

# Matematica discreta

Giacomo De Liberali

29 febbraio 2016

## Indice

<b>1</b>	<b>Insiemistica</b>	<b>4</b>
1.1	Operazioni . . . . .	4
1.2	Leggi di De Morgan . . . . .	4
1.3	Operatori matematici . . . . .	5
1.4	Teorema . . . . .	5
1.5	Teorema . . . . .	5
<b>2</b>	<b>Relazioni</b>	<b>6</b>
<b>3</b>	<b>Funzioni</b>	<b>7</b>
3.1	Funzioni iniettive e surgettive . . . . .	7
3.2	Tutorato . . . . .	9
3.3	Ordinamenti parziali . . . . .	10
<b>4</b>	<b>Principio di induzione</b>	<b>11</b>
4.1	Esercizi . . . . .	11
4.1.1	Esercizio 1 . . . . .	11
4.1.2	Esercizio 2 . . . . .	12
4.1.3	Esercizio 3 . . . . .	13
4.1.4	Esercizio 4 . . . . .	14
4.1.5	Esercizio 5 . . . . .	14
4.2	Tutorato . . . . .	15
4.2.1	Esempio - numeri binari . . . . .	15
4.2.2	Esempio . . . . .	16
4.2.3	Esempio . . . . .	16
4.2.4	Esempio . . . . .	17
4.2.5	Esempio . . . . .	17
4.2.6	Esempio: $n$ divisibile per $x$ . . . . .	17
4.2.7	Esempio: funzioni ricorsive . . . . .	18
4.2.8	Esempio: funzioni ricorsive 2 . . . . .	19
<b>5</b>	<b>Principio di induzione completo</b>	<b>20</b>
5.1	Dati induttivi . . . . .	21
5.2	Proprietà delle stringhe . . . . .	21
5.2.1	Esempio . . . . .	21
5.2.2	Esercizio . . . . .	22
5.3	Il principio del buon ordinamento e di induzione . . . . .	22
5.3.1	Induzione implica buon ordinamento . . . . .	22
5.3.2	Il buon ordinamento implica induzione . . . . .	23
5.4	Esercizi . . . . .	23
5.4.1	Esercizio 1 . . . . .	23
5.4.2	Esercizio 1 . . . . .	23

<b>6</b>	<b>Funzioni ricorsive</b>	<b>24</b>
6.1	Fattoriale . . . . .	24
6.2	Elevamento a potenza della base 2 . . . . .	24
6.3	Elevamento a potenza della base 5 . . . . .	24
6.4	Esempio . . . . .	24
6.5	Successioni . . . . .	25
6.5.1	Fibonacci . . . . .	25
<b>7</b>	<b>Logica matematica</b>	<b>27</b>
7.1	Connettivi logici . . . . .	27
7.1.1	Tabella di verità . . . . .	27
7.2	Esercizi formalizzazione . . . . .	28
7.2.1	Esercizio . . . . .	28
7.3	Regola . . . . .	29
7.3.1	Esercizio . . . . .	29
7.4	Equivalenze logiche . . . . .	29
7.5	Limitazione portata . . . . .	30
7.5.1	Esempio . . . . .	30
7.6	Esercizi . . . . .	31
7.6.1	Esercizio 1 . . . . .	31
7.6.2	Esercizio 2 . . . . .	31
7.7	Tutorato . . . . .	32
7.7.1	Esercizio formalizzazione . . . . .	32
7.7.2	Esercizio dimostrazione . . . . .	32
7.7.3	Esercizio connettivi . . . . .	32
7.7.4	Esercizio formalizzazione . . . . .	33
7.7.5	Esercizio formalizzazione . . . . .	33
7.7.6	Esercizio formalizzazione . . . . .	34
7.7.7	Esercizio formalizzazione . . . . .	34
7.7.8	Esercizio formalizzazione . . . . .	35
7.7.9	Esercizio dimostrazione . . . . .	35
7.7.10	Esercizio dimostrazione . . . . .	35
7.7.11	Esercizio dimostrazione per casa . . . . .	36
<b>8</b>	<b>Tecniche di dimostrazione</b>	<b>37</b>
8.1	Esempi di dimostrazioni . . . . .	38
<b>9</b>	<b>Aritmetica modulare</b>	<b>39</b>
9.1	Proprietà . . . . .	39
9.2	Proprietà fondamentali del modulo . . . . .	40
9.2.1	Esempi di utilizzo . . . . .	40
9.3	Periodo . . . . .	40
9.4	MCD e teorema di Eulero . . . . .	41
9.5	Proprietà di Bezut . . . . .	42
9.6	Equivalenze . . . . .	43
9.7	Congruenze lineari . . . . .	44
9.7.1	Esempio 1 . . . . .	44
9.7.2	Esempio 2 . . . . .	44
9.7.3	Esempio 3 . . . . .	44
9.7.4	Esempio 4 . . . . .	44
9.8	Teorema cinese del resto . . . . .	45
9.8.1	Esempio senza teorema cinese . . . . .	45
9.9	Piccolo teorema di Fermat . . . . .	46
9.9.1	Teorema . . . . .	47
9.10	Teorema di Eulero . . . . .	47
9.11	Esercizi . . . . .	48
9.11.1	Esercizio 1 . . . . .	48
9.11.2	Esercizio 2 . . . . .	48
9.11.3	Esercizio 3 . . . . .	48
9.11.4	Esercizio 4 . . . . .	48
9.11.5	Esercizio 5 . . . . .	48

9.12	Tutorato . . . . .	48
9.12.1	Esercizio 1 . . . . .	48
9.12.2	Esercizio 2 . . . . .	49
9.12.3	Esercizio 3 . . . . .	49
9.12.4	Esercizio 4 . . . . .	49
9.12.5	Esercizio 4 . . . . .	49
9.12.6	Esercizio 6 . . . . .	49
<b>10</b>	<b>Relazioni</b>	<b>50</b>
10.1	Relazione di ordinamento parziale . . . . .	50
10.2	Relazione di equivalenza . . . . .	50
10.3	Esempi . . . . .	51
10.3.1	Esercizio 1 . . . . .	51
10.3.2	Esercizio 2 . . . . .	51
10.3.3	Esercizio 3 . . . . .	52
10.3.4	Esercizio 4 . . . . .	52
10.4	Teorema . . . . .	53
10.5	Partizioni . . . . .	53
10.5.1	Esempi . . . . .	54
10.6	Lemma . . . . .	54
10.7	Esercizi . . . . .	55
10.7.1	Esercizio 1 . . . . .	55
10.7.2	Esercizio 2 . . . . .	55
10.8	Tutorato . . . . .	56
10.8.1	Proprietà delle relazioni . . . . .	56
10.8.2	Classi di equivalenza . . . . .	56
10.8.3	Esercizi . . . . .	56
<b>11</b>	<b>Combinatoria</b>	<b>58</b>
11.1	Principio moltiplicativo . . . . .	58
11.1.1	Esempi . . . . .	58
11.2	Principio additivo . . . . .	58
11.2.1	Esempi . . . . .	58
11.2.2	Regola generale . . . . .	59
11.2.3	Esempio complesso . . . . .	59
11.2.4	Figure combinatorie . . . . .	60
11.3	Esercizi vari . . . . .	62
11.3.1	Esercizio 1 . . . . .	62
11.3.2	Esercizio 2 . . . . .	63
11.3.3	Esercizio 3 . . . . .	63
11.3.4	Esercizio 4 . . . . .	63
11.3.5	Esercizio 5 . . . . .	63
11.4	Tutorato . . . . .	64
11.4.1	Esercizio 1 . . . . .	64
11.4.2	Esercizio 2 . . . . .	64
11.4.3	Esercizio 3 . . . . .	64
11.4.4	Esercizio 4 . . . . .	64
11.4.5	Esercizio 5 . . . . .	64
11.4.6	Esercizio 6 . . . . .	65
11.4.7	Esercizio 7 . . . . .	65

# 1 Insiemistica

## 1.1 Operazioni

- Unione -  $A \cup B = \{x : x \in A \vee x \in B\}$
- Intersezione -  $A \cap B = \{x : x \in A \wedge x \in B\}$
- Complementazione -  $A \setminus B = \{x : x \in A \wedge x \notin B\}$
- Prodotto cartesiano -  $A \times B = \{(x, y) : x \in A, y \in B\}$

*Tutte queste regole seguono le logiche dell'algebra booleana (Boole).*

## 1.2 Leggi di De Morgan

- Idempotenza:
  - $A \cup A = A$
  - $A \cap A = A$
- Associatività:
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
- Commutabilità:
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Distributività:
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Assorbimento:
  - $A \cup (A \cap B) = A$
  - $A \cap (A \cup B) = A$
- Complementazione:
  - $(X \setminus A) \cup A = X$  con  $A \subseteq X$
  - $(X \setminus A) \cap A = \emptyset$
- Altre leggi
  - $(A \cup B)' = A' \cap B'$
  - $(A \cap B)' = A' \cup B'$

### 1.3 Operatori matematici

- AND:  $\wedge$
- OR:  $\vee$

### 1.4 Teorema

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

Prova: siano  $A$  e  $B$  insiemi [una dimostrazione si inizia sempre così]

$$C \subseteq D \wedge D \subseteq C \Rightarrow C = D$$

- (I)  $A \subseteq A \cup (A \cap B)$ 
  - $x \in A \Rightarrow x \in A \cup (A \cap B)$  [vero per definizione di unione]
- (II)  $A \cup (B \cap C) \subseteq A$ 
  - $x \in A \cup (B \cap C) \Rightarrow x \in A$ 
    - (a)  $x \in A \Rightarrow x \in A$  [vero]
    - (b)  $x \in A \cup B \Rightarrow x \in A \wedge x \in B \Rightarrow x \in A$  [vero]

### 1.5 Teorema

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \text{ [verifico che sia vero]}$$

Prova: siano  $A, B$  e  $C$  insiemi [prendo un elemento arbitrario dal primo insieme e verifico sia presente anche negli altri]

- (I)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ 
  - $x \in A \cap (B \cup C) \Rightarrow x \in A \wedge x \in B \cup C$
  - $x \in B \cup C \Rightarrow x \in B \vee x \in C$
  - Posso supporre che:
    - (a)  $x \in B \Rightarrow x \in A \cap B \Rightarrow x \in (A \cap B) \cup (A \cap C)$  [poiché è un sottoinsieme]
    - (b)  $x \in A \cap C \Rightarrow x \in (A \cap C) \cup (A \cap B)$  [poiché è un sottoinsieme]
- (II)  $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ 
  - (a)  $x \in A \cap B \Rightarrow x \in A \wedge x \in B$ 
    - $x \in B \Rightarrow x \in B \cup C \Rightarrow x \in A \cap (B \cup C)$
  - (b)  $x \in A \cap C \Rightarrow x \in A \wedge x \in C$ 
    - $x \in C \Rightarrow x \in (B \cup C) \Rightarrow x \in A \cap (B \cup C)$  [fine dimostrazione]

## 2 Relazioni

Una relazione non è una funzione quando dato un input ricevo più output.

essere studenti di professore [*relazione binaria, non è una funzione*]

Dominio = studenti, Codominio = professori

(Marco, Simeoni) ∈ Relazione? Sì.

Una relazione binaria  $R$  di dominio  $A$  e codominio  $B$  è un sottoinsieme di  $A \times B$ :

$$Relazione \subseteq Studenti \times Professori$$

$$\{(x, y) \in Relazione : x \in Studenti \wedge y \in Professori \wedge x \text{ è uno studente del professore } y\}$$

### 3 Funzioni

Una relazione è una funzione quando ad ogni elemento del dominio corrisponde un solo elemento del codominio.

Una funzione

$$f : A \rightarrow B$$

è una relazione binaria

$$(f \subseteq A \times B)$$

tali che per ogni  $a \in A$  esiste un unico elemento  $b \in B$  tali che  $(a, b) \in R$ .

**06.10.2015**

$$R = \{(x, y) : x, y \in A \wedge x \text{ ha la stessa altezza di } y\}$$

dove  $A$  è l'insieme delle persone presenti in questo momento in aula 1.

Una funzione è tale solo se dato un input ricevo un solo output.

Esempio:

$$R = \{(x, y) : x \in \mathbb{Z}, y \in \mathbb{N} \wedge x = y^2\}$$

Non è una funzione, in quanto  $\nexists y : (2, y) \in R$  [non esiste un numero naturale la cui radice sia 2]

#### 3.1 Funzioni iniettive e surgettive

Una funzione  $f : A \rightarrow B$  è iniettiva se per ogni  $x, y \in A$  abbiamo che

$$f(x) = f(y) \Rightarrow x = y$$

Una funzione è surgettiva se per ogni  $y \in B$  esiste un  $x \in A$  tale che

$$f(x) = y$$

Siano  $A$  e  $B$  insiemi finiti. Se  $f : A \rightarrow B$  è:

- iniettiva, allora  $|A| \leq |B|$       dove  $|A|$  è la cardinalità di  $A$ , numero di elementi
- suriettiva, allora  $|B| \leq |A|$
- bigettiva, allora  $|A| = |B|$

Una funzione  $f : A \rightarrow B$  è invertibile se esiste  $g$  tale che  $B \rightarrow A$ :

$$f \circ g \quad [f \text{ composto } g, \text{ ovvero applico prima } g \text{ e poi } f]$$

Una funzione  $f : A \rightarrow B$  è bigettiva se  $f$  è invertibile.

$f : A \rightarrow B$  è invertibile se esiste  $g : B \rightarrow A$  tale che

$$g \circ f = I_A$$

$$f \circ g = I_B$$

$$\underbrace{A \xrightarrow{f} B \xrightarrow{g} A}_{\text{identità di } A, I_A}$$

$$\underbrace{B \xrightarrow{g} A \xrightarrow{f} B}_{\text{identità di } B, I_B}$$

**Dimostrazione**

Supponendo che  $f : A \rightarrow B$  sia bigettiva [stessa cardinalità].

$g : B \rightarrow A$       $g(y) = x$     dove  $x$  è l'elemento di  $A$  tale che  $f(x) = y$  dove  $y \in B$

$$(g \circ f)x = g(f(x)) \quad \text{con } x \in A$$

$$(f \circ g)y = f(g(y)) \quad \text{con } y \in B$$

Supponiamo  $f$  sia invertibile:

allora esiste  $g : B \rightarrow A$  tale che  $g \circ f = I_A$       $f \circ g = I_B$

Poniamo che  $f$  sia iniettiva:

$$f(x) = f(y) \Rightarrow x = y \quad \text{con } x, y \in A$$

$$g(f(x)) = g(f(y)) \rightarrow \underbrace{(g \circ f)x}_{I_A(x)=x} = \underbrace{(g \circ f)y}_{I_B(y)=y}$$

Poniamo che  $f$  sia surgettiva: per ogni  $y \in B$  esiste  $x \in A$  tale che  $f(x) = y$

$$f(\underbrace{g(y)}_A) = y$$



## 3.2 Tutorato

Una funzione  $f$  associa ad ogni elemento di un insieme  $A$ , detto dominio, uno ed un solo elemento dell'insieme  $B$ , detto codominio:

$$f : A \mapsto B$$

Esempio pratico:

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

$$B = \{1, 2, 3\}$$

$f(a) = 1$ , dove 1 è l'immagine di  $a$  e  $a$  è la controimmagine di 1.

### Funzioni iniettive

Una funzione  $f$  è iniettiva se ogni elemento del codominio è mappato al massimo da un elemento del dominio.

Se  $\underbrace{|B| < |A|}_{\text{cardinalità}}$  non può essere iniettiva.

### Funzioni suriettive

Una funzione  $f$  è surgettiva se ogni elemento del codominio è mappato da almeno un elemento del dominio.

Se  $|B| > |A|$  non può essere surgettiva.

