Esercizi sull'aritmetica modulare (sezione 8)

15.1 Inverso di una classe di resto

Per risolvere questo esercizio, vai al punto 8.2.3

15.1.1 Inverso della classe di resto

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Delle seguenti classi resto dire quali sono invertibili e di quelle invertibili calcolare l'inversa.

- | | | | | | | |
|----------------|----------------|-----------------|-----------------|-----------------|-----------------|------------------|
| 1. $[4]_9$ | 5. $[6]_9$ | 9. $[7]_{10}$ | 13. $[8]_{10}$ | 17. $[2]_{11}$ | 21. $[7]_{12}$ | 25. $[6]_{14}$ |
| 2. $[7]_{15}$ | 6. $[9]_{15}$ | 10. $[9]_{20}$ | 14. $[9]_{21}$ | 18. $[7]_{22}$ | 22. $[10]_{23}$ | 26. $[5]_{24}$ |
| 3. $[15]_{24}$ | 7. $[9]_{29}$ | 11. $[18]_{30}$ | 15. $[19]_{30}$ | 19. $[11]_{32}$ | 23. $[3]_{34}$ | 27. $[10]_{36}$ |
| 4. $[13]_{36}$ | 8. $[23]_{40}$ | 12. $[35]_{42}$ | 16. $[17]_{55}$ | 20. $[39]_{80}$ | 24. $[10]_{95}$ | 28. $[71]_{100}$ |

Soluzione:

1. Per $[4]_9$ abbiamo $\text{MCD}(9,4)=1$
quindi è invertibile:
L'identità di Bézout è: $1=1\cdot 9 - 2\cdot 4$
Calcoliamo $-2 : 9 = 9 \cdot (-1) + 7$
Abbiamo quindi: $[4]_9^{-1} = [7]_9$

2. Per $[7]_{15}$ abbiamo: $\text{MCD}(15,7):$
 $15 = 2\cdot 7 + 1$
 $7 = 7\cdot 1 + 0$
 $\text{MCD}(15,7)=1$ quindi è invertibile:
L'identità di Bézout è: $1 = 1\cdot 15 - 2\cdot 7$
Calcoliamo $-2 : 15 = 15 \cdot (-1) + 13$
Abbiamo quindi $[7]_{15}^{-1} = [13]_{15}$

3. Per $[15]_{24}$ abbiamo $\text{MCD}(24,15):$
 $24 = 1\cdot 15 + 9$
 $15 = 1\cdot 9 + 6$
 $9 = 1\cdot 6 + 3$
 $6 = 2\cdot 3 + 0$
 $\text{MCD}(24,15)=3$
quindi $[15]_{24}$ è uno 0-divisiore,
pertanto non è invertibile.

4. Per $[13]_{36}$ abbiamo $\text{MCD}(36,13):$
 $36 = 2\cdot 13 + 10$
 $13 = 1\cdot 10 + 3$
 $10 = 3\cdot 3 + 1$
 $3 = 3\cdot 1 + 0$
 $\text{MCD}(36,13)=1$ quindi è invertibile:
L'identità di Bézout è:
 $1 = 10 - 3\cdot 3 =$
 $= 36 - 2\cdot 13 - 3 \cdot (13 - 1\cdot 10) =$
 $= 36 - 2\cdot 13 - 3\cdot 13 + 3\cdot 10 =$
 $= 36 - 5\cdot 13 + 3 \cdot (36 - 2\cdot 13) =$
 $= 36 - 5\cdot 13 + 3\cdot 36 - 6\cdot 13 =$
 $= 4\cdot 36 - 11\cdot 13 = 1$
Calcoliamo $-11 : 36 = 36 \cdot (-1) + 25$
Abbiamo quindi $[13]_{36}^{-1} = [25]_{36}$

5. Per $[6]_9$ abbiamo $\text{MCD}(9,6):$
 $9 = 1\cdot 6 + 3$
 $6 = 2\cdot 3 + 0$
 $\text{MCD}(9,6)=3$
quindi $[6]_9$ è uno 0-divisiore,
pertanto non è invertibile.

6. Per $[9]_{15}$ abbiamo $\text{MCD}(15,9):$
 $15 = 1\cdot 9 + 6$
 $9 = 1\cdot 6 + 3$
 $6 = 2\cdot 3 + 0$
 $\text{MCD}(15,9)=3$
quindi $[9]_{15}$ è uno 0-divisiore,
pertanto non è invertibile.

