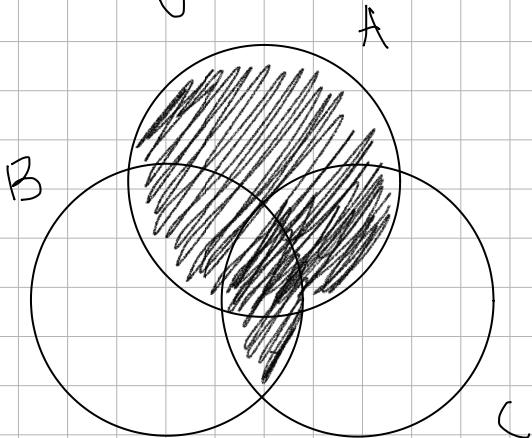


## Svolgimenti

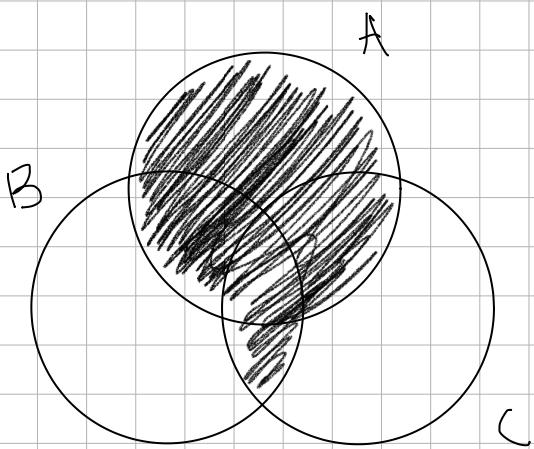
**Esercizio** Siano  $A, B, C$  insiemi. È vero che  

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

## - Diagramm



$$A \cup ((A \cup B)_n C)$$



A ∨ (B ∧ C)

## - Tabelle 2

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

- Dimostrazione

Sia  $x \in A \cup ((A \cup B) \cap C) \Rightarrow$  o  $x \in A$  o  $x \in (A \cup B) \cap C$

Se  $x \in A \Rightarrow x \in A \cup (B \cap C) \Rightarrow$  OK.

Se  $x \in (A \cup B) \cap C \Rightarrow x \in (A \cup B)$  e  $x \in C \Rightarrow$  o  $x \in (A \cup B)$  e  $x \in C$ .

Se  $x \in A \Rightarrow x \in A \cup (B \cap C) \Rightarrow$  OK.

Se  $x \in B \Rightarrow x \in B \in x \in C \Rightarrow x \in B \cap C \Rightarrow x \in A \cup (B \cap C)$

$\Rightarrow$  OK.

Viceversa

Sia  $x \in A \cup (B \cap C) \Rightarrow$  o  $x \in A$  o  $x \in B \cap C$ .

Se  $x \in A \Rightarrow x \in A \cup ((A \cup B) \cap C) \Rightarrow$  OK.

Se  $x \in B \cap C \Rightarrow x \in B$  e  $x \in C \Rightarrow x \in A \cup B$  e  $x \in C$

$\Rightarrow x \in (A \cup B) \cap C \Rightarrow x \in A \cup ((A \cup B) \cap C) \Rightarrow$  OK.

Svolgimento

Dizogrammi - Disegno  $\cup$  (unione),  $\cap$  (intersezione)

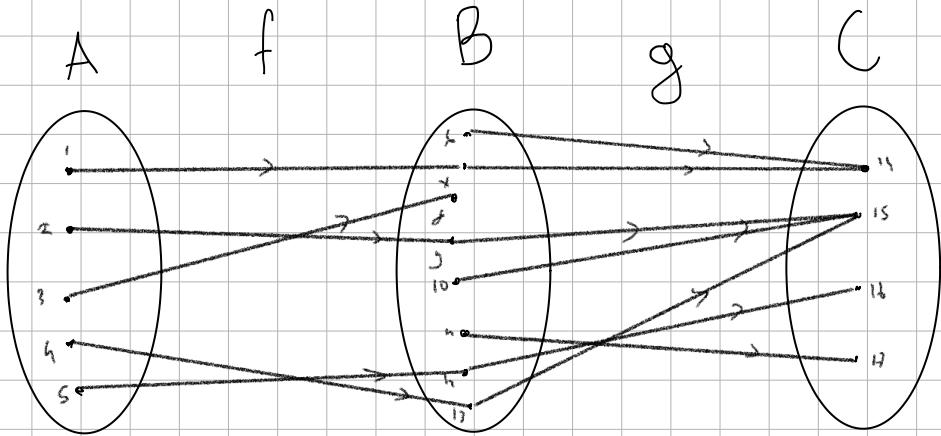
Tabelle di verità

Dimostrazioni: fai appartenere  $x$  ad uno dei due e

scomponi finché non potrai dimostrare che è presente nell'

altro

**Es** Siano  $f: A \rightarrow B$  e  $g: B \rightarrow C$ , tali che  $f$  è iniettiva e  $g$  è suriettiva è vero che  $g \circ f$  è iniettiva, suriettiva,



$\Rightarrow$  NO,  $g \circ f$  non è iniettiva (punti: 2, 5 di A)  
di mostriamo se è suriettiva

In effetti siano:

$$A: \{1, 2, 3, 4, 5\}, B: \{6, 7, 8, 9, 10, 11, 12, 13\}, C: \{14, 15, 16, 17\}$$

e siano  $f: A \rightarrow B$  e  $g: A \rightarrow B$  definite ponendo:

$$f(1) = 7, f(2) = 9, f(3) = 7, f(4) = 13, f(5) = 12, \dots$$

$$g(7) = 14, g(9) = 15, g(11) = 17, g(12) = 15, g(13) = 15, \dots$$

$$\text{ma } (g \circ f)(2) = g(f(2)) = g(12) = 15 \quad \text{e}$$

$$(g \circ f)(5) = g(f(5)) = g(12) = 15$$

$\Rightarrow g \circ f$  non è iniettiva

Sia  $z \in C$ . Poiché  $g$  è suriettiva  $\Rightarrow \exists y \in B$  tale che  $g(y) = z$   
ma  $g \circ f$  non è suriettiva perché  $\exists x \in A$  tale che  
 $(g \circ f)(x) = z$ . Nel nostro caso  $g(1) = 1$

## Svolgimento

Disegna per capire meglio

Dimostra con fatti

Eso Sia  $f: [s] \rightarrow [h]$  definita da:

$$f(1) = 4, f(2) = 3, f(3) = 1, f(4) = 4, f(5) = 1. \quad \text{Siano} \\ X = \{1, 3, 5\} \quad \text{e} \quad Y = \{2, 4\}$$

Calcolare  $f(X)$  e  $f^{-1}(Y)$

Abbiamo che

$$f(X) = f(\{1, 3, 5\}) = \{f(1), f(3), f(5)\} = \{4, 1\}$$

$$f^{-1}(Y) = \{\alpha \in [s] : \alpha \in Y\} = \{\alpha \in [s] : \alpha \in \{2, 4\}\} = \{1, 4\}$$

## Svolgimento

Avendo  $X$  e  $Y$  li sostituiamo a  $f(X)$  e  $f^{-1}(Y)$

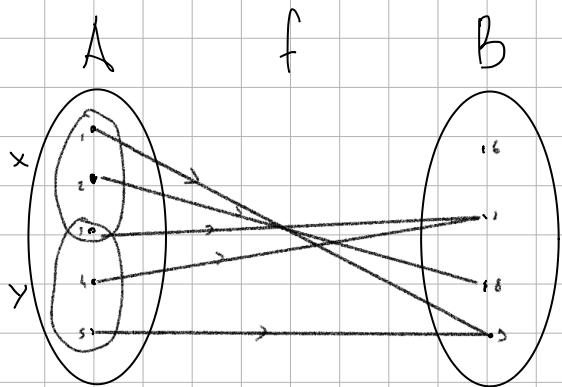
In  $f$  gli elementi di  $X(\alpha)$  gli applichiamo ad  $f(f(\alpha))$  così

da trovare a quali numeri corrispondono dato  $x$  fatto  $f(x)$  ed esce  $f$

In  $f^{-1}$  vediamo quali risultati corrispondono agli elementi di  $y$  dato  $y$  troviamo  $\alpha$ :  $f(\alpha) = b$   $b \in Y$