### Funzioni bigettive

Una funzione  $f$  è surgettiva quando è sia iniettiva che surgettiva, ovvero quando ogni elemento del codominio è mappato esattamente da un elemento del dominio. Può essere bigettiva solo se  $|A| = |B|$

Esempi:

$$f : \mathbb{Z} \mapsto \mathbb{N} \quad f(x) = \text{abs}(x) \quad [\text{suriettiva}] \quad (1)$$

$$f : \mathbb{N} \mapsto \mathbb{N} \quad f(x) = x + 1 \quad [\text{iniettiva}] \quad (2)$$

$$f : \mathbb{Z} \mapsto \mathbb{Z} \quad f(x) = x + 1 \quad [\text{bigettiva}] \quad (3)$$

$$f : \mathbb{Z} \mapsto \mathbb{Z} \quad f(x) = x^2 \quad [\text{ne iniettiva ne suriettiva}] \quad (4)$$

$$f : \mathbb{R} \mapsto \mathbb{R} \quad f(x) = x^2 \quad [\text{ne iniettiva ne suriettiva}] \quad (5)$$

$$f : \mathbb{N} \mapsto \mathbb{N} \quad f(x) = x^2 \quad [\text{iniettiva ma non suriettiva}] \quad (6)$$

### 3.3 Ordinamenti parziali

Proprietà degli ordinamenti parziali sui numeri naturali:

- $x \leq y$  sse  $\exists z(x + z = y)$
- proprietà riflessiva:  $\forall x(x \leq x)$
- proprietà transitiva:  $\forall xyz(x \leq y \wedge y \leq z \Rightarrow x \leq z)$
- proprietà antisimmetrica:  $\forall xyz(x \leq y \wedge y \leq x \Rightarrow x = y)$

## 4 Principio di induzione

Serve per verificare che una certa proprietà valga per tutti gli elementi di un insieme. Data una proposizione  $P$ , se  $P$  vale per  $x_0$ , bisogna dimostrare che  $P$  vale anche per  $x + 1$ , ovvero che  $P$  valga per tutti gli elementi:

$$P(x_0) \wedge (P(k) \rightarrow P(k+1)) \rightarrow \forall x \geq x_0, P(x)$$

Esempio:  $\{x : x \in \mathbb{N}, x \text{ è primo}\} \leq \mathbb{N} \rightarrow \underline{P}$

$$\underbrace{\underline{P}(0)}_{[0 \text{ ha la proprietà } \underline{P}]} \quad \text{e } \forall x (\underline{P}(x) \Rightarrow \underline{P}(x+1)) \Rightarrow \forall x \quad \underline{P}(x)$$

[se  $x$  ha la stessa proprietà  $\underline{P}$  e  $x+1$  ha la stessa proprietà, essa vale per l'intero campo numerico]

### 4.1 Esercizi

#### 4.1.1 Esercizio 1

Dimostrare che

$$\sum_{i=0}^x i = 1 + 2 + 3 + \dots + (x-1) + x = \frac{x(x+1)}{2}$$

vale per ogni  $x \in \mathbb{N}$ .

Inizio dimostrazione:

$$\underline{P}(x) \text{ sse } \sum_{i=0}^x i = \frac{x(x+1)}{2}$$

$$\underline{P}(0) = \sum_{i=0}^0 i = \frac{0(0+1)}{2} = 0 \quad \text{vero}$$

Supponiamo per ipotesi di induzione che  $x$  abbia la proprietà  $\sum_{i=0}^x i = \frac{x(x+1)}{2}$

$$\begin{aligned} \sum_{i=0}^{x+1} i &= \frac{(x+1)(x+2)}{2} \rightarrow \sum_{i=0}^x i + (x+1) \rightarrow \underbrace{\frac{x(x+1)}{2}}_{\text{induzione}} + (x+1) \\ &\rightarrow \frac{x(x+1) + 2(x+1)}{2} \rightarrow \frac{(x+1)(x+2)}{2} \quad \text{dimostrato.} \end{aligned}$$

#### 4.1.2 Esercizio 2

Dimostrare che

$$\sum_{k=0}^x (2k+1) = (x+1)^2$$

Studio risoluzione:

1	3	5	7	...
7	5	3	1	...
8	8	8	8	...

$$\sum_{k=0}^3 (2k+1) = 1 + 3 + 5 + 7 = 16$$

Inizio dimostrazione per induzione. Base 0:

$$\sum_{k=0}^0 (2k+1) = (0+1)^2 = 1 \quad \text{vero}$$

La base è valida, supponiamo per induzione che  $\sum_{k=0}^x (2k+1) = (x+1)^2$

$$\sum_{k=0}^{x+1} (2k+1) = \left( \sum_{k=0}^x (2k+1) \right) + (2(x+1)+1) = (x+1)^2 + 2(x+1) + 1 = \underbrace{((x+1)+1)^2}_{\text{prodotto notevole}} \quad [\text{dimostrato}]$$

Se la proprietà vale per  $x+1$ , vale per l'intero campo numerico!

### 4.1.3 Esercizio 3

Dato un insieme  $A$  di cardinalità  $n$ , allora  $\mathcal{P}(A) = \{B : B \subseteq A\}$  ha cardinalità  $2^n$ , dove  $\mathcal{P}(A)$  è l'insieme delle parti di  $A$ .

**Caso base:**  $n = 0$

Se  $n = 0$ ,  $A = \emptyset$ . Se  $A = \emptyset$ , l'insieme delle parti di  $A[\mathcal{P}(A)]$  vale  $\{\emptyset\}$ .

$$2^0 = 1 \rightarrow 2^0 = 1 \quad [vero]$$

Dato che il caso base è vero, inizio la dimostrazione:

*Supponiamo per ipotesi di induzione che l'insieme delle parti di un insieme di cardinalità  $n$  abbia cardinalità  $2^n$ .*

$$|\mathcal{P}(A)| = 2^{n+1}$$

prendo  $B \subseteq A \rightarrow a_{n+1} \in B$ ?

Partiziono  $\mathcal{P}(A)$  in sottoinsiemi che contengono  $a_{n+1}$  e quelli che non contengono  $a_{n+1}$

$A = \{a, b, c\} \rightarrow$  fisso l'ultimo elemento  $[c]$

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Partizioni che contengono l'ultimo elemento:  $\{c\}, \{a, c\}, \{b, c\}, \{a, b, c\} \rightarrow 4 \text{ elementi} \rightarrow 2^2$

Partizioni che non contengono l'ultimo elemento:  $\{\emptyset\}, \{a\}, \{b\}, \{a, b\} \rightarrow 4 \text{ elementi} \rightarrow 2^2$

Esempio riportato al caso generico:  $2^n + 2^n = 2^{n+1}$

$$\{B : B \subseteq A \wedge a_{n+1} \in B\}$$

$$\{B : B \subseteq A \wedge a_{n+1} \notin B\}$$

L'insieme delle parti di  $A$  è l'unione dei due insiemi sopracitati.

Se  $f$  è iniettiva suppongo che:

$$f(b) = f(c) \xrightarrow{\text{implica}} B = C$$

Sfrutto la definizione di  $f(b)$  e ottengo:

$$B \setminus \{a_{n+1}\} = C \setminus \{a_{n+1}\}$$

$$B \setminus \{a_{n+1}\} \cup \{a_{n+1}\} = B \rightarrow C \setminus \{a_{n+1}\} \cup \{a_{n+1}\} = C$$

segue che  $B = C$  e  $f$  è iniettiva:

$$f : \{B : B \subseteq A \wedge a_{n+1} \in B\} \mapsto \{B \subseteq A : a_{n+1} \notin B\}$$

#### 4.1.4 Esercizio 4

Dimostrare che:

per ogni  $n \geq 1$  si ha  $2^n \geq n + 1$

**Caso base:**  $n = 1$

$$2^1 = 1 + 1 = 2 \xrightarrow{\text{equivalente}} 2^1 = 2 \quad [\text{vero}]$$

Dato che la verifica del caso base è andata a buon fine, iniziamo la dimostrazione.

Suppongo per induzione che  $2^n \geq n + 1$  sia vero

$$2^{n+1} = 2 \cdot 2^n \xrightarrow{\text{per induzione}} 2 \cdot 2^n \geq 2 \cdot (n + 1) = 2n + 2 = (n + 2) + n \rightarrow \underbrace{(n + 2) + n \geq n + 2}_{\text{perché } n \geq 1} \Rightarrow 2 \cdot 2^n \geq n + 2$$

Fine, dimostrato.

#### 4.1.5 Esercizio 5

Dimostrare che:

per ogni  $n \geq 0$  si ha che 8 divide  $(3^{2n} - 1)$

**Caso base:**  $n = 0$

$$3^{2 \cdot 0} - 1 = 0 \quad [\text{vero, ogni numero divide } 0]$$

Dato che la verifica del caso base è andata a buon fine, iniziamo la dimostrazione.

Suppongo per induzione che  $8 \mid (3^{2n} - 1)$  sia vero. Dimostro che  $(3^{2(n+1)} - 1)$  sia divisibile per 8.

$$\begin{aligned} 3^{2n+2} - 1 &= 3^{2n} \cdot 3^2 - 1 \xrightarrow{\text{per induzione}} (3^{2n} \underbrace{-1 + 1}_{\text{li aggiungo}}) \cdot 3^2 - 1 = \\ &= \underbrace{(3^{2n} - 1)}_{\text{induzione}} \cdot (3^2) + \underbrace{(3^2 - 1)}_{8 \mid 8 \rightarrow \text{vero}} \end{aligned}$$

E' divisibile per 8 in quanto un numero divisibile per 8 (l'induzione) moltiplicata per una costante  $k$ , resta divisibile per 8. Se a questo valore aggiungiamo un multiplo di 8 (oppure 8 stesso), otteniamo nuovamente un numero  $d$  divisibile per 8. Segue

$$d = k \cdot n$$

dove  $n$  è multiplo di 8,  $k$  è una costante  $\in \mathbb{N}$ .

## 4.2 Tutorato

Dimostrare per induzione  $\forall x \geq x_0, P(x)$ :

1. Caso base  $P(x_0)$
2. Assumiamo che la proprietà sia vera per un certo  $k$ , cioè che  $P(k)$  sia vera (ipotesi di induzione)
3. Per il principio di induzione la proprietà è vera  $\forall x \geq x_0$

### 4.2.1 Esempio - numeri binari

$$\begin{cases} \overbrace{11}^2 = 2^0 + 2^1 = 3 = 2^2 - 1 \\ \underbrace{111}_3 = 2^0 + 2^1 + 2^2 = 7 = 2^3 - 1 \end{cases}$$

$$P(n) : \sum_{i=0}^{n-1} 2^i = 2^n - 1 \quad \forall n \geq 1$$

Caso base:  $n=1$

$$P(1) = \sum_{i=0}^0 2^i = 2^0 = 1 \xrightarrow{\text{equivalente}} 2^1 - 1 = 0 \quad [\text{vero}]$$

Assumiamo  $P(k) \rightarrow \sum_{i=0}^{k-1} 2^i = 2^k - 1$ . Dobbiamo dimostrare che  $P(k+1) \rightarrow \sum_{i=0}^{k+1-1} 2^i = 2^{k+1} - 1$

$$\begin{aligned} 2^{k+1} - 1 &= 2^k \cdot 2 - 1 \\ &= 2^k + 2^k - 1 \\ &= 2^k + \underbrace{\sum_{i=0}^{k-1} 2^i}_{\text{per ipotesi di induzione}} \Rightarrow 2^0 + 2^1 + \dots + 2^{k-1} + 2^k \\ &= \sum_{i=0}^{k+1-1} 2^i = 2^{k+1} - 1 \end{aligned}$$

Per il principio di induzione  $\forall x \geq 1, P(k)$  vale.

#### 4.2.2 Esempio

Dimostrare che  $\forall n \geq 4$

$$\left( \sum_{i=1}^n i \right) \leq n(n+1) \leq n!$$

Base:  $n = 4$

$$\sum_{i=1}^4 = 1 + 2 + 3 + 4 \leq 4 \cdot 5 \leq 4! \rightarrow 10 \leq 20 \leq 24 \quad \text{vero}$$

Inizio la dimostrazione per  $n + 1$ , visto il caso base

$$\begin{aligned} \sum_{i=1}^{n+1} i &\leq (n+1)(n+2) \leq (n+1)! \\ \sum_{i=1}^n i + (n+1) &\leq n(n+1) + 2(n+1) \leq n! \cdot (n+1) \\ \dots \end{aligned}$$

#### 4.2.3 Esempio

Dimostrare che  $\forall n \geq 1$

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

Base:  $n = 1$

$$\sum_{i=1}^1 (2i-1) = 2-1 = 1 = 1^2 \quad \text{vero}$$

Vista la base inizio la dimostrazione

$$\begin{aligned} \sum_{i=1}^{n+1} (2i-1) &= (n+1)^2 \\ \sum_{i=1}^n (2i-1) + 2(n+1) - 1 &= (n+1)^2 \\ \underbrace{n^2}_{\text{induzione}} + 2n + 1 &= (n+1)^2 \\ (n+1)^2 &= (n+1)^2 \end{aligned}$$



#### 4.2.4 Esempio

Dimostrare che  $\forall n \geq 3$

$$2n + 1 \leq 2^n$$

...

#### 4.2.5 Esempio

Dimostrare che  $\forall n \geq 6$

$$5n + 5 \leq n^2$$

Base:  $n = 6$

$$5 \cdot 6 + 5 \leq 6^2 \quad \text{vero}$$

Vista la base inizio la dimostrazione

$$5(n + 1) + 5 \leq (n + 1)^2$$

$$\text{Semplifico il termine a sinistra: } 5(n + 1) + 5 = \underbrace{5n + 5}_{\text{forma iniziale}} + 5$$

Sommando o sottraendo lo stesso termine a destra e a sinistra di una disuguaglianza si ottiene la medesima disuguaglianza

$$5n + 5 + 5 \leq n^2 + 5$$

$$5n + 5 + 5 \leq n^2 + 2n + 1$$

$$5 \leq 2n + 1 \quad \text{vero}$$

#### 4.2.6 Esempio: n divisibile per x

Dimostrare che  $\forall n \in \mathbb{N}$

$$n^3 + 2n \text{ è divisibile per } 3$$

Base:  $n = 0$

$$0^3 + 2 \cdot 0 = 0 \quad \underbrace{\quad}_{\text{divide}} \quad 3 \quad \text{vero, ogni numero divide } 0$$

Vista la base inizio la dimostrazione

$$(n + 1)^3 + 2(n + 1)$$

$$n^3 + 3n^2 + 3n + 1 + 2n + 2$$

$$n^3 + 2n + 3n^2 + 3n + 3$$

$$\underbrace{(n^3 + 2n)}_{\text{per induzione è divisibile per } 3} + \underbrace{3(n^2 + n + 1)}_{\text{divisibile per } 3} \quad \text{vero}$$

#### 4.2.7 Esempio: funzioni ricorsive

Dimostrare che

$$f(n) \begin{cases} 3 & \text{con } n = 1 \\ 5 & \text{con } n = 2 \\ 3f(n-1) - 2f(n-2) \end{cases}$$

è uguale a

$$g(n) = 2^n + 1$$

Inizio la dimostrazione verificando il caso base:

$$\begin{array}{lll} n = 1 & 2^1 + 1 = 3 & \checkmark \\ n = 2 & 2^2 + 1 = 5 & \checkmark \end{array}$$

I casi base sono veri, quindi suppongo vero

$$f(x) = g(x) = 2^n + 1 \quad \forall i(1 \leq i \leq k), k \in \mathbb{N}$$

Devo dimostrare ora che l'uguaglianza vale anche per  $(x+1)$ :

$$\begin{aligned} f(x+1) &= 3f(k) - 2f(k-1) = g(k+1) \\ &= 3g(k) - 2g(k-1) \quad \text{per ipotesi di induzione forte} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) \\ &= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2 \\ &= 3 \cdot 2^k + 3 - 2^1 \cdot 2^{-1} \cdot 2^k - 2 \\ &= 3 \cdot 2^k + 3 - \cancel{(2^1 \cdot 2^{-1})} \cdot 2^k - 2 \\ &= 3 \cdot 2^k - 2^k + 1 \\ &= 2^k(3 - 1) + 1 \\ &= 2^k \cdot 2 + 1 \\ &= 2^{k+1} + 1 \quad \text{dimostrato} \end{aligned}$$

#### 4.2.8 Esempio: funzioni ricorsive 2

Data la funzione ricorsiva

$$f(n) \begin{cases} 1 & \text{con } n = 1 \\ 1 & \text{con } n = 2 \\ f(n-1) + f(n-2) & \end{cases}$$

dimostrare che

$$\sum_{i=1}^n f(i)^2 = f(n) \cdot f(n+1) \quad \forall n \in \mathbb{N}$$

Inizio la dimostrazione verificando il caso base:

$$n = 1 \quad \sum_{i=1}^1 f(i)^2 = f(1)^2 = 1 \cdot 1 = f(1) \cdot f(2) \quad \checkmark$$

$$n = 2 \quad \sum_{i=1}^2 f(i)^2 = f(2)^2 = f(1)^2 + f(2)^2 = 1 + 1 = f(2) \cdot f(3) \quad \checkmark$$

I casi base sono veri, quindi suppongo vero

$$\sum_{i=1}^k f(i)^2 = f(k) \cdot f(k+1) \quad \forall k \in \mathbb{N}$$

Devo dimostrare ora che l'uguaglianza vale anche per  $(k+1)$ :

$$\begin{aligned} \sum_{i=1}^{k+1} f(i)^2 &= \sum_{i=1}^k f(i)^2 + f(k+1)^2 \\ &= \underbrace{f(k) \cdot f(k+1)}_{\text{induzione}} + f(k+1)^2 \\ &= f(k+1)[f(k) + f(k+1)] \\ &= f(k+1)f(k+2) \quad \text{per definizione ricorsiva} \rightarrow f(k+2) = f(k+2-1) + f(k+2-2) = f(k+1) + f(k) \end{aligned}$$

## 5 Principio di induzione completo

Suppongo che  $P(x)$  valga da 0 a  $x$ , e vado a dimostrare che  $P(x)$  vale anche per  $x + 1$ .

$$P(0) \wedge \forall x (P(0) \wedge P(1) \wedge \dots \wedge P(x) \rightarrow P(x+1)) \Rightarrow \forall x P(x)$$

Se la proprietà  $P$  vale per 0 e vale per ogni  $y$  nell'intervallo  $[0, x]$ , allora  $P$  vale per ogni  $x > 0$ .

$$P(0) \wedge \forall x (\forall y \in [0, x], P(y) \rightarrow P(x+1)) \Rightarrow \forall x P(x)$$

### Esempio

Ogni numero naturale  $n \geq 2$  è scomponibile in fattori primi

Caso base:  $n = 2 \rightarrow$  vero, *[due è primo, quindi è scomposto in fattori primi]*

Ora supponiamo che il teorema valga per tutti i numeri tra 2 e  $n$  e dimostriamolo per  $n + 1$ .