<p>7. Per $[9]_{29}$abbiamo MCD($29,9$):</p> $\begin{aligned} 29 &= 3 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$ <p>MCD($29,9$)=1 quindi è invertibile: L'identità di Bézout è:</p> $\begin{aligned} 1 &= 9 - 4 \cdot 2 = \\ &= 9 - 4 \cdot (29 - 3 \cdot 9) = \\ &= 9 - 4 \cdot 29 + 12 \cdot 9 = \\ &= -4 \cdot 29 + 13 \cdot 9 = 1 \end{aligned}$ <p>Abbiamo quindi $[9]_{29}^{-1} = [13]_{29}$</p>	<p>8. Per $[23]_{40}$abbiamo MCD($40,23$):</p> $\begin{aligned} 40 &= 1 \cdot 23 + 17 \\ 23 &= 1 \cdot 17 + 6 \\ 17 &= 2 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$ <p>MCD($40,23$)=1 quindi è invertibile: L'identità di Bézout è:</p> $\begin{aligned} 1 &= 6 - 1 \cdot 5 = \\ &= (23 - 1 \cdot 17) - 1 \cdot (17 - 2 \cdot 6) = \\ &= (23 - 1 \cdot 17) - 1 \cdot 17 + 2 \cdot 6 = \\ &= 23 - 1 \cdot 17 - 1 \cdot 17 + 2 \cdot (23 - 1 \cdot 17) = \\ &= 23 - 1 \cdot 17 - 1 \cdot 17 + 2 \cdot 23 - 2 \cdot 17 = \\ &= 3 \cdot 23 - 4 \cdot 17 = \\ &= 3 \cdot 23 - 4 \cdot (40 - 1 \cdot 23) = \\ &= 3 \cdot 23 - 4 \cdot 40 + 4 \cdot 23 = \\ &= 7 \cdot 23 - 4 \cdot 40 = \end{aligned}$ <p>Abbiamo quindi $[23]_{40}^{-1} = [7]_{40}$</p>
<p>9. Per $[7]_{10}$abbiamo MCD($10,7$):</p> $\begin{aligned} 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$ <p>MCD($10,7$)=1 quindi è invertibile: L'identità di Bézout è:</p> $\begin{aligned} 1 &= 7 - 2 \cdot 3 = \\ &= 7 - 2 \cdot (10 - 1 \cdot 7) = \\ &= 7 - 2 \cdot 10 + 2 \cdot 7 = \\ &= 3 \cdot 7 - 2 \cdot 10 = 1 \end{aligned}$ <p>Abbiamo quindi $[7]_{10}^{-1} = [3]_{10}$</p>	<p>10. Per $[9]_{20}$abbiamo MCD($20,9$):</p> $\begin{aligned} 20 &= 2 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$ <p>MCD($20,9$)=1 quindi è invertibile: L'identità di Bézout è:</p> $\begin{aligned} 1 &= 9 - 4 \cdot 2 = \\ &= 9 - 4 \cdot (20 - 2 \cdot 9) = \\ &= 9 - 4 \cdot 20 + 8 \cdot 9 = \\ &= +9 \cdot 9 - 4 \cdot 20 = 1 \end{aligned}$ <p>Abbiamo quindi $[9]_{20}^{-1} = [9]_{20}$</p>
<p>11. Per $[18]_{30}$abbiamo MCD($30,18$):</p> $\begin{aligned} 30 &= 2 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$ <p>MCD($30,18$)=6 quindi $[18]_{30}$ è uno 0-divisiore, pertanto non è invertibile.</p>	<p>12. Per $[35]_{42}$abbiamo MCD($42,35$):</p> $\begin{aligned} 42 &= 1 \cdot 35 + 7 \\ 35 &= 5 \cdot 7 + 0 \end{aligned}$ <p>MCD($42,35$)=7 quindi $[35]_{42}$ è uno 0-divisiore, pertanto non è invertibile.</p>
<p>13. Per $[8]_{10}$abbiamo MCD($10,8$):</p> $\begin{aligned} 10 &= 1 \cdot 8 + 2 \\ 8 &= 4 \cdot 2 + 0 \end{aligned}$ <p>MCD($10,8$)=2 quindi $[8]_{10}$ è uno 0-divisiore, pertanto non è invertibile.</p>	<p>14. Per $[9]_{21}$abbiamo MCD($21,9$):</p> $\begin{aligned} 21 &= 2 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$ <p>MCD($21,9$)=3 quindi $[9]_{21}$ è uno 0-divisiore, pertanto non è invertibile.</p>

15. Per $[19]_{30}$ abbiamo $\text{MCD}(30,19)$:
- $$\begin{aligned}30 &= 1 \cdot 19 + 11 \\19 &= 1 \cdot 11 + 8 \\11 &= 1 \cdot 8 + 3 \\8 &= 2 \cdot 3 + 2 \\3 &= 1 \cdot 2 + 1 \\2 &= 2 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(30,19) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$\begin{aligned}1 &= 3 - 1 \cdot 2 = \\&= 11 - 1 \cdot 8 - 1 \cdot 2 = \\&= 11 - 1 \cdot (19 - 1 \cdot 11) - 1 \cdot 2 = \\&= 11 - 1 \cdot 19 + 1 \cdot 11 - 1 \cdot 2 = \\&= 2 \cdot 11 - 1 \cdot 19 - 1 \cdot 2 = \\&= 2 \cdot (30 - 1 \cdot 19) - 1 \cdot 19 - 1 \cdot 2 = \\&= 2 \cdot 30 - 2 \cdot 19 - 1 \cdot 19 - 1 \cdot 2 = \\&= 2 \cdot 30 - 3 \cdot 19 - 1 \cdot (8 - 2 \cdot 3) = \\&= 2 \cdot 30 - 3 \cdot 19 - 1 \cdot 8 + 2 \cdot 3 = \\&= 2 \cdot 30 - 3 \cdot 19 - 1 \cdot (19 - 1 \cdot 11) + 2 \cdot 3 = \\&= 2 \cdot 30 - 3 \cdot 19 - 1 \cdot 19 + 1 \cdot 11 + 2 \cdot 3 = \\&= 2 \cdot 30 - 4 \cdot 19 + 1 \cdot 11 + 2 \cdot (11 - 1 \cdot 8) = \\&= 2 \cdot 30 - 4 \cdot 19 + 1 \cdot 11 + 2 \cdot 11 - 2 \cdot 8 = \\&= 2 \cdot 30 - 4 \cdot 19 + 3 \cdot 11 - 2 \cdot (19 - 1 \cdot 11) = \\&= 2 \cdot 30 - 4 \cdot 19 + 3 \cdot 11 - 2 \cdot 19 + 2 \cdot 11 = \\&= 2 \cdot 30 - 6 \cdot 19 + 5 \cdot 11 = \\&= 2 \cdot 30 - 6 \cdot 19 + 5 \cdot (30 - 1 \cdot 19) = \\&= 2 \cdot 30 - 6 \cdot 19 + 5 \cdot 30 - 5 \cdot 19 = \\&= 7 \cdot 30 - 11 \cdot 19 = 1\end{aligned}$$
- Calcoliamo $-11 : 30 = 30 \cdot (-1) + 19$
Abbiamo quindi $[19]_{30}^{-1} = [19]_{30}$

16. Per $[17]_{55}$ abbiamo $\text{MCD}(55,17)$:
- $$\begin{aligned}55 &= 3 \cdot 17 + 4 \\17 &= 4 \cdot 4 + 1 \\4 &= 1 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(55,17) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$\begin{aligned}1 &= 17 - 4 \cdot 4 = \\&= 17 - 4 \cdot (55 - 3 \cdot 17) = \\&= 17 - 4 \cdot 55 + 12 \cdot 17 = \\&= -4 \cdot 55 + 13 \cdot 17 = 1\end{aligned}$$

Abbiamo quindi $[17]_{55}^{-1} = [13]_{55}$

17. Per $[2]_{11}$ abbiamo $\text{MCD}(11,2)$:
- $$\begin{aligned}11 &= 5 \cdot 2 + 1 \\2 &= 2 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(11,2) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$1 = 11 - 5 \cdot 2$$
- Calcoliamo $-5 : 11 = 11 \cdot (-1) + 6$
Abbiamo quindi $[2]_{11}^{-1} = [6]_{11}$