Es. Sia  $f: A \rightarrow B$  e siano  $X, Y \subseteq A$  è vero che

$$f(X \cap Y) = f(X) \cap f(Y)$$



$$f(X) = \{7, 8, 9\}$$

$$f(Y) = \{7, 9\}$$

$$f(X \cap Y) = \{7\}$$

$$f(X) \cap f(Y) = \{7, 9\}$$

$\Rightarrow$  NO, non è sempre vero

### Svolgimento

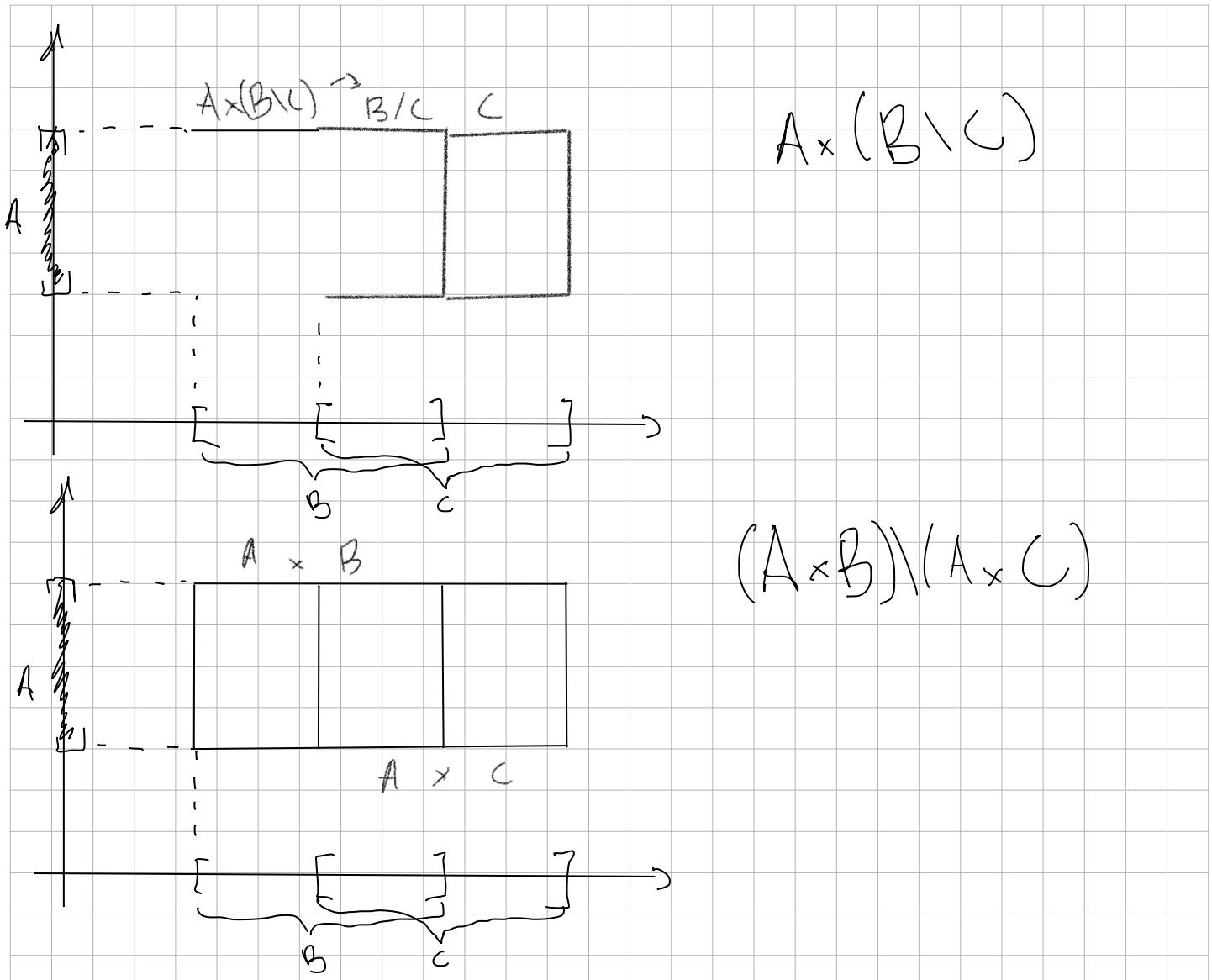
Disegnare, stare attenti dato che puoi decidere tu dove vanno le frecce e quindi puoi mettere frecce di  $x$  e  $y$  che vanno allo stesso  $B$

Es.  $2, b, c$  insiem. è vero che

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C) ?$$

Posso usare i diagrammi di Venn?

Avere bisogno di 4 dimensioni. Ma 2 volte si può fare.



Dimostrazione

S.i.a  $(x, y) \in A \times (B \setminus C) \Rightarrow x \in A \text{ e } y \in B \setminus C$   
 $\Rightarrow x \in A \text{ e } y \in B \text{ e } y \notin C \Rightarrow (x, y) \in A \times B \text{ e}$   
 $(x, y) \notin A \times C \Rightarrow (x, y) \in (A \times B) \setminus (A \times C) \Rightarrow \text{OK.}$

Viceversa

S.i.a  $(x, y) \in (A \times B) \setminus (A \times C) \Rightarrow (x, y) \in A \times B \text{ e}$   
 $(x, y) \notin A \times C \Rightarrow x \in A \text{ e } y \in B \text{ e } y \notin C \text{ (se}$   
 $y \in C \Rightarrow (x, y) \in A \times C, \text{ assurdo}) \Rightarrow x \in A \text{ e}$   
 $y \in B \setminus C \Rightarrow (x, y) \in A \times (B \setminus C).$

## T2bella verita

$x$	$y$	$\bar{y}$	$\bar{y}$	$(x, y)$	$(x, \bar{y})$	$(\bar{x}, y)$	$(\bar{x}, \bar{y})$
$A$	$B$	$C$	$B \setminus C$	$A \times (B \setminus C)$	$A \times B$	$A \times C$	$(A \times B) \setminus (A \times C)$
1	1	1	0	0	1	1	0
1	1	0	1	1	1	0	1
1	0	1	0	0	0	0	0
1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	-1
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0

## Svolgimento

Quando c'è il  $\times$  si usa il grafo per il diagramma di Venn con  $\times$  che sta per intersezione

Per la dimostrazione si utilizzano  $x$  e  $y$  come le assisse e coordinate

La tab. verità si può fare ma non è raccomandata.

Es. Sia  $R$  la relazione su  $\mathbb{Z}$  definita ponendo

$$mRn \iff m=n \text{ o } m+n=5 \quad \forall n, m \in \mathbb{Z}$$

Equivalezza!

1) Riflessività? ogni elemento di  $\mathbb{Z}$  è in relazione con se stesso

Sia  $n \in \mathbb{Z} \Rightarrow n=n \Rightarrow nRn \Rightarrow \text{OK.}$

2) Simmetria? se due elementi sono in relazione allora anche scambiandoli sono in relazione

Siano  $m, n \in \mathbb{Z}$  tali che  $mRn \Rightarrow$  o  $m=n$  o  $m+n=5$

Se  $m=n \stackrel{m=n}{\Rightarrow} nRm \stackrel{nRm=mRn}{\Rightarrow} OK$

è simmetrica

Se  $m+n=5 \stackrel{m+n=5}{\Rightarrow} nRm \stackrel{nRm=mRn}{\Rightarrow} OK$

3) Transitività?

presi 3 numeri vediamo che il 1° è in relazione con il 3°

Siano  $m, h, k \in \mathbb{Z}$  tali che  $mRn$  e  $nRk$  (o  $m=h$   
o  $m+h=5$ ) e ( $o n=k$  o  $n+k=5$ ).

