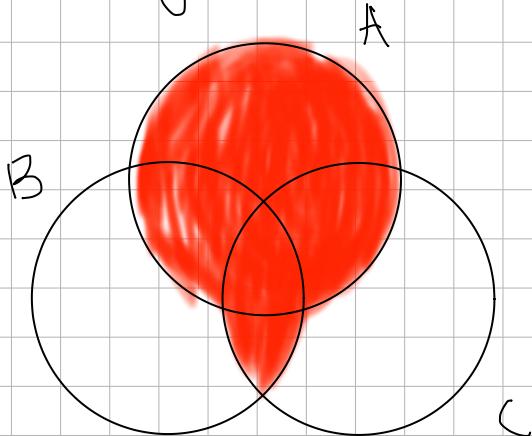


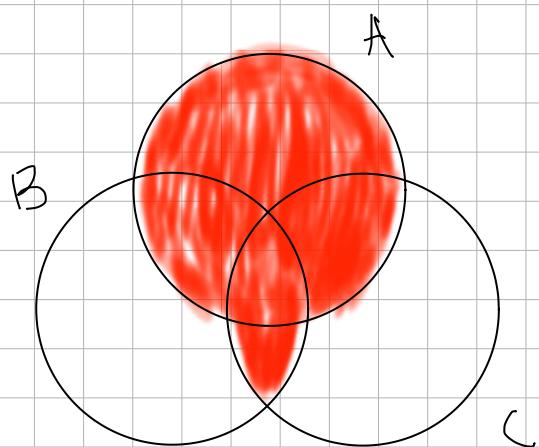
**ED**, Siano  $A, B, C$  insiemi è vero che  

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

- Diagramma



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



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

- Dimostrazione

$$\text{Sia } x \in A \cup ((A \cup B) \cap C) \Rightarrow x \in A \cup x \in (A \cup B) \cap C$$

$$\text{Se } x \in A \Rightarrow x \in A \cup (B \cap C) \Rightarrow \text{OK}$$

$$\text{Se } x \in (A \cup B) \cap C \Rightarrow x \in A \cup B \text{ e } x \in C \Rightarrow$$

$$\text{Se } x \in A \Rightarrow x \in A \cup (B \cap C) \Rightarrow \text{OK}$$

$$\text{Se } x \in B \Rightarrow x \in B \cap C \Rightarrow x \in A \cup (B \cap C) \Rightarrow \text{OK}$$

Viceversa

$$\text{Sia } x \in A \cup (B \cap C) \Rightarrow$$

$$\text{Se } x \in A \Rightarrow x \in A \cup ((A \cup B) \cap C) \Rightarrow \text{OK}$$

$\subseteq x \in B \cap C \Rightarrow x \in B \text{ e } x \in C \Rightarrow x \in A \cup B$   
 $x \in C \Rightarrow x \in (A \cup B) \cap C \Rightarrow x \in A \cup ((A \cup B) \cap C)$   
 $\Rightarrow \text{OK}$

- Tabella di verità

$$\begin{array}{ccccccccc}
 A & B & C & A \cup B & B \cap C & (A \cup B) \cap C & A \cup ((A \cup B) \cap C) & A \cup (B \cap C)
 \end{array}$$

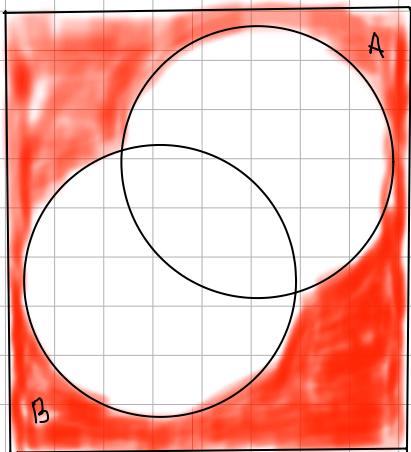
1	1	1	1	1	1	1	1
1	1	0	1	0	0	1	1
1	0	1	1	0	1	1	1
1	0	0	1	0	0	1	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0

Risposta: è vero.

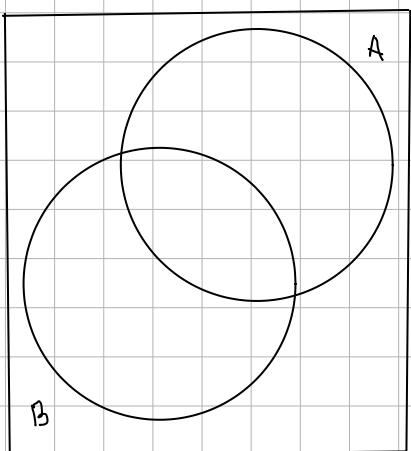
Esercizio, Dimostrare le leggi di De Morgan

Siano  $A, B$  insiemi allora

$$(A \cup B)' = (A') \cap (B') \quad \text{e} \quad (A \cap B)' = (A')' \cup (B')'$$



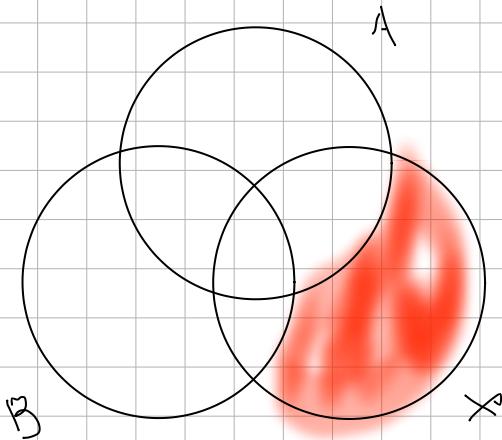
$$(A \cup B)'$$



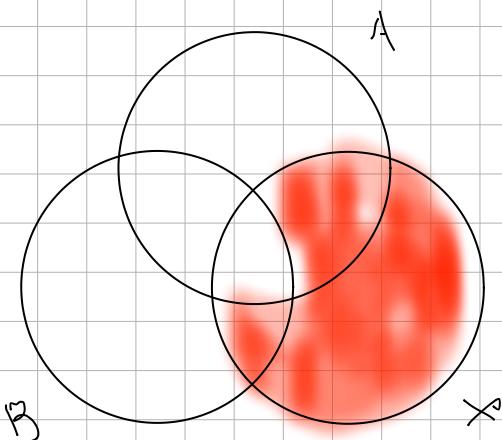
$$(A') \cap (B')$$

Esercizio 2-] Siano  $A, B, X$  insiemi. È vero che  
 $X \setminus (A \cup B) = (X \setminus A) \cup (X \setminus B)$ ?

sempre



$$X \setminus (A \cup B)$$



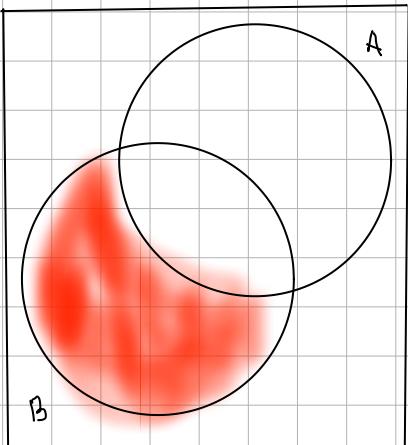
$$(X \setminus A) \cup (X \setminus B)$$

Tabella di verità

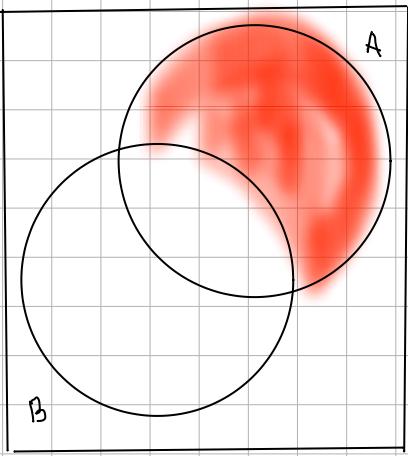
$A$	$B$	$X$	$A \cup B$	$X \setminus A$	$X \setminus B$	$X \setminus (A \cup B)$	$(X \setminus A) \cup (X \setminus B)$
1	1	1	1	0	0	0	0
1	1	0	1	0	0	0	0
1	0	1	1	0	1	0	1
1	0	0	1	0	0	0	0
0	1	1	1	1	0	0	1
0	1	0	1	0	0	0	0
0	0	1	0	1	1	1	1
0	0	0	0	0	0	0	0

Risposta: è falso

Esercizio 2] A, B insiemi è vero che  
 $A = B \Leftrightarrow A' \cap B = \emptyset$  e  $A \cap B' = \emptyset$ ?

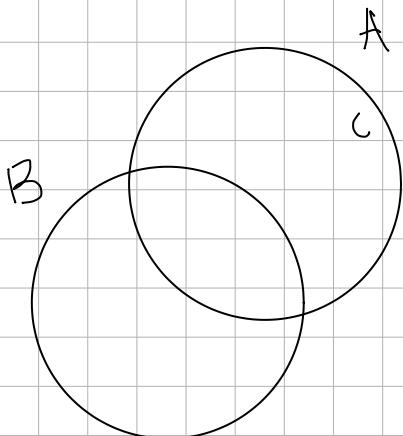


$$A' \cap B$$



$$A \cap B'$$

Es [1+] A, B, C insiemi è vero che  
 $C \subseteq A \Rightarrow (A \cap B) \cup C = A \cap (B \cup C)$ ?



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

Se  $x \in B \Rightarrow x \in A \cap B \Rightarrow x \in (A \cap B) \cup C \Rightarrow \text{OK}$

Se  $x \in C \Rightarrow x \in C \cup (A \cap B) \Rightarrow \text{OK}$

Viceversa

$\Rightarrow x \in (A \cap B) \cup C \Rightarrow x \in A \cap B \text{ o } x \in C$

Se  $x \in C \Rightarrow x \in A \Rightarrow x \in C \cup B \text{ e } x \in A \Rightarrow x \in A \cap (B \cup C) \Rightarrow \text{OK}$

Se  $x \in A \cap B \Rightarrow x \in A \text{ e } x \in B \Rightarrow x \in A \text{ e } x \in B \cup C \Rightarrow x \in A \cap (B \cup C) \Rightarrow \text{OK}$

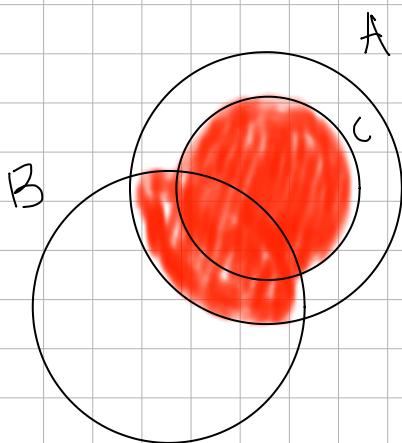


Tavola di verità

A	B	C	$A \cap B$	$B \cup C$	$(A \cap B) \cup C$	$A \cap (B \cup C)$
1	1	1	1	1	1	1
1	1	0	0	1	1	1
1	0	1	0	1	1	1
1	0	0	0	0	0	0
0	1	1	0	1	0	0
0	1	0	0	1	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

i due casi sbagliati sono impossibili perché  $C \subseteq A$

E<sub>n</sub>[2] Chi è  $(\mathbb{N} \times \mathbb{Z}) \cap (\mathbb{Z} \times \mathbb{P})$ ?

tutti i numeri interi positivi?