18. Per $[7]_{22}$ abbiamo $\text{MCD}(22,7)$:
- $$\begin{aligned}22 &= 3 \cdot 7 + 1 \\7 &= 7 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(22,7) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$1 = 22 - 3 \cdot 7$$
- Calcoliamo $-3 : 22 = 22 \cdot (-1) + 19$
Abbiamo quindi $[7]_{22}^{-1} = [19]_{22}$

19. Per $[11]_{32}$ abbiamo $\text{MCD}(32,11)$:
- $$\begin{aligned}32 &= 2 \cdot 11 + 10 \\11 &= 1 \cdot 10 + 1 \\10 &= 1 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(32,11) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$\begin{aligned}1 &= 11 - 1 \cdot 10 = \\&= 11 - 1 \cdot (32 - 2 \cdot 11) = \\&= 11 - 1 \cdot 32 + 2 \cdot 11 = \\&= -1 \cdot 32 + 3 \cdot 11 =\end{aligned}$$
- Abbiamo quindi $[11]_{32}^{-1} = [3]_{32}$

20. Per $[39]_{80}$ abbiamo $\text{MCD}(80,39)$:
- $$\begin{aligned}80 &= 2 \cdot 39 + 2 \\39 &= 19 \cdot 2 + 1 \\2 &= 2 \cdot 1 + 0\end{aligned}$$
- $\text{MCD}(80,39) = 1$ quindi è invertibile:
L'identità di Bézout è:
- $$\begin{aligned}1 &= 39 - 19 \cdot 2 = \\&= 39 - 19 \cdot (80 - 2 \cdot 39) = \\&= 39 - 19 \cdot 80 + 38 \cdot 39 = \\&= -19 \cdot 80 + 39 \cdot 39 = 1\end{aligned}$$
- Abbiamo quindi $[39]_{80}^{-1} = [39]_{80}$

<p>21. Per $[7]_{12}$abbiamo MCD(12,7):</p> $\begin{aligned} 12 &= 1 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \\ \text{MCD}(12,7) &= 1 \text{ quindi è invertibile:} \\ \text{L'identità di Bézout è:} \\ 1 &= 5 - 2 \cdot 2 = \\ &= (12 - 1 \cdot 7) - 2 \cdot (7 - 1 \cdot 5) = \\ &= 12 - 1 \cdot 7 - 2 \cdot 7 + 2 \cdot 5 = \\ &= 12 - 3 \cdot 7 + 2 \cdot 5 = \\ &= 12 - 3 \cdot 7 + 2 \cdot (12 - 1 \cdot 7) = \\ &= 12 - 3 \cdot 7 + 2 \cdot 12 - 2 \cdot 7 = \\ &= +3 \cdot 12 - 5 \cdot 7 = 1 \end{aligned}$ <p>Calcoliamo $-5 : 12 = 12 \cdot (-1) + 7$ Abbiamo quindi $[7]_{12}^{-1} = [7]_{12}$</p>	<p>22. Per $[10]_{23}$abbiamo MCD(23,10):</p> $\begin{aligned} 23 &= 2 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \\ \text{MCD}(23,10) &= 1 \text{ quindi è invertibile:} \\ \text{L'identità di Bézout è:} \\ 1 &= 10 - 3 \cdot 3 = \\ &= 10 - 3 \cdot (23 - 2 \cdot 10) = \\ &= 10 - 3 \cdot 23 + 6 \cdot 10 = \\ &= -3 \cdot 23 + 7 \cdot 10 = \\ \text{Abbiamo quindi } [10]_{23}^{-1} &= [7]_{23} \end{aligned}$
<p>23. Per $[3]_{34}$abbiamo MCD(34,3):</p> $\begin{aligned} 34 &= 11 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \\ \text{MCD}(34,3) &= 1 \text{ quindi è invertibile:} \\ \text{L'identità di Bézout è:} \\ 1 &= 34 - 11 \cdot 3 \\ \text{Calcoliamo } -11 : 34 &= 34 \cdot (-1) + 23 \\ \text{Abbiamo quindi } [3]_{34}^{-1} &= [23]_{34} \end{aligned}$	<p>24. Per $[10]_{95}$abbiamo MCD(95,10):</p> $\begin{aligned} 95 &= 9 \cdot 10 + 5 \\ 10 &= 2 \cdot 5 + 0 \\ \text{MCD}(95,10) &= 5 \\ \text{quindi } [10]_{95} \text{ è uno 0-divisiore,} \\ \text{pertanto non è invertibile.} & \end{aligned}$
<p>25. Per $[6]_{14}$abbiamo MCD(14,6):</p> $\begin{aligned} 14 &= 2 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \\ \text{MCD}(14,6) &= 5 \\ \text{quindi } [6]_{14} \text{ è uno 0-divisiore,} \\ \text{pertanto non è invertibile.} & \end{aligned}$	<p>26. Per $[5]_{24}$abbiamo MCD(24,5):</p> $\begin{aligned} 24 &= 4 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \\ \text{MCD}(24,5) &= 1 \text{ quindi è invertibile:} \\ \text{L'identità di Bézout è:} \\ 1 &= 5 - 1 \cdot 4 = \\ &= 5 - 1 \cdot (24 - 4 \cdot 5) = \\ &= 5 - 1 \cdot 24 + 4 \cdot 5 = \\ &= -1 \cdot 24 + 5 \cdot 5 = \\ \text{Abbiamo quindi } [5]_{24}^{-1} &= [5]_{24} \end{aligned}$
<p>27. Per $[10]_{36}$abbiamo MCD(36,10):</p> $\begin{aligned} 36 &= 3 \cdot 10 + 6 \\ 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0 \\ \text{MCD}(36,10) &= 2 \\ \text{quindi } [10]_{36} \text{ è uno 0-divisiore,} \\ \text{pertanto non è invertibile.} & \end{aligned}$	<p>28. Per $[71]_{100}$abbiamo MCD(100,71):</p> $\begin{aligned} 100 &= 1 \cdot 71 + 29 \\ 71 &= 2 \cdot 29 + 13 \\ 29 &= 2 \cdot 13 + 3 \\ 13 &= 4 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \\ \text{MCD}(100,71) &= 1 \text{ quindi è invertibile:} \\ \text{L'identità di Bézout è:} \\ 1 &= 13 - 4 \cdot 3 = \\ &= (71 - 2 \cdot 29) - 4 \cdot (29 - 2 \cdot 13) = \\ &= 71 - 2 \cdot 29 - 4 \cdot 29 + 8 \cdot 13 = \\ &= 71 - 6 \cdot 29 + 8 \cdot 13 = \\ &= 71 - 6 \cdot 29 + 8 \cdot (71 - 16 \cdot 29) = \\ &= -22 \cdot 29 + 9 \cdot 71 = \\ &= -22 \cdot (100 - 1 \cdot 71) + 9 \cdot 71 = \\ &= -22 \cdot 100 + 22 \cdot 71 + 9 \cdot 71 = \\ &= -22 \cdot 100 + 31 \cdot 71 = \\ \text{Abbiamo quindi } [71]_{100}^{-1} &= [31]_{100} \end{aligned}$

15.2 Funzione φ di Eulero

Per risolvere questo esercizio vedere i punti 8.2.5, 8.2.7 e 8.2.8

Utilizza la tabella dei numeri primi al punto 5.4.2 per risolvere più velocemente alcuni punti.