Se  $m=h$  e  $n=k \Rightarrow m=k \Rightarrow mRk \Rightarrow OK$

Se  $m=n$  e  $n+k=5 \Rightarrow m+k=5 \Rightarrow mRk \Rightarrow OK$

Se  $m+h=5$  e  $n=k \Rightarrow m+k=5 \Rightarrow mRk \Rightarrow OK$

Se  $m+n=5$  e  $n+k=5 \Rightarrow n=5-m$  e  $n=5-k \Rightarrow$   
 $m=k \Rightarrow mRk \Rightarrow OK$ . E' f. equivalenza

Chi sono le classi di equivalenza?

Sia  $n \in \mathbb{Z}$ , allora

$$[n]_R = \{m \in \mathbb{Z} : mRn\} = \{m \in \mathbb{Z} : o m=n o m+n=5\}$$
$$= \{n, 5-n\} \text{ es } (5,0), (4,-1), (6,1), (10,5) \dots$$

Svolgimento

Vedere se è riflessiva, quindi se ogni elemento è in relazione  
con se stesso,

Se è simmetrica, quindi se due elementi sono in relazione  
anche il loro cambio è in relazione  $(n,m) (m,n)$  allora si

Se è transitiva, presi tre elementi, il primo con il secondo e

il secondo con il terzo vedere se sono collegati: il primo con il terzo  $(n,m) \sim (m,k)$  se  $(n,k)$  ok.

Per le classi di equivalenza basta selezionare i numeri che rispettano la relazione

E.s. Consideriamo la Relazione  $\sim$   
nell'insieme di tutte le proposizioni

Rifl. ? Simm. ? Trans. ?

✓ ✓ ✓

$P$  = prop allora è vero che?

$P \hookrightarrow P$ :

<u>P</u>	<u><math>P \hookrightarrow P</math></u>	è riflessiva
V	V	
F	V	

$P$  e  $Q$  prop.:  $P \hookrightarrow Q$  allora è vero che?

$Q \hookrightarrow P$

<u>P</u>	<u>Q</u>	<u><math>P \hookrightarrow Q</math></u>	<u><math>Q \hookrightarrow P</math></u>	
V	V	V	V	le colonne
V	F	F	F	Sono uguali
F	V	F	F	
F	F	V	V	è simmetrica

$P, Q, R$  prop.:  $P \rightarrow Q, Q \rightarrow R \Rightarrow P \rightarrow R$

$P \quad Q \quad R \quad P \rightarrow Q \quad Q \rightarrow R \quad P \rightarrow R$

V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	F	V
V	F	F	F	V	F
F	V	V	F	V	V
F	V	F	F	F	V
F	F	V	V	F	F
F	F	F	V	V	V

V F F F F V

$(P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow P \rightarrow R$ : tutti veri      transitiva

Se  $P$  equivale a  $Q$  e  $Q$  equivale a  $R$  ciò implica che  $P$  equivale a  $R$ ?

### Svolgimento

Bisogna sapere tutti i simboli. Per la riflessiva.

Applicarlo su se stesso, per la simmetrica controllare se le colonne sono uguali, per la transitiva bisogna far attenzione ad usare and e implica. Usare le tavole di verità

Ese. è vero che  $((A \rightarrow B) \wedge (A \circ B)) \rightarrow A$ ?

A	B	$A \rightarrow B$	$A \circ B$	$(A \rightarrow B) \wedge (A \circ B)$	f	
V	V	V	F	F	V	non sempre
V	F	F	V	F	V	verso
F	V	V	V	V	F	
F	F	V	F	F	V	

### Svolgimento

Tavole di verità

**Es.** Consideriamo l'affermazione:

"Tutti i tutori di M.D che hanno seguito MD hanno preso  
" 30

usando i predicati:

$S(x)$ : "hanno seguito MD"

$L(x)$ : "hanno preso 30"

$T(x)$ : "sono tutori di MD"

$$\forall x. ((T(x) \wedge S(x)) \rightarrow L(x))$$

**Svolgimento**

Dividere l'affermazione in predicati,

Creare il risultato con i predicati trovati, tenendo d'occhio le parole chiavi "e" sarebbe " e " ciascun "  $\forall x$ , "esiste un"  $\exists x$ . "allora"  $\rightarrow$ ,

Si possono creare predicati con più variabili: esempio

$E(x, y) = "x manda mail a y"$

**Es.** Trovare tutte le soluzioni  $x, y \in \mathbb{Z}$  tali che

$$875x + 235y = 10$$

Sappiamo dalla teoria che esistono soluzioni se e solo se  $(875, 235) = 10$

Step 1:  $\text{MCD}(875, 235)$

$$875 = 235 \cdot 3 + 170 \quad (875, 235) = 5 \quad m_2 \quad 5/10$$

$$235 = 170 \cdot 1 + 65 \quad \text{quindi ci sono soluzioni}$$

$$170 = 65 \cdot 2 + 40$$

$$65 = 40 \cdot 1 + 25$$

$$40 = 25 \cdot 1 + 15$$

$$25 = 15 \cdot 1 + 10$$

$$15 = 10 \cdot 1 + 5$$

$$10 = 5 \cdot 2 + 0$$

Step 2: ID Bezout

$$5 = 15 + (-1)10$$

$$= 15 + (-1)(25 + (-1)15)$$

$$= (2)15 + (-1)25$$

$$= (-1)25 + (2)(40 + (-1)25)$$

$$= (-3)25 + (2)40$$

$$= (2)40 + (-3)(65 + (-1)40)$$

$$= (5)40 + (-3)65$$

$$= (-3)65 + (5)(170 + (-2)65)$$

$$= (-13)65 + (5)170$$

$$= (5)170 + (-13)(235 + (-1)170)$$

$$= (18)170 + (-13)235$$

$$= (-13)235 + (18)(875 + (-3)235)$$

$$= (-67)235 + (18)875 = 5$$

TD di Bezout

$$= (-134)235 + (36)875 = 10$$

dato che a noi interessa  
10 moltiplichiamo x2

Step 3: Formula

Troviamo che  $x = 36$  e  $y = -134$

Tutte le soluzioni sono nella forma:

$$\begin{cases} x = x_0 - \frac{b}{(a,b)} t \\ y = y_0 + \frac{a}{(a,b)} t \end{cases}$$

quindi

$$\begin{cases} x = x_0 - \frac{235}{5} t \\ y = y_0 + \frac{875}{5} t \end{cases} \quad t \in \mathbb{Z}$$

esplicito

$$x = 36 - 47t$$

$$y = -134 + 175t$$

Svolgimento

Dato la formula trovare l'MCD ( $a, b$ ) se combinazione

Se combinazione con r allora ci sono soluzioni:  $0 = b \cdot q + r$

Successivamente  $b = r \cdot q + r_2$  finché non si arriva a 0.