1. Se  $n + 1$  è primo, allora il teorema è valido in quanto  $n + 1$  è già scomposto in fattori primi
2. Se  $n + 1$  non è primo, allora è divisibile per un numero  $k$  compreso tra  $1 < k < (n + 1)$

$$n + 1 = k(r) \text{ per un certo } r \in \mathbb{N} \wedge 1 < r < (n + 1)$$

Si deduce che  $r, k \leq n \wedge r, k \geq 2$

Per il teorema di induzione completa

$$r = p_1 \cdot p_2 \cdot \dots \cdot p_i$$

$$k = q_1 \cdot q_2 \cdot \dots \cdot q_j$$

$$n + 1 = k \cdot r = q_1 \cdot q_2 \cdot \dots \cdot q_j \cdot p_1 \cdot p_2 \cdot \dots \cdot p_i$$

## 5.1 Dati induttivi

### Numeri

1. 0 è un numero naturale
2. Se  $x$  è un numero naturale, allora  $x + 1$  è un numero naturale
3. Nient'altro è un numero naturale

### Stringhe

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

1.  $\varepsilon$  è una stringa
2. Se  $\alpha$  è una stringa, allora la concatenazione  $\alpha_a$  di  $\alpha$  e  $a$  è una stringa  
Se  $\beta$  è una stringa, allora la concatenazione  $\beta_b$  di  $\beta$  e  $b$  è una stringa
3. Nient'altro è una stringa

## 5.2 Proprietà delle stringhe

$$P(\varepsilon) \wedge \forall \alpha (P(\alpha) \rightarrow P(\alpha_a)) \Rightarrow \forall \alpha P(\alpha)$$

La lunghezza di una stringa si indica con  $l : A^* \mapsto \mathbb{N}$ , dove  $A^*$  è l'insieme delle stringhe di alfabeto  $A$

Aggiungendo un carattere ad una stringa, si otterrà una nuova stringa con lunghezza incrementata di uno:

$$\begin{cases} l(\varepsilon) = 0 \\ l(\alpha_a) = l(\alpha) + 1 \\ l(\alpha_b) = l(\alpha) + 1 \end{cases}$$

Nella pratica:

$$\begin{aligned} l(aba) &= \underbrace{l(ab)}_{\alpha} + 1 \\ &= (l(a) + 1) + 1 \\ &= ((\underbrace{l(\varepsilon)}_{\text{caso base}} + 1) + 1) + 1 \\ &= 0 + 1 + 1 + 1 \\ &= 3 \end{aligned}$$

### 5.2.1 Esempio

Caratteri dell'alfabeto:  $a, 0, 1, [, ], +, *$

1.  $a, 0, 1$  sono espressioni
2. Se  $E_1$  e  $E_2$  sono espressioni, allora  $[E_1 + E_2]$  e  $[E_1 * E_2]$  sono espressioni
3. Nient'altro è espressioni

$$\underbrace{P(a) \wedge P(0) \wedge P(1)}_{\text{casi base}} \wedge \forall E_1 \forall E_2 (P(E_1) \wedge P(E_2) \rightarrow P([E_1 + E_2]) \wedge P([E_1 * E_2])) \Rightarrow \forall E, P(E)$$

### 5.2.2 Esercizio

Dimostrare che ogni espressione ha un numero pari di parentesi

Base: "a", "0", "1" hanno 0 parentesi

Supponiamo per induzione che  $E_1$  e  $E_2$  siano espressioni con una somma pari di parentesi

$$[E_1 + E_2] \rightarrow 2 + n(E_1) + n(E_2) \quad \text{dove } n(E) \text{ è il numero di parentesi di } E$$

Dato che la somma di 3 numeri pari è pari, la dimostrazione è stata verificata

## 5.3 Il principio del buon ordinamento e di induzione

Il principio di induzione sui numeri naturali è equivalente al seguente principio:

ogni sottoinsieme non vuoto di numeri naturali ha *minimo elemento*.

Questo principio prende il nome di **buon ordinamento**.

Nel campo dei numeri naturali, anche il principio del buon ordinamento implica il principio di induzione.

$$\begin{cases} P(0) \text{ vero} \\ \forall x (P(x) \rightarrow P(x+1)) \end{cases} \Rightarrow \forall x, P(x)$$

### 5.3.1 Induzione implica buon ordinamento

Sia  $X \neq \emptyset \subseteq \mathbb{N} \rightarrow [X \text{ deve avere almeno un elemento}]$

$$P(n) \equiv n \in X \rightarrow [X \text{ ha minimo elemento}]$$

Dimostrare che  $\forall n, P(n)$

Base: 0 ha la proprietà  $P$ ?

$$P(0) = 0 \in X \Rightarrow X \text{ ha minimo elemento}$$

Due casi  $\begin{cases} 0 \in X \rightarrow X \text{ ha minimo elemento (lo 0 stesso)} \\ 0 \notin X \rightarrow \text{l'ipotesi dell'implicazione è falsa, quindi la conclusione è vera} \end{cases}$

Quando l'ipotesi dell'implicazione è vera, devo controllare la conclusione, mentre se l'ipotesi è falsa, la conclusione è sempre vera: Supponiamo che  $n$  soddisfi la proprietà  $P$ . Dimostriamo che  $P$  vale anche per  $n+1$ .

A	B	A→B
0	0	1
0	1	1
1	0	0
1	1	1

Tabella 1: Tabella implicazione

$$P(n) = n \in X \rightarrow \text{ha minimo elemento}$$

Suppongo che  $x+1 \in X$  sia vero.

$\begin{cases} n+1 \text{ è il minimo di } X \\ n+1 \text{ non è il minimo. Vi è dunque un numero più piccolo di } n+1 \text{ che sta in } X. \text{ Quindi esiste un } k < n+1, k \in X. \end{cases}$

In entrambi i casi esiste minimo elemento, e lo ho dimostrato. Quindi si deduce che

$$\forall n, P(n) \wedge \exists r \in X : P(r) = r \in X \rightarrow X \text{ ha minimo}$$

### 5.3.2 Il buon ordinamento implica induzione

Supponiamo  $Q(0)$  vero.

$$\forall x(Q(x) \rightarrow Q(x+1))$$

Supponiamo per assurdo che  $\forall x, Q(x)$  sia falso.

$\exists k \in \mathbb{N} : Q(k)$  è falso  $\rightarrow$  esiste almeno un elemento di  $\mathbb{Q}$  che lo rende falso

Quindi

$$X = \{n \in \mathbb{N} : Q(n) \text{ è falso}\} \rightarrow \text{insieme} \neq \emptyset$$

Si deduce che  $X$  ha minimo elemento, ma  $\emptyset$  non appartiene a  $X$

$$\emptyset \neq m = \min(X) \Rightarrow m > 0 \Rightarrow m-1 > 0 \rightarrow m-1 \notin X$$

segue che  $Q(m-1)$  è vero, mentre  $Q(m)$  è falso

$$\forall m(Q(\underbrace{m-1}_x) \rightarrow Q(\underbrace{m}_{x+1})) \Rightarrow \text{falso}$$

## 5.4 Esercizi

### 5.4.1 Esercizio 1

Dimostrare per induzione che  $\forall n > 0$  è sempre vero che

$$2^n \geq n+1$$

Soluzione:

$$\text{Base: } n=0 \quad 2^0 = 1 \geq 1 \quad \checkmark$$

$$2^{n+1} \geq n+2$$

$$2^n \cdot 2 \geq n+2$$

$$2(n+1) \geq n+2 \quad \text{induzione}$$

$$2n+2 \geq n+2$$

$$n+n+2 \geq n+2 \quad \forall n > 0 \quad \checkmark$$

### 5.4.2 Esercizio 1

Dimostrare per induzione che  $\forall n > 0$  è sempre vero che

$$F(n) \leq 2^n$$

$$F(0) = 1$$

$$F(1) = 1$$

$$F(n+1) = F(n) + F(n-1)$$

Soluzione:

$$\text{Base: } n=0 \quad F(0) = 1 \leq 2^0 = 1 \quad \checkmark$$

$$\text{suppongo per induzione che } F(i) \leq 2^i \quad \forall i \leq n$$

$$F(n+1) = F(n) + F(n-1) \leq 2^n + 2^{n-1} \leq 2^n + 2^n = 2^{n+1} \quad \checkmark$$

Curiosità...

L'ennesimo numero di Fibonacci può essere ottenuto anche non ricorsivamente:

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_1 \\ F_0 \end{bmatrix} = \begin{bmatrix} F_2 \\ F_1 \end{bmatrix} \quad \text{quindi} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} F_1 \\ F_0 \end{bmatrix} = \begin{bmatrix} F_{n+1} \\ F_n \end{bmatrix}$$

## 6 Funzioni ricorsive

Sono funzioni ben definite che richiamano se stesse, e hanno dei casi base di uscita

### 6.1 Fattoriale

$$\begin{cases} f(0) = 1 \\ f(n+1) = (n+1) \cdot f(n) \end{cases}$$

La proprietà  $P(n)$  vale in  $n$  sse la funzione  $f(n)$  è ben definita in  $n$ .  
Supponiamo  $f(n)$  sia ben definita, proviamo che  $f(n+1)$  sia definita.

### 6.2 Elevamento a potenza della base 2

$$\begin{cases} f(0) = 1 \\ f(n+1) = 2 \cdot f(n) \end{cases} \Rightarrow f(n) = 2^n$$

Caso base:  $n = 0$

$$f(0) = 1 \xrightarrow{\text{equivalente}} 2^0 = 1 \quad [\text{vero}]$$

Supponiamo per induzione

$$f(n) = 2^n \rightarrow f(n+1) = 2 \cdot f(n) = 2 \cdot 2^n = 2^{n+1}$$

Prova numerica

$$f(5) = 2 \cdot f(4) = 2 \cdot 2 \cdot f(3) = 2 \cdot 2 \cdot 2 \cdot f(2) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot f(1) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot f(0) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 1 = 2^5 \rightarrow 2^n$$

### 6.3 Elevamento a potenza della base 5

$$\begin{cases} f(0) = 1 \\ f(1) = 5 \\ f(n) = 20 \cdot f(n-2) + f(n-1) \end{cases} \Rightarrow f(n) = 5^n$$

Casi base

$$\begin{cases} n = 0 \rightarrow 5^0 = 1 & \text{vero} \\ n = 1 \rightarrow 5^1 = 5 & \text{vero} \end{cases}$$

Inizio dimostrazione

per casa...

### 6.4 Esempio

Dominio:  $\forall n \in \mathbb{N}^+$

$$\begin{cases} f(1) = 3 \\ f(2) = 5 \\ f(n) = 3 \cdot f(n-1) - 2 \cdot f(n-2) \end{cases} \Rightarrow f(n) = 2^n + 1$$

Casi base

$$\begin{cases} n = 1 \rightarrow 1 & \text{vero} \\ n = 2 \rightarrow 5 & \text{vero} \end{cases}$$

Inizio dimostrazione

per casa...



## 6.5 Successioni

Una successione è una funzione  $f : \mathbb{N} \mapsto \mathbb{N}$

### 6.5.1 Fibonacci

$$F(0) = 0 \quad [\text{base}]$$

$$F(1) = 1 \quad [\text{base}]$$

$$F(n+1) = F(n) + F(n-1) \quad \text{con } n \geq 1, \text{ poiché } n-1 \geq 0$$

$$F(2) = F(1) + F(0) = 1 + 0 = 1$$

$$F(3) = F(2) + F(1) = 1 + 1 = 2$$

$$F(4) = F(3) + F(2) = 2 + 1 = 3$$

$$F(5) = F(4) + F(3) = 3 + 2 = 5$$

$$F(6) = F(5) + F(4) = 5 + 3 = 8$$

...

Fibonacci è collegato alla sezione aurea (proporzioni perfette)...

Un esempio dell'utilità di Fibonacci è la costruzione dei coefficienti di un prodotto notevole:

$$(x+y)^2 = x^2 + 2xy + y^2 \rightarrow 1 \quad 2 \quad 1$$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 \rightarrow 1 \quad 3 \quad 3 \quad 1$$

Possiamo ricavare

$$(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \quad \text{con } \binom{n}{i} = \frac{n!}{i! \cdot (n-i)!}$$

**Esempio**

$$\begin{array}{cccc} \binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3} \\ 1 & 3 & 3 & 1 \end{array}$$

**Dimostrare che**  $(x+y)^n = \sum_{i=0}^n \binom{n}{i} x^i y^{n-i}$

Base:  $n = 0$

$$(x+y)^0 = \sum_{i=0}^0 \binom{0}{i} = \binom{0}{0} = 1 \quad [vero]$$

Dimostrazione per induzione

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n \cdot (x+y) \\ &= \left( \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right) \cdot (x+y)\end{aligned}$$

$$\sum_{i=0}^{n+1} \binom{n+1}{i} x^i y^{n+1-i}$$

$$\begin{aligned}(x+y)^{n+1} &= (x+y)^n \cdot (x+y) \\ &= \left( \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \right) \cdot (x+y) \\ &= \left( \sum_{i=0}^n \binom{n}{i} x^{i+1} y^{n-i} \right) + \left( \sum_{i=0}^n \binom{n}{i} x^i y^{n+1-i} \right) \\ &\rightarrow \sum_{i=0}^n 2^{i+1} = 2^1 + 2^2 + 2^3 + 2^4 \Rightarrow \sum_{i=0}^4 2^j \quad \text{con } j = i+1 \\ &= \left( \sum_{j=0}^{n+1} \binom{n}{j-1} x^j y^{n-(j-1)} \right) + \left( \sum_{i=0}^n \binom{n}{i} x^i y^{n+1-i} \right) \\ &= \text{to be continued...}\end{aligned}$$

## 7 Logica matematica

Non tutto ciò che viene utilizzato in matematica può essere rappresentato su un computer. Per esempio  $\forall x$ ,  $\exists x$  non possono essere rappresentate in quanto sono infiniti.