15.2.1 Calcolare $\varphi(n)$

Calcolare il valore $\varphi(n)$ della funzione di Eulero per i seguenti valori di n :

124, 245, 300, 320, 408, 667, 820, 837, 1.350, 1.375, 3.969

Soluzione:

Scomponiamo tutti i numeri:

124	2	245	5	300	5	320	5	408	2	3.969	3
62	2	49	7	60	5	64	2	204	2	1.323	3
31	31	7	7	12	3	32	2	102	2	441	3
1				4	2	16	2	51	3	147	3
				2	2	8	2	17	17	49	7
				1		4	2	1		7	7
						2	2			1	
						1					
667	23	820	2	837	3	1.350	5	1.375	5		
29	29	410	2	279	3	270	5	275	5		
1		205	5	93	3	54	3	55	5		
		41	41	31	31	18	3	11	11		
		1		1		6	3	1			
						2	2				
						1					

Quindi calcoliamo:

$$\varphi(124) = \varphi(2^2 \cdot 31) = \varphi(2^2) \cdot 30 = 2 \cdot 30 = 60$$

$$\varphi(245) = \varphi(7^2 \cdot 5) = \varphi(7^2) \cdot 4 = 7 \cdot 6 \cdot 4 = 168$$

$$\varphi(300) = \varphi(5^2 \cdot 3 \cdot 2^2) = \varphi(5^2) \cdot \varphi(2^2) \cdot 2 = 5 \cdot 4 \cdot 2 \cdot 2 = 80$$

$$\varphi(320) = \varphi(5 \cdot 2^6) = 4 \cdot \varphi(2^6) = 4 \cdot 2^5 = 128$$

$$\varphi(408) = \varphi(17 \cdot 3 \cdot 2^3) = 16 \cdot 2 \cdot 2^2 = 128$$

$$\varphi(3.969) = \varphi(7^2 \cdot 3^4) = 7 \cdot 6 \cdot 3^3 \cdot 2 = 2.268$$

$$\varphi(667) = \varphi(23 \cdot 29) = 22 \cdot 28 = 616$$

$$\varphi(820) = \varphi(41 \cdot 5 \cdot 2^2) = 40 \cdot 4 \cdot 2 = 320$$

$$\varphi(837) = \varphi(31 \cdot 3^3) = 30 \cdot 3^2 \cdot 2 = 540$$

$$\varphi(1.350) = \varphi(5^2 \cdot 3^3 \cdot 2) = 5 \cdot 4 \cdot 3^2 \cdot 2 = 360$$

$$\varphi(1.375) = \varphi(11 \cdot 5^3) = 10 \cdot 5^2 \cdot 4 = 1.000$$

15.3 Congruenze lineari

15.3.1 Risoluzione di congruenze lineari

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 8.2.3 e 8.3.2

Dire quali delle seguenti congruenze lineari sono risolvibili e in caso in cui lo siano, elencare tutte le soluzioni.

- | | | | |
|----------------------------|----------------------------|-----------------------------|-------------------------------|
| 1. $3X \equiv 5 \pmod{10}$ | 4. $6X \equiv 7 \pmod{12}$ | 7. $8X \equiv 6 \pmod{14}$ | 10. $2X \equiv 10 \pmod{15}$ |
| 2. $3X \equiv 8 \pmod{20}$ | 5. $7X \equiv 2 \pmod{21}$ | 8. $10X \equiv 6 \pmod{24}$ | 11. $15X \equiv 5 \pmod{25}$ |
| 3. $6X \equiv 9 \pmod{30}$ | 6. $7X \equiv 8 \pmod{40}$ | 9. $9X \equiv 11 \pmod{54}$ | 12. $12X \equiv 16 \pmod{64}$ |

1. $3X \equiv 5 \pmod{10}$:

Calcoliamo MCD(10,3):

$$10 = 3 \cdot 3 + 1$$

$$3 = 1 \cdot 3 + 0$$

MCD(10,3) = 1 quindi possiamo procedere:

L'identità di Bézout è: $1 = 10 - 3 \cdot 3$

Calcoliamo $-1 : 10 = 10 \cdot (-1) + 9$

Abbiamo quindi $[3]_{10}^{-1} = [9]_{10}$

Calcoliamo: $9 \cdot 5 = 45$

$$45 : 10 = 10 \cdot 4 + 5$$

$$X \equiv 5 \pmod{10}$$

2. $3X \equiv 8 \pmod{20}$:

Calcoliamo MCD(20,3):

$$20 = 6 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 1 \cdot 1 + 0$$

MCD(20,3) = 1

quindi possiamo procedere:

L'identità di Bézout è:

$$1 = 3 - 1 \cdot 2 =$$

$$= 3 - 1 \cdot (20 - 6 \cdot 3) =$$

$$= 3 - 1 \cdot 20 + 6 \cdot 3 =$$

$$= -1 \cdot 20 + 7 \cdot 3 = 1$$

Abbiamo quindi $[3]_{20}^{-1} = [7]_{20}$

Calcoliamo: $7 \cdot 8 = 56$

$$56 : 20 = 20 \cdot 2 + 16$$

$$X \equiv 16 \pmod{20}$$

3. $6X \equiv 9 \pmod{30}$:

Calcoliamo MCD(30,6):

$$30 = 5 \cdot 6 + 0$$

$$\text{MCD}(30,6) = 6$$

6 non divide 9,

Non esistono soluzioni per X

4. $6X \equiv 7 \pmod{12}$:

Calcoliamo MCD(12,6):

$$12 = 2 \cdot 6 + 0$$

$$\text{MCD}(12,6) = 6$$

6 non divide 7.