Es. Sia  $f: [5] \rightarrow [4]$  definita da

$$f(1) = 4, f(2) = 3, \underset{\text{intervalli}}{\overset{\text{a } 5}{\text{intervalli}}} f(3) = 1, f(4) = 4, f(5) = 1$$

Siano  $X = \{1, 3, 5\}$  e  $Y = \{2, 4\}$

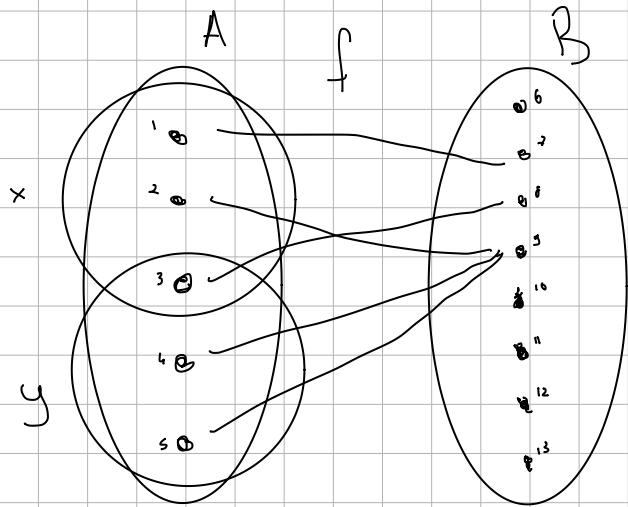
Calcolare  $f(x)$  e  $f^{-1}(y)$

Per definizione abbiamo che

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

$$\begin{aligned} f^{-1}(y) &= \{x \in [5] : f(x) \in Y\} = \{x \in [5] : f(x) \in \{2, 4\}\} \\ &= \{1, 4\} \end{aligned}$$

Ese Sia  $f: A \rightarrow B$  e siano  $x, y \in A$  è vero che  $f(x \cap y) = f(x) \cap f(y)$



$$f(x) = \{7, 8, 9\} \quad f(y) = \{8, 9\}$$

$$f(x \cap y) = \{8\} \Rightarrow$$

$\Rightarrow$  non è sempre vero

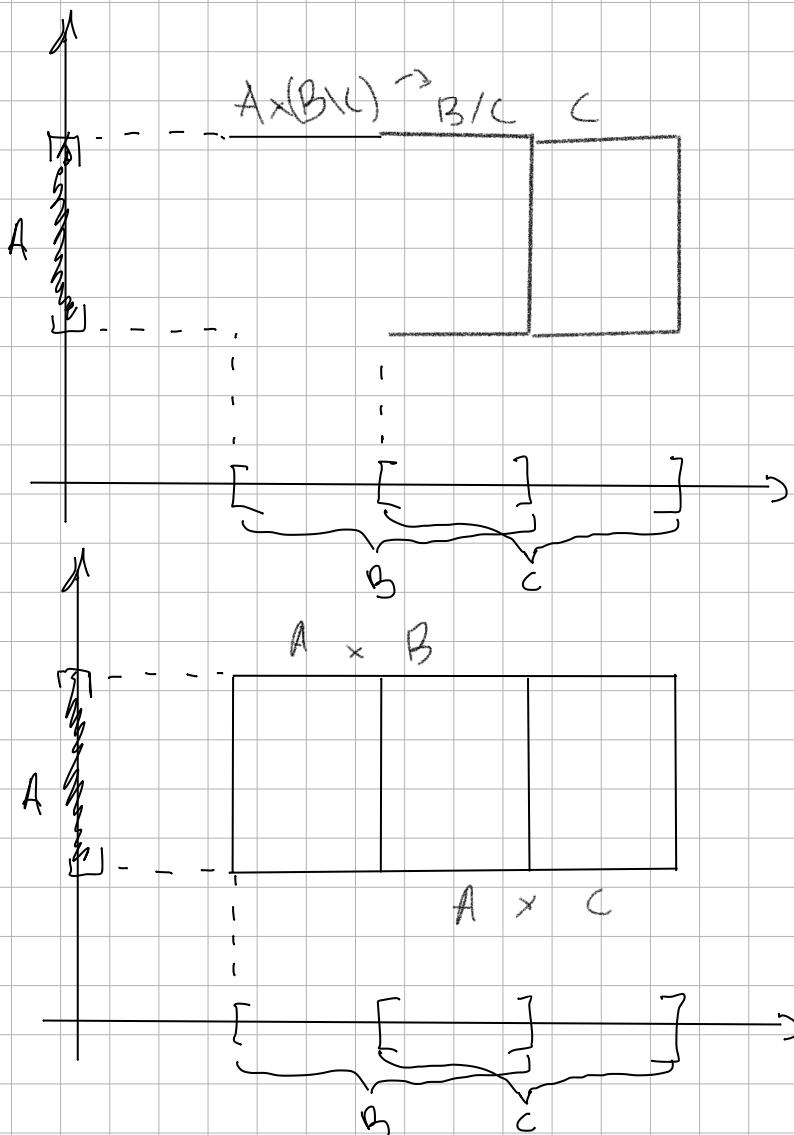
In effetti sia  $A = [5]$ ,  $B = [13] \setminus [5]$ . E siano  $x = \{1, 2, 3\}$ ,  $y = \{3, 4, 5\}$  e sia  $f: A \rightarrow B$  definita ponendo  $f(1) = 7$ ,  $f(2) = 9$ ,  $f(3) = 8$ ,  $f(4) = 9$ ,  $f(5) = 9$ . Allora  $f(x) = \{7, 9, 8\}$ ,  $f(y) = \{8, 9\}$  e  $f(x \cap y) = f(\{3\}) = 9$ . Ma  $f(x) \cap f(y) = \{8, 9\}$  quindi non è sempre vero.

Es [+] sia  $f : A \rightarrow B$  dimostrare che  
 $f(f^{-1}(B)) = B \Leftrightarrow f$  è suriettiva

Es. [2-] Quante relazioni di equivalenza ci sono su  $[3]$ ? (risposte s)

Es.  $A, B, C$  insiemi. E' vero che  
 $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$ ?

Penso usare i diagrammi di Venn?  
 Avrei bisogno di 4 dimensioni ma 2 volte si puo fare.



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

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

Sembra di sì. dimostriamo.

$$\text{Sia } (x, y) \in A \times (B \setminus C) \Rightarrow x \in A \text{ e } y \in B \setminus C$$

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

Viceversa sia  $(x, y) \in (A \times B) \setminus (A \times C) \Rightarrow (x, y) \in A \times B$   
e  $(x, y) \notin A \times C \Rightarrow x \in A$  e  $y \in B$  e  $y \notin C$  (se  
 $y \in C \Rightarrow (x, y) \in A \times C$ , contradiction)  $\Rightarrow x \in A$  e  
 $y \in B \setminus C \Rightarrow (x, y) \in A \times (B \setminus C)$ .

Tavola di verità si può fare in 2 righe (not recommended):

$x$	$y$	$y$	$y$	$(x, y)$	$(x, y)$	$(x, y)$	$(x, y)$
$A$	$B$	$C$	$B \setminus C$	$A \times (B \setminus C)$	$A \times B$	$A \times C$	$(A \times B) \setminus (A \times C)$
1	1	1	0	0	1	1	0
1	1	0	1	1	1	0	1
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
1	0	0	1	0	0	0	0
1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	1	0	1	0	0	0	0

Le colonne corrispondenti  $A \times (B \setminus C)$   
e  $(A \times B) \setminus (A \times C)$  sono uguali  $\Rightarrow$  è sempre vero

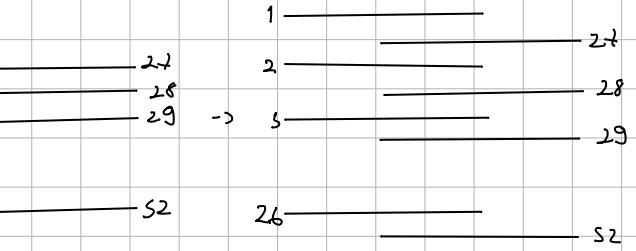
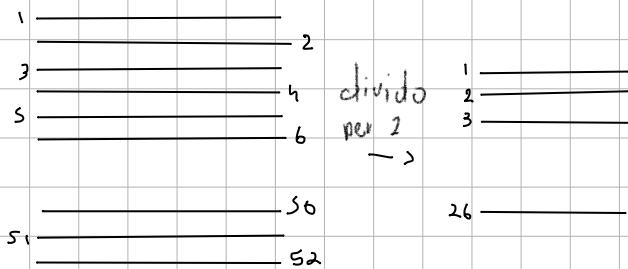
Ese. [2-] Si sia  $p \in S_{S_2}$  definita da

$$p = 1 \ 27 \ 2 \ 28 \ 3 \ 29 \dots 26 \ 51 \ 26 \ 52$$

calcolare il più piccolo  $K \in \mathbb{P}$  tale che

$$\underbrace{p \circ p \circ p \dots \circ p}_K = \text{Id}_{[S_2]}.$$

Oss.  $p$  è la "smazza perfetta"



Quindi  $K$  è il minimo numero di smazzate perfette dopo le quali il mazzo torna nell'ordine iniziale.

E5. Sia  $f: A \rightarrow B$  e siano  $X, Y \subseteq B$  dimostrare  
che  $f^{-1}(X \setminus Y) = f^{-1}(X) \setminus f^{-1}(Y)$

Sia  $\alpha \in f^{-1}(X \setminus Y) \Rightarrow f(\alpha) \in X \setminus Y \Rightarrow f(\alpha) \in X$  e  
 $f(\alpha) \notin Y \Rightarrow \alpha \in f^{-1}(X)$  e  $\alpha \notin f^{-1}(Y) \Rightarrow$   
 $f^{-1}(X) \setminus f^{-1}(Y)$  vi avversa

Sia  $\alpha \in f^{-1}(X) \setminus f^{-1}(Y) \Leftrightarrow \alpha \in f^{-1}(X)$  e  
 $\alpha \notin f^{-1}(Y) \Rightarrow f(\alpha) \in X$  e  $f(\alpha) \notin Y \Rightarrow f(\alpha) \in X \setminus Y \Rightarrow$   
 $\alpha \in f^{-1}(X \setminus Y)$ .