Ese:  $(24, 10) \Rightarrow 24 = 10 \cdot 2 + 4 \quad 4 = 2 \cdot 2 + 0 \quad 10 = 4 \cdot 2 + 2$

Per trovare l'ID di Bezout si dovrà percorrere il tutto e ritroso dal penultimo in su, raggruppando i resti dopo ogni passaggio.

es:

$$\begin{aligned} 2 &= 10 + (-2)4 \\ &= 10 + (-2)(24 + (-2)10) \\ &= (5)10 + (-2)24 = \text{ID Bezout} \end{aligned}$$

Infine per trovare le formule esplicative usiamo:

$$bx + ay = (a,b) \quad \begin{cases} x = x_0 - \frac{b}{(a,b)}t \\ y = y_0 + \frac{a}{(a,b)}t \end{cases}$$

In caso di multiplo si dovrà moltiplicare per far combaciare  $(a,b)$  con l'originale.

es:

$$\begin{cases} x = 5 - \frac{24}{2}t \\ y = -2 + \frac{10}{2}t \end{cases} \quad \begin{aligned} x &= 5 - 12t \\ y &= -2 + 5t \end{aligned} \quad t \in \mathbb{Z}$$

Esempio. Sia  $f \in S_g$  definita ponendo  $f = 321987654$ . Sia  $K \in \mathbb{P}$  quale è il più piccolo intero positivo t.c.

$$\underbrace{f \cdot f \cdot \dots \cdot f}_K = 123456789$$

:	1	2	3	6	5	4	7	8	9
3	2	1	9	8	7	6	5	4	

$$1 \geq 3, \quad 2^2, \quad 4 \geq 9, \quad 5 \geq 8, \quad 6 \geq 7$$

$$K=2$$

## Svolgimento

prendere  $f$  e dividerla assegnando un indice: ad ogni numero, iniziare dall'indice 1 e vedere il contenuto, il contenuto sarà il prossimo indice da vedere, così finché non torna alla posizione iniziale.

Fatto ciò per tutti i numeri, il più lungo trovato sarà il nostro  $K$ .

**Esercizio.** Calcolare le ultime due cifre di

$$7^{91}$$

quindi calcolare  $[7^{91}]_{100}$ .  $(7, 100) = 1$  quindi

$$\left[ 7^{\varphi(100)} \right]_{100} = [1]_{100} \text{ teorema euleriano}$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40 \text{ quindi}$$

$$\left[ 7^{40} \right]_{100} = [1]_{100} \text{ ma allora}$$

$$\left[ 7^{91} \right]_{100} = \left[ (7^{40})^2 \right]_{100} \cdot \left[ 7^{11} \right]_{100} = \left( \left[ 7^{40} \right]_{100} \right)^2 \cdot \left[ 7^{11} \right]_{100} =$$

$$= \left( [1]_{100} \right)^2 \cdot \left[ 7^{11} \right]_{100} = \left[ 7^{11} \right]_{100} \text{ ma}$$

$$\left[ 7^2 \right]_{100} = [49]_{100}, \quad \left[ 7^4 \right]_{100} = \left( \left[ 7^2 \right]_{100} \right)^2 = \left[ 49^2 \right]_{100} =$$

dato che ha 2 cifre ed è  
mod 100 si prendono le ultime 2

$$= [2001]_{100} = [1]_{100}, \quad [7^8]_{100} = ([7^4]_{100})^2 = ([1]_{100})^2 = [1]_{100}$$

pertanto

$$\begin{aligned} [7^{11}]_{100} &= [7^{8+2+1}]_{100} = [7^8]_{100} \cdot [7^2]_{100} \cdot [7]_{100} = \\ &= [1]_{100} \cdot [49]_{100} \cdot [7]_{100} = [343]_{100} = [43]_{100} \end{aligned}$$

concludendo

$$[7^{91}]_{100} = [7^{11}]_{100} = [43]_{100}$$

le ultime due cifre sono 43.

### Svolgimento

Dato che vengono chieste le ultime 2 cifre si vede la classe di resto mod 100.

Vedere se  $(a, b) = 1$ , se si si utilizza il teo. di Euler. Altrimenti si prenderà un  $K \in \mathbb{N}$  tale che  $[a^x]_b \sim [k]_b$ . Esisterà quindi un  $n \in \mathbb{N}$  tale che  $\alpha = n \cdot b + K$  se  $K \equiv_a 0$  allora si troverà  $l \equiv_a K$  ottenendo così  $a^{x-1} = n \cdot \frac{b}{a} + l$  e così via finché  $m \equiv_a 1$

utilizzando così euler su  $(a, m)$

$[K]^{\varphi(n)} = [1]_n$ , quindi si calcola  $\varphi(n)$  con la formula

$\varphi(n) = n \cdot (1 - \frac{1}{p}) \cdots (1 - \frac{1}{q})$  dove  $p$  e  $q$  sono i numeri primi che

moltiplicati danno  $n$ .  $25 = 5^2$ ,  $100 = 2^2 \cdot 5^2$  etc.

Si prende quindi il risultato e lo si riscrive in modo che egualino:  $[7^{91}]_{100} = [7^{40}]_{100} \cdot [7^{60}]_{100} \cdot [7^1]_{100}$   
 si sostituisce poi con la classe di  $[1]_n$ .  $[1]_{100} \cdot [7^1]_{100} = [7^1]_{100}$   
 Successivamente si calcola k trovato, utilizzando le potenze di 2, trovate le corrispondenti classi  $[2^8]_{100} \cdot [2^2]_{100} \cdot [2^1]_{100} = [2^1]_{100}$

Si moltiplica il tutto facendo attenzione a vedere quali sono uguali 20 e 1 e si ottiene il risultato.  $[2^{43}]_{100} = [43]_{100}$

In caso di sostituzione con K si dovrà ricavare m, l, k e così via così da ottenere il risultato  $[2^{2022}] = [6]_{100}$  last 2 cifre sono ok

**Esercizio.** Calcolare l'inverso moltiplicativo di  $[28]_{125}$  se esiste.

Sappiamo dalla teoria che tale inverso moltiplicativo esiste se e solo se  $(125, 28) = 1$   
 Calcolare  $(125, 28)$  con l'A.E.

$$125 = 28 \cdot 4 + 13$$

$$28 = 13 \cdot 2 + 2$$

$$13 = 2 \cdot 6 + 1 \quad \text{MCD } (125, 28) = 1 \quad \exists! \text{ inverso moltiplicativo}$$

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

$$n \cdot 28 \leq 1 - \text{mul} | 125$$

$$1 = 13 + (-6 \cdot 2) =$$

$$(-6)(28 + (13 - 2)) + 13 =$$

$$(13)_{125} + (-6)_{28} =$$

$$(13)(125 + (-6 \cdot 28)) + (-6)_{28} =$$

$$(-58)_{28} + (13)_{125}$$

$1 = (-58)_{28} - (13)_{125}$  è l'ID di Bezout

$$\text{pertanto } (-58) \cdot 28 \equiv 1 \pmod{125} \Rightarrow [(-58)_{28}]_{125} = [1]_{125}$$
$$\Rightarrow [-58]_{125} \cdot [28]_{125} = [1]_{125}$$

quindi l'inversa moltiplicativa di

$$[28]_{125} \text{ è } [-58]_{125} = [67]_{125}$$

## Svolgimento

Fare MCD, solo se esce 1 allora esiste, successivamente si calcola l'ID di Bezout e si ottiene

$$1 = xa + yb \text{ dove } (x)a \equiv 1 \pmod{b} \text{ quindi:}$$

$$[xa]_b = [1]_b \text{ allora } [x]_b \cdot [a]_b = [1]_b \text{ quindi}$$

$$\text{l'inversa moltiplicativa di } [a]_b = [x]_b$$

**Ese.** Siano  $p, q, n, d, e$  come in RSA, se conosco  $\Phi(n)$ , posso trovare  $p$  e  $q$ ? Sì.

Abbiamo che  $n = p \cdot q$  e  $\Phi(n) = (p-1) \cdot (q-1)$ . quindi:

$$q = \frac{n}{p} \text{ e } \Phi(n) = pq - p - q + 1 = n - p - \frac{n}{p} + 1$$

$$p \cdot \Phi(n) = p \cdot n - p^2 - n + p = p^2 + p(\Phi(n) - n - 1) + n = 0$$

$$p = \frac{n+1 - \Phi(n) + \sqrt{(\Phi(n)-n-1)^2 - 4n}}{2}$$

$$q = \frac{n}{p}.$$

## Svolgimento

Formule che possono essere utili

**Esercizio** Costruire un sistema di codifica RSA usando i primi  $p=47$ ,  $q=83$ . Codificare e decodificare un messaggio