Non esistono soluzioni per X

5. $7X \equiv 2 \pmod{21}$:
 Calcoliamo MCD(21,7):
 $21 = 3 \cdot 7 + 0$
 $\text{MCD}(21,7) = 7$
 7 non divide 2
 Non esistono soluzioni per X

6. $7X \equiv 8 \pmod{40}$:
 Calcoliamo MCD(40,7):
 $40 = 5 \cdot 7 + 5$
 $7 = 1 \cdot 5 + 2$
 $5 = 2 \cdot 2 + 1$
 $2 = 2 \cdot 1 + 0$
 $\text{MCD}(40,7) = 1$
 quindi possiamo procedere:
 $1 = 5 - 2 \cdot 2 =$
 $= (40 - 5 \cdot 7) - 2 \cdot (7 - 1 \cdot 5) =$
 $= 40 - 5 \cdot 7 - 2 \cdot 7 + 2 \cdot 5 =$
 $= 40 - 7 \cdot 7 + 2 \cdot 5 =$
 $= 40 - 7 \cdot 7 + 2 \cdot (40 - 5 \cdot 7) =$
 $= 40 - 7 \cdot 7 + 2 \cdot 40 - 10 \cdot 7 =$
 $= -17 \cdot 7 + 3 \cdot 40 = 1$
 Calcoliamo:
 $-17 : 40 = 40 \cdot (-1) + 23$
 $23 \cdot 8 = 184$
 $184 : 40 = 40 \cdot 4 + 24$
 $X \equiv 24 \pmod{40}$

7. $8X \equiv 6 \pmod{14}$:
 Calcoliamo MCD(14,8):
 $14 = 1 \cdot 8 + 6$
 $8 = 1 \cdot 6 + 2$
 $6 = 3 \cdot 2 + 0$
 $\text{MCD}(14,8) = 2$
 2 divide 6 quindi possiamo procedere:
 Dividiamo tutti i termini noti per 2.
 Risolviamo: $4X \equiv 3 \pmod{7}$:
 Calcoliamo MCD(7,4):
 $7 = 1 \cdot 4 + 3$
 $4 = 1 \cdot 3 + 1$
 $3 = 3 \cdot 1 + 0$
 $\text{MCD}(7,4) = 1$
 $1 = 4 - 1 \cdot 3 =$
 $= 4 - 1 \cdot (7 - 1 \cdot 4) =$
 $= 4 - 1 \cdot 7 + 1 \cdot 4 =$
 $= -1 \cdot 7 + 2 \cdot 4 = 1$
 Otteniamo quindi la classe di resto $[6]_7$
 X ha esattamente 2 soluzioni:
 Calcoliamo la seconda soluzione: $6 + 7 = 13$
 Le soluzioni sono:
 $X \equiv 6 \pmod{14}$ e $X \equiv 13 \pmod{14}$

8. $10X \equiv 6 \pmod{24}$:
 Calcoliamo MCD(24,10):
 $24 = 2 \cdot 10 + 4$
 $10 = 2 \cdot 4 + 2$
 $4 = 2 \cdot 2 + 0$
 $\text{MCD}(24,10) = 2$
 2 divide 6 quindi possiamo procedere:
 Dividiamo tutti i termini noti per 2.
 Risolviamo: $5X \equiv 3 \pmod{12}$
 Calcoliamo MCD(12,5):
 $12 = 2 \cdot 5 + 2$
 $5 = 2 \cdot 2 + 1$
 $2 = 2 \cdot 1 + 0$
 $\text{MCD}(12,5) = 1$
 $1 = 5 - 2 \cdot 2 =$
 $= 5 - 2 \cdot (12 - 2 \cdot 5) =$
 $= 5 - 2 \cdot 12 + 4 \cdot 5 =$
 $= -2 \cdot 12 + 5 \cdot 5 = 1$
 Calcoliamo $5 \cdot 3 = 15$ quindi: $[15]_{24}$
 X ha esattamente 2 soluzioni:
 Calcoliamo la seconda soluzione:
 $15 + 12 = 27$
 Riduciamo la soluzione:
 $27 : 24 = 24 \cdot 1 + 3$
 Le soluzioni sono:
 $X \equiv 15 \pmod{24}$ e $X \equiv 3 \pmod{24}$

<p>9. $9X \equiv 11 \pmod{54}$: Calcoliamo MCD(54,9): $54 = 6 \cdot 9 + 0$ $\text{MCD}(54,9) = 9$ 9 non divide 11, Non esistono soluzioni per X</p>	<p>10. $2X \equiv 10 \pmod{15}$: Calcoliamo MCD(15,2): $15 = 7 \cdot 2 + 1$ $2 = 2 \cdot 1 + 0$ $\text{MCD}(15,2) = 1$ quindi possiamo procedere: L'identità di Bézout è: $1 = 15 - 7 \cdot 2$ Calcoliamo: $-7 : 15 = 15 \cdot (-1) + 8$ Calcoliamo: $8 \cdot 10 = 80$ Adattiamo la soluzione: $80 : 15 = 15 \cdot 5 + 5$ $X \equiv 5 \pmod{15}$</p>
<p>11. $15X \equiv 5 \pmod{25}$: Calcoliamo MCD(25,15): $25 = 1 \cdot 15 + 10$ $15 = 1 \cdot 10 + 5$ $10 = 2 \cdot 5 + 0$ $\text{MCD}(25,15) = 5$ 5 divide 15 quindi possiamo procedere: Dividiamo tutti i termini noti per 5. Risolviamo: $3X \equiv 1 \pmod{5}$: Calcoliamo MCD(5,3): $5 = 1 \cdot 3 + 2$ $3 = 1 \cdot 2 + 1$ $2 = 2 \cdot 1 + 0$ $\text{MCD}(5,3) = 1$ $1 = 3 - 1 \cdot 2 =$ $= 3 - 1 \cdot (5 - 1 \cdot 3) =$ $= 3 - 1 \cdot 5 + 1 \cdot 3 =$ $= -1 \cdot 5 + 2 \cdot 3 = 1$ Otteniamo quindi la classe di resto $[2]_5$ X ha esattamente 5 soluzioni: Calcoliamo la seconda soluzione: $2 + 5 = 7$ Calcoliamo la terza soluzione: $7 + 5 = 12$ Calcoliamo la quarta soluzione: $12 + 5 = 17$ Calcoliamo la quinta soluzione: $17 + 5 = 22$ Le soluzioni sono: $X \equiv 2 \pmod{25}$, $X \equiv 7 \pmod{25}$, $X \equiv 12 \pmod{25}$, $X \equiv 17 \pmod{25}$ e $X \equiv 22 \pmod{25}$</p>	<p>12. $12X \equiv 16 \pmod{64}$: Calcoliamo MCD(64,12): $64 = 5 \cdot 12 + 4$ $12 = 3 \cdot 4 + 0$ $\text{MCD}(64,12) = 4$ 4 divide 16 quindi possiamo procedere: Dividiamo tutti i termini noti per 4. Risolviamo: $3X \equiv 4 \pmod{16}$: Calcoliamo MCD(16,3): $16 = 5 \cdot 3 + 1$ $3 = 3 \cdot 1 + 0$ $\text{MCD}(16,3) = 1$ L'identità di Bézout è: $1 = 16 - 5 \cdot 3$ Calcoliamo: $-5 : 16 = 16 \cdot (-1) + 11$ Calcoliamo: $11 \cdot 4 = 44$ Adattiamo la soluzione: $44 : 16 = 16 \cdot 2 + 12$ X ha esattamente 4 soluzioni: Calcoliamo la seconda soluzione: $12 + 16 = 28$ Calcoliamo la terza soluzione: $28 + 16 = 44$ Calcoliamo la quarta soluzione: $44 + 16 = 60$ Le soluzioni sono: $X \equiv 12 \pmod{64}$, $X \equiv 28 \pmod{64}$, $X \equiv 44 \pmod{64}$ e $X \equiv 60 \pmod{64}$</p>