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) Riflessiva? 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) Simmetrica? se due elementi sono in relazione allora anche scambiandoli sono in relazione

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

Se  $m=n \Rightarrow nRm \Rightarrow \text{OK}$  è simmetrica

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

3) Transitiva? presi 3 numeri vedere che il 2° è in relazione con il 3°

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

Se  $m=n$  e  $n=k \Rightarrow m=k \Rightarrow mRk \Rightarrow \text{OK}$

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

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

Se  $m+n=5$  e  $n+k=5 \Rightarrow n=5-m$  e  $n=5-k \Rightarrow$   
 $m=k \Rightarrow mRk \Rightarrow \text{OK}$ . È d. equivalenza

Chi sono le classi di equivalenza?

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

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

Eso. Sia  $R$  la relazione su  $\mathbb{Z} \times \mathbb{Z}^*$ ,

$\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$  definita da

$$(a,b)R(c,d) \iff ad = bc \quad \forall (a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$$

Equivalentza?

1) Riflessiva?

Sia  $(a,b) \in \mathbb{Z} \times \mathbb{Z}^* \Rightarrow ab = ba \Rightarrow (a,b)R(a,b) \Rightarrow$  OK.

2) Simmetrica?

Sia  $(a,b), (c,d) \in \mathbb{Z} \times \mathbb{Z}^*$  tali che  $(a,b)R(c,d) \Rightarrow ad = bc$

$$\Leftrightarrow cb = da \Rightarrow \text{OK.}$$

3) Transitiva?

Sia  $(a,b)(c,d)(e,f) \in \mathbb{Z} \times \mathbb{Z}^*$  tali che  $(a,b)R(c,d)$

e  $(c,d)R(e,f) \Rightarrow ad = bc$  e  $cf = de \stackrel{\times f \neq b}{\Rightarrow} af = be$  e

$baf = bde \Rightarrow bcf = fbc \Rightarrow 2fd = bde$ ,  $d \neq 0$   $\stackrel{\text{perche' in}}{\Rightarrow} af = be$

$$\Rightarrow (a,b)R(e,f) \Leftrightarrow af = be \quad \text{Quindi} \Rightarrow \text{OK.}$$

E' di Equivalentza.

Chi sono le classi di Equivalentza?

Sia  $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$ , allora

$$[(a,b)]_R = \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* : (a,b)R(c,d)\}$$

$$= \{(c,d) \in \mathbb{Z} \times \mathbb{Z}^* : ad = bc\}$$

$$= \left\{ \frac{a}{b} = \frac{c}{d} \right\}$$

Es. [2-] Si è R la relaz. su  $\mathbb{Z}$  definita ponendo

$mRn \Leftrightarrow m-n$  è pari       $2|(m-n)$   
 $\forall m, n \in \mathbb{Z}$ . Equivalenza?

Rifl.?      Simm.?      Trasf.?  
 ✗            ✓            ✓

$$2|m-m \Rightarrow 2|0 \text{ No}$$

$$2|m-n \rightarrow 2|n-m \Rightarrow 2|5-3 \rightarrow 2|3-5 \Rightarrow 5,$$

$$\begin{aligned} 2|m-n &\rightarrow 2|n-p \rightarrow 2|m-p \Rightarrow 2|10-8 \rightarrow \\ &\rightarrow 2|8-4 \rightarrow 2|10-4 \end{aligned}$$

Es. Consideriamo le seguenti relaz. su  $\mathbb{Z}$   
 $m \leq n$ ,  $m=n$  o  $m-n$  è dispari,  $|m-n| \leq 3$ ,  $m|n$   
 $\forall m, n \in \mathbb{Z}$ .

QUESTE SONO LE REGOLE riflessiva simmetrica transitiva  
 NON LE CONDIZIONI

$m \leq n$

$m=n$  siccome  $m-n$  disp.

$|m-n| \leq 9$

$m|n$

Si perché $m=m$	No $\begin{array}{l} 1 \leq 2 \\ 2 \neq 1 \end{array}$	Si $\Rightarrow m \leq p$
Si $m=m$	Si $\begin{array}{l} 5-4=1 \\ 4-5=-1 \end{array}$	No
Si $ m-n  \leq 9$	Si $\begin{array}{l}  5-6 =1 \leq 9 \\  5-4 =1 \leq 9 \end{array}$	No $\begin{array}{l}  5-6  \leq 9 \\  6-2  \leq 9 \\  5-2  \leq 9 \end{array}$
Si $5 5$	No $2 10 \rightarrow 10 2$	Si $\begin{array}{l} 6 10 \quad 10 20 \\ 5 20 \end{array}$

Ese. Consideriamo 3 relazioni su l'insieme delle persone:

$a R b \Leftrightarrow a e b$  hanno la stessa età

$a R b \Leftrightarrow a e b$  hanno gli stessi genitori

$a R b \Leftrightarrow a e b$  hanno una lingua in comune

Rifl.      Simm.      Trans.

$R_1$       ✓              ✓      ✓

$R_2$       ✓              ✓      ✓

$R_3$       ✓              ✓      ✗

Ese. Considerando la relazione " $A \geq B$ " su  $\mathcal{P}(\{1, 2, 3\})$

Rifl.?      Simm.?      Trans?

✓              ✗              ✓

$A \geq A$        $A \geq B$        $B \geq A$        $A \geq B$        $B = C$        $A \geq C$

$$\begin{cases} \{1, 2\} \geq \{1, 2\} \\ \{2, 3\} \geq \{2, 3, 4\} \end{cases}$$

$$\begin{cases} \{2, 3, 4\} \geq \{2, 3\} \\ \{2, 3\} \geq \{2, 3, 4\} \end{cases}$$

Ese. Consideriamo la relazione "Battle"

nell'insieme:

{Carta, forbice, Sasso}

Rifl.? Simm.? Trans.?  
 X X X

Carta non batte carta  
 Carta batte sasso ma sasso non batte carta  
 Carta batte sasso, sasso batte forbice ma carta  
 non batte forbice

E.D. Consideriamo la relazione vuota su  $\mathbb{R}$   
 $aRb \Leftrightarrow \text{mai } \forall a, b \in \mathbb{R}$ .

Rifl.? Simm.? Trans.?  
 X ✓ V

$aRa \Rightarrow$  ho Rifl. mi, nessun  $i$  in  $\mathbb{R}$  con ness.

$aRb \rightarrow bRa \Rightarrow$  dato che  $aRb$  mai allora

anche  $bRa$  sarà mai  $\Rightarrow$  vero

$aRb \rightarrow bRc \rightarrow aRc \Rightarrow$  tutte e tre mai, il ris.

non cambia, 10.2 10.5 10.6 14.7 libro M/T

E.D. Consideriamo la Relazione  $\Leftrightarrow$  "equivalenza logica"  
 nell'insieme di tutte le proposizioni

Rifl.? Simm.? Trans.?  
 V V V

$P = \text{prop}$  allora è vero che?

$P \leftrightarrow P$ :

<u>P</u>	<u><math>P \leftrightarrow P</math></u>
V	V
F	V

$P \wedge Q$  prop.:  $P \leftrightarrow Q$  allora è vero che?

$Q \leftrightarrow P$

<u>P</u>	<u>Q</u>	<u><math>P \leftrightarrow Q</math></u>	<u><math>Q \leftrightarrow P</math></u>
V	V	V	V
V	F	F	F
F	V	F	F
F	F	V	V

le colonne

Sono uguali

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

<u>P</u>	<u>Q</u>	<u>R</u>	<u><math>P \rightarrow Q</math></u>	<u><math>Q \rightarrow R</math></u>	<u><math>P \rightarrow R</math></u>
V	V	V	V	V	V
V	V	F	V	F	F
V	F	V	F	F	F
F	F	F	F	V	V
V	V	F	F	V	V
F	F	V	V	F	F
F	F	F	V	V	V

$(P \rightarrow Q) \wedge (Q \rightarrow R) \rightarrow P \rightarrow R$ : V F V F F V F V  
Vguali

E<sub>b</sub> E<sub>i</sub>] Siano  $P$  e  $Q$  prop. è vero che:

$$\text{"} P \rightarrow Q \text{" e "} \neg P \rightarrow \neg Q \text{"}$$

Sono equivalenti?

$P$	$Q$	$\neg P$	$\neg Q$	$P \rightarrow Q$	$\neg P \rightarrow \neg Q$	
V	V	F	F	V	V	
V	F	F	V	F	V	
F	V	V	F	V	F	
F	F	V	V	V	V	

non sono  
uguali

E<sub>b</sub>. Siano  $P, Q, R$  prop. è vero che:

$$\text{"} \neg(P \wedge (Q \wedge R)) \text{" e "} (\neg P) \vee ((\neg Q) \vee (\neg R)) \text{"}$$

Sono equivalenti?

$P$	$Q$	$R$	$\neg P$	$\neg Q$	$\neg R$	$Q \wedge R$	$\neg(Q \wedge R)$	$\neg P \vee \neg(Q \wedge R)$
V	V	V	F	F	F	V	F	F
V	V	F	F	F	V	F	V	V
V	F	V	F	V	F	F	V	V
V	F	F	F	V	V	F	V	V
F	V	V	V	F	F	V	F	F
F	V	F	V	F	V	F	V	V
F	F	V	V	V	F	F	V	V
F	F	F	V	V	V	F	V	V

$$P \wedge (Q \wedge R) \quad (\neg P) \vee ((\neg Q) \vee (\neg R)) \quad \neg(P \wedge (Q \wedge R))$$

U	F	F
F	V	V
F	V	V
F	V	V
F	V	V
F	V	V
F	V	V
F	V	V



sono uguali

le colonne sono equiv.