Abbiamo

$$n = 47 \cdot 83 = 3901, \quad \Phi(n) = (p-1)(q-1) = 46 \cdot 82 = 3772$$

Trovare  $e$  coprimo con  $\Phi(n)$ ,  $e=127$ . Calcolare inversa moltiplicativa di  $[e]_{\Phi(n)} = [127]_{3772}$

$$3772 = 127 \cdot 29 + 89$$

$$1 = 13 + 12 \cdot (-1)$$

$$127 = 89 \cdot 1 + 38$$

$$= 13 + (38 + 13 \cdot (-2))(-1) =$$

$$89 = 38 \cdot 2 + 13$$

$$= (3)13 + (-1)38 =$$

$$38 = 13 \cdot 2 + 12$$

$$= (-1)38 + (3)(89 + 38 \cdot (-2))$$

$$13 = 12 \cdot 1 + 1$$

$$= (3)89 + (-1)(38)$$

$$12 = 1 \cdot 12 + 0$$

$$= (3)89 + (-1)(127 + 89 \cdot (-1))$$

$$[-29]_{3772}, \quad [3475]_{3772}$$

$$= (-1)127 + (10)89$$

$$= (-1)127 + (10)(3772 + 127 \cdot (-29))$$

$$d = 3475$$

$$= (10)3772 + (-297)127 = 1$$

Codifichiamo il messaggio  $m = 3$ . Calcolare  $[\tilde{m}]_n =$

$$= [m^e]_n = [3^{127}]_{3901} \quad 127 = 64 + 32 + 16 + 8 + 4 + 2 + 1$$

$$[3^2] = [9]_{3901}, [3^4] = [81]_{3901}, [3^8] = [2660]_{3901}$$

$$[3^{16}] = [3087]_{3901}, [3^{32}] = [3327]_{3901}, [3^{64}] = [1792]_{3901}$$

$$[\tilde{m}]_{3901} = [3^{127}]_{3901} = [3^{64}] \cdot [3^{32}] \cdot [3^{16}] \cdot [3^8] \cdot [3^4] \cdot [3^2] \cdot [3] = \\ = [1792] \cdot [3327] \cdot [3087] \cdot [2660] \cdot [81] \cdot [9] \cdot [3] = [267]_{3901}$$

$$[\tilde{m}]_{3901} = [267]_{3901}$$

Decodifichiamo il messaggio  $\tilde{m}$ . Calcolare  $[\tilde{m}^d]_n =$

$$= [267^{3475}]_{3901} \quad 3475 = 2048 + 1024 + 256 + 128 + 64 + 2 + 1$$

$$[267^2] = [2694]_{3901}, [267^4] = [1892]_{3901} \dots \dots \dots$$

$$[2694] \cdot [1892] \cdot \dots \dots = [3]_{3901}$$

## Svolgimento

Dati  $p$  e  $q$  si calcola  $n = \Phi(n)$ , si prende un  $e$  a caso  $(\text{mod } \Phi(n))$  e si calcola la sua inversa moltiplicativa

Troviamo quindi  $d$ . Per interlocutore

Codificare: calcolare  $[m^e]_n \rightarrow$  interlocutore

Decodificare: calcolare  $[m^d]_n \rightarrow$  proprio

Es. Calcolare

$$|\{A \subseteq [9] : 2 \notin A \circ 8 \in A\}|$$

abbiamo che

$$\{A \subseteq [9] : 2 \notin A \circ 8 \in A\} = X \cup Y$$

dove

$$X := \{A \subseteq [9] : 2 \notin A\} \quad Y := \{A \subseteq [9] : 8 \in A\}$$

ma per principio di I-E:

$$|X \cup Y| = |X| + |Y| - |X \cap Y|$$

abbiamo

$$X = \{A \subseteq \{1, 3, 4, 5, 6, 7, 8, 9\}\}$$

$$Y = \{A \subseteq \{1, 2, 3, 4, 5, 6, 7, 9\}\}$$

$$X \cap Y = \{A \subseteq \{1, 3, 4, 5, 6, 7, 9\}\}$$

pertanto per 4.3.1

$$|X| = 2^8, |Y| = 2^8, |X \cap Y| = 2^7 \\ = 2^8 + 2^8 - 2^7 = 2^7(2+2-1) = 2^7(3) = 3 \cdot 2^7$$

Svolgimento

Dato un def, ottenere una formula tipo  $X \cup Y$  e utilizzare il principio di I-E come mostrato e calcolare il tutto.

"o"  $\rightarrow$   $\cup \rightarrow$  principio di I-E, "e"  $\rightarrow$  facile  $\rightarrow$  ok  
non facile  $\rightarrow$  de Morgan  $\rightarrow$  I-E

**Esercizio** Quanti numeri di cellulare (7 cifre tra 0 e 9) ci sono che hanno 3 cifre consecutive uguali?

$$\left\{ (x_1, \dots, x_7) \in [0,9]^7 : x_i = x_{i+1} = x_{i+2} \text{ per qualche } 1 \leq i \leq 5 \right\}$$

Sia  $X$  questo insieme notiamo che

$$X = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$$

$$A_1 := \left\{ (x_1, x_2, x_3) \in [0,9]^3 : x_1 = x_2 = x_3 \right\}$$

$$A_2 := \left\{ (x_2, x_3, x_4) \in [0,9]^3 : x_2 = x_3 = x_4 \right\}$$

$$\vdots$$

$$A_5 := \left\{ (x_5, x_6, x_7) \in [0,9]^3 : x_5 = x_6 = x_7 \right\}$$

Applichiamo principio I-E, abbiamo

$$|A_1 \cup \dots \cup A_5| = |A_1| + \dots + |A_5| - |A_1 \cap A_2| - \dots - |A_4 \cap A_5|$$

$$+ |A_1 \cap A_2 \cap A_3| + \dots + |A_3 \cap A_4 \cap A_5| -$$

$$|A_1 \cap A_2 \cap A_3 \cap A_4| - \dots - |A_2 \cap A_3 \cap A_4 \cap A_5|$$

$$+ |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5|$$

ma

$$|A_1| = \left| \left\{ (x_1, \dots, x_7) \in [0,9]^7 : x_1 = x_2 = x_3 \right\} \right| = 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10^3 = 10^5$$

$$\text{Simil. } |A_2| = |A_3| = |A_4| = |A_5| = 10^5$$

Concludiamo

$$|A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5| = (5 \cdot 10^5) \left( 4 \cdot 10^6 + 6 \cdot 10^3 \right) + (3 \cdot 10^3 + 6 \cdot 10^2 + 10) - (2 \cdot 10^2 + 3 \cdot 10) + 10 =$$

$$|X| = 5 \cdot 10^5 - 4 \cdot 10^6 - \cancel{6 \cdot 10^3} + \cancel{3 \cdot 10^3} + \cancel{6 \cdot 10^2} - \cancel{2 \cdot 10^2} - \cancel{3 \cdot 10} + 10 \\ = 5 \cdot 10^5 - 4 \cdot 10^6 - 3 \cdot 10^3 + 6 \cdot 10^2 - 2 \cdot 10 = 657390$$

### Svolgimento

Dopo aver tradotto il tutto in una formula con unioni e intersezioni. Applicare principio I-E per ottenere il risultato, come es precedente stare attenti a "e" e "o".