15.4 Applicazioni pratiche

15.4.1 Criteri di divisibilità

Per risolvere questo esercizio, vedere il punto 8.4.1

Dei seguenti numeri, dire quali sono divisibili per 2, 3, 5, 9 e 11.

1. 372.405.912.042 2. 2.517.090.248.794 3. 74.100.761.224.335 4. 9.113.703.764.402

Soluzione:

1. È divisibile per 2 perché la sua ultima cifra è pari.

La somma delle sue cifre è:

$$3 + 7 + 2 + 4 + 0 + 5 + 9 + 1 + 2 + 0 + 4 + 2 = 39$$

È divisibile per 3 perché 39 è divisibile per 3.

non è divisibile per 5 perché

la sua ultima cifra non è né 5 né 0.

non è divisibile per 9 perché

la somma delle sue cifre non è divisibile per 9.

La somma delle cifre in posizione pari è:

$$2 + 0 + 1 + 5 + 4 + 7 = 19$$

La somma delle cifre in posizione dispari è:

$$4 + 2 + 9 + 0 + 2 + 3 = 20$$

non è divisibile per 11 perché:

$$20 - 19 = 1 \text{ e } 1 \text{ non è divisibile per 11.}$$

3. Non è divisibile per 2.

la somma delle sue cifre è 45.

è divisibile per 3.

è divisibile per 5 perché termina con 5.

è divisibile per 9.

La somma delle cifre in posizione pari è:

$$5 + 3 + 2 + 1 + 7 + 0 + 4 = 22$$

La somma delle cifre in posizione dispari è:

$$3 + 4 + 2 + 6 + 0 + 1 + 7 = 22$$

non è divisibile per 11.

2. È divisibile per 2.

la somma delle sue cifre è 58.

non è divisibile per 3.

non è divisibile per 5.

non è divisibile per 9.

La somma delle cifre in posizioni pari è:

$$4 + 7 + 4 + 0 + 0 + 1 + 2 = 18$$

La somma delle cifre in posizioni dispari è:

$$9 + 8 + 2 + 9 + 7 + 5 = 40$$

è divisibile per 11 perché $40 - 18 = 22$

4. È divisibile per 2.

la somma delle sue cifre è 47.

non è divisibile per 3.

non è divisibile per 5.

non è divisibile per 9.

La somma delle cifre in posizione pari è:

$$2 + 4 + 6 + 3 + 7 + 1 + 9 = 32$$

La somma delle cifre in posizione dispari è:

$$0 + 4 + 7 + 0 + 3 + 1 = 15$$

non è divisibile per 11.

15.4.2 Determinare l'ultima cifra di un numero (classi di resto modulo 10^n)

Per risolvere questo esercizio vedere il punto 8.4.2

Determinare la cifra finale dei seguenti numeri:

$$3^{755.042}, \quad 3^{905.041} + 7^{448.065}, \quad 13^{899.243} - 3^{577.097}, \quad 7^{299.047} - 4^{377.001}$$

Soluzione:

Calcoliamo $\varphi(10) = \varphi(5 \cdot 2) = \varphi(5) \cdot \varphi(2) = (5 - 1) \cdot (2 - 1) = 4$

1. Per $3^{755.042}$ calcoliamo

$$3^{755.042 \bmod \varphi(10)} \equiv r \bmod 10$$

Calcoliamo quindi $755.042 \bmod 4$:

$755.042 : 4 = 4 \cdot 188.760 + 2$. Per trovare l'ultima cifra è quindi sufficiente calcolare:

$$3^2 \equiv r \bmod 10$$

$9 : 10 = 10 \cdot 0 + 9$. L'ultima cifra di $3^{755.042}$ è 9.

2. Per $3^{905.041} + 7^{448.065}$ calcoliamo prima le singole cifre e successivamente le sommiamo:

Per $3^{905.041}$ calcoliamo: $905.041 : 4 = 4 \cdot 226.260 + 1$. Quindi risolviamo:

$$3 \equiv r \bmod 10$$

L'ultima cifra di $3^{905.041}$ è 3. Per $7^{448.065}$ calcoliamo:

$448.065 : 4 = 4 \cdot 112.016 + 1$. Quindi risolviamo:

$$7 \equiv r \bmod 10$$

L'ultima cifra di $7^{448.065}$ è 7. La somma è quindi $3 + 7 = 10$, ma siccome a noi interessa solo l'ultima cifra:

L'ultima cifra di $3^{905.041} + 7^{448.065}$ è 0.

3. Usiamo lo stesso approccio del punto precedente. Per $13^{899.243}$ calcoliamo:

$899.243 : 4 = 4 \cdot 224.810 + 3$. Quindi risolviamo:

$$13^3 \equiv r \bmod 10$$

$13^3 : 10 = 10 \cdot 219 + 7$. L'ultima cifra di $13^{899.243}$ è 7.