**Es.** In pratica è più comodo usare il "nand" ("not and") invece di "v", "¬" e "Λ".

$$P \quad Q \quad P \Box Q$$

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

**Es.** Esprimere "v", "Λ" e "¬" in funzione del "□". NAND

$$A \Box B = \neg(A \wedge B) \text{ in effetti:}$$

A	B	$A \Box B$	$A \wedge B$	$\neg(A \wedge B)$
V	V	F	V	F
V	F	V	F	V
F	V	V	F	V
F	F	V	F	V

Pertanto sono uguali quindi:

$$A \wedge B = \neg(A \Box B)$$

$$A \Box A = \neg(A \wedge A) = \neg A$$

$$A \Box B = (\neg A) \vee (\neg B) \quad (\text{DM})$$

$$\neg \neg A = A \Box A$$

$$A \wedge B = (A \Box B) \Box (A \Box B)$$

$$(\neg A) \Box (\neg B) = A \vee B$$

$$A \vee B = (A \Box A) \Box (B \Box B)$$

Es. C'è stato un delitto e Poirot ha determinato che:

- i sospettati sono 9: 1, 2, 3, ..., 9
- i colpevoli sono almeno 3
  - 1, 2 sono innocenti
  - Se 3 o h sono colpevoli  $\Rightarrow$  tutti sono colpevoli
  - Se 1 è colpevole  $\Rightarrow$  2 è colpevole
  - Se 5 è colpevole  $\Rightarrow$  3 è colpevole
  - Se 6 o 7 sono colpevoli  $\Rightarrow$  8 è innocente
  - Se 6 o 2 sono colpevoli  $\Rightarrow$  9 è innocente

Scrivere una prop. composta che esprima queste affermazioni e trovare i colpevoli

- $\exists_x \exists_y \exists_z ((x \neq y) \wedge (y \neq z) \wedge (x \neq z) \wedge x \neq 1 \wedge x \neq 2)$
- $(\neg 1) \vee (\neg 2)$
- $(\neg 3 \vee 4) \rightarrow (1, 2, \dots, 9)$
- $(\neg 1 \rightarrow 2)$
- $(\neg 5 \rightarrow 3)$
- $(\neg 6 \vee 7) \rightarrow 78$  processo lungo
- $(\neg 6 \vee 2) \rightarrow 79$

Ese. è vero che

$$((A \vee B) \wedge (A \rightarrow B)) \rightarrow A ? \quad \xrightarrow{\text{NO}}$$

$$A \quad B \quad A \vee B \quad A \rightarrow B \quad ((A \vee B) \wedge (A \rightarrow B)) \quad ((A \vee B) \wedge (A \rightarrow B)) \rightarrow A$$

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

Ese. è vero che

$$((A \rightarrow B) \wedge (A \circ B)) \rightarrow A \quad \rightarrow \text{NO non è sempre vera}$$

$$A \quad B \quad A \rightarrow B \quad A \circ B \quad ((A \rightarrow B) \wedge (A \circ B)) \quad ((A \rightarrow B) \wedge (A \circ B)) \rightarrow A$$

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

Ese. esprimere le seguenti affermazioni:

"ci sono studenti che hanno seguito m.d e hanno preso 30"

come un predicato, usando predicati

$S(x) = "x ha seguito M.D."$

$L(x) = "x ha preso 30"$

( $x \in$  universo degli studenti)

$$\exists x . ((S(x) \wedge L(x)))$$

Ese. Consideriamo l'affermazione:

"Tutti i tutori di MD che hanno seguito MD  
hanno preso 30"

usando i predicati di prima e

$T(x) = "x è tutore di MD"$

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

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

Ese. Consideriamo l'affermazione:

"Esiste uno studente che ha spedito una posta  
elettronica ad esattamente due studenti, tranne  
forse a se stesso.

Scrivere un predicato equivalente usando il predicato

$E(x, y) := "x ha spedito una mail ad y"$

$\exists x . \exists y . \exists z . ((x \neq y) \wedge (x \neq z) \wedge (y \neq z) \wedge$   
 $((E(x, y) \wedge E(x, z)) \vee (E(x, y) \wedge E(x, z) \wedge E(x, x))) \wedge$   
 $(\forall w . (((w \neq x) \wedge (w \neq y) \wedge (w \neq z)) \rightarrow \neg E(x, w))).$

**Esercizio.** Comporre un predicato  $P(n)$  che esprime l'affermazione "n è primo" usando i simboli di  $\neg, \leq, +, \cdot$  ma non costanti  $(1, 2, \dots)$  ( $n \in \mathbb{P}$ )

Conviene definire prima il pred.

$$D(n, m) = "n divide m"$$

Potremmo scrivere

$$D(n, m) = \exists k. (m = n \cdot k)$$

Abbiamo bisogno di un predicato  $U(n) = "n = 1"$ .

Potremmo scrivere

$$U(n) = (n \cdot n = n)$$

Potremmo allora scrivere

$$P(n) = \forall m. ((D(m, n) \wedge (m < n)) \rightarrow U(m))$$

**Esercizio.** Scrivere un predicato  $G(n)$  che esprima la congettura di Goldbach. Dato  $n \in \mathbb{P}, n > 2$ ,  $n$  pari  $\Rightarrow \exists p, q$  primi tali che

$$n = p + q$$

Potremmo scrivere prima un pred.  $\Phi(n)$  che esprima " $n = 2$ "

$$\Phi(n) = (n \cdot n = n + n)$$

poi potremmo avere:

$$\forall n . \left( \exists_{\substack{n \\ i \text{ pari}}}^{} (E(n) \wedge \forall m . (F(m) \rightarrow n > m)) \rightarrow \exists_{p,q} . (P(p) \wedge P(q) \wedge \lambda(n = p + q))) \right)$$

Esercizio 3 Dimostrare che esistono infiniti numeri  
 $k \in \mathbb{P}$  tali che

$$6k + 5$$

è primo

(sugg. generalizzare la dim. di 3.4.2)

Esercizio. Costruire un predicato che esprimesse  
"Ci sono infiniti numeri primi"  
potremmo scrivere:

$$\forall n . \exists m . ((m > n) \wedge P(m))$$

Sondaggio 1.

Si dà  $f : [5] \rightarrow [5]$  definita ponendo

$$f(1) = 5, f(2) = 3, f(3) = 5, f(4) = 1, f(5) = 2$$

Allora

$$f^{-1}(\{1, 4\}) \quad \text{è}$$

- a)  $\{1, 5\}$    b)  $\emptyset$   
 c)  $\{4\}$    d)  $\{1, 4\}$

e) nessun<sup>o</sup> tra queste

### Sondaggio 2

Siano  $P$  e  $Q$  prop. allora una prop. logicamente equivalente a

$\neg(p \rightarrow q)$  è:

- a)  $\neg p \rightarrow \neg q$       b)  $p \rightarrow \neg q$   
 b)  $\neg q \rightarrow \neg p$       c)  $\neg q \rightarrow p$   
 e) N.D.Q V

$p$	$q$	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg(p \rightarrow q)$
V	V	F	F	V	F
V	F	F	V	F	V
F	V	V	F	V	F
F	F	V	V	F	V

Eb[+]: Siano  $a, b \in \mathbb{P}$  è vero che

$$\text{MCD}(a, b) = 1 \Rightarrow \text{MCD}(a+b, a-b) = 1 ?$$

Ese. Sia  $\alpha \in \mathbb{Q}$  dimostrare usando il WOP, che esistono  $a, b \in \mathbb{Z}$  tali che  $b > 0$ ,  $\alpha = \frac{a}{b}$ , e  $(a, b) = 1$ .

Sia

$$S := \left\{ d \in \mathbb{P} : \exists c \in \mathbb{Z} \text{ per cui } \alpha = \frac{c}{d} \right\}$$

Allora  $S \subseteq \mathbb{P}$  e  $S \neq \emptyset$  (perché  $\alpha \in \mathbb{Q}$ )

per il WOP  $\Rightarrow \exists b \in \mathbb{P}$  tale che  $b \in S$

$$b \leq d \quad \forall d \in S. \quad (\times)$$

poiché  $b \in S \Rightarrow \exists a \in \mathbb{Z}$  per cui  $\alpha = \frac{a}{b}$

Allora  $(a, b) = 1$  infatti sia  $c \in \mathbb{P}$  tale che  $c | a$  e  $c | b \Rightarrow \exists k, l \in \mathbb{Z}$  tali che  $a = c \cdot k$  e  $b = c \cdot l$   
 $\Rightarrow l | b \Rightarrow l < b$ , ma allora

$$\alpha = \frac{a}{b} = \frac{ck}{cl} = \frac{k}{l}$$

$l \in S$  e  $l < b$ . assurdo per  $(\times)$

Ese. Consideriamo un torneo all'italiana tra  $n$  squadre  $(1, 2, \dots, n)$  una classifica

$T = T(1) T(2) \dots T(n) \in S_n$  è ragionevole se

$T(i)$  ha battuto  $T(i+1)$   $\forall 1 \leq i \leq n-1$ . dimostrare che esiste sempre una classifica ragionevole  
 Induzione su  $n \geq 1$ . chiaro se  $n=1$  o  $n=2$

Supponiamo  $n \geq 3$ . Sia

$$A := \{ i \in [n-1] : i \text{ ha battuto } 1 \} \setminus \{1\}$$

$$B := \{ j \in [n-1] : 1 \text{ ha battuto } j \} \setminus \{1\}$$

Allora  $|A| \leq n-1$  e  $|B| \leq n-1$ . Quindi per induzione  $\exists p$  e  $\sigma$  classifiche ragionevoli di  $A$  e  $B$ . Allora

$p \circ \sigma$

è una classifica ragionevole

$$p(1) \text{ ha battuto } p(2)$$

$$p(2) \text{ ha battuto } p(3) \quad (p \text{ è ragionevole})$$

$$p(|A|) \text{ ha battuto } 1$$

$$1 \text{ ha battuto } \sigma(1)$$

$$\sigma(1) \text{ ha battuto } \sigma(2) \quad (\sigma \text{ è ragionevole})$$

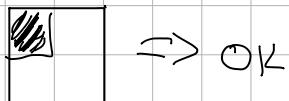
Es. Sia nel P. abbiamo una piazza  $2^h \cdot 2^n$

vogliamo erigere una statua al "centro" della piazza e pavimentare il resto con mattonelle di forma

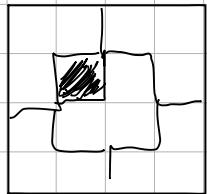


è sempre possibile questo?

Vediamo se  $n=1$



$n=2$



Dim. per induzione

Se si puo fare  $\Rightarrow \frac{2^n}{3}$  deve dare resto 1

il viceversa potrebbe non essere vero, non posso pavimentare con  $\boxed{\phantom{0}}$  ma solo con  $\boxed{\phantom{0}}\boxed{\phantom{0}}$

Rafforzamento dell'ipotesi

Dimostriamo che possiamo pavimentare una pizza  $2^r \cdot 2^r$  con mattonelle  $\boxed{\phantom{0}}$ , dunque mettiamo la statua

E.d. Consideriamo il seguente teorema. Sia  $\alpha \in \mathbb{Z}$ ,  $\alpha \neq 0$  e sia  $n \in \mathbb{N}$  allora

$$\alpha^n = 1 \quad *$$

Dim. Induzione su  $n \geq 0$ . Se  $n=0 \Rightarrow \alpha^0 = \alpha^0 = 1$

Supponiamo \* vero  $\forall m \in \mathbb{N}$  tale che  $m \leq n$  allora:

$$\alpha^{n+1} = \frac{\alpha^n \cdot \alpha^n}{\alpha^{n-1}} = \frac{1 \cdot 1}{1} = 1$$

dove c'è l'errore?