Per ovviare a questo problemi dobbiamo definire formalmente il linguaggio matematico, e creare definizioni a partire dal linguaggio naturale.

Esempio:

$3 \rightarrow$  è un espressione/termine

Ma il 3 è un simbolo che per convenzione rappresenta quel valore.

Oltre alle espressioni esistono le **formule**, che possono essere **atomiche** o **non atomiche**.

Esempio:

3 divide 21

Il "3" è un'espressione, il "divide" una relazione (binaria in questo caso) mentre il "21" è un'espressione costante.

Esempio:

$11 + 6$  è un numero primo

Il simbolo "+" è un'operazione. La differenza tra un'operazione e una relazione è che mentre una relazione restituisce un booleano, un'operazione ritorna un numero.

### 7.1 Connettivi logici

- AND,  $\wedge$ , e
- OR,  $\vee$ , oppure
- NOT,  $\neg$ , non
- implicazione,  $\rightarrow$ ,  $\Rightarrow$
- sse,  $\leftrightarrow$ ,  $\Leftrightarrow$

#### 7.1.1 Tabella di verità

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$\neg A \vee \neg B$
0	0	0	0	1	1
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	1	1	1

## 7.2 Esercizi formalizzazione

Esempio:

$\underbrace{\forall}_{\text{quantificatore}} x(x \text{ divide } 11) \Rightarrow \text{Ogni numero divide } 11$

### 7.2.1 Esercizio

"*Ogni studente ama tutti i professori*", formalizzare in linguaggio matematico.

Come prima cosa fisso l'universo del discorso, in questo caso gli *essere umani*.

Dopo mi accorgo che "*Ogni ... tutti*" corrisponde al quantificatore universale (mentre se fosse stato "*Ogni ... qualche*" sarebbe stato il quantificatore esistenziale).

Traduzione di  $x$  ama  $y$ :

$$xAy \Leftrightarrow x \text{ ama } y$$

$$S(x) \Leftrightarrow x \text{ è uno studente}$$

$$P(x) \Leftrightarrow x \text{ è un professore}$$

$$\forall x(xAy) \rightarrow \text{Ogni essere umano ama } y \text{ (} x \text{ variabile vincolata, } y \text{ libera)}$$

$$\forall x \forall y(xAy) \rightarrow \text{Ogni essere umano ama ogni altro essere umano}$$

$$\exists x \forall y(xAy) \rightarrow \text{Esiste un essere umano che ama tutti gli esseri umani}$$

$$\forall y \exists x(xAy) \rightarrow \text{Ogni essere umano è amato da almeno un altro essere umano}$$

$$\forall x(S(x) \wedge xAy) \rightarrow \text{Ogni essere umano è uno studente, ed inoltre ama } y$$

$$\forall x(S(x) \rightarrow xAy) \rightarrow \text{Comunque scelgo un essere umano, nel caso sia uno studente, allora ama } y$$

$$\rightarrow \text{Ogni essere umano che è uno studente ama } y$$

$$\rightarrow \text{Ogni studente ama } y$$

$$\forall x(S(x) \rightarrow \exists y(P(y) \wedge xAy)) \rightarrow \text{Ogni studente ama qualche professore}$$

$$\forall x(S(x) \rightarrow \exists y(P(y) \rightarrow xAy)) \rightarrow \text{Ogni studente ama qualche professore}$$

### 7.3 Regola

Per limitare la portata di un **quantificatore universale** con la proprietà P:

$$\forall z(P(z) \rightarrow \dots)$$

mentre per limitare la portata di un **quantificatore esistenziale** con la proprietà P:

$$\exists z(P(z) \wedge \dots)$$

#### 7.3.1 Esercizio

"Nessuno studente ama ogni corso", formalizzare in linguaggio matematico.

$$xAy \Leftrightarrow x \text{ ama } y$$

$$S(x) \Leftrightarrow x \text{ è uno studente}$$

$$C(x) \Leftrightarrow x \text{ è un corso}$$

$$\text{sono equivalenti} \Rightarrow \left\{ \begin{array}{l} \underbrace{\neg \exists (S(x))}_{\text{nessuno studente}} \wedge \underbrace{\forall y (C(y) \rightarrow xAy)}_{\text{ogni corso ama}} \\ \underbrace{\forall x (S(x))}_{\text{ogni studente}} \rightarrow \underbrace{\exists y (C(y) \wedge \neg (xAy))}_{\text{qualche corso non ama}} \end{array} \right.$$

### 7.4 Equivalenze logiche

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$$

$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

$$\neg(A \rightarrow B) \Leftrightarrow \neg(\neg A \vee \neg B) \Leftrightarrow \neg\neg A \wedge \neg\neg B \Leftrightarrow A \wedge \neg B$$

$$\neg\forall P(x) \Leftrightarrow \exists x\neg P(x)$$

$$\neg\exists xP(x) \Leftrightarrow \forall x\neg P(x)$$

Esempio di utilizzo:

$\begin{aligned} \forall x(S(x) \rightarrow \exists y(C(y) \wedge \neg(xAy))) &\Leftrightarrow \forall x\neg(S(x) \wedge \forall y(C(y) \rightarrow xAy)) \\ &\Leftrightarrow \forall x(\neg S(x) \vee \neg\forall y(C(y) \rightarrow xAy)) \\ &\Leftrightarrow \forall x(\neg S(x) \vee \exists y\neg(C(y) \rightarrow xAy)) \\ &\Leftrightarrow \forall x(\neg S(x) \vee \exists y(C(y) \wedge \neg(xAy))) \\ &\Leftrightarrow \forall x(S(x) \rightarrow \exists y(C(y) \wedge \neg(xAy))) \end{aligned}$	<p><i>Regole utilizzate</i></p> <p><i>De Morgan</i></p> <p><math>\neg\forall y \Leftrightarrow \exists y\neg</math></p> <p><math>\neg(A \rightarrow B) \Leftrightarrow A \wedge \neg B</math></p> <p><math>\neg A \vee B \Leftrightarrow A \rightarrow B</math></p>
--	---

## 7.5 Limitazione portata

Se  $n$  è un numero dispari, allora

$$D(x) \text{ è dispari sse. } x \text{ è dispari sse. } \exists k(x = 2k + 1)$$

Se l'universo del discorso è quello dei numeri reali allora

$$\forall n \exists k(n = 2k + 1) \quad \text{dove le variabili} \in \mathbb{R}$$

ovvero che esiste un  $k$  tale che  $n$  si scrive come  $2k + 1$ . Tradotto in linguaggio naturale: "per ogni numero reale ne esiste un altro che è uguale al doppio più uno del numero".

Ora però devo limitare la portata delle variabili ai soli numeri naturali:

$$\forall n(\text{se } n \text{ è un intero} \rightarrow \exists k(k \text{ è un intero} \wedge n = 2k + 1))$$

Inizio ora a definire la portata

$$I(x) \Leftrightarrow x \text{ è un intero}$$

posso ora riscrivere

$$\forall n(I(n) \rightarrow \exists k(I(k) \wedge n = 2k + 1))$$

### 7.5.1 Esempio

Se 0 è un intero, allora  $(x + 1)$ ,  $(x - 1)$  sono interi.

Nient'altro è intero.

Definisco la portata:

$$I(x) \Leftrightarrow x = 0 \vee \exists k(I(k) \wedge ((x = k + 1) \vee (x = k - 1)))$$

Definisco la legge:

$$P(x) \Leftrightarrow (x \neq 0) \wedge (x \neq 1) \wedge \forall k(\exists q(x = kq) \rightarrow k = 1 \vee k = x)$$

## 7.6 Esercizi

### 7.6.1 Esercizio 1

Formalizzare: *Ogni studente che ama la combinatoria non ama l'analisi*

$$\left. \begin{array}{l} xAy \Leftrightarrow x \text{ ama } y \\ \text{analisi} \text{ è analisi} \\ \text{combinatoria} \text{ è combinatoria} \\ S(x) \Leftrightarrow x \text{ è uno studente} \\ M(x) \Leftrightarrow x \text{ è una materia di studio} \end{array} \right\} \text{definisco le variabili e le relazioni}$$

$$\forall x (S(x) \wedge (x A \text{ combinatoria}) \rightarrow \neg(x A \text{ analisi}))$$

### 7.6.2 Esercizio 2

Formalizzare: *Giovanni non ama ogni animale non feroce*

$$\left. \begin{array}{l} xAy \Leftrightarrow x \text{ ama } y \\ G \text{ è Giovanni} \\ An(x) \Leftrightarrow x \text{ è un animale} \\ F(x) \Leftrightarrow x \text{ è feroce} \end{array} \right\} \text{definisco le variabili e le relazioni}$$

$$\forall y (An(y) \wedge \neg(F(y)) \rightarrow \neg(GAy))$$

## 7.7 Tutorato

### 7.7.1 Esercizio formalizzazione

Tradurre in linguaggio matematico la seguente espressione:

Il professore dice: "se studierete passerete l'esame"

Definisco le variabili:

$S(x) \Leftrightarrow x$  ha studiato

$P(x) \Leftrightarrow x$  ha passato l'esame

Il professore dice la verità? Nei casi dove l'ultima colonna è 1, significa che il professore ha detto la verità

studiato	passo l'esame	studio $\rightarrow$ passo l'esame
0	0	1
0	1	1
1	0	0
1	1	1

### 7.7.2 Esercizio dimostrazione

Dimostrare che

$$\forall n \in \mathbb{N} \quad n^2 \text{ è pari} \rightarrow n \text{ è pari}$$

Inizio la dimostrazione, sapendo che  $A \rightarrow B \Rightarrow \neg B \rightarrow \neg A$

$$\neg(n \text{ è pari}) \rightarrow \neg(n^2 \text{ è pari})$$

$$(n \text{ è dispari}) \rightarrow (n^2 \text{ è dispari})$$

$$2k + 1 \rightarrow (2k + 1)^2 \quad \text{è dispari}$$

$$(2k + 1)^2 = 4k^2 + 4k + 1$$

$$= 2(2k^2 + 2k) + 1$$

$$\underbrace{\quad\quad\quad}_{\text{pari}} + 1$$
$$\underbrace{\quad\quad\quad}_{\text{dispari}}$$

### 7.7.3 Esercizio connettivi

Dimostriamo che la seguente proposizione è una tautologia (sempre vera):

$$(((B \wedge \neg C) \wedge (A \wedge C)) \vee B) \rightarrow (A \vee B)$$

Ci chiediamo quando è falsa. Se non lo è mai, è sempre vera:

$$A \vee B = 0 \quad \text{sse} \quad A = 0, B = 0$$

$$A \wedge C = 0$$

$$(B \wedge \neg C) \wedge (A \wedge C) = 0$$

$$(B \wedge \neg C) \wedge (A \wedge C) \vee B = 0$$



#### 7.7.4 Esercizio formalizzazione

Formalizzare la seguente frase:

*Marco legge solo romanzi gialli*

Definisco le variabili:

$m = \text{Marco}$  [costante]

$L(x, y) \Leftrightarrow x$  legge  $y$

$G(x) \Leftrightarrow x$  è un romanzo giallo

Inizio formalizzazione

$\exists x(G(x) \wedge L(m, x))$  esiste un romanzo giallo letto da Marco

$\neg \exists x(\neg G(x) \wedge L(m, x))$  non esiste un libro non giallo che Marco non abbia letto

$\forall x(L(m, x) \rightarrow G(x))$  ogni libro letto da marco è un romanzo giallo

#### 7.7.5 Esercizio formalizzazione

Formalizzare la seguente frase:

*Marco ha letto tutti i romanzi di Camilleri e nient'altro*

Definisco le variabili:

$m = \text{Marco}$  [costante]

$L(x, y) \Leftrightarrow x$  legge  $y$

$C(x) \Leftrightarrow x$  è un romanzo di Camilleri

Inizio formalizzazione

$\forall x(C(x) \rightarrow L(m, x)) \wedge \forall x(L(m, x) \rightarrow C(x))$

Ogni libro di Camilleri è stato letto da Marco, e tutti i libri che Marco ha letto sono di Camilleri

### 7.7.6 Esercizio formalizzazione

Formalizzare la seguente frase:

*Non è vero che a tutti gli studenti a cui piace matematica piace anche la fisica*

Definisco le variabili:

$m$  = matematica [costante]

$f$  = fisica [costante]

$P(x, y) \Leftrightarrow$  a  $x$  piace  $y$

$S(x) \Leftrightarrow x$  è uno studente

Inizio formalizzazione

$\exists x(S(x) \wedge P(x, m) \wedge \neg P(x, f))$

Esiste un essere umano, che è uno studente, a cui piace la matematica e non la fisica

### 7.7.7 Esercizio formalizzazione

Formalizzare la seguente frase:

*I romanzi letti da Marco, sono tutti di autori diversi*

Definisco le variabili:

$m$  = Marco [costante]

$L(x, y) \Leftrightarrow x$  legge  $y$

$A(x, y) \Leftrightarrow x$  è autore di  $y$

$S(x) \Leftrightarrow x$  è uno scrittore

$R(x) \Leftrightarrow x$  è un romanzo

Inizio formalizzazione

La frase è logicamente equivalente a: "Due romanzi distinti letti da Marco sono di autori diversi".

$$\forall xyz \left( \underbrace{R(x) \wedge R(y) \wedge x \neq y \wedge S(z) \wedge L(m, x) \wedge L(m, y)}_{\text{premissa}} \wedge \overbrace{A(z, x) \rightarrow \neg(A(z, y))}^{\text{sono di autori diversi}} \right)$$

se  $z$  è uno scrittore
se  $m$  li ha letti entrambi
implicazione

Regole per la trasformazione:

$$\forall P(x) \Leftrightarrow \neg \neg \forall x P(x)$$

$$\forall xyz P(xyz) \Leftrightarrow \neg \neg (\exists xyz (P(xyz)))$$

$$\Leftrightarrow \neg (\exists xyz (\neg P(xyz)))$$

Altra formalizzazione

$$\neg \exists xyz (R(x) \wedge R(y) \wedge x \neq y \wedge S(z) \wedge L(m, x) \wedge L(m, y) \wedge A(z, x) \wedge A(z, y))$$

### 7.7.8 Esercizio formalizzazione

Formalizzare la seguente frase:

*Esistono solamente due numeri naturali distinti la cui somma è 4*

Inizio formalizzazione

$$\exists xy \in \mathbb{N}((x \neq y \wedge x + y = 4) \vee kj \in \mathbb{N}(4 = k, j \rightarrow k = x \vee j = y))$$

### 7.7.9 Esercizio dimostrazione

Dimostrare:

$$\forall x \in A(P(x) \vee Q(x)) \Leftrightarrow ((\forall x \in A(P(x))) \vee (\forall x \in A(Q(x))))$$

Inizio dimostrazione

Dimostro con un controesempio che l'enunciato è falso:

$$A = \mathbb{N}$$

$$P(x) \Leftrightarrow x \text{ è un numero primo}$$

$$Q(x) \Leftrightarrow x \text{ non è un numero primo}$$

$$\forall x \in \mathbb{N}(x \text{ è primo} \vee x \text{ non è primo})$$



per ogni numero intero positivo, o è primo o non lo è

ogni numero intero positivo non è primo

$$\forall x \in \mathbb{N}(x \text{ è primo}) \vee \forall x \in \mathbb{N}(x \text{ non è primo})$$



ogni numero intero positivo è primo

L'enunciato è falso in quanto non sono logicamente equivalenti

### 7.7.10 Esercizio dimostrazione

Dimostrare:

$$\exists x \in \mathbb{N}(P(x) \wedge Q(x)) \Leftrightarrow (\exists x \in A(P(x))) \wedge (\exists x \in A(Q(x)))$$

Inizio dimostrazione

Dimostro con un controesempio che l'enunciato è falso:

$$A = \mathbb{N}$$

$$P(x) \Leftrightarrow x \text{ è un numero primo}$$

$$Q(x) \Leftrightarrow x \text{ non è un numero primo}$$

$$\exists x \in \mathbb{N}(P(x) \wedge Q(x)) \Leftrightarrow (\exists x \in A(P(x))) \wedge (\exists x \in A(Q(x)))$$

ogni numero è primo e non è primo



esiste un numero non primo in  $\mathbb{N}$



L'enunciato è falso in quanto non sono logicamente equivalenti

### 7.7.11 Esercizio dimostrazione per casa

Dimostrare:

$$\exists n \in \mathbb{N}^+ \left( \sum_{i=1}^{2n} i = 2n^2 \right)$$

Inizio dimostrazione

Per casa 03-11-2015

## 8 Tecniche di dimostrazione

Tecniche elementari di dimostrazione

- **Dimostrazione enunciato universale:**

$$\forall x P(x)$$

*Prova:* Supponiamo che  $x$  sia un elemento arbitrario dell'universo ...  $x$  verifica la proprietà  $P$

- **Dimostrare che**

$$\forall x P(x) \quad \text{è falso}$$

Ovvero dimostrare che  $\neg \forall x P(x)$  è vero.