Per $3^{577.097}$ calcoliamo:

$577.097 : 4 = 4 \cdot 144.274 + 1$. Quindi risolviamo:

$$3 \equiv r \bmod 10$$

L'ultima cifra di $3^{577.097}$ è 3. L'ultima cifra dell'operazione: $13^{899.243} - 3^{577.097}$ è $7 - 3 = 4$

4. Per $7^{299.047}$:

$299.047 : 4 = 4 \cdot 74.761 + 3$. Quindi risolviamo:

$$7^3 \equiv r \bmod 10$$

$7^3 : 10 = 10 \cdot 34 + 3$. L'ultima cifra di $7^{299.047}$ è 3.

Per $4^{377.001}$ calcoliamo:

$377.001 : 4 = 4 \cdot 94.250 + 1$. Quindi risolviamo:

$$4 \equiv r \bmod 10$$

L'ultima cifra di $4^{377.001}$ è 4. L'ultima cifra dell'operazione: $7^{299.047} - 4^{377.001}$ è $7 - 4 = -1$, tuttavia, in quel caso si scalerebbe dell'unità successiva, ripartendo essenzialmente da 9, quindi l'ultima cifra dell'operazione: $7^{299.047} - 4^{377.001}$ è 0.

15.4.3 Determinare le ultime cifre di un numero (classi di resto modulo 10^n)

ATTENZIONE: QUESTO ESERCIZIO È SU PIÙ PAGINE

(è troppo grande per una sola pagina)

Per risolvere questo esercizio, vedere i punti 8.4.2 e 8.3.1

Determinare le due cifre finali dei seguenti numeri:

$$17^{894.283}, \quad 11^{437.241} + 29^{722.602}, \quad 35^{396.689}, \quad 41^{488.936} - 37^{472.288}$$

Soluzione:

Ragionando, possiamo notare che ottenere le ultime cifre di un numero n qualunque, significa il resto r della divisione $n : 10^c$ dove c rappresenta il numero di cifre che vogliamo ottenere. Quindi per le ultime 2 cifre $c = 2$.

1. Per $17^{894.283}$ stiamo cercando $17^{894.283} \equiv r \pmod{10^2}$. Questo equivale a:

$$17^{894.283 \text{ mod } \varphi(10^2)} \equiv r \pmod{10^2}$$

$$\varphi(10^2) = \varphi(10 \cdot 10) = \varphi(5^2 \cdot 2^2) = \varphi(5^2) \cdot \varphi(2^2) = [5^{2-1} \cdot (5-1)] \cdot [2^{2-1} \cdot (2-1)] = 5 \cdot 4 \cdot 2 \cdot 1 = 40$$

$$894.283 \text{ mod } 40:$$

$$894.283 : 40 = 40 \cdot 22.357 + 3$$

$894.283 \text{ mod } 40 = 3$. Abbiamo quindi:

$$17^3 \equiv r \pmod{10^2}$$

Per le proprietà delle congruenzeabbiamo che $17^3 \equiv r \pmod{10^2}$ se e solo se $r \equiv 17^3 \pmod{10^2}$.

Quindiabbiamo $r = 17^3 \pmod{10^2}$:

$$17^3 : 10^2 = 10^2 \cdot 49 + 13$$

$$r = 13$$

$17^{894.283}$ termina con le cifre 13.

2. Per $11^{437.241} + 29^{722.602}$ possiamo scomporre il problema trovando prima le ultime 2 cifre di $11^{437.241}$, per poi trovare le ultime 2 cifre di $29^{722.602}$ e sommare insieme i risultati.

Stiamo cercando $11^{437.241} \equiv r \pmod{10^2}$, quindi utilizziamo il valore calcolato precedentemente di $\varphi(10^2) = 40$ e calcoliamo:

$$437.241 : 40 = 40 \cdot 10.931 + 1. \text{ Abbiamo quindi:}$$

$$11^1 \equiv r \pmod{10^2}$$

Troviamo r :

$$11 : 10^2 = 10^2 \cdot 0 + 11$$

Quindi $11^{437.241}$ termina con il numero 11.

Per $29^{722.602}$, calcoliamo: $722.602 : 40 = 40 \cdot 18.065 + 2$. Abbiamo quindi

$$29^2 \equiv r \pmod{10^2}$$

$$\text{Troviamo } r: 29^2 : 10^2 = 10^2 \cdot 8 + 41$$

Quindi $29^{722.602}$ termina con il numero 41.

Sommiamo: $41 + 11 = 52$. Il numero $11^{437.241} + 29^{722.602}$ termina con le cifre 52.

3. Per $35^{396.689}$, esattamente come per gli altri calcoliamo il nuovo esponente:

$$396.689 : 40 = 40 \cdot 9.917 + 9. \text{ Stiamo quindi cercando:}$$

$$35^9 \equiv r \pmod{10^2}$$

La calcolatrice non risolve questo tipo di quesito. Pertanto possiamo usare una delle proprietà delle congruenze:

In particolare, se: $35^9 \equiv r \pmod{10^2}$ allora anche $35^8 \cdot 35 \equiv n^8 \cdot n \pmod{10^2}$ (se fissiamo $n^9 = r$)

Abbiamo:

$$35^2 \equiv r \pmod{10^2}$$

Abbiamo quindi: $35^2 : 10^2 = 10^2 \cdot 12 = 25$

Perciò possiamo scrivere $35^7 \cdot 25 \equiv r \pmod{10^2}$

Quindi vale anche $25^2 \equiv r \pmod{10^2}$:

Calcoliamo: $25^2 : 10^2 = 10^2 \cdot 6 + 25$

Quindi le potenze pari ritornano a 25.

Pertanto il problema è ridotto a $35 \cdot 25 \equiv r \pmod{10^2}$

Calcoliamo $875 : 10^2 = 10^2 \cdot 8 + 75$

$35^{396.689}$ termina con le cifre 75.