Ese. Calcolare  $\text{MCD}(389, 167)$  e la corrispondente identità di Bezout. Usiamo A.E.abbiamo

$$389 = 167 \cdot 2 + 55 \quad 1$$

$$167 = 55 \cdot 3 + 2 \quad 2 \quad \text{MCD}(389, 167) = 1$$

$$55 = 2 \cdot 27 + 1 \quad 3$$

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

per calcolare bezout. Svolgiamo A.E. 2 ritroso

$$1 = 55 + (-27) \cdot 2$$

$$2 = 55 + (-27)(167 + (-3) \cdot 55) = -27 \cdot 167 + 82 \cdot 55$$

$$3 = (-27)167 + (82)(389 + (-2)(167)) = (82)389 + (-19_1)167$$

quindi l'identità di bezout è:

$$1 = (82)389 + (-19_1)167$$

Ese. calcolare

$$\text{MCD} \left( \underbrace{17^8 \cdot 31^5 \cdot 37^2 \cdot 53^{100}}_a, \underbrace{19^{12}}_b, \overbrace{37^{12}}^{\frac{3678}{53}} \right)$$

notiamo che  $17, 31, 37, 53, 19, 53$  sono tutti numeri primi quindi

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

infatti  $\exists$   $p \in \mathbb{P}$ ,  $p$  primo, tale che  $p | a$  e  $p | b$

3.6.3  
 $\Rightarrow (p \mid 17 \circ p \mid 21 \circ p \mid 37 \circ p \mid 59) \wedge (p \mid 19 \circ p \mid 37 \circ p \mid 53) \Rightarrow (p = 17 \circ p = 31 \circ p = 37 \circ p = 59) \wedge (p = 19 \circ p = 37 \circ p = 53) \Rightarrow p = 37$  unico numero in comune  
 $37^2 \mid a, 37^2 \mid b$  mentre  $37^3 \nmid a$

- D. Calcolare  $\text{MCD}(1137, 419)$  e la corrispondente identità di Bezout

$$1137 = 419 \cdot 2 + 299$$

$$419 = 299 \cdot 1 + 120$$

$$\text{MCD}(1137, 419) = 1$$

$$299 = 120 \cdot 2 + 59$$

$$120 = 59 \cdot 2 + 2$$

$$59 = 2 \cdot 29 + 1 \quad \text{ultimo resto non nullo}$$

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

$$1 = 59 + (-29)2$$

$$= (-29)(120 + (-2)59) + (1)59$$

$$= 59 \cdot 59 + (-29)120$$

$$= 59(299 + (-2)120) + (-29)120$$

$$= (-147)120 + (59)299$$

$$= (-147)(419 + (-1)299) + (59)299$$

$$= (206)299 + (-147)419$$

$$= (206)(1137 + (-2)419) + (-147)419$$

$$= (-559)419 + 206(1137)$$

$$1 = (-559)_{419} + 206_{(1137)} = \text{ID Bezout}$$

**E.d.** Siano  $a, b \in \mathbb{P}$   $a \geq b$ ,  $b \geq 2$  Dimostrare che l'A.E. termina in al più

$$2 \cdot \log_2(b)$$

Iterazioni

Induzione su  $b \geq 2$ .

Se  $b=2$  l'A.E. termina in al più 2 iterazioni  
(1 se  $a$  è pari, 2 se  $a$  è dispari).

$$2 \log_2(b) = 2 \log_2(2) = 2 \cdot 1 = 2 \Rightarrow \text{OK.}$$

Se  $b \geq 3$ . Abbiamo che

$$a = b \cdot q + r \quad 0 \leq r < b$$

$$b = q_1 \cdot r + r_1 \quad 0 \leq r_1 < r$$

Notiamo che

$$r_1 \leq \frac{b}{2}$$

Infatti, se  $r \leq \frac{b}{2} \Rightarrow r_1 < r \leq \frac{b}{2} \Rightarrow \text{OK.}$

Se  $r > \frac{b}{2} \Rightarrow 2r > b \Rightarrow q_1 = 1$  e  $r_1 = b - r < b - \frac{b}{2} = \frac{b}{2} \Rightarrow \text{OK}$

$$\text{In 2 } \text{MCD}(a, b) = \text{MCD}(b, r) = \text{MCD}(r, r_1)$$

poiché  $r_1 \leq \frac{b}{2} \Rightarrow$  l'A.E. per il  $\text{MCD}(r, r_1)$

termina in 2 più  $2 \log_2(r_1)$  iterazioni

Quindi l'A.E. per MCD(a,b) termina in 2 più:

2 + 2  $\log_2(r_1)$  iterazioni

$$\text{ma } r_1 \leq \frac{b}{2} \text{ pertanto } 2 + 2 \log_2(r_1) \leq 2 + 2 \log_2\left(\frac{b}{2}\right)$$

$$= 2 + 2(\log_2(b) - \log_2(2)) = 2 + 2 \log_2(b) - 2 =$$

$$2 \log_2(b)$$

E5. Siano  $a, b \in \mathbb{P}$ . è vero che  $\text{MCD}(a+1, b+1)$

$$\text{MCD}(a, b) + 1 ?$$

Se fosse vero  $\Rightarrow \text{MCD}(a+1, b+1) \geq 2 \quad \forall a, b \in \mathbb{P}$ .

$$\text{MCD}(12, 11) = 1 \Leftrightarrow \text{se } a = 16 \text{ e } b = 10 \Rightarrow \text{MCD}(a+1, b+1) = 1$$

ma  $\text{MCD}(a, b) + 1 = 2 + 1 = 3 \neq 1$  quindi è falso.

O7 (11)

E6. Siano  $a, b \in \mathbb{P}$  dimostrare che  $(a, b) = 1 \Rightarrow (a^2, b) = 1$

Dim per assurdo. Si  $(a^2, b) \geq 2 \Rightarrow \exists p \in \mathbb{P}, p \text{ primo}$

tale che  $p | (a^2, b) \Rightarrow p | a^2 \text{ e } p | b \stackrel{(3.6.2)}{\Rightarrow} p | a \text{ e } p | b$

$\Rightarrow p | (a, b) \Rightarrow p \nmid 1$  assurdo.

più in generale

$$(a, b) =_1 \Rightarrow (a^n, b^m) =_1 \forall n, m \in \mathbb{P}$$

E.s. Siano  $a, b, c \in \mathbb{Z}$  dimostrare che

$$(a, c) =_1 \text{ e } (b, c) =_1 \Rightarrow (a, b, c) =_1$$

Ragionamento per assurdo.

S.i.  $(a, b, c) =_1 \Rightarrow \exists p \in \mathbb{P}$ ,  $p$  primo tale che  
 $p | ab$  e  $p | c \Rightarrow (p | a \text{ o } p | b)$  e  $p | c \Rightarrow$   
 $\circ (p | a \text{ e } p | c) \circ (p | b \text{ e } p | c) \Rightarrow$  assurdo o assurdo

$p$  non può dividere sì:

b che c perché  
coprimi

E.s. [1+] Calcolare il minimo  $k \in \mathbb{P}$  tale che

$$\underbrace{[3]_{17} \cdot [3]_{17} \cdot [3]_{17} \cdots}_{k \text{ volte}} = [1]_{17}$$

$k$  volte

E.s. Trovare tutti i numeri  $x, y \in \mathbb{Z}$  tali che

$$89x + 43y = 1 \quad (*)$$

Sappiamo dalla teoria che esistono  $x, y \Leftrightarrow (89, 43) \mid 1$

Calcoliamo  $(89, 43)$  con A.E.

$$89 = 43 \cdot 2 + 3$$

$$43 = 3 \cdot 14 + 1 \rightarrow (89, 43) = 1$$

$$3 = 1 \cdot 3 + 0$$

$1 \mid 1 \rightarrow$  ci sono soluzioni per \*

$$1 = 43 + (-14)3$$

$$= (-14)(89) + (43)(-2) + (1)43$$

$$= 29(43) + (-14)(89)$$

$$\text{identità di Bezout} : (29)43 + (-14)89$$

pertanto  $x = -14, y = 29 \rightarrow$  una soluzione di \*

Sappiamo allora dalla teoria che tutte le soluz.

$x, y \in \mathbb{Z}$  di \* sono della forma:

$$\begin{cases} x = x_0 - \frac{43}{(89, 43)} t \\ y = y_0 + \frac{89}{(89, 43)} t \end{cases} \quad \forall t \in \mathbb{Z}$$

quindi

$$\begin{cases} x = -14 - 43t \\ y = 29 + 89t \end{cases} \quad t \in \mathbb{Z}$$

esplicito

x	y	t
-14	29	0
-57	118	1
29	-60	-1

A.E  
Bezout  
classi  
funz. [1 mod 2]  
inverso moltiplicativo

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

$$875x + 235y = 10$$

Sappiamo dall'2 teoria che esistono soluzioni  
Se e solo se  $(875, 235) = 10$

$$875 = 235 \cdot 3 + 170$$

$$235 = 170 \cdot 1 + 65$$

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

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

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

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

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

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

$$b = 15 + (-1 \cdot 10)$$

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

$$\approx 2(15) + (-1)(25)$$

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

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

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

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

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

$$\begin{aligned}
 &= -13(65) + 5(170) \\
 &= 5(170) + (-13)(235) \\
 &= 18(170) + (-13)(235) \\
 &= (-13)(235) + (18)(875 + 253 \cdot (-3)) \\
 &= (-67)(235) + (18)875 = 5 \quad = \text{identità di Bezout}
 \end{aligned}$$

ma a me interessa 10 e non 5 perciò  
moltiplichiamo l'ID di Bezout per 2:

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

pertanto  $x=36, y=-134$  una sol.

Sappiamo dalla teoria che tutte le soluzioni  $x, y \in \mathbb{Z}$   
sono della forma:

$$\left\{
 \begin{array}{l}
 x = x_0 - \frac{235}{s} t \\
 y = y_0 + \frac{875}{s} t
 \end{array}
 \right. \quad \text{con } (t \in \mathbb{Z})$$

espliato

$$\left\{
 \begin{array}{l}
 x = 36 - \frac{235}{5} t = 36 - 47t \\
 y = -134 + \frac{875}{5} t = -134 + 175t
 \end{array}
 \right.$$

$$\begin{array}{ccc}
 x & y & t \\
 36 & -134 & 0
 \end{array}$$

- 11

41

1

83

- 309

- 1

**Esercizio.** Sia  $p = 1, 27, 2, 28, 3, 29, \dots, 26, 52 \in S_{S_2}$   
 calcolare il minimo  $k \in \mathbb{P}$  tale che

$$\underbrace{p \cdot p \cdot p \cdots p}_K = \text{Id} \quad (= 1, 2, 3, 4, \dots, 52)$$

abbiamo che dopo 8 smazzi si tornano tutte al loro posto

**Esercizio.** Siano  $p, q \in \mathbb{P}$ ,  $p \neq q$ ,  $p, q$  primi  
 $p \geq 3, q \geq 3$ , dimostrare che  $n = p \cdot q$  non è perfetto

I divisori di  $n$  sono  $1, p \cdot q, p, q$

Per assurdo. Sia  $n$  perfetto, allora

$$p \cdot q = 1 + p + q = 2pq = (\overset{\text{(uguale)}}{1+p})(\overset{\text{(uguale)}}{1+q})$$

$$\text{ma } p \equiv 1 \pmod{2} \Rightarrow \exists k \in \mathbb{Z} \text{ t.c. } p = 2k + 1$$

$$\Rightarrow 2pq = 2(k+1)(1+q) = pq = (1+k)(1+q)$$

$$\text{ma } q \equiv 1 \pmod{2} \Rightarrow \exists l \in \mathbb{Z} \text{ t.c. } q = 2l + 1$$

$$\Rightarrow pq = (1+k)(l+1)_2 \Rightarrow 2 \mid pq \Rightarrow \circ 2 \mid p \circ 2 \mid q$$

assurdo perché  $p$  e  $q$  primi  $\geq 3$  quindi non divisibili per 2.