**Esercizio.** 10 persone si dividono in 5 gruppi. Ogni gruppo ha 2 persone. In quanti modi possono essere divisi? Le persone sono distinguibili  $\Rightarrow \{\text{persone}\} \leftrightarrow [10]$ . I gruppi sono distinguibili  $\Leftrightarrow \{\text{Gruppi}\} \leftrightarrow \{\text{scatole numerate}\}$ . Pertanto il numero richiesto è:

$$\binom{10}{2,2,2,2,2} = \frac{10!}{2!^5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{2^8}$$

$$= 113400 \text{ modi}$$

### Svolgimento

Si utilizza il coefficiente multinomiale sopra di cui in ciascuna scatola ci sono 2 scelte.

**E**n Quante parole diverse si possono formare permutando (cioè anagrammando) le lettere della parola mississippi?

Si chiede il numero di permutazioni del multinsieme:

$$m := \{m^1, i^4, s^4, p^2\}$$

Pertanto il numero richiesto è (4.6)

$$|m| = \binom{h+u+2+1}{h,u,2,1} = \frac{11!}{u!u!2!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{4 \cdot 4 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2}$$

= 34650 modi

Svolgimento

Come prima

**E**n. Ricorsioni lineari 2 coeff. costanti:

$$f(n+3) = -f(n-2) + 8f(n-1) + 12f(n) \quad \forall n \in \mathbb{N}$$

con le C.I.

$$f(0) = 0, f(1) = 5, f(2) = 0$$

rappresentare l'eq. caratteristica

$$-x^3 + x^2 + 16x - 12$$

$$x^3 - x^2 + 8x + 12 = 0$$

$$x^3 - x^2 - 8x - 12 = 0$$

$$x = -2 \text{ è radice} \Rightarrow (x+2) \mid (x^3 + x^2 - 8x - 12 = 0)$$

$$\begin{array}{r|l} x^3 + x^2 - 8x - 12 & x+2 \\ \hline -x^3 - 2x^2 & x^2 - x - 6 \\ -x^2 - 8x - 12 & \\ +x^2 + 2x & \\ -6x - 12 & \\ +6x + 12 & \end{array}$$

$$(x^2 - x - 6)(x + 2) = x = -2$$

$$\frac{d \cdot \sqrt{1+24}}{2}, \frac{1-s}{2} = 3, -2$$

quindi le radici sono:

$$\gamma_1 = 3 \quad \gamma_2 = -2$$

con molteplicità:  $\delta_1 = 1 \quad \delta_2 = 2$

$$x^3 + x^2 - 8x - 12 = (x - 3)^1 (x + 2)^2$$

Sappiamo dalla Teoria che:

$\exists P_1(x), P_2(x) \in \mathbb{C}[x]$  tali che:

tanti polinomi quante radici

$$f(n) = P_1(n)x + P_2(n)x^n \quad \forall n \in \mathbb{N}$$

$$\deg(P_i) \leq \delta_i - 1 \quad \forall i = 1, 2, \quad \deg(P_1) \leq 1 \quad \deg(P_2) \leq 0$$

quindi  $\exists a, b, c \in \mathbb{C}$  tali che

$$f(n) = (a + b n)(-2)^n + c (3)^n \quad \forall n \in \mathbb{N}$$

Per trovare  $a, b, c$  usiamo le C.I

$$0 = f(0) = a + c$$

$$5 = f(1) = -2a - 2b + 3c$$

$$0 = f(2) = 4a + 8b + 9c$$

$$\begin{cases} a + c = 0 \\ -2a - 2b + 3c = 5 \\ 4a + 8b + 9c = 0 \end{cases}$$

$$\begin{cases} a = -c \\ -2b + 5c = 5 \\ 8b + 5c = 0 \end{cases}$$

$$\begin{cases} a = -c \\ -2b + 5c = 5 \\ 5c = -8b \end{cases}$$

$$\begin{cases} a = -\frac{4}{5} \\ -2b - 8b = 5 = -10b = 5 \Rightarrow b = -\frac{1}{2} \\ c = \frac{4}{5} \end{cases}$$

$$f(n) = \left(-\frac{4}{5} - \frac{1}{2}\right)(-2)^n + \frac{4}{5}(3)^n \quad \forall n \in \mathbb{N}$$

## Svolgimento

Data una ricorsione lineare a coeff costanti e delle condizioni iniziali, prima la si imposta in modo corretto

$$f(n+3) + f(n+2) + f(n+1) + f(n) = 0 \text{ poi si trova l'eq caratteristica:}$$

$ax^3 + bx^2 + cx + d$  dove  $x^3$  è  $f(n+3)$  e così via. Si trovano le  $x$ , alcune volte bisogna utilizzare Ruffini trovando

già una radice, successivamente trovate le radici  $\gamma$ , le

moltiplità  $d$  sono quante volte sono state trovate,

e si otterrà che  $x^3 + x^2 + x + 1 = (x - \gamma_1)^{d_1} (x - \gamma_2)^{d_2} (x - \gamma_3)^{d_3}$ , all'aumentare del grado aumentano anche molteplicità e radici. Esistono quindi

dei polinomi  $P(x)$  quante le radici tali che  $f(n) = P(n), \gamma_1, \gamma_2, \gamma_3, \dots$

$\forall n \in \mathbb{N}$  e sappiamo che i gradi di questi sono:  $\deg(P_i) \leq d_i - 1$

Trovare quindi i gradi dei polinomi trovati, successivamente

sappiamo che  $\exists a, b, \dots \in \mathbb{C}$  tali che:  $f(n) = a(\gamma_1)^n + \dots$  in base

a quanti polinomi sono stati trovati e al grado, se il grado è 0

viene scritto solo  $a$ , se è di grado 1 è  $(a + bn)(\gamma_1)^n$  e così via

infine mettere a sistema il tutto utilizzando le cond. iniziali

così da trovare  $a, b, c$  e riscrivere  $f(n)$  sostituendo  $a, b, c$ .

E.s. Trovare una formula chiusa per

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

poiche  $f(x) = x^2 + x$  è un polinomio  $\Rightarrow \exists g(x) \in \mathbb{R}[x]$   
 tale che  $deg(g) \leq 3$

$$\sum_{k=0}^n (k+k^2) = g(n) \quad \forall n \in \mathbb{N}$$

Quindi  $\exists a, b, c, d \in \mathbb{R}$  tali che

$$\sum_{k=0}^n (k+k^2) = an^3 + bn^2 + cn + d \quad \forall n \in \mathbb{N}$$

(2) calcolare le condizioni iniziali

$$0 = f(0) = d$$

$$2 = f(1) = a+b+c+d$$

$$8 = f(2) = 8a+4b+2c+d$$

$$20 = f(3) = 27a+9b+3c+d$$

$$\left\{ \begin{array}{l} d=0 \\ a+b+c=2 \\ 8a+4b+2c=8 \\ 27a+9b+3c=20 \end{array} \right.$$

$$\left\{ \begin{array}{l} b=-a-c+2 \\ 8a-4a-4c+2c+8=8 \quad = \quad 4a-2c=0 \\ 27a-9a-9c+3c+18=20 \quad = \quad 18a-6c=2 \end{array} \right.$$

$$\begin{cases} a = \frac{1}{2}c \\ 9c - 6c = 2 \\ b = -\frac{3}{6} - \frac{6}{6} + \frac{12}{6} = \frac{5}{6} \end{cases}$$

$$a = \frac{1}{2}, b = \frac{5}{6}, c = \frac{2}{3}, d = 0$$

$$g(n) = \frac{1}{2}n^3 + \frac{5}{6}n^2 + \frac{2}{3}n$$

### Svolgimento

Dato una sommatoria per trovare la formula chiusa, prima riscriviamo il polinomio  $f(n)$ , sappiamo che questo sarà uguale al polinomio  $g(n)$  di grado  $\deg(f(n))+1$ , riscriviamo quindi il polinomio  $g(x)$  di tot gradi e calcoliamo le condizioni iniziali  $f(0) = g(0)$  per trovare tutti gli elementi di  $g(n)$  e quindi la formula chiusa.