4. Usiamo lo stesso metodo del punto 2. Iniziamo con $37^{472.288}$:
 Calcoliamo $472.288 : 40 = 40 \cdot 11.807 + 8$. Stiamo quindi cercando $37^8 \equiv r \pmod{10^2}$.
 Anche qui la calcolatrice non può gestire numeri così grandi, pertanto, procediamo calcolando:
 Per $37^2 \equiv r \pmod{10^2}$
 Abbiamo quindi: $37^2 : 10^2 = 10^2 \cdot 13 + 69$
 Per $37^3 \equiv r \pmod{10^2}$
 Abbiamo: $37^3 : 10^2 = 10^2 \cdot 506 + 53$
 Per $37^4 \equiv r \pmod{10^2}$
 Abbiamo: $37^4 : 10^2 = 10^2 \cdot 18.741 + 61$
 Per $37^6 \equiv r \pmod{10^2}$
 Abbiamo: $37^6 : 10^2 = 10^2 \cdot 25.657.264 + 9$
 Lo scopo era quello di identificare un ciclo. Non ci sono riuscito, tuttavia, questo è un buon risultato.
 Possiamo quindi scrivere: $69 \cdot 9 \equiv r \pmod{10^2}$
 Calcoliamo $69 \cdot 9 = 621$
 $621 : 10^2 = 10^2 \cdot 6 + 21$
 $37^{472.288}$ termina con le cifre 21.
 Calcoliamo ora le ultime due cifre di $41^{488.936}$:
 $488.936 : 40 = 40 \cdot 12.223 + 16$
 Stiamo cercando $41^{16} \equiv r \pmod{10^2}$.
 Proviamo a cercare $41^4 \equiv r \pmod{10^2}$:
 $41^4 : 10^2 = 10^2 \cdot 28.257 + 61$
 61^4 è già gestibile dalla calcolatrice. Calcoliamo quindi: $61^4 \equiv r \pmod{10^2}$:
 $61^4 : 10^2 = 10^2 \cdot 138.458 + 41$
 $41^{488.936}$ termina con le cifre 41.
 Abbiamo quindi che la sottrazione $41^{488.936} - 37^{472.288}$ termina con le cifre: $41 - 21 = 20$.

15.4.4 Classi di resto con esponenti grandi

Per risolvere questo esercizio, vedere il punto 8.4.2

Calcolare le seguenti classi resto:

$$[3^{207.859}]_5, \quad [7^{240.974}]_{11}, \quad [6^{66.095}]_{14}, \quad [15^{96.603}]_{24}, \quad [9^{391.203} + 13^{286.341}]_{25}$$

Soluzione:

1. Per $3^{207.859} \equiv r \pmod{5}$ abbiamo: $3^{207.859 \pmod{\varphi(5)}} \equiv r \pmod{5}$

$$\varphi(5) = 4, \text{ quindi } 207.849 \pmod{4}:$$

$$207.859 : 4 = 4 \cdot 51.964 + 3$$

Abbiamo quindi $3^3 \equiv r \pmod{5}$. Adattiamo la soluzione al modulo:

$$3^3 : 5 = 5 \cdot 5 + 2, \text{ pertanto: } 3^{207.859} \equiv 2 \pmod{5}$$

2. Per $7^{240.974} \equiv r \pmod{11}$ abbiamo: $7^{240.974 \pmod{\varphi(11)}} \equiv r \pmod{11}$

$$\varphi(11) = 10, \text{ quindi } 240.974 \pmod{10}:$$

$$240.974 : 10 = 10 \cdot 24.097 + 4$$

Abbiamo quindi $7^4 \equiv r \pmod{11}$. Adattiamo la soluzione al modulo:

$$7^4 : 11 = 11 \cdot 218 + 3, \text{ pertanto: } 7^{240.974} \equiv 3 \pmod{11}$$

3. Per $6^{66.095} \equiv r \pmod{14}$ abbiamo: $6^{66.095 \pmod{\varphi(14)}} \equiv r \pmod{11}$

$$\begin{array}{r|l} 14 & 2 \\ \hline 7 & 7 \\ \hline 1 & \end{array}$$

$$\varphi(14) = \varphi(2 \cdot 7) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6, \text{ quindi } 66.095 \pmod{6}:$$

$$66.095 : 6 = 6 \cdot 11.015 + 5$$

Abbiamo quindi $6^5 \equiv r \pmod{14}$. Adattiamo la soluzione al modulo:

$$6^5 : 14 = 14 \cdot 555 + 6, \text{ pertanto: } 6^{66.095} \equiv 6 \pmod{14}$$

4. Per $15^{96.603} \equiv r \pmod{24}$ abbiamo: $15^{96.603 \pmod{\varphi(24)}} \equiv r \pmod{24}$

$$\begin{array}{r|l} 24 & 2 \\ \hline 12 & 2 \\ \hline 6 & 2 \\ \hline 3 & 3 \\ \hline 1 & \end{array}$$

$$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = 2^2 \cdot 2 = 8, \text{ quindi } 96.603 \pmod{8}:$$

$$96.603 : 8 = 8 \cdot 12.075 + 3$$

Abbiamo quindi $15^3 \equiv r \pmod{24}$. Adattiamo la soluzione al modulo:

$$15^3 : 24 = 24 \cdot 140 + 15, \text{ pertanto: } 15^{96.603} \equiv 15 \pmod{24}$$

5. Per $[9^{391.203} + 13^{286.341}]$ vale $[9^{391.203} + 13^{286.341}]_{25} = [9^{391.203}]_{25} + [13^{286.341}]_{25}$.

$$\text{Calcoliamo } \varphi(25) = \varphi(5^2) = 5^{2-1} \cdot (5-1) = 20$$

Per $9^{391.203} \equiv r \pmod{25}$ abbiamo: $9^{391.203 \pmod{\varphi(25)}} \equiv r \pmod{25}$

$$931.203 : 25 = 25 \cdot 37.248 + 3$$

Abbiamo quindi $9^3 \equiv r \pmod{25}$. Adattiamo la soluzione al modulo:

$$9^3 : 25 = 25 \cdot 29 + 4, \text{ pertanto: } 9^{391.203} \equiv 4 \pmod{25}$$

Per $13^{286.341} \equiv r \pmod{25}$ abbiamo: $13^{286.341 \pmod{\varphi(25)}} \equiv r \pmod{25}$

$$286.341 : 25 = 25 \cdot 11.453 + 16$$

Abbiamo quindi $13^{16} \equiv r \pmod{25}$. Calcoliamo:

$$13^8 \equiv r \pmod{25}$$

$$13^8 : 25 = 25 \cdot 32.629.228 + 21, \text{ quindi } 13^{16} \equiv 21^2 \equiv r \pmod{25}$$

Calcoliamo: $21^2 : 25 = 25 \cdot 17 + 16$ pertanto: $13^{286.341} \equiv 16 \pmod{25}$

Il risultato è: $[9^{391.203} + 13^{286.341}]_{25} = [4 + 16]_{25} = [20]_{25}$