Eso. Siano  $p_1, \dots, p_r \in \mathbb{P}$   $p_1, \dots, p_r$  primi  
t.c.  $p_1 \geq 3, \dots, p_r \geq 3$ . Dimostrare che:

$n = p_1 \cdots p_r$  non è perfetto.

Eso. Calcolare le ultime due cifre di  $7^{91}$

S. chiede di calcolare  $[7]_{100}^{91}$  ma  $(7, 100) = 1$   
 $\Rightarrow$  per il teorema di Eulero:

$$[7^{\varphi(100)}]_{100} = [1]_{100}$$

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

quindi  $[7^{40}]_{100} = [1]_{100}$

ma allora

$$[7^{91}]_{100} = [(7^{40})^2]_{100} \cdot [7^{11}]_{100} = ([7^{40}]_{100})^2 \cdot [7^{11}]_{100} \approx \\ = ([1]_{100})^2 \cdot [7^{11}]_{100} = [7^{11}]_{100}$$

$$\text{ma: } [7^2]_{100} = [49]_{100}, \quad [7^6]_{100} = ([7^2]_{100})^3 = [49^2]_{100} \\ = [2401]_{100} = [1]_{100}$$

$$[7^8] = ([7^4]_{100})^2 = [1]_{100} \quad \text{perche } [7^6]_{100} = 1$$

Pertanto:  $[7^{11}]_{100} = [7^{8+2+1}]_{100} = [7^8]_{100} [7^2]_{100} \cdot [7]_{100}$

$$= [1]_{100} \cdot [49]_{100} \cdot [7]_{100} = [343]_{100} = [43]_{100}$$

Concludendo:  $[7^{91}]_{100} = [7^{11}]_{100} = [43]_{100}$   
 $\Rightarrow$  le ultime 2 cifre di  $7^{91}$  sono 43

E.s. dimostrare che

$$T(n) \equiv 0 \pmod{2} \quad \forall n \in \mathbb{P}, n \geq 3$$

S.i. 2 n dispari  $\Rightarrow n = 2m+1$  con  $n \in \mathbb{P}$

Allora  $(m, n) = (m, 2m+1) = 1$ . Inoltre

$$\left| \left\{ 1 \leq i \leq m : (i, n) = 1 \right\} \right| = \left| \left\{ m+1 \leq i \leq n : (i, n) = 1 \right\} \right|$$

infatti, la funzione

$$\varphi: \left\{ 1 \leq i \leq m : (i, n) = 1 \right\} \xrightarrow{\text{f. biuniv.}} \left\{ m+1 \leq i \leq n : (i, n) = 1 \right\}$$

definita ponendo

$$\varphi(i) := n - i \quad \forall i, \text{ e' una biezione.}$$

S.i.  $1 \leq i \leq m$  t.c.  $(i, n) = 1$  allora  $(\varphi(i), n) = (n-i, n) = 1$  (se  $p \in \mathbb{P}$ ,  $p$  primo e t.c.  $p \nmid n$  e  $p \nmid n-i$   
 $\Rightarrow p \mid (n - (n-i)) \Rightarrow p \mid i$  assurdo perché coprimi).  
 e' chiaro che  $\varphi$  e' una biezione  $\Rightarrow$  OK.

S.i.  $n \equiv 0 \pmod{2} \Rightarrow n = 2m$  per qualche  $m \in \mathbb{P}$   
 $\Rightarrow (n, m) = (2m, m) = m \Rightarrow (n, m) \neq 1$ .

S.i.  $S \subseteq \mathbb{N}$ , poniamo  $\text{EVL}(S) := \{i \in S : (i, n) = 1\}$

$$\text{allora } \text{EUL}([2m]) = \text{EUL}([m-1]) \cup \text{EUL}([m+1, 2m-1])$$

$(A \cup B \cup C) = \text{significa } A = B \cup C \text{ e } B \cap C = \emptyset$

Sia  $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}$  definita ponendo  $\varphi(i) := 2m-i$

allora  $\varphi$  è iniettiva e suriettiva e

$\varphi: \text{EUL}([m-1]) \rightarrow \text{EUL}([m+1, 2m-1])$  (perché  
 $(i, 2m) = 1 \Rightarrow (2m-i, 2m) = 1$ . pertanto)

$$|\text{EUL}([m-1])| = |\text{EUL}([m+1, 2m-1])|$$

quindi:

$$\overline{\Phi}(n) = \overline{\Phi}(2m) = |\text{EUL}([2m])| = 2 |\text{EUL}([m-1])|$$

E.D. 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.

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

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

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

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

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

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

$$(13) \cdot 13 + (-6) \cdot 28 =$$

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

$$(-58) \cdot 28 + (13) \cdot 125$$

$1 = (-58) \cdot 28 + (13) \cdot 125$  è l'ID di Bezout

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

quindi l'inverso moltiplicativo di  
 $[28]_{125}$  è  $[-58]_{125} = [67]_{125}$

E.d. Calcolare le inverse moltiplicative di:

$$[172]_{221} \text{ e } [221]_{172}$$

Sappiamo dalla teoria che tali inverse moltiplicative esistono solo se  $(221, 172) = 1$ .

Calcolare con l'AE

$$221 = 172 \cdot 1 + 49$$

$$172 = 49 \cdot 3 + 25$$

$$49 = 25 \cdot 1 + 24$$

$$25 = 24 \cdot 1 + 1 \quad (221, 172) = 1$$

$$24 = 1 \cdot 24 + 0$$

Calcolare ID di Bezout

$$1 = 25 + (-1 \cdot 24) =$$

$$(-1)(49 + (-1)(25)) + 25 =$$

$$(2) 25 + (-1) 49 =$$

$$(2)(172 + (-3)49) + (-1)49 =$$

$$(-2)49 + (2)172 =$$

$$(-2)(221 + 172(-1)) + (2)(172) =$$

$$(9)172 + (-8)221$$

$1 = (9)172 + (-8)221$  é l'ID di Bezout

$$\text{pertanto } (9)_{172} \equiv 1 \pmod{221} \Rightarrow [(9)_{172}]_{221} \in [1]_{221}$$

$$\Rightarrow [9]_{221} \cdot [172]_{221} = [1]_{221}$$

$$\text{ma } (-7)_{221} \equiv 1 \pmod{185} \Rightarrow [-7]_{182} \cdot [221]_{172} = [1]_{172}$$

pertanto l'invers. mult. di

$$[172]_{221} \text{ è } [9]_{221} \text{ e } [221]_{182} \overset{165}{\text{è}} [-8]_{172}$$

E.D. Siano  $p, q \in \mathbb{P}$ , t.c.  $p, q$  hanno 1000 cifre decimali. Quante cifre decimali ha  $p \cdot q$ ?

**Esercizio.** 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:

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

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

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

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

**Esercizio.** Calcolare

$$\left| \{A \subseteq [9] : 2 \notin A \text{ o } 8 \in A\} \right|$$

abbiamo che

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

dove

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

ma per principio di I-E:

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

abbiamo

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

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

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

Pertanto per 4.3.1,

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

Esercizio (calcolare)

$$|\{f \in S_g : f(2) \neq 2 \text{ e } f(u) \neq u\}|$$

Euristiche: "O"  $\rightarrow$   $\cup$   $\rightarrow$  Principio di I-E  $\leftarrow$   
 "e": FACILE!  $\rightarrow$  OK.; NON FACILE  $\rightarrow$  de Morgan  $\Rightarrow$

Usiamo de Morgan: abbiamo che

$$S_g \setminus \{f \in S_g : f(2) \neq 2 \text{ e } f(u) \neq u\} =$$

$$= \{f \in S_g : f(2) = 2 \text{ o } f(u) = u\} = X \cup Y$$

dove

$$X := \{f \in S_g : f(2) = 2\} \quad Y := \{f \in S_g : f(u) = u\}$$

pertanto per I-E:

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

$$|X| = |\{f \in S_g : f(2) = 2\}| = a_1, a_2, \dots, a_9 = 8!$$

un posto occupato, ha una scelta in meno quindi: al posto di 8! si ha 7!

$$|Y| = |\{f \in S_g : f(u) = u\}| = 8! \quad \text{e} \quad \text{perche hai 2 posti occupati}$$

$$|X \cap Y| = |\{f \in S_g : f(2) = 2 \text{ e } f(u) = u\}| = 7!$$

$$= 8! \times 8! - 7! = |X \cup Y| = \text{concludendo}$$

$$|\{f \in S_9 : f(2) \neq 2 \text{ e } f(4) \neq 4\}| = 8! - |X \cup Y| =$$

$$8! - 8! - 8! + 7! = (72 - 8 - 8 - 1) 7! = 57 \cdot 7!$$

**E.** Nel 2021 presso l'uni for vergata si sono laureati 28 studenti in informatica, 22 in mate e 21 in fisica. Di questi, 8 si sono laureati sia in matematica che in info, 6 sia in mat che fis, 1 sia in inf che in fis e 1 in tutte e 3 le materie. Quanti studenti s. sono laureati in almeno 2 di queste materie?