*Prova:* si cerca un controesempio, ovvero un elemento dell'universo per cui  $P(e)$  è falsa

- **Dimostrazione enunciato esistenziale**

$$\exists x P(x)$$

*Prova:* cerco un elemento dell'universo che verifica  $P$

- **Dimostrare che**

$$\exists x P(x) \quad \text{è falso}$$

*Prova:* verifico che ogni elemento  $x$  dell'universo verifica la proprietà  $\neg P(x)$ . Sia  $x$  un elemento dell'universo ...  $x$  non verifica  $P$

- **Dimostrare che**

$$\exists x P(x)$$

*Prova:* supponiamo per assurdo che non esista  $x$  che soddisfi la proprietà  $P$  ... contraddizione

- **Dimostrazione contropositiva**

se  $A$  allora  $B$

*Prova:* provo che  $\neg B \rightarrow \neg A$

## 8.1 Esempi di dimostrazioni

**Teorema:**

$$\forall n(n^2 + 7n + 12) \text{ è pari}$$

*Prova:* sia  $n$  un numero naturale

$$n^2 + 7n + 12 \quad \text{tolgo il 12 perché è pari}$$

$$n(n + 7)$$

dividiamo la prova per casi:

$$\begin{cases} n \text{ dispari: } \text{dispari} + \text{dispari} = \text{pari} [(n + 7)]. \text{ dispari} \times \text{pari} = \text{pari} [n(n+7)] \\ n \text{ pari: } \text{pari} \times \text{dispari} = \text{pari} [n(n + 7)] \end{cases}$$

**Teorema:**

$$\forall n(7n + 2) \text{ è un quadrato}$$

*Prova:* controesempio:  $n = 7$

$$7 \cdot 7 + 2 = 51 \quad \text{non è un quadrato, enunciato falso}$$

**Teorema:**

*Esistono numeri irrazionali  $A$  e  $B$  tali che  $A^B$  è razionale*

*Prova:* supponiamo per assurdo che l'enunciato sia falso

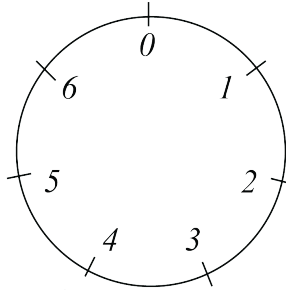
$$A = B = \sqrt{2}$$

$$A^B = (\sqrt{2})^{\sqrt{2}} \quad \text{è irrazionale}$$

$$\left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} \quad \text{è irrazionale} \rightarrow (\sqrt{2})^{\sqrt{2}} = 2 \quad \text{contraddizione, 2 è razionale}$$

se 2 è razionale, abbiamo dimostrato che il teorema è vero, in quanto inizialmente supposto falso.

## 9 Aritmetica modulare



Comunque scelgo un numero  $\in \mathbb{N}$  riesco a rappresentarlo tramite  $n \bmod 7$ . Così facendo riduco l'aritmetica a 7 numeri.

Quando due numeri sono rappresentabili dalla stessa cifra? Quando il resto della divisione intera è uguale:

$$x \equiv y \Leftrightarrow x \bmod n = y \bmod n$$

Quando  $x - y$  è divisibile per  $n$ ?

$$\left. \begin{array}{l} x = q_1 \cdot n + r_1 \\ y = q_2 \cdot n + r_2 \end{array} \right\} 0 \leq r < 7$$

$$x - y = \underbrace{(q_1 - q_2)n}_{\text{divisibile per } n} + \cancel{(r_1 - r_2)}$$

### 9.1 Proprietà

#### Somma

- $x + (y + z) = (x + y) + z$
- $x + y = y + x$
- $x + (-x) = 0$       elemento opposto
- $x + 0 = x$       elemento neutro

La somma è un gruppo additivo che è commutativo

#### Prodotto

- $x(yz) = (xy)z$
- $xy = yx$
- $x \cdot 1 = x$       elemento neutro
- $x \cdot 0 = 0$
- $x \cdot x^{-1} = 1$        $\forall x \neq 0$       inverso

Gruppo moltiplicativo

**Calcolo dell'inverso:** l'inverso si può calcolare solo quando il modulo è un numero primo, altrimenti, in caso di modulo non primo, gli unici numeri invertibili sono quelli primi fra loro con il modulo.  
In modulo 7 per esempio:

$$\begin{aligned} 2 \cdot 4 &\equiv_7 1 && \text{l'inverso del 2 è il 4, in aritmetica modulare mod 7} \\ 3 \cdot 5 &\equiv_7 1 \\ 6 \cdot 6 &\equiv_7 1 \end{aligned}$$

Quando siamo in un aritmetica modulare modulo  $n$ , ed  $n$  è un numero primo, abbiamo un campo numerico.

## 9.2 Proprietà fondamentali del modulo

Tre **proprietà fondamentali** nell'aritmetica modulare:

Presi due numeri interi  $A$  e  $B$ :

$$\begin{aligned} (A + B) \bmod n &= ((A \bmod n) + (B \bmod n)) \bmod n \\ (A \cdot B) \bmod n &= ((A \bmod n) \cdot (B \bmod n)) \bmod n \\ A^k \bmod n &= (A \bmod n)^k \bmod n \end{aligned}$$

### 9.2.1 Esempi di utilizzo

Calcolare il modulo di numeri molto grandi

$$\begin{aligned} (125342\color{red}{3} \cdot 13443\color{red}{2}) \bmod 5 &= \\ &= (3 \cdot 2) \bmod 5 \\ &= 6 \bmod 5 = 1 \end{aligned}$$

$$\begin{aligned} 2^{99} \bmod 7 &= \\ &= 2^{9 \cdot 11} = (2^9)^{11} \\ &= (2^3 \cdot 2^3 \cdot 2^3)^{11} = \\ &= (1 \cdot 1 \cdot 1)^{11} \equiv_7 1 \end{aligned}$$

$$\begin{aligned} 34^{217} \bmod 7 &= \\ &= 37 \equiv_7 -1 \\ &= (-1)^{217} \equiv_7 -1 \equiv_7 6 \end{aligned}$$

$$3^{1227645} \bmod 12 \equiv 3 \quad \text{perchè } 3^i \bmod 12 = 1, \underbrace{3, 9}_{\text{periodo}}, 3, 9, 3, 9, \dots$$

## 9.3 Periodo

L'operazione  $a^b \bmod n$  è periodica a partire da un valore  $h \leq n$  con periodo di un certo  $t$ .

Esempio in aritmetica modulo 7:

$$\begin{array}{ccccccc} \underbrace{2^0 \equiv 1 \quad 2^1 \equiv 2 \quad 2^2 \equiv 4}_{\text{periodo}} & 2^3 \equiv 1 & 2^4 \equiv 2 & 2^5 \equiv 4 & \dots & t = 3 \\ \underbrace{3^0 \equiv 1 \quad 3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6}_{\text{periodo}} & 3^4 \equiv 1 & 3^5 \equiv 3 & \dots & t = 4 \end{array}$$



### Dimostrare il periodo

$$\begin{aligned}
& a^1 \bmod n \quad a^2 \bmod n \quad \dots \quad a^{n+1} \bmod n \\
& \left. \begin{aligned} 1 \leq h \leq n+1 \\ 1 \leq k \leq n+1 \end{aligned} \right\} a^h \bmod n = a^k \bmod n \\
& a^{h+1} \bmod n = a^{k+1} \bmod n \Rightarrow a^{h+i} \bmod n = a^{k+i} \bmod n \quad \forall i
\end{aligned}$$

### 9.4 MCD e teorema di Eulero

$$\text{MCD}(a, b) \in \mathbb{N}$$

$$\text{mcm}(a, b) \in \mathbb{N}$$

Come si calcolano MCD e mcm?

$$\begin{aligned}
100 &= 2 \cdot 5^2 & 46 &= 2 \cdot 23 \\
\text{MCD}(100, 46) &= 2 & \text{mcm}(100, 46) &= 2^2 \cdot 23 \cdot 5^2
\end{aligned}$$

#### Teorema di Eulero

$$\begin{aligned}
& \text{MCD}(a, b) = b \text{ se } b \mid a \text{ altrimenti} \\
& \text{se } b \nmid a \text{ allora } \text{MCD}(a, b) = \text{MCD}(b, \text{resto}(a, b))
\end{aligned}$$

Perché questo teorema è più efficiente?

Dati due numeri  $a$  e  $b$ , posso scrivere  $a$  come  
 $a = b \cdot q + r$  con  $0 < r < b$   
 ora prendo un divisore comune di  $a$  e  $b$  :  
 se il divisore  $\mid a$ , allora divide anche  $a - q \cdot b$  (ovvero il resto)

$$\begin{aligned}
a &= d \cdot s_1 & b &= d \cdot s_2 \\
r &\rightarrow a - q \cdot b = d \cdot s_1 - d \cdot s_2 = \underbrace{d(s_1 - s_2)}_{d \mid r}
\end{aligned}$$

$$\begin{aligned}
a &= q \cdot b + r \\
&= q(e \cdot t_1) + e \cdot t_2 \\
&= \underbrace{e(q \cdot t_1 + t_2)}_{e \mid a}
\end{aligned}$$

Regola generalizzata

$$\begin{aligned}
a &= b \cdot q_1 + r_1 & \text{con } 0 \leq r_1 < b \\
b &= r_1 \cdot q_2 + r_2 & \text{con } 0 \leq r_2 < r_1 \\
r_1 &= r_2 \cdot q_3 + r_3 & \text{con } 0 \leq r_3 < r_2 \\
r_2 &= r_3 \cdot q_4 + r_4 & \text{con } 0 \leq r_4 < r_3 \\
r_{n-1} &= r_n \cdot q_n + r_{n+1} & \text{con } 0 \leq r_{n+1} < r_{n-2} \\
r_n &= r_{n+1} \cdot q_{n+1} + \textcolor{red}{r_{n+2}} & \text{con } 0 \leq r_{n+2} < r_{n+1}
\end{aligned}$$

Dove MCD è l'ultimo resto diverso da zero  $[r_{n+2}]$

### Esercizio

$$\text{MCD}(1024, 666) =$$

$$1024 = 1 \cdot 666 + 358$$

$$666 = 1 \cdot 358 + 308$$

$$358 = 1 \cdot 308 + 50$$

$$308 = 6 \cdot 50 + 8$$

$$50 = 6 \cdot 8 + 2 \rightarrow \text{MCD}$$

$$8 = 4 \cdot 2 + 0$$

Due numeri si dicono primi fra loro se il loro MCD è uguale a 1.

## 9.5 Proprietà di Bezut

Siano  $a, b, c \neq 0$  allora l'equazione  $ax + by = c$  ha soluzioni intere se  $\text{MCD}(a, b)$  divide  $c$ .

In particolare se  $\text{MCD}(a, b) = 1$  allora l'equazione  $ax + by = c$  ha soluzione per ogni  $c$ .

### Esempio

$$120x + 8y = 12$$

$$\text{MCD}(120, 8) = 8 \quad \text{quindi devo trovare una combinazione lineare che dia 3}$$

$$\text{MCD}\left(\frac{120}{8}, \frac{8}{8}\right) = \frac{3}{1} \rightarrow \text{MCD}(15, 1) = 1$$

$$40x + 27y = 1$$

$$-2 \cdot 40 + 3 \cdot 27 = 1$$

$$12 \cdot (-2 \cdot 40) + 12 \cdot (3 \cdot 27) = 12 \cdot 1$$

$$-960 + 972 = 12$$

$$-960 = -960$$

$$0 = 0 \quad \checkmark$$

### Esempio

Trovare la combinazione lineare che soddisfi

$$7x + 14y = 5$$

5 non divide 7

$$\text{MCD}(7, 14) = 7 \quad \text{non ammette soluzioni intere}$$

## 9.6 Equivalenze

$$ax \equiv_c b$$

### Esercizio

$$3x \equiv_5 2$$

$$5 \mid \underline{3x + 2}$$

combinazione lineare di 3 e 2

$$3^{-1} \cdot 3x = 3^{-1} \cdot 2 \Rightarrow$$

$$x = 3^{-1} \cdot 2$$

$$x = 2 \cdot 2$$

$$x = 4 \quad \checkmark$$

### Esercizio

$$4x \equiv_{13} 11 \quad 11 \text{ è un numero primo, forma un campo numerico. Tutti i numeri } \neq 0 \text{ sono invertibili}$$

$$x = 4^{-1} \cdot 11$$

$$= 10 \cdot 11 \quad \text{mod } 13$$

$$= 110 \text{ mod } 13$$

$$= 6$$

$$4 \cdot 6 \equiv_{13} 11$$

$$24 \equiv_{13} 11$$

### Esercizio

$$2x \equiv_{15} 7 \quad 15 \text{ non è un numero primo. Gli unici numeri invertibili sono quelli primi fra loro con il modulo}$$

$$x = 2^{-1} \cdot 7$$

$$= 8 \cdot 7 \quad \text{mod } 15$$

$$= 56 \text{ mod } 15$$

$$= 11$$

$$2 \cdot 11 \equiv_{15} 7$$

$$22 \equiv_{15} 7 \quad \checkmark$$

## 9.7 Congruenze lineari

$$ax \equiv_n c \quad (n \geq 2, a \not\equiv_n 0)$$

$$n \mid ax - c \rightarrow ax - c = q \cdot n$$

$$ax - q \cdot n = c \rightarrow 1 \text{ soluzione intera se } MCD(a, n) \mid c$$

In una congruenza lineare, ci sono tante soluzioni quante  $MCD(a, n)$  E

### 9.7.1 Esempio 1

$$3x \equiv_{12} 6$$

$$MCD(3, 6) = 3 \mid 6? \text{ Si, 1 soluzione intera, } \rightarrow x = 2$$

### 9.7.2 Esempio 2

$$224x \equiv_8 46$$

$$MCD(224, 8) = 8 \mid 46? \text{ No, nessuna soluzione}$$

### 9.7.3 Esempio 3

$$ax + by$$

$$124x \equiv_{71} 17$$

$$MCD(124, 71) = 1 \mid 17? \text{ Si, 1 soluzione, ma quale?}$$

$$x \equiv_{71} 124^{-1} \cdot 17 \quad 124 \equiv_{71} 53$$

$$x \equiv_{71} 53^{-1} \cdot 17 \text{ e cerco la soluzione ...}$$

oppure

Controllo che 17 sia una combinazione lineare di 53 e 71:

$$53x + \underbrace{71y}_{\equiv_{71} 0} \equiv_{71} 17$$

$$53 \cdot 3 + 71 \cdot (-2) \equiv_{71} 17$$

$$x = 3 \quad y = -2$$

### 9.7.4 Esempio 4

$$7074x \equiv_{123} 865 \quad 865 \equiv_{123} 4$$

$$7074x \equiv_{123} 4 \quad 7074 \equiv_{123} 63$$

$$63x \equiv_{123} 4 \rightarrow$$

$$123 = 3 \cdot 41$$

$$63 = 3 \cdot 21$$

$$MCD(123, 63) = 3 \mid 4? \text{ No, nessuna soluzione}$$

## 9.8 Teorema cinese del resto

Siano  $n_1, \dots, n_k$  interi positivi a due a due primi fra loro

$$MCD(n_i, n_j) = 1 \quad \text{se } i \neq j$$

$$x \equiv_{n_1} a_1$$

$$x \equiv_{n_2} a_2$$

...