**Esercizio:** Trovare una formula chiusa per

$$\sum_{i=0}^n \sum_{j=0}^m 3^{i+j}$$

proviamo a calcolare la somma intera abbiamo

$$\begin{aligned} \sum_{j=0}^m 3^{i+j} &= 3^i + 3^{i+1} + \dots + 3^{i+m} = 3^i + 3^i \cdot 3 + 3^i \cdot 3^2 \dots + 3^i \cdot 3^m \\ &= 3^i \left( 1 + 3 + 3^2 + \dots + 3^m \right) \stackrel{(5.1)}{=} 3^i \cdot \frac{3^{m+1} - 1}{3 - 1} \end{aligned}$$

pertanto

$$\begin{aligned}
 & \sum_{i=0}^n \sum_{j=0}^m 3^{i+j} = \sum_{i=0}^n 3^i \frac{3^{m+1}-1}{3-1} = \\
 & = 3^1 \cdot \frac{3^{m+1}-1}{2} + \dots + 3^n \cdot \frac{3^{m+1}-1}{2} = \frac{3^{m+1}-1}{2} \cdot \sum_{i=0}^n 3^i = \quad (S.1.1) \\
 & \frac{3^{m+1}-1}{2} \cdot \frac{3^{n+1}-1}{2} = \frac{(3^{m+1}-1)(3^{n+1}-1)}{4}
 \end{aligned}$$

Svolgimento

In caso di sommatoria doppia, scriviamo una sommatoria come se fosse parte del polinomio, successivamente raggruppiamo e scriviamo l'altra sommatoria come somma geometrica, la spostiamo all'esterno e scriviamo l'altra somma geometrica moltiplichiamo il tutto e otteniamo la formula chiusa.

E.s. Trovare una formula chiusa o asintoticamente chiusa per:

$$\sum_{k=1}^n 2k \ln(k)$$

La funzione  $f(x) = 2x \ln(x)$  è continua per  $x > 0$  e monotona crescente per  $x \in \mathbb{R}_{>0}$ .

Sappiamo dalla Teoria S.3.1 che

$$f(1) + \int_1^n f(x) dx \leq \sum_{k=1}^n 2k \ln(k) \leq f(n) + \int_1^n f(x) dx \quad \forall x > 0$$

M2

$$\int_1^n 2x \ln(x) dx = x^2 \ln(x) - \frac{x^2}{2} \Big|_1^n = n^2 \ln(n) - \frac{n^2}{2} + \frac{1}{2}$$

otteniamo

$$n^2 \ln(n) - \frac{n^2}{2} + \frac{1}{2} \leq \sum_{k=1}^n 2k \ln(k) \leq 2n \ln(n) + n^2 \ln(n) - \frac{n^2}{2} + \frac{1}{2}$$

$\forall n \in \mathbb{R}$ . il termine che tende all'infinito più rapidamente per  $n \rightarrow +\infty$  a sinistra è  $n^2 \ln(n)$ , mentre a destra è  $n^2 \ln(n)$ . Sono uguali allora visto a dividere

$$\frac{n^2 \ln(n) - \frac{n^2}{2} + \frac{1}{2}}{n^2 \ln(n)} \leq \frac{\sum_{k=1}^n 2k \ln(k)}{n^2 \ln(n)} \leq \frac{2n \ln(n) + n^2 \ln(n) - \frac{n^2}{2} + \frac{1}{2}}{n^2 \ln(n)}$$

$$\frac{n^2 \ln(n)}{(1+0+0)} \quad \frac{n^2 \ln(n)}{(0+1+0+0)} \quad \frac{n^2 \ln(n)}{(0+1+0+0)}$$

$$1 \leq \frac{\sum_{k=1}^n 2k \ln(k)}{n^2 \ln(n)} \leq 1$$

per il teorema del confronto

$$\lim_{n \rightarrow +\infty} \frac{\sum_{k=1}^n 2k \ln(k)}{n^2 \ln(n)} = 1 \quad \text{ovvero}$$

$$\frac{n^2 \ln(n)}{\text{formula}}$$

$$\sum_{k=1}^n 2k \ln(k) \underset{\text{se } n \rightarrow +\infty}{\approx} n^2 \ln(n)$$

Svolgimento

Fare parte delle somme non polinomiali, verificare che la funzione

Si è continua e monotona e vedere se è crescente o decrescente così da applicare rispettivamente:

$$f(1) + \int_1^n f(x) dx \leq \sum_{i=1}^n f(i) \leq f(n) + \int_n^n f(x) dx \quad \forall n \in \mathbb{N}$$

$$f(1) + \int_1^n f(x) dx \geq \sum_{i=1}^n f(i) \geq f(n) + \int_n^n f(x) dx \quad \forall n \in \mathbb{N}$$

si può fare la derivata per capire se è crescente  
 Fare poi gli integrali definiti con n, prendere il termine  
 che  $\rightarrow \infty$  più rapidamente (quello di grado maggiore)  
 presente in entrambi i termini e lo si divide per tutto il  
 confronto. Troviamo quindi la formula chiusa ma se dal  
 confronto il risultato è 1 allora sono anche asintoticamente  
 equivalenti, chiamata anche formula asintoticamente chiusa

**Es** Trovare una formula chiusa per

$$\prod_{i=1}^n \prod_{j=1}^n 2^i \cdot 3^j$$

Il prodotto interno è

$$\begin{aligned} \prod_{j=1}^n 2^i \cdot 3^j &= 2 \cdot 3 \cdot 2 \cdot 3^2 \cdots 2 \cdot 3^n = \\ &= (2^i)^n \cdot 3^1 \cdot 3^2 \cdots 3^n = \\ &= (2^i)^n \cdot 3^{1+2+\dots+n} = \\ &= 2^{n \cdot i} \cdot 3^{\binom{n+1}{2}} \end{aligned}$$

Pertanto

$$\begin{aligned} \prod_{i=1}^n \prod_{j=1}^n 2^i \cdot 3^j &= \prod_{i=1}^n 2^{ni} \cdot 3^{\binom{n+1}{2}} = \\ &= 2^n \cdot 3^{\binom{n+1}{2}} \cdot 2^{2n} \cdot 3^{\binom{n+1}{2}} \dots 2^{nn} \cdot 3^{\binom{n+1}{2}} = \\ &= \left(3^{\binom{n+1}{2}}\right)^n \cdot 2^{n+2n+\dots+nn} = \\ &= 3^n \left(\binom{n+1}{2}\right) \cdot 2^{n(n+2+\dots+n)} = \\ &= 3^n \left(\binom{n+1}{2}\right) \cdot 2^n \left(\binom{n+1}{2}\right) = \\ &= 6^n \left(\binom{n+1}{2}\right) \text{ risultato finale} \end{aligned}$$

Svolgimento

Come per la sommatoria si calcola il prodotto interno. Trovatela formula dopo vari raggruppamenti; si calcola anche il secondo prodotto, lo si raggruppa e si ottiene la formula chiusa. La somma dei numeri da 1 a  $n$  è  $\binom{n+1}{2}$

Ed. Siano  $f(n) = \log_2(n)$  e  $g(n) = \log_{10}(n) \quad \forall n \in \mathbb{P}$

Quale delle relazioni  $<$ ,  $=$ ,  $>$ ,  $\leq$ ,  $\geq$  valgono tra  $f$  e  $g$ ?