Si chiede:  $|M \cup I \cup F|$  dove

$$M = \{\text{stud. laureati in mat}\}$$

$$I = \{\text{,, ,,, ,,, info}\}$$

$$F = \{\text{,, ,,, ,,, fis}\}$$

$$|I| = 28, |M| = 22, |F| = 21, |M \cap F| = 6,$$

$$|I \cap M| = 8, |I \cap F| = 6, |M \cap F \cap I| = 3$$

applichiamo I-E:

$$|M \cup I \cup F| = M + I + F - |M \cap F| - |I \cap M| - |I \cap F|$$

$$+ |I \cap M \cap F| = 22 + 28 + 21 - 6 - 8 - 6 + 3 = 56$$

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

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

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

$$\begin{aligned} |A_1 \cup \dots \cup A_5| &= |A_1| + \dots + |A_5| - |A_1 \cap A_2| - |A_1 \cap A_3| - \\ &- |A_1 \cap A_4| - |A_1 \cap A_5| - |A_2 \cap A_3| - |A_2 \cap A_4| - |A_2 \cap A_5| - \\ &- |A_3 \cap A_4| - |A_3 \cap A_5| - |A_4 \cap A_5| + |A_1 \cap A_2 \cap A_3| + \\ &+ |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_2 \cap A_5| + |A_1 \cap A_3 \cap A_4| + \\ &+ |A_1 \cap A_3 \cap A_5| + |A_1 \cap A_4 \cap A_5| + |A_2 \cap A_3 \cap A_4| + \\ &+ |A_2 \cap A_3 \cap A_5| + |A_2 \cap A_4 \cap A_5| + |A_3 \cap A_4 \cap A_5| - \\ &- |A_1 \cap A_2 \cap A_3 \cap A_4| - |A_1 \cap A_2 \cap A_3 \cap A_5| - \\ &- |A_1 \cap A_2 \cap A_4 \cap A_5| - |A_1 \cap A_3 \cap A_4 \cap A_5| - \end{aligned}$$

$$|A_2 \cap A_3 \cap A_6 \cap A_5| + |A_1 \cap A_2 \cap A_3 \cap A_6 \cap A_5|$$

10 possibilità  $\begin{smallmatrix} 10 \\ 10 \\ 10 \\ 10 \\ 10 \end{smallmatrix}$  309

m2

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

$$\text{Simil. } |A_2| = |A_3| = |A_6| = |A_5| = 10^5$$

$$|A_1 \cap A_2| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3 = x_4\}| = 10^4$$

$$|A_1 \cap A_3| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3 = x_5\}| = 10^3$$

$$|A_1 \cap A_6| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3, x_4 = x_5 = x_6\}| = 10^3$$

$$|A_1 \cap A_5| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3, x_5 = x_6 = x_7\}| = 10^3$$

$$|A_2 \cap A_3| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_2 = x_3 = x_4 = x_5\}| = 10^4$$

$$|A_2 \cap A_6| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_2 = x_3 = x_5 = x_6\}| = 10^3$$

$$|A_2 \cap A_5| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_2 = x_3 = x_4, x_5 = x_6 = x_7\}| = 10^3$$

$$|A_3 \cap A_4| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_3 = x_4 = x_5 = x_6\}| = 10^4$$

$$|A_3 \cap A_5| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_3 = x_4 = x_5 = x_6 = x_7\}| = 10^3$$

$$|A_4 \cap A_5| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_4 = x_5 = x_6 = x_7\}| = 10^4$$

$$|A_1 \cap A_2 \cap A_3| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3 = x_4 = x_5\}| = 10^3$$

$$|A_1 \cap A_2 \cap A_6| = |\{(x_1, \dots, x_7) \in [0, 9]^7 : x_1 = x_2 = x_3 = x_6 = x_7\}| = 10^2$$

$$|A_1 \cap A_2 \cap A_5| = 10^2$$

$$|A_1 \cap A_3 \cap A_6| = 10^2$$

$$|A_1 \cap A_3 \cap A_5| = 10$$

$$|A_1 \cap A_6 \cap A_5| = 10^2$$

$$|A_2 \cap A_3 \cap A_6| = 10^3$$

$$|A_2 \cap A_3 \cap A_5| = 10^2$$

$$|A_2 \cap A_6 \cap A_5| = 10^2$$

$$|A_3 \cap A_6 \cap A_5| = 10^3$$

$$|A_1 \cap A_2 \cap A_3 \cap A_6| = 10^2$$

$$\begin{aligned} |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| &= 10 & |A_1 \cap A_3 \cap A_4 \cap A_5| &= 10 \\ |A_1 \cap A_2 \cap A_4 \cap A_5| &= 10 & |A_2 \cap A_3 \cap A_4 \cap A_5| &= 10^2 \\ |A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| &= 10 \end{aligned}$$

Concludiamo

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

$$\begin{aligned} |X| &= 5 \cdot 10^5 - 4 \cdot 10^4 - \cancel{6 \cdot 10^3} + \cancel{3 \cdot 10^3} + \cancel{6 \cdot 10^2} - \cancel{2 \cdot 10^2} - \cancel{3 \cdot 10} + 10 = 457390 \\ &= 5 \cdot 10^5 - 4 \cdot 10^4 - 3 \cdot 10^3 + 6 \cdot 10^2 - 2 \cdot 10 = 457390 \end{aligned}$$

**Esercizio.** Trovare una ricorsione per  $f(n)$  dove  $f(n)$  è il numero di sottoinsiemi di  $[n]$  che non contengono due numeri consecutivi ( $n \in \mathbb{P}$ )

Si chiede una ricorsione per  $f(n)$

$$f(n) = |\{S \subseteq [n] : i \in S \Rightarrow i+1 \notin S\}|$$

$\forall i = 1, \dots, n-1$

Vediamo:

$$f(1) = |\{\emptyset, \{1\}\}| = 2$$

$$f(2) = |\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}| = 4$$

$$f(3) = |\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}| = 8$$

$$f(4) = 13$$

Sembra essere Fibonacci.

$$f(n) = f(n-1) + f(n-2) \quad \forall n \geq 3$$

Si dia  $S \subseteq [n]$ . Diciamo che  $S$  è sparso se  
 $i \in S \Rightarrow i+1 \notin S \quad \forall i = 1, \dots, n-1$ . Abbiamo:

$$\{S \subseteq [n] : S \text{ sparso}\} =$$

$$\begin{aligned} & \{S \subseteq [n] : S \text{ sparso}, n \notin S\} \\ & \{S \subseteq [n] : \text{"/ " }, n \in S\} \end{aligned} \quad (+)$$

ma

$$\{S \subseteq [n] : \text{"/ " }, n \notin S\} = \{S \subseteq [n-1] : S \text{ sparso}\}$$

pertanto

$$\{S \subseteq [n] : S \text{ sparso}, n \notin S\} = f(n-1)$$

Se  $S \subseteq [n]$ ,  $n \in S$  e  $S$  è sparso  $\Rightarrow n-1 \notin S$ .

Definiamo una funzione:

$$\begin{aligned} \Psi : & \{S \subseteq [n] : S \text{ sparso}, n \in S\} \text{ e} \\ & \{T \subseteq [n-2] : T \text{ sparso}\} \end{aligned}$$

Ponendo

$$\Psi(S) := S \setminus \{n\} \quad \forall S \subseteq [n].$$

Allora  $\Psi$  è una biezione ( $T \mapsto T \cup \{n\}$ ) è  
 l'inversa (se  $T \subseteq [n-2]$ ,  $T$  sparso  $\Rightarrow T \cup \{n\} \subseteq [n]$ ,  
 $n \in T \cup \{n\}$ , e  $T \cup \{n\}$  è sparso).

pertanto

$$|\{S \subseteq [n] : S \text{ sparso}, n \in S\}| = f(n-2)$$

concludendo

$$\begin{aligned} f(n) &= |\{S \subseteq [n] : S \text{ sparso}\}| = \\ &= |\{S \subseteq [n] : S \text{ sparso}, n \in S\}| + \\ &+ |\{S \subseteq [n] : S \text{ sparso}, n \notin S\}| = \\ &= f(n-2) + f(n-1) \end{aligned}$$

Pertanto, se  $\{F_n\}_{n=0,1,\dots}$  è la successione di Fibonacci (quindi,  $F_0 = F_1 = 1$  e  $F_n = F_{n-1} + F_{n-2}$   $\forall n \geq 2$ ) allora  $f(n) = F_n$ ,  $\forall n \in \mathbb{N}$

ED. 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:

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

$$= 113400 \text{ modi}$$

**E>D** 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)

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

= 34650 modi.

**E>D** Trouve una ricorsione per il numero  $f(n)$  di composizioni di  $n$  in parti  $\in \{1, 2\}$ .

Si ha che:

$$f(n) = |\{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n \text{ k.e.p}\}|$$

per es.

$$f(1) = |\{1\}| = 1$$

$$f(2) = |\{(1, 1), (2)\}| = 2$$

$$f(3) = |\{(1, 1, 1), (2, 1), (1, 2)\}| = 3$$

$$f(4) = |\{(1, 1, 1, 1), (2, 2), (2, 1, 1), (1, 2, 1), (1, 1, 2)\}| = 5$$

$$f(5) = 8$$

Sembra essere fibonacci, dimostrare che

$$f(n) = f(n-1) \times f(n-2) \quad \forall n \geq 2$$

Abbiamo che

$$\left\{ (\alpha_1, \dots, \alpha_k) \in [1,2]^k : \alpha_1 + \dots + \alpha_k = n, k \in \mathbb{P} \right\} =$$

$$= \left\{ (\alpha_1, \dots, \alpha_k) \in [1,2]^k : \text{" " } \alpha_k = 1 \right\} \cup$$

$$\left\{ (\alpha_1, \dots, \alpha_k) \in [1,2]^k : \text{" " } \alpha_k = 2 \right\}$$

La funzione  $(\alpha_1, \dots, \alpha_k) \mapsto (\alpha_1, \dots, \alpha_{k-1})$   
è una biezione tra

$$\left\{ (\alpha_1, \dots, \alpha_k) \in [1,2]^k : \alpha_1 + \dots + \alpha_k = n, \alpha_k = 1 \right\}$$

$$\left\{ (\alpha_1, \dots, \alpha_{k-1}) \in [1,2]^{k-1} : \alpha_1 + \dots + \alpha_{k-1} = n-1 \right\}$$

(L'inversa è  $(\alpha_1, \dots, \alpha_{k-1}) \mapsto (\alpha_1, \dots, \alpha_{k-1}, 1)$ )

quindi

$$|\{(\alpha_1, \dots, \alpha_k) \in [1,2]^k : \alpha_1 + \dots + \alpha_k = n, \alpha_k = 1\}| = f(n-1)$$

Similmente, la funzione

$$(\alpha_1, \dots, \alpha_k) \mapsto (\alpha_1, \dots, \alpha_{k-1})$$

è una biezione tra

$$\left\{ \begin{array}{l} \{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n, a_k = 2\} \\ \{(a_1, \dots, a_{k-1}) \in [1, 2]^{k-1} : a_1 + \dots + a_{k-1} = n-2 \end{array} \right\} \text{ e}$$

(L'inverso è  $(a_1, \dots, a_{k-1}) \mapsto (a_1, \dots, a_{k-1}, 2)$ )

quindi

$$|\{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n, a_k = 2\}| = f(n-2)$$

Concludendo

$$\begin{aligned} f(n) &= |\{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n\}| = \\ &= |\{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n, a_k = 1\}| + \\ &\quad |\{(a_1, \dots, a_k) \in [1, 2]^k : a_1 + \dots + a_k = n, a_k = 2\}| = \\ &= f(n-1) + f(n-2) \end{aligned}$$

Pertanto, se  $\{F_n\}_{n=0,1,\dots}$  è la successione di Fibonacci (quindi,  $F_0 = F_1 = 1$  e  $F_n = F_{n-1} + F_{n-2}$   $\forall n \geq 2$ ) allora  $f(n) = F_n \quad \forall n \in \mathbb{N}$

### Sondaggio 3

Siano  $x, y \in \mathbb{Z}$  tali che  $28x + 45y = 3$

Allora è sempre vero che:

- a)  $(x, y) \mid 3$
- b)  $3 \mid (x, y)$
- c)  $3 \mid y$
- d)  $y \mid 3$
- e) N.D.Q.