$$x \equiv_{n_k} a_k$$

ammette un'unica soluzione minore di  $n_1 \cdot n_2 \cdot \dots \cdot n_k$

### 9.8.1 Esempio senza teorema cinese

$$x \equiv_3 2 \quad a$$

$$x \equiv_5 3 \quad b$$

$$x \equiv_7 2 \quad c$$

Il sistema ammette 1 unica soluzione  $< 3 \cdot 5 \cdot 7 = 105$

$$\left. \begin{array}{l} a : \quad 2, 5, 8, 11, \dots, 2 + 3k \\ b : \quad 3, 8, 13, 18, \dots, 3 + 5s \\ c : \quad 2, 9, 16, 23, \dots, 2 + 7l \end{array} \right\} \text{ prendo la soluzione in comune}$$

$$\left. \begin{array}{l} a : \quad 8, 23, 38, 53, 68, 83, 98, \dots \\ b : \quad 23\dots \\ c : \quad 23\dots \end{array} \right\} \rightarrow 23 < 105$$

prova

$$N_r = n_1 \cdot n_2 \cdot \dots \cdot n_{r-1} \cdot n_{r+1} \cdot \dots \cdot n_k$$

$$MCD(N_r, n_r) = 1 \rightarrow \text{sono primi fra loro}$$

$$\bar{x} = a_1 \cdot \underbrace{N_1}_{\equiv_{n_1} 1} \cdot x_1 + a_2 \cdot N_2 \cdot x_2 + \dots + a_k \cdot N_k \cdot x_k$$

$$N_r x \equiv_{n_r} 1 \rightarrow \text{esiste una soluzione}$$

$$x \equiv_3 2 \quad n_1 = 3 \quad N_1 = 5 \cdot 7 = 35$$

$$x \equiv_5 3 \quad n_2 = 5 \quad N_2 = 3 \cdot 7 = 21$$

$$x \equiv_7 2 \quad n_3 = 7 \quad N_3 = 3 \cdot 5 = 15$$

$$MCD(n_1, N_1) = 1 \quad \text{primi fra loro}$$

$$MCD(n_2, N_2) = 1 \quad \text{primi fra loro}$$

$$MCD(n_3, N_3) = 1 \quad \text{primi fra loro}$$

$$\left. \begin{array}{l} N_1 x_1 \equiv_{n_1} 1 \\ N_2 x_2 \equiv_{n_2} 1 \\ N_3 x_3 \equiv_{n_3} 1 \end{array} \right\} \rightarrow \text{ammette una soluzione intera, } MCD(N_1 \cdot x_1, n_1) = 1 \mid \quad \checkmark$$

$$35x_1 \equiv_3 1 \quad 35 \equiv_3 2 \quad 2x_1 \equiv_3 1 \quad x_1 \equiv_3 1 \cdot 2^{-1} \quad x_1 \equiv_3 2$$

$$21x_2 \equiv_5 1 \quad 21 \equiv_5 1 \quad x_2 \equiv_5 1$$

$$15x_3 \equiv_7 1 \quad 15 \equiv_7 1 \quad x_3 \equiv_7 1$$

$$\bar{x} = (a_1 \cdot N_1 \cdot x_1) + (a_2 \cdot N_2 \cdot x_2) + (a_3 \cdot N_3 \cdot x_3)$$

$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1$$

$$= 233 \equiv_{105} 23 \quad \checkmark$$

## 9.9 Piccolo teorema di Fermat

Se  $p$  è un numero primo, e  $p$  non divide  $a$ , allora

$$a^{p-1} \equiv_p 1$$

**Esempio:**

$$5^6 \equiv_7 1$$

$$5^{30} \equiv_{31} 1$$

$$20^{30} \equiv_3 11$$

Se prendo i multipli di  $a$

$$a, 2a, 3a, \dots, (p-1)a$$

ovvero  $(p-1)$  multipli, deduco che

$$ka \not\equiv_p ra \quad \text{con } 1 \leq k \neq r \leq (p-1)$$

Se suppongo per assurdo che  $ka \equiv_7 ara$  sia vero. Se è vero allora

$$p \mid ka - ra = a(k-r)$$

da cui segue che

$$\underbrace{p \mid k-r}_{\text{impossibile}} \quad \text{perché } (k-r) < p$$

Quindi

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1) \cdot a \equiv_p (p-1)!$$

**Esempio numerico:**

$$p = 7 \quad a = 3$$

multipli di  $a$ : 3, 6, 2, 5, 1, 4 [tutti i numeri da 1 a 6 in disordine]

$$3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4 \equiv_7 6!$$

$$a^{p-1} \cdot (p-1)! \mod 7 \Rightarrow a^{p-1} \equiv_7 1 \quad \checkmark$$

**Esercizio:**

$$4^{253} \equiv_7 ?$$

Soluzione

$$4^{253} = 4^{6 \cdot 42 + 1} = 4 \cdot (4^6)^{42} \equiv_7 4 \cdot 1^{42} = 4$$

### 9.9.1 Teorema

Se  $p$  è un numero primo, allora  $a^p \equiv_p a$ .

#### Dimostrazione

$$\text{se } p \mid a, a^p \equiv_p 0$$

$$\text{se } p \nmid a, a^{p-1} \equiv_p 1$$

$$a \cdot a^{p-1} \equiv_p a$$

$$a^p \equiv_p a$$

#### Dimostrazione per induzione

Base:  $a = 0$  il teorema è ovvio ✓

Suppongo per induzione che  $a^p \equiv_p a$ :

$$(a+1)^p = a+1$$

$$= \sum_{i=0}^p \binom{p}{i} a^i \cdot 1^{p-i} = \binom{p}{0} + \underbrace{\binom{p}{1} a}_{\text{a lo divide}} + \cancel{\binom{p}{2} a^2} + \dots + \cancel{\binom{p}{p-1} a^{p-1}} + \binom{p}{p} a^p$$

$$\text{sapendo che } \binom{p}{i} = \frac{p!}{i!(p-i)!} \quad \binom{p}{0} = 1 \quad \binom{p}{p} = 1 \quad \text{deduco che}$$

$$(a+1)^p \equiv_p 1 + a^p \equiv_p 1 + a \quad \checkmark$$

Se  $p$  e  $q$  sono numeri primi diversi,  $a^p \equiv_p a$  e  $a^q \equiv_q a$ , allora  $a^{pq} \equiv_{pq} a$ .

#### Esempio:

$$p = 11 \quad q = 31$$

$$2^{11} \equiv_{31} 2$$

$$2^{31} \equiv_{11} 2$$

### 9.10 Teorema di Eulero

$\phi(n)$  = numero di elementi minori di  $n$  che sono relativamente primi con  $n$ .

Es.  $\phi(9) = 1, 2, 4, 5, 7, 8 = 6$

Se  $p$  è primo, allora  $\phi(p^k) = p^k - p^{k-1} = p^k \cdot (1 - \frac{1}{p})$

Se  $a$  e  $n$  sono primi fra loro,  $a^{\phi(n)} \equiv_n 1$

La funzione di Eulero è moltiplicativa:

$$\phi(nk) = \phi(n) \cdot \phi(k) \quad \text{se } n \text{ e } k \text{ sono primi fra loro}$$

#### Esempio:

$$\phi(9) = \phi(3^2) = 3^2 - 3 = 6$$

$$\phi(100) = \phi(4 \cdot 25) = \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2) = (2^2 - 2)(5^2 - 5) = 2 \cdot 20 = 20$$

## 9.11 Esercizi

### 9.11.1 Esercizio 1

Determinare  $12^{26} \equiv_{13}$

$$12 \equiv_{13} -1$$

$$\begin{aligned} 12^{26} &\equiv_{13} (-1)^{26} \\ &\equiv_{13} 1 \end{aligned}$$

### 9.11.2 Esercizio 2

Determinare le soluzioni di  $2x \equiv_4 3$

$$\text{MCD}(2, 4) = 2 \mid 3? \text{ No, nessuna soluzione}$$

### 9.11.3 Esercizio 3

Determinare le soluzioni di  $3x \equiv_4 2$ . Le soluzioni sono  $x = 2 + 4k, k \in \mathbb{Z}$

### 9.11.4 Esercizio 4

Determinare le soluzioni di  $6x \equiv_4 2$ . Le soluzioni sono  $x \equiv_4 2 + 4k, k \in \mathbb{Z}$

### 9.11.5 Esercizio 5

Determinare le soluzioni di  $3x \equiv_4 2$ . Le soluzioni sono  $x = 2 + 4k, k \in \mathbb{Z}$

## 9.12 Tutorato

### 9.12.1 Esercizio 1

Determinare  $-1027 \equiv_{16} ?$

$$\begin{aligned} -1027 &= -1(1024 + 3) \\ &= -1(2^{10} + 3) \\ &= -1(2^{4+6} + 3) \\ &= -1(16 \cdot 2^6 + 3) \\ &= -1(0 + 3) \\ &= -3 \\ &= 13 \bmod 16 \end{aligned}$$

$$\begin{aligned} (-1027)^{17} &\equiv_{16} (-3)^{17} \\ &\equiv_{16} (-3)^{4+4+4+4+1} \\ &\equiv_{16} (-3)^{4 \cdot 4 + 1} \\ &\equiv_{16} ((-3)^4)^4 \cdot (-3)^1 \\ &\equiv_{16} (81)^4 \cdot (-3) \\ &\equiv_{16} 1^4 \cdot (-3) \\ &\equiv_{16} -3 \\ &\equiv_{16} 13 \end{aligned}$$



### 9.12.2 Esercizio 2

Determinare  $19693^{12} \equiv_7 ?$

$$\begin{aligned} 19693^{12} &\equiv_7 (14770 + 4923)^{12} \\ &\equiv_7 4923^{12} \\ &\equiv_7 (4921 + 2)^{12} \\ &\equiv_7 2^{12} \\ &\equiv_7 2^{3 \cdot 4} \\ &\equiv_7 (2^3)^4 \\ &\equiv_7 (1)^4 \\ &\equiv_7 1 \end{aligned}$$

### 9.12.3 Esercizio 3

Determinare  $243^{270} \equiv_8 ?$

$$\begin{aligned} 243 &\equiv_8 (240 + 3)^{270} \\ &\equiv_8 3^{270} \\ &\equiv_8 3^2 \cdot 3^{268} \\ &\equiv_8 (3^2)^{268} \\ &\equiv_8 (1)^{268} \\ &\equiv_8 1 \end{aligned}$$

### 9.12.4 Esercizio 4

Determinare  $172! \equiv_{330} ?$

Dato che il fattoriale si compone come

$$172 \cdot 171 \cdot \dots \cdot 33 \cdot \dots \cdot 10 \dots \cdot 1$$

sarà sicuramente divisibile per 330, e quindi

$$172! \equiv_{330} 0$$

### 9.12.5 Esercizio 4

Determinare  $215^{26} \equiv_{13} ?$

$$\begin{aligned} 215^{26} &\equiv_{13} 7^{26} \\ &\equiv_{13} 7^{12+14} \\ &\equiv_{13} 1 \cdot 7^{12} \cdot 7^2 \quad \text{piccolo teorema di Fermat} \\ &\equiv_{13} 1 \cdot 1 \cdot 49 \bmod 13 \\ &\equiv_{13} 10 \end{aligned}$$

### 9.12.6 Esercizio 6

Determinare  $512^{99} \equiv_{11} ?$

$$\begin{aligned} 512^{99} &\equiv_{11} (512^{11})^9 \\ &\equiv_{11} ((2^9)^{11})^9 \\ &\equiv_{11} (2^9)^9 \quad \text{teorema di Fermat} \\ &\equiv_{11} 2^{81} \\ &\equiv_{11} 2^{80+1} \\ &\equiv_{11} 2^{8 \cdot 10 + 1} \\ &\equiv_{11} (2^{10})^8 \cdot 2 \\ &\equiv_{11} 1^8 \cdot 2 \quad \text{piccolo teorema di Fermat} \\ &\equiv_{11} 2 \end{aligned}$$

## 10 Relazioni

17-11-2015

Una relazione  $R$  di dominio  $A$  e codominio  $A$  è un sottoinsieme di  $A \times A$ :

$$R \subseteq A \times A$$

Le relazioni si dividono in due fasce:

- relazione di **ordinamento parziale**
- relazione di **equivalenza**

### 10.1 Relazione di ordinamento parziale

1. **proprietà riflessiva**: ogni elemento è in relazione con se stesso

$$\forall x(xRx)$$

2. **proprietà transitiva**: se  $x$  è in relazione con  $y$  e  $y$  è in relazione con  $z$  allora  $x$  è in relazione con  $z$

$$\forall xyz(xRy \wedge yRz \rightarrow xRz)$$

3. **proprietà antisimmetrica**: se  $x$  è in relazione con  $y$  e  $y$  è in relazione con  $x$  allora  $x = y$

$$\forall xy(xRy \wedge yRx \rightarrow x = y)$$

### 10.2 Relazione di equivalenza

1. **proprietà riflessiva**: ogni elemento è in relazione con se stesso

$$\forall x(xRx)$$

2. **proprietà transitiva**: se  $x$  è in relazione con  $y$  e  $y$  è in relazione con  $z$  allora  $x$  è in relazione con  $z$


$$\forall xyz(xRy \wedge yRz \rightarrow xRz)$$

3. **proprietà simmetrica**: se  $x$  è in relazione con  $y$  e  $y$  allora  $y$  è in relazione con  $x$

$$\forall xy(xRy \rightarrow yRx)$$

Da notare che la proprietà riflessiva, comune ad entrambe le fasce, non vale nel sottoinsieme ristretto

$2 \leq 2$  ha la proprietà riflessiva? 

$2 < 2$  ha la proprietà riflessiva? 

## 10.3 Esempi

### 10.3.1 Esercizio 1

Verifichiamo quali proprietà valgono in

$$xRy \text{ sse } x + y = 5 \quad \text{con } x, y \in \mathbb{N}$$

- proprietà riflessiva:

$$\forall x \in \mathbb{N} (xRx) \rightarrow x + x = 5$$

$$2x = 5$$

$$\text{controesempio: } 2 \cdot 10 = 5 \quad \text{✗}$$

- proprietà transitiva:

$$\begin{cases} x + y = 5 \\ x + z = 5 \end{cases} \text{ implica } x + z = 5$$

$$\text{controesempio: } x = 2, y = 3, z = 2$$

$$x + y = 2 + 3 = 5$$

$$y + z = 3 + 2 = 5$$

$$x + z = 2 + 2 = 5 \quad \text{✗}$$

- proprietà simmetrica:

$$x + y = 5 \rightarrow y + x = 5 \quad \text{✓}$$

- proprietà antisimmetrica:

$$x = 3, y = 2$$

$$\begin{cases} 3 + 2 = 5 \\ 2 + 3 = 5 \end{cases} \rightarrow 2 = 5 \quad \text{✗}$$

### 10.3.2 Esercizio 2

Verifichiamo quali proprietà valgono in

$$xRy \text{ sse } x \text{ e } y \text{ hanno la stessa altezza} \quad \text{con } x, y \in \{\text{aula 1}\}$$

- proprietà riflessiva: ✓
- proprietà transitiva: ✓
- proprietà simmetrica: ✓
- proprietà antisimmetrica: ✗

Questa relazione è una relazione di equivalenza, in quanto vengono soddisfatte tutte le proprietà necessarie.

### 10.3.3 Esercizio 3

Verifichiamo quali proprietà valgono in

$$xRy \text{ sse } x \equiv_5 y \quad \text{con } x, y \in \mathbb{Z}$$

- proprietà riflessiva:

$$x \equiv_5 x ?$$

$$5 \mid (x - x) \quad \checkmark$$

- proprietà transitiva:

$$\circ 5 \mid x - y$$

$$\circ 5 \mid y - z$$

$$x - y = 5 \cdot k \quad \text{per un certo } k$$

$$y - z = 5 \cdot r \quad \text{per un certo } r$$

$$(x - y) + (y - z) = 5k + 5r$$

$$5 \mid x - z = 5(k + r) \quad \checkmark$$

- proprietà simmetrica:

$$x \equiv_5 y \rightarrow y \equiv_5 x$$

$$5 \mid x - y \rightarrow x - y = 5 \cdot k \quad \text{per un certo } k$$

$$5 \mid y - x \rightarrow y - x = -5 \cdot k \quad \text{per un certo } k \quad \checkmark$$

- proprietà antisimmetrica: se vale la proprietà simmetrica, non può valere anche quella antisimmetrica.