Sappiamo che

$$\log_2(n) = \frac{\ln(n)}{\ln(2)}, \quad \log_{10}(n) = \frac{\ln(n)}{\ln(10)} \quad \forall n \in \mathbb{P}$$

2bbi 2mo

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} = \lim_{n \rightarrow +\infty} \frac{\ln(10)}{\ln(2)} = \frac{\ln(10)}{\ln(2)} \quad (*)$$

quindi  $f \neq o(g)$  e  $f \not\approx g$ . Similmente

$$\lim_{n \rightarrow +\infty} \neq 0 \quad \lim_{n \rightarrow +\infty} \neq 1$$

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = \lim_{n \rightarrow +\infty} \frac{\ln(2)}{\ln(10)} = \frac{\ln(2)}{\ln(10)}$$

quindi  $g \neq o(f)$ . Sappiamo da b.6.4 che  $*$  implica

$$\lim_{n \rightarrow +\infty} \neq 0$$

che  $f = O(g)$ , simil.  $g = O(f)$ . Quindi (def. di  $\Theta$ )

$\lim_{n \rightarrow +\infty}$  è un numero

$f = \Theta(g)$  e  $g = \Theta(f)$ . Infine (5.6.7)  $f = \omega(g)$  e  $g = \omega(f)$   
(perché  $f = O(g) \Leftrightarrow g = \omega(f)$ ).

## Svolgimento

Per sapere quali relazioni tra  $o, O, \Theta, \omega, \not\approx$  valgono tra  $f$  e  $g$ . Si utilizzano i seguenti calcoli:

$$\begin{aligned} \lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} &= 0 \Rightarrow f = o(g) \\ &1 \Rightarrow f \not\approx g \\ &< \Rightarrow f = \omega(g) \end{aligned}$$

$$\begin{aligned} N \rightarrow \mathbb{R} \\ \Rightarrow f = O(g) \\ \Rightarrow f = \Omega(g) \end{aligned}$$

$\mathbb{N} \rightarrow \mathbb{R}$ 

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = 0 \Rightarrow g = o(f)$$

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} = 1 \Rightarrow g \approx f$$

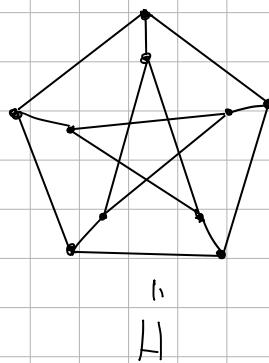
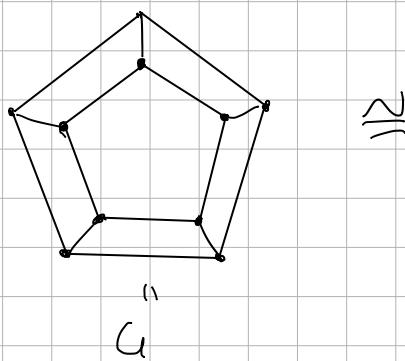
$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} < \infty \Rightarrow g = O(f)$$

se  $f = O(g)$  e  $g = O(f) \Rightarrow f = \Theta(g)$  e  $g = \Theta(f)$

$$f = O(g) \Leftrightarrow g = \omega(f) \Rightarrow g = \omega(f)$$

$$g = O(f) \Leftrightarrow f = \omega(g) \Rightarrow f = \omega(g)$$

**E<sub>D</sub>.**



no, perché  $G$  ha un ciclo di lunghezza 4 e  $H$  no

**Svolgimento**

Isomorfismo significa che cambiando nome ai vertici il risultato è lo stesso:  $\square_n^2$ ,  $\bigtriangleup_n$  sono isomorfi, se non lo

si capisce si guardano le proprietà che devono essere uguali

"invariante per isomorfismo".

tutti i sottoinsiemi di interi da 1 a n di  
cardinalità k  $\binom{n}{k}$

**E<sub>D</sub>.** Si dà  $G = (V, E)$  dove  $V = \binom{[n]}{2} \cup \binom{[n]}{3}$  ( $n \in \mathbb{P}$ )

e dove

$$\{x, y\} \in E \Leftrightarrow \begin{cases} x \subseteq y \\ y \subseteq x \end{cases} \quad \forall x, y \in V, x \neq y$$

Allora  $G$  è bipartito ( $V_1 = \binom{[n]}{2}$ ,  $V_2 = \binom{[n]}{3}$ ).

Esiste un accoppiamento di  $V_1$  in  $V_2$ ?

$$\left\{ \begin{array}{l} \{1, 3\}, \{1, 3, 4\} \end{array} \right\} \subset E$$

$$\left\{ \begin{array}{l} \{1, 3\}, \{1, 4, 5\} \end{array} \right\} \not\subset E$$

$G$  è legato nei gradi?

$\text{Si}_2 x \in V_1$ ,  $\text{Si}_2 x = \{a, b\}$  ( $a, b \in [n]$ ) ( $a \neq b$ )

$$d(x) := |\{y \in V_2 : \{x, y\} \in E\}|$$

$$= |\{y \in \binom{[n]}{3} : X \stackrel{\rightarrow a, b}{\subseteq} Y\}|$$

$$= |\{Y \subseteq [n] : |Y| = 3, \{a, b\} \subseteq Y\}|$$

$= n-2$  perché  $a, b$  già scelti e deve essere di

$\text{Si}_2 y \in V_2$ ,  $\text{Si}_2 y = \{a, b, c\}$  ( $a, b, c \in [n]$ ,  $a, b, c$  distinti). Allora

$$d(y) := |\{x \in V_1 : \{x, y\} \in E\}|$$

$$= |\{x \in \binom{[n]}{2} : X \subseteq Y\}|$$

$$= |\{X \subseteq [n] : |X| = 2, X \subseteq Y\}|$$

$$= (\{X \subseteq \{a, b, c\} : |X| = 2\}) = \binom{3}{2} = 3$$

(4.2)

Quindi se  $n \geq 5$  allora

$$d(x) = n-2 \geq 3 \Rightarrow d(y) \quad \forall x \in V_1 \text{ e } \forall y \in V_2$$

(e quindi legato 2 dei gradi se  $n \geq 5 \Rightarrow$

(6.22)

$\Rightarrow$  esiste un accoppiamento di  $V_1$  in  $V_2$  se  
 $n \geq 5$

## Svolgimento

Dato un'impostazione, per vedere se un grafo è bipartito bisogna vedere se  $V = V_1 \cup V_2$ , cioè se  $V$  è uguale all'unione di  $V_1$  e  $V_2$  con intersezione vuota. Per vedere se esiste un accoppiamento si utilizza il teorema di Hall o vedere se è legato nei gradi. Prendere un  $V_1$  e un  $V_2$  e calcolarne il grado, dato che è bipartito quindi sicuramente avrà i vertici di  $V_2$  collegati e dopo vari passaggi si ottiene una formula, fare lo stesso così in  $V_2$ . Calcolati entrambi i gradi vedere quanto fa  $n$ :  $d(v_1) = f(v_1) \geq f(v_2) = d(v_2)$   
si ottiene che  $G$  ha un accoppiamento quando  $f(v_1) \geq f(v_2)$

Esercizio. Si consideri  $G = ([10]^3, E)$  dove

solo i v in comune per:

$$\{(a_1, a_2, a_3), (b_1, b_2, b_3)\} \in E \iff |\{i \in [3] : a_i \neq b_i\}| = 1$$

$$\text{es: } \{(1, 2, 3), (3, 5, 2)\} \in E$$

$$\{(1, 2, 3), (1, 3, 4)\} \in E$$

è possibile colorare  $G$  con al più 30 colori?

$$\chi(G) = \max_{v \in V} \{d(v)\} + 1$$

$$\text{Calcolare } d(v): (a_1, a_2, a_3) \in [10]^3$$

$$d(a_1, a_2, a_3) = |\{(b_1, b_2, b_3) \in [10]^3 : (a_1, a_2, a_3), (b_1, b_2, b_3) \in E\}|$$

$$= |\{(b_1, b_2, b_3) \in [10]^3 : |\{i \in \{1, 2, 3\} : a_i \neq b_i\}| = 1\}| =$$

$\forall \varepsilon \exists A$  Negation  $\rightarrow$

$$\forall x A(x) \rightarrow B(x)$$

$$\exists (+) A(x) \wedge \neg B(x)$$

$$\neg(A(x) \vee B(x))$$

$$A(x) \Leftrightarrow B(x)$$