Questa è una relazione di equivalenza a 5 classi.

### 10.3.4 Esercizio 4

Sia  $\mathbb{N}$  l'insieme dei numeri naturali.  $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$

$$R \subseteq \mathbb{N}^2 \times \mathbb{N}^2$$

$$(a, b)R(c, d) \text{ sse } a + b + 3 = c + d + 1$$

Verifico quali proprietà possiede

- riflessiva:  $\forall (x, y) \quad (x, y)R(x, y)$

$$x + y + 3 = x + y + 1 \quad \times$$

- irriflessiva:  $\forall (x, y) \quad \neg [(x, y)R(x, y)]$

$$x + y + 3 \neq x + y + 1 \quad \checkmark$$

- simmetrica:  $\forall (x, y) \quad (x, y)R(a, b) \rightarrow (a, b)R(x, y)$

$$a + b + 3 = c + d + 1$$

$$c + d + 3 = a + b + 1$$

$$c + d + 3 = (c + d + 1) + 2 = (a + b + 3) + 2 = a + b + 5 \neq a + b + 1 \quad \times$$

- transitiva:  $(a, b)R(c, d) \wedge (c, d)R(e, f) \rightarrow (a, b)R(e, f)$

$$a + b + 3 = c + d + 1 \quad \wedge \quad c + d + 3 = e + f + 1 \quad \rightarrow \quad a + b + 3 = e + f + 1$$

$$a + b + 3 = c + d + 1 = (c + d + 3) - 2 = (e + f + 1) - 2 = e + f - 1 \quad \times$$

- antisimmetrica:  $(a, b)R(c, d) \wedge (c, d)R(a, b) \rightarrow (a, b) = (c, d)$

$$a + b + 3 = c + d + 1 \rightarrow (a + b) - (c + d) = -2$$

$$c + d + 3 = a + b + 1 \rightarrow (a + b) - (c + d) = 2$$

l'ipotesi dell'implicazione è falsa, proprietà verificata  $\checkmark$

## 10.4 Teorema

Sia  $R \subseteq A \times A$  una relazione di equivalenza, allora se  $a \in A$ :

$$[a]_R = \{b \in A : aRb\}$$

Questa notazione indica una classe di equivalenza, ovvero il sottoinsieme di tutti gli elementi equivalenti ad  $a$ . Una notazione equivalente è  $a/_R = \{b \in A : aRb\}$

## 10.5 Partizioni

Una partizione di  $A$  è una famiglia di insiemi  $\{A_i\}$   $i \in \overset{\text{indici}}{I}$  tali che

- $A = \bigcup_{i \in I} A_i$
- Ogni coppia  $A_i, A_j$  con  $i \neq j$

$$A_i \cap A_j = \emptyset$$

### 10.5.1 Esempi

#### Esempio 1

$$A = \{1, 2, \dots, 16\}$$

$$I = \{a, b, c\}$$

Ogni indice deve essere associato ad un sottoinsieme di  $A$ .

---

Verificare che questa suddivisione sia una partizione di  $A$ :

$$A_a = \{2, 7, 8, 11, 15, 16\}$$

$$A_b = \{1, 3, 5\}$$

$$A_c = \{4, 9, 10\}$$

Controllo le intersezioni:

$$A_a \cap A_b = \emptyset$$

$$A_a \cap A_c = \emptyset$$

$$A_b \cap A_c = \emptyset$$

$$A_a \cup A_b \cup A_c \subsetneq A \quad \times$$

In quanto l'unione delle partizioni dovrebbe darmi l'insieme di partenza, questa suddivisione non è una partizione. Possiamo notare infatti che all'unione mancano gli elementi  $\{5, 6, 12, 13, 14\}$ .

---

Verificare che questa suddivisione sia una partizione di  $A$ :

$$A_a = \{n \in A : n \equiv 0 \pmod{3}\} = \{3, 6, 9, 12, 15\}$$

$$A_b = \{n \in A : n \equiv 1 \pmod{3}\} = \{1, 4, 7, 10, 13, 16\}$$

$$A_c = \{n \in A : n \equiv 2 \pmod{3}\} = \{2, 8, 11, 14\}$$

Controllo le intersezioni:

$$A_a \cap A_b = \emptyset$$

$$A_a \cap A_c = \emptyset$$

$$A_b \cap A_c = \emptyset$$

$$A_a \cup A_b \cup A_c \subseteq A \quad \checkmark$$

L'unione delle partizioni è uguale all'insieme di partenza, quindi questa suddivisione è una partizione.

#### Esempio 2

$$x \equiv_7 y$$

$$I = \{0, 1, 2, 3, 4, 5, 6\} \quad \text{insieme degli indici}$$

$$Z_i = \{n \in Z : n \equiv_7 i\} \quad \text{partizioni}$$

$$\bigcup_{i=0}^6 Z_i = Z \quad \checkmark$$

unione di tutte le partizioni

### 10.6 Lemma

Ogni partizione definisce una relazione di equivalenza, e viceversa:

$$xRy \text{ sse } x, y \in A \wedge \exists i \in I (x, y \in A_i)$$

Se  $x$  e  $y$  si trovano nello stesso insieme di una partizione, sono equivalenti.

## 10.7 Esercizi

### 10.7.1 Esercizio 1

Verificare quali proprietà ha la relazione:

$$(a, b)R(c, d) \Leftrightarrow \frac{3^a \cdot 5^b}{3^c \cdot 5^d} \leq 1$$

**Inizio soluzione:**

Prendo due coppie a caso e provo a sviluppare:

$$(5, 7)R(1, 2) ? \quad \frac{3^5 \cdot 5^7}{3^1 \cdot 5^2} \leq 1 \quad \times$$

controllo con un'altra coppia:

$$(1, 2)R(5, 7) ? \quad \frac{3^1 \cdot 5^2}{3^5 \cdot 5^7} \leq 1 \quad \checkmark$$

Dato che ho preso due coppie invertite, possiamo già ricavare che la relazione non è simmetrica (questo è un controesempio). Controllo le restanti proprietà:

- riflessiva:  $\forall x(xRx)$  dove  $x = (a, b)$

$$\frac{3^a \cdot 5^b}{3^a \cdot 5^b} \leq 1 \quad \checkmark$$

- transitiva:  $\forall xyz(xRy \wedge yRz \rightarrow xRz)$

$$\frac{3^a \cdot 5^b}{3^c \cdot 5^d} \leq 1 \quad \wedge \quad \frac{3^c \cdot 5^d}{3^e \cdot 5^f} \leq 1 \rightarrow \left( \frac{3^a \cdot 5^b}{\cancel{3^c \cdot 5^d}} \cdot \frac{\cancel{3^c \cdot 5^d}}{3^e \cdot 5^f} \right) \leq 1 \quad \checkmark$$

perché due numeri minori di 1 moltiplicati fra loro sono sempre minori di 1.

- antisimmetrica:  $\forall xy(xRy \wedge yRx \rightarrow x = y)$

$$\frac{3^a \cdot 5^b}{3^c \cdot 5^d} \leq 1 \quad \Rightarrow \quad 3^a \cdot 5^b \leq 3^c \cdot 5^d$$

$$\frac{3^c \cdot 5^d}{3^a \cdot 5^b} \leq 1 \quad \Rightarrow \quad 3^c \cdot 5^d \leq 3^a \cdot 5^b$$

queste due condizioni implicano  $3^a \cdot 5^b = 3^c \cdot 5^d$ , da cui  $a = c$  e  $b = d$   $\checkmark$

Dato che la relazione gode di queste proprietà è un'ordinamento parziale di coppie di numeri naturali. Controllando viene verificata anche la proprietà totale (o una coppia è minore uguale ad un'altra o viceversa), quindi la relazione è un ordinamento totale su  $\mathbb{N}^2$

### 10.7.2 Esercizio 2

Quante funzioni iniettive e suriettive abbiamo da

$$\mathbb{N} \mapsto \{0, 1, 2\}$$

- iniettive: 0, perché la cardinalità di  $\mathbb{N}$  è maggiore di quella del codominio
- suriettive:  $\infty$

Quante funzioni iniettive e suriettive abbiamo invece da

$$\{a, b\} \mapsto \{0, 1, 2\}$$

- suriettive: 0, perché la cardinalità del dominio non basta a coprire quella del codominio
- iniettive:  $2 \cdot 3 = 6$  funzioni iniettive
- non iniettive: 3, quando entrambi i valori del dominio coprono lo stesso del codominio

## 10.8 Tutorato

### 10.8.1 Proprietà delle relazioni

relazioni di equivalenza	relazioni di ordinamento		
	<i>parziale</i>	<i>stretto</i>	<i>totale</i>
riflessiva	riflessiva	irriflessiva	riflessiva
simmetrica	anti-simmetrica	anti-simmetrica	anti-simmetrica
transitiva	transitiva	transitiva	transitiva

La relazione totale è determinata come:

$$\forall xy(xRy \vee yRx)$$

mentre la relazione irriflessiva

$$\forall x(\neg xRx)$$

### 10.8.2 Classi di equivalenza

Se  $R$  è una relazioni di equivalenza nell'insieme  $A$ ,  $A$  può essere partizionato in più insiemi (almeno 1) in modo che tutti gli elementi di una partizione sono in relazione tra loro e non sono in relazione con gli elementi delle altre partizioni.

### 10.8.3 Esercizi

**Esercizio 1** Verificare di quali proprietà gode  $\forall xy \in \mathbb{Z} \quad xRy$  sse  $x + y$  è pari

- proprietà riflessiva

$$x + x \text{ è pari} = 2x \text{ è pari} \quad \checkmark$$

- proprietà transitiva

$$x + y = 2k$$

$$y + z = 2r$$

$$x + z = (2k - y) + (2r - y)$$

$$= 2k + 2r - 2y$$

$$= 2(k + r - y) \text{ sempre pari} \quad \checkmark$$

**Esercizio 2** Determinare di quali proprietà gode la relazione

$$R: \quad xRy \text{ sse } x^2 + y \geq 0 \quad \forall xy \in \mathbb{Z}$$

Inizio soluzione

- proprietà riflessiva:  $\forall x(xRx)$

$$\text{due casi} \begin{cases} x \geq 0 \rightarrow x^2 + x = x(x+1) \geq 0 \text{ vero perché } x \geq 0 \wedge x+1 \geq 1 & \checkmark \\ x \leq 0 \rightarrow x^2 + x = x(x+1) \leq 0 \text{ vero perché } x \leq 0 \wedge x+1 \leq 1 & \checkmark \end{cases}$$

- irriflessiva:  $\forall x \neg(xRx)$ . E' già riflessiva, non può essere irriflessiva

- simmetrica:  $\forall xy(xRy \rightarrow yRx)$

è equivalente dire che  $\exists xy \in \mathbb{Z} \quad xRy \wedge \neg(yRx)$

trovo un controesempio:

$$x^2 + y = (-2)^2 + 1 = 4 + 1 \geq 0 \quad xRy$$

$$y^2 + x = 1^2 - 2 = -1 \geq 0 \quad \neg(xRy) \quad \text{falso} \quad \times$$



- antisimmetrica:  $\forall xy(xRy \wedge yRx \rightarrow x = y)$

trovo un controesempio:

$$x = 2 \quad y = 1$$

$$x^2 + y = 2^2 + 1 = 5 \geq 0$$

$$y^2 + x = 1^2 + 2 = 3 \geq 0$$

$$5 \neq 3 \rightarrow x \neq y \quad \text{✗}$$

- transitiva:  $\forall xyz(xRy \wedge yRz \rightarrow xRz)$

trovo un controesempio:

$$x = 2 \quad y = -4 \quad z = -16$$

$$x^2 + y = 2^2 - 4 = 0 \geq 0 \quad xRy$$

$$y^2 + z = (-4)^2 - 16 = 0 \geq 0 \quad yRz$$

$$x^2 + z = 2^2 - 16 = -12 \underset{\text{falso}}{\geq} 0 \quad \neg(xRz) \quad \text{✗}$$

- totale:  $\forall xy(xRy \vee yRx)$

la relazione totale può essere scritta anche  $\forall xy \neg(xRy) \rightarrow xRy$

suppongo che  $\neg(xRy) \Leftrightarrow \neg(x^2 + y \geq 0) \Leftrightarrow x^2 + y < 0$

allora

$$y = -x^2$$

$$= -x^2 - k \quad k > 0$$

$$y^2 + x = (-x^2 - k)^2 + x$$

$$> (-x^2)^2 + x$$

$$= x^4 + x$$

$$\geq x^2 + x$$

$$\geq 0 \quad yRx$$

cazzo è sta roba?!

## 11 Combinatoria

### 11.1 Principio moltiplicativo

Se un elemento  $x$  viene scelto tra  $m$  elementi ed un elemento  $y$  viene scelto tra  $k$  elementi, allora le possibili scelte di  $x$  e  $y$  sono  $m \cdot k$

$$\begin{array}{l} x_1 \dots m_1 \quad \text{scelte} \\ \vdots \\ x_r \dots m_r \quad \text{scelte} \end{array}$$

le scelte possibili sono quindi

$$\prod_{i=1}^r m_i$$

#### 11.1.1 Esempi

##### Esempio 1

$$A = \{a, b, c, d, e\}$$

quante sono le possibili combinazioni di lunghezza 2?

$$\underline{5} \cdot \underline{5} = 25$$

##### Esempio 2

$$A = \{0, 1, \dots, 9\}$$

quante sono i numeri di lunghezza 6?

$$\underline{9} \cdot \underline{10} \cdot \underline{10} \cdot \underline{10} \cdot \underline{10} \cdot \underline{10} = 9 \cdot 10^5$$

perché nessun numero comincia con lo zero, la prima cifra varia da 1 a 9

### 11.2 Principio additivo

#### 11.2.1 Esempi

**Esempio 1** se  $|A| = k$  e  $|B| = n$ , quanto vale  $|A \cup B|$ ?

se  $A \cap B = \emptyset$  allora  $|A \cup B| = k + n$

se  $A \cap B \neq \emptyset$  allora  $|A \cup B| = (k + n) - |A \cap B|$

Ma questo caso si applica solo con due insiemi. Se avessimo più insiemi?

**Esempio 2** Regola a 3 insiemi:

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

Prova numerica:

$$\begin{aligned} A &= \{a, b, c, d, e\} \\ B &= \{c, e, f, g\} \\ C &= \{a, b, c, f, h\} \end{aligned}$$

$$|A \cup B \cup C| = 14 - 2 - 3 - 2 + 1 = 8 \quad \checkmark$$

### 11.2.2 Regola generale

Si deduce quindi che la regola generale per determinare la cardinalità dell'unione di più insiemi è:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n| - \sum_{i \neq j} (|A_i \cap A_j|)$$

### 11.2.3 Esempio complesso

Quante sono le targhe in cui compare solo una lettera 'A'?



Nelle targhe italiane le targhe sono formate da 2 numeri, 3 lettere e due numeri:

$X_1$  = insieme delle targhe con la 'A' in posto 1

$X_2$  = insieme delle targhe con la 'A' in posto 2

$X_6$  = insieme delle targhe con la 'A' in posto 6

$X_7$  = insieme delle targhe con la 'A' in posto 7

Quindi l'insieme delle targhe italiane con almeno una 'A' è determinato da

$$\begin{aligned} |X_1 \cup X_2 \cup X_6 \cup X_7| &= |X_1| + |X_2| + |X_6| + |X_7| \\ &\quad - |X_1 \cap X_2| - |X_1 \cap X_6| - |X_1 \cap X_7| \\ &\quad - |X_2 \cap X_6| - |X_2 \cap X_7| \\ &\quad - |X_6 \cap X_7| \\ &\quad - |X_1 \cap X_2 \cap X_6 \cap X_7| \\ &\quad + |X_1 \cap X_6 \cap X_7| \\ &\quad + |X_1 \cap X_2 \cap X_6| \\ &\quad + |X_1 \cap X_2 \cap X_7| \\ &\quad + |X_2 \cap X_6 \cap X_7| \\ &= 4 \cdot 26^3 \cdot 10^3 \text{ targhe con almeno una 'A'} \end{aligned}$$

Le targhe con esattamente una 'A' sono:  $4 \cdot 25^3 \cdot 10^3$

Le targhe che non hanno alcuna 'A' sono:  $25^4 \cdot 10^3$

Le targhe che non hanno alcun '7' sono:  $26^4 \cdot 9^3$

Le targhe che hanno solo una 'A' e solo un '7' sono:

$$\underbrace{26^4 \cdot 10^3}_{\text{totali}} - \overbrace{25^4 \cdot 10^3}^{\text{senza 'A'}} - \underbrace{26^4 \cdot 9^3}_{\text{senza '7'}} + \overbrace{25^4 \cdot 9^3}^{\text{senza 'A' e senza '7'}} = 17'981'121$$

### 11.2.4 Figure combinatorie

Disordine	Ordine
combinazioni semplici	disposizioni semplici
combinazioni con ripetizioni	disposizioni con ripetizioni

#### Disposizioni semplici

**Esempio 1** dato un insieme  $A$  di  $n$  elementi, i posti a disposizione sono

$$\underbrace{\quad}_1 \quad \underbrace{\quad}_2 \quad \dots \quad \underbrace{\quad}_k$$

$$D_{n,k} = n(n-1)(n-2)\dots(n-k+1) = n!$$

**Esempio 2** dato un insieme  $A = \{a_1, a_2, \dots, a_n\}$ , le stringhe su  $A$  di lunghezza  $k$  senza ripetizioni di caratteri sono

$$D_{n,k} \quad \text{con } k \leq n$$

#### Disposizioni con ripetizioni

**Esempio 1** dati gli insiemi  $A = \{a_1, \dots, a_n\}$  e  $B = \{b_1, \dots, b_k\}$ , il numero di funzioni non iniettive da  $B \rightarrow A$  sono

$$\left. \begin{array}{l} b_1 \mapsto a_1 \\ b_2 \mapsto a_2 \\ \vdots \\ b_k \mapsto a_n \end{array} \right\} D'_{n,k} = n^k$$

**Combinazioni semplici** Sia  $A$  un insieme di  $n$  elementi. Sia  $k \leq n$ . Una combinazione semplice di ordine  $k$  di un insieme  $A$  di  $n$  elementi è un sottoinsieme di  $A$  di cardinalità  $k$ .

**Esempio 1** l'insieme delle parti di un insieme è un esempio:

$$A = \{a, b, c, d\} \quad |A| = 4 \quad |\mathcal{P}(A)| = ?$$

							<b>1</b>
						$\emptyset$	
			$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	<b>4</b>
	$\{a, b\}$	$\{a, c\}$	$\{a, d\}$	$\{b, d\}$	$\{c, d\}$	$\{b, c\}$	<b>6</b>
		$\{a, b, c\}$	$\{a, b, d\}$	$\{b, c, d\}$	$\{a, c, d\}$		<b>4</b>
			$\{a, b, c, d\}$				<b>1</b>

$$|\mathcal{P}(A)| = \sum_{k=0}^n \binom{n}{k} = \sum_{k=0}^4 \binom{4}{k} = 2^4 = 16$$

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

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

## Combinazioni con ripetizioni

**Esempio 1** multi insiemi: sono insiemi che permettono al loro interno la ripetizione dello stesso elemento

$$A = \{a, b, c, d\} \quad |A| = 4$$

$$M = [a, a, d, d, d]$$

Il multi insieme  $M$  può essere visto come una funzione  $f : A \mapsto \mathbb{N}$  dove

$$f(a) = 2$$

$$f(d) = 3$$

$$f(x) = 0 \quad \text{per } x \neq a, d$$

mentre l'insieme  $B = \{a, b\} \subseteq A$  può essere visto come una funzione  $g$

$$g(a) = 1$$

$$g(b) = 1$$

$$g(c) = 0$$

$$g(d) = 0$$

dove 1 indica che l'elemento è presente nell'insieme e 0 indica la non presenza.

Ora posso costruire una stringa binaria per rappresentare il multi insieme:

$$\underbrace{\quad}_a 0 \underbrace{\quad}_b 0 \underbrace{\quad}_c 0 \underbrace{\quad}_d \rightarrow 1100011$$

Quante sono le stringhe binarie di lunghezza 8 con 3 zeri e 5 uni?

conto quanti possibili sottinsiemi di lunghezza  $k=3$  su 8 elementi

$$\underbrace{\binom{8}{3}}_{\text{fisso gli 0}} = \overbrace{\binom{8}{5}}^{\text{fisso gli 1}} = \binom{4-1+5}{5} = \binom{4-1+5}{3}$$

il numero 8 è determinato da: ordine +  $|A| - 1$

$$\binom{n-1+k}{k} = C'_{n,k} = \binom{n-1+k}{n-1}$$

$$|A| = n \quad A = \{a_1, a_2, \dots, a_n\}$$

$$\underbrace{\quad}_{a_1} 0 \underbrace{\quad}_{a_2} 0 \underbrace{\quad}_{\dots} 0 \underbrace{\quad}_{a_{n-1}} 0 \underbrace{\quad}_{a_n} \quad \text{quindi} \quad \begin{matrix} n-1 : & 0 \\ k : & 1 \end{matrix}$$

**Esempio 2** quante sono le sequenze reali ordinate crescenti di lunghezza 7 composte dai numeri tra 1 e 12 compresi?

sarà uguale al numero di sottinsiemi di lunghezza 7 dell'insieme  $A = \{1, 2, \dots, 12\} : \binom{12}{7}$ .

seq. ordinate crescenti  $\mapsto$  sottinsiemi di cardinalità 7

dato che l'ordine negli insiemi non conta.

**Esempio 3** date 12 liste composte da 10 candidati ciascuna, determinare il numero di votazioni possibili sapendo che scelta una lista, si possono esprimere al più 2 preferenze.

Quindi:

12 preferenze per le liste

per ogni lista:  $\binom{10}{2} + \binom{10}{1} + \binom{10}{0}$  2 oppure 1 oppure 0 preferenze

in totale:  $12 \cdot \left[ \binom{10}{2} + \binom{10}{1} + \binom{10}{0} \right] = 12(45 + 10 + 1) = 672$  votazioni differenti

**Esempio 4** in quanti modi è possibile ottenere 24 con 3 numeri naturali non nulli? L'ordine degli addendi non è importante.

Quindi:

$$C'_{n,k} = C'_{3,21} = \binom{n-1+k}{k} = \binom{2+21}{21} = \frac{23!}{21! \cdot 2!} = 253$$

$n = 3$  perché sono 3 numeri

$k = 21$  perché i 3 numeri devono essere non nulli, quindi il caso -ad esempio-  $24 + 0 + 0$  non è ammissibile

## 11.3 Esercizi vari

### 11.3.1 Esercizio 1

- Quante targhe finiscono con il carattere 'T'?
- Quante targhe finiscono con 'T' e non hanno altre 'T'?
- Quante targhe hanno almeno una 'T'?
- Quante targhe hanno una sola 'T'?

Inizio soluzioni

- le prime due lettere si possono scegliere tra 26, i numeri sono invariati, la penultima lettera anche. Solo l'ultima lettera è vincolata a 'T', quindi rimane una sola scelta per l'ultimo carattere:

$$\underline{26} \cdot \underline{26} \cdot \underline{10} \cdot \underline{10} \cdot \underline{10} \cdot \underline{26} \cdot \underline{1} = 26^3 \cdot 10^3$$

- l'ultimo carattere è limitato alla lettera 'T', mentre tutte le altre lettere sono quelle dell'alfabeto (26) meno la lettera 'T', quindi  $26 - 1$ :

$$\underline{25} \cdot \underline{25} \cdot \underline{10} \cdot \underline{10} \cdot \underline{10} \cdot \underline{25} \cdot \underline{1} = 25^3 \cdot 10^3$$

- le targhe con almeno una 'T' sono determinate dal numero di targhe complessive, meno quelle che non hanno nessuna 'T'. Le targhe totali sono  $26^4 \cdot 10^3$ , mentre quelle senza 'T' sono  $25^4 \cdot 10^3$ . Le targhe che hanno almeno una 'T' sono quindi:

$$26^4 \cdot 10^3 - 25^4 \cdot 10^3$$

- le targhe con una sola 'T' possono averla in una delle 4 possibili posizioni, e solo in quella, quindi:

$$4 \cdot 25^3 \cdot 10^3$$

### 11.3.2 Esercizio 2

In un ristorante a prezzo fisso si possono scegliere tra:

- 3 tipi di antipasto
- 2 tipi di primo piatto
- 2 tipi di secondo piatto
- 1 dolce oppure 1 frutto

Quante sono le possibili scelte che un cliente può fare?

Le possibili scelte si calcolano tramite il principio moltiplicativo, quindi:  $3 \cdot 2 \cdot 2 \cdot (1 + 1) = 24$

### 11.3.3 Esercizio 3

In una competizione partecipano 40 atleti, e la premiazione avviene secondo lo schema:

- al primo viene assegnata una coppa
- dalla 2° alla 5° posizione viene assegnata una medaglietta indistinguibile

In quanti modi possono venire premiati i partecipanti?

- i partecipanti sono 40
- una volta che il primo è arrivato ne restano 39
- gli atleti che rimangono da premiare sono il 2°, 3°, 4°, 5° quindi 4
- quindi il numero di premiazioni sarà:

$$40 \cdot \binom{39}{4}$$

### 11.3.4 Esercizio 4

Quante sono le relazioni binarie su un insieme di  $n$  elementi?

Sapendo che una relazione binaria è definita come  $R \subseteq A \times A$  e che  $|\mathcal{P}(A \times A)| = 2^{n^2}$

Se  $A = \{a, b\}$  quindi  $|A| = 2$  allora  $A \times A = \{(a, a), (a, b), (b, a), (b, b)\}$  da cui  $|A \times A| = 4$ .

$$\begin{aligned} 2^4 &= \binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} \\ &= 1 + 4 + 6 + 4 + 1 \end{aligned}$$

### 11.3.5 Esercizio 5

Determinare il numero delle funzioni suriettive  $f: \mathbb{N} \mapsto \{0, 1\}$ .

Il numero sarà uguale al numero di sottoinsiemi dell'insieme delle parti di  $\mathbb{N}$ .

$$A \subseteq \mathbb{N}, A \neq \emptyset, \mathbb{N}$$

$$f_A(x) = \begin{cases} 0 & \text{sse } x \in A \\ 1 & \text{sse } x \notin A \end{cases}$$

esempio numerico: 5

$$f_5(x) = \begin{cases} 0 & \text{sse } x = 5 \\ 1 & \text{sse } x \neq 5 \end{cases}$$

esempio generico:  $n$

$$f_n(x) = \begin{cases} 0 & \text{sse } x = n \\ 1 & \text{sse } x \neq n \end{cases}$$

$$|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| = 2^{\aleph}$$

## 11.4 Tutorato

### 11.4.1 Esercizio 1

Dado un lucchetto con 3 numeri da 0 a 9, determinare:

- a) quante sono le combinazioni possibili
- b) quante quelle con almeno un 4
- c) quante quelle con esattamente un 4

Soluzione

- a) ci sono 3 posti e 10 possibili valori. Quindi  $10^3$  combinazioni possibili
- b) le combinazioni con almeno un quattro sono date da quelle totali meno quelle senza 4. Quindi  $10^3 - 9^3 = 271$
- c) mentre quelle con esattamente un 4 sono:  $3 \cdot 9^2$ , ovvero: 3 posti e 9 numeri tra cui scegliere

### 11.4.2 Esercizio 2

Nel biliardo ci sono 15 palle numerate. Con un colpo solo mettiamo in buca tutte le palle nelle 6 buche (esclusa la palla bianca che non rientra tra le 15). In quanti modi si possono mettere le palle in buca?

Ogni palla ha 6 possibilità diverse (6 buche). Quindi la prima palla ha 6 possibilità, la seconda 6, la terza 6 e così via:

$$\underbrace{6 \cdot 6 \cdot \dots \cdot 6}_{15 \text{ volte}} = 6^{15} = D'_{6,15}$$

### 11.4.3 Esercizio 3

Vi sono 3 contenitori che contengono 10 palline numerate ciascuno. Ogni contenitore contiene palline di un solo colore, rispettivamente rosso, verde e blu. Estraendo 3 palline ognuna da un contenitore diverso, in quanti modi si possono ottenere tutte palline con numeri diversi?

Prendo una pallina al primo contenitore, e scelgo tra 10. Ora prendo una dal secondo, e dato che non deve avere il numero uguale alla prima, posso scegliere tra 9. peso anche con dal terzo contenitore, ma non potendo essere uguale alle due già pescate, posso scegliere solo tra 8 palline. Quindi:

$$10 \cdot 9 \cdot 8 = 720 = D_{10,3}$$

### 11.4.4 Esercizio 4

Mimmo ha vinto una promozione per cenare gratis con 2 amici in 3 serate con menù a tema. Se Mimmo ha 5 amiche, in quanti modi diversi le può invitare a cena?

Ogni serata Mimmo invita una coppia a cena. La coppia viene scelta tra 5 persone, quindi:  $\binom{5}{2} = \frac{5!}{2! \cdot 3!} = 10$  coppie tra cui scegliere ogni sera. Ora vi sono 3 posti, a cui possono accedere 10 coppie, quindi  $D'_{10,3} = 10^3$  modi diversi per invitarle a cena.

### 11.4.5 Esercizio 5

Mafia lavora in una pizzeria. Se in pizzeria sono disponibili 12 ingredienti diversi, quante pizze può preparare Mafia usando almeno 3 elementi?

Me pizze che Mafia può preparare sono quelle con esattamente 3 ingredienti più quelle con 4 più ... più quelle con 12 ingredienti, quindi Mafia può preparare:

$$\binom{12}{3} + \binom{12}{4} + \dots + \binom{12}{12} = \sum_{i=3}^{12} \binom{12}{i}$$



### 11.4.6 Esercizio 6

Ad una classe di 12 studenti viene assegnato un progetto da svolgere in gruppi di 3 persone. In quanti modi diversi si possono formare i gruppi?

Con 12 persone e gruppi di 3 persone si possono formare 4 gruppi. Il primo gruppo sarà determinato da  $\binom{12}{3}$ , il secondo da  $\binom{9}{3}$  in quanto le persone già assegnate non possono coesistere in due gruppi diversi, e così via. Tuttavia devo poter riscegliere le persone dai gruppi precedenti, quindi devo moltiplicare i coefficienti binomiali. Così facendo, tuttavia, conto tutte le permutazioni dei 4 gruppi. Quindi risolvo dividendo il tutto per  $4!$ :

$$\frac{\binom{12}{3} + \binom{9}{3} + \dots + \binom{3}{3}}{4!} = \frac{1}{4!} \prod_{i=1}^4 \binom{3i}{3} = 92400$$

### 11.4.7 Esercizio 7

Siano  $A = \{1, 2, 3, 4\}$  e  $B = \{a, b, c\}$ . Quante funzioni suriettive si possono definire da  $A \mapsto B$ ?

Tutte le funzioni  $A \mapsto B$  possono essere identificate come  $\{f(1), f(2), f(3), f(4)\}$ , dove ogni  $f(i)$  può essere uguale ad uno dei valori del codominio:  $a, b, c$ . Uno stesso elemento, può essere ripetuto.

Pertanto il numero di tutte le funzioni  $A \mapsto B$  è dato da:  $2^4 = 16$ , sapendo  $|A| = 4$  e  $|B| = 3$ , ovvero  $D'_{4,3}$ .

Sappiamo poi che se  $X$  ed  $Y$  sono due insiemi di cardinalità rispettivamente  $n$  ed  $m$ , allora il numero delle funzioni  $f : X \mapsto Y$  è dato da:  $m^n$ .

Trovato il numero di tutte le funzioni  $A \mapsto B$ , ci basta sottrarre quelle non suriettive. Esse sono solo e soltanto 3, infatti una funzione è suriettiva se tutti gli elementi dell'insieme d'arrivo vengono raggiunti, le uniche possibilità affinché la nostra funzione non sia suriettiva sono:

- tutti gli elementi di  $A$  hanno come immagine  $a$
- tutti gli elementi di  $A$  hanno come immagine  $b$
- tutti gli elementi di  $A$  hanno come immagine  $c$

e non vi sono altre possibilità.

Pertanto il numero funzioni suriettive  $A \mapsto B = 16 - 3 = 13$ .