**E5.** Trovare una formula per i numeri di Fibonacci

$$\{F_n\}_{n=0,1,\dots}$$

Sappiamo che  $F_{n+2} = F_{n+1} + F_n \quad \forall n \in \mathbb{N}$  e  $F_0 = F_1 = 1$

Questa è una ricorsione lineare a coefficienti costanti, con  $d=2$ ,  $a_1=1$ ,  $a_0=1$ .

L'eq. caratteristica è  $x^2 = x + 1$  cioè

$$x^2 - x - 1 = 0. \text{ le sue radici sono}$$

$$x = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

quindi

$$\gamma_1 = \frac{1+\sqrt{5}}{2}, \quad \gamma_2 = \frac{1-\sqrt{5}}{2}$$

con molteplicità  $d_1=1$ ,  $d_2=1$

$$x^2 - x - 1 = \left(x - \frac{1+\sqrt{5}}{2}\right)^1 \left(x - \frac{1-\sqrt{5}}{2}\right)^1$$

pertanto, sappiamo da CAP. 4 che  $\exists P_1(x)$ ,

$P_2(x) \in \mathbb{C}[x]$  tali che  $\deg(P_i) \leq d_i$ ,

$\forall i = 1, 2, \dots$  tali che

$$F_n = P_1(n) (\gamma_1)^n + P_2(n) (\gamma_2)^n \quad \forall n \in \mathbb{N}$$

nel nostro caso  $d_1 = d_2 = 1 \Rightarrow$

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

$$\deg P_1(x) = \deg P_2(x) = 0 \text{ e}$$

$$f_n = P_1(n) \left(\frac{1+\sqrt{5}}{2}\right)^n + P_2(n) \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Quindi esistono  $a, b \in \mathbb{C}$  tali che

$$f_n = a \left(\frac{1+\sqrt{5}}{2}\right)^n + b \left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}$$

ma  $f_0 = f_1 = 1$  pertanto

$$1 = f_0 = a + b$$

$$1 = f_1 = a \left(\frac{1+\sqrt{5}}{2}\right) + b \left(\frac{1-\sqrt{5}}{2}\right)$$

quindi

$$a = 1 - b \Rightarrow$$

$$(1-b) \left(\frac{1+\sqrt{5}}{2}\right) + b \left(\frac{1-\sqrt{5}}{2}\right) = 1 \Rightarrow$$

$$b \left(\frac{1-\sqrt{5}}{2} - \frac{1+\sqrt{5}}{2}\right) = 1 - \frac{1+\sqrt{5}}{2} \Rightarrow$$

$$b \left(-\sqrt{5}\right) = \frac{1-\sqrt{5}}{2} \Rightarrow$$

$$b = \frac{1-\sqrt{5}}{-2\sqrt{5}} = \frac{\sqrt{5}-1}{10} = \frac{6-\sqrt{5}}{10} \Rightarrow$$

$$a = 1 - b = 1 - \frac{6-\sqrt{5}}{10} = \frac{6+\sqrt{5}}{10}$$

$$f_n = \frac{6+\sqrt{5}}{10} \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{6-\sqrt{5}}{10} \left(\frac{1-\sqrt{5}}{2}\right)^n \quad \forall n \in \mathbb{N}$$

$E_D[+]$  è vero che  $n^5 = (2n)^5$

$E_D[-]$  è vero che  $e^n \leq e^{2n}$ ?

$E_D[ \cdot ]$  è vero che  $\ln(n) \leq \ln(2n)$ ?

$E_D[ \rightarrow ]$  siano  $f, g : \mathbb{N} \rightarrow \mathbb{R}_{>0}$  tali che  $\lim_{n \rightarrow +\infty} g(n) = +\infty$

dimostrare che  $f \asymp g$  se e solo se

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

$E_s.$  Risolvere le ricorisoni lineari 2 coeff. costanti

$$f(n) = 2f(n-1) + f(n-2) \quad \forall n \geq 2 \text{ con } f(0) = 1, f(1) = 3$$

Riscriviamo le ricorisoni in forma standard

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

l'eq. caratteristica è

$$x^2 = 2x + 1$$

$$x^2 - 2x - 1 = 0$$

$$x = 1 \pm \sqrt{2}$$

quindi le radici sono:

$$\gamma_1 = 1 + \sqrt{2} \quad \gamma_2 = 1 - \sqrt{2}$$

Con molteplicità  $d_1 = 1, d_2 = 1$

$$x^2 - 2x - 1 = (x - (1 + \sqrt{2})) (x - (1 - \sqrt{2}))$$

Sappiamo dalla teoria che  $\exists a, b \in \mathbb{C}$  tali che

$$f(n) = a(1 + \sqrt{2})^n + b(1 - \sqrt{2})^n \quad \forall n \in \mathbb{N}$$

per calcolare  $a$  e  $b$  usiamo le condizioni iniziali, otteniamo

$$1 = f_0 = a + b$$

$$3 = f_1 = a(1 + \sqrt{2}) + b(1 - \sqrt{2})$$

quindi

$$a = -b \Rightarrow$$

$$(1 - b)(1 + \sqrt{2}) + b(1 - \sqrt{2}) = 3$$

$$b(-2\sqrt{2}) = 3 - 1 - \sqrt{2}$$

$$b = \frac{2 - \sqrt{2}}{-2\sqrt{2}} = \frac{2\sqrt{2} - 2}{-4} = \frac{1 - \sqrt{2}}{2}$$

$$a = 1 - \frac{1 - \sqrt{2}}{2} = \frac{1 + \sqrt{2}}{2}$$

$$f_n = \frac{1 + \sqrt{2}}{2} (1 + \sqrt{2})^n + \frac{1 - \sqrt{2}}{2} (1 - \sqrt{2})^n \quad \forall n \in \mathbb{N}$$

Esercizio. Risolvere la ricorsione lineare 2 coeff. costanti:

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

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

Scrivere l'eq cartesiana:

$$x^3 + 2x^2 + 2x + 4 = 0 \quad x_{1,2,3} = ?, -2, ?$$

$$x^3 + 2x^2 + 2x + 4 = 0$$

Vediamo quindi che  $x = -2$  è radice  $\Rightarrow (x+2) | x^3 + 2x^2 + \dots$   
Usiamo ruffini:

$$\begin{array}{r|l} x^3 + 2x^2 + 2x + 4 & x + 2 \\ \hline -x^3 - 2x^2 & x^2 + 2 \\ & + 2x + 4 \\ & - 2x - 2 \end{array}$$

$$(x^2 + 2)(x + 2) = 0 \quad x_{1,2,3} = -2, \pm \sqrt{-2} = -2, \pm i\sqrt{2}$$

quindi le radici sono

$$\lambda_1 = -2, \lambda_2 = i\sqrt{2}, \lambda_3 = -i\sqrt{2}$$

di molteplicità:  $d_1 = 1, d_2 = 1, d_3 = 1$

quante volte sono state trovate

$$x^3 + 2x^2 + 2x + 4 = (x - (-2)) (x - (-i\sqrt{2})) (x - (i\sqrt{2}))$$

$$x^3 + 2x^2 + 2x + 4 = (x + 2) (x + i\sqrt{2}) (x - i\sqrt{2})$$

Sappiamo dalla teoria che:

$\exists P_1(x), P_2(x), P_3(x) \in (\mathbb{C}[x])$  tali che

$$f(n) = P_1(n)(\gamma_1)^n + P_2(n)(\gamma_2)^n + P_3(n)(\gamma_3)^n \quad \forall n \in \mathbb{N}$$

$$\deg(f_i) \leq d_{i-1} \quad \forall i = 1, 2, 3$$

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

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

Per calcolare  $a, b, c$  usiamo le cond. iniziali

$$0 = f(0); \quad a + b + c$$

$$2 = f(1); \quad a(-2) + b(i\sqrt{2}) + c(-i\sqrt{2})$$

$$0 = f(2); \quad a(-2)^2 + b(i\sqrt{2})^2 + c(-i\sqrt{2})^2$$

quindi

$$\begin{cases} a + b + c = 0 \\ -2a + i\sqrt{2}b - i\sqrt{2}c = 2 \\ 4a - 2b - 2c = 0 \end{cases}$$

||

$$\begin{cases} a = -b - c \\ -2(-b - c) + i\sqrt{2}b - i\sqrt{2}c = 2 \\ 4(-b - c) - 2b - 2c = 0 \end{cases}$$

$$\begin{cases} a = -b - c \\ 2b + 2c + i\sqrt{2}b - i\sqrt{2}c = 2 \\ -6b - 6c = 0 \end{cases}$$

$$\begin{cases} a = -c + c \\ -c(2 + i\sqrt{2}) - c(2 - i\sqrt{2}) = 2 \\ b = -c \end{cases}$$

$$\begin{cases} a = 0 \\ c = \frac{i\sqrt{2}}{2} \\ b = \frac{-i\sqrt{2}}{2} \end{cases}$$

$$f(n) = -\frac{i\sqrt{2}}{2} \left(i\sqrt{2}\right)^n + \frac{i\sqrt{2}}{2} \left(-i\sqrt{2}\right)^n \quad \forall n \in \mathbb{N}$$

En. 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.

$$-x^3 + x^2 + 16x - 12 = 0$$

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

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

$$x_1, x_2, x_3 = 1, 3, -1$$

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

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

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

$$\frac{x \pm \sqrt{1+24}}{2} = \frac{x \pm 5}{2} = 3, -2$$

quindi le radici sono:

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

con molteplicità:  $d_1 = 1 \quad d_2 = 2$

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

Sappiamo dalla teoria che:

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

tanti polinomi quante radici

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

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

quindi  $\exists a, b, c \in \mathbb{C}$  tali che  $a(3)^n + b(3)^n + c(-2)^n$

$\checkmark \deg(P_i)$  è massimo e quindi  $a+b+c$  è grado

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

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

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

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

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

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

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

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

$$\begin{cases} a = -\frac{4}{5} \\ -2b - 8b = s = -10b = s = b = -\frac{1}{2} \\ c = \frac{6}{5} \end{cases}$$

concludendo

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

Esercizio. Trovare una formula chiusa per

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

poiché  $f(x) = x^2 + x$  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

$$\sum_{k=0}^n (k+k^2) = \alpha n^3 + b n^2 + c n + d \quad \forall n \in \mathbb{N}$$

(2) calcolare le condizioni iniziali

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

$$2 = f(1) = \alpha + b + c + d$$

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

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

$$\begin{cases} d = 0 \\ \alpha + b + c = 2 \\ 8\alpha + 4b + 2c = 8 \\ 27\alpha + 9b + 3c = 20 \end{cases}$$

$$\begin{cases} b = -\alpha - c + 2 \\ 8\alpha - 4\alpha - 4c + 2c + 8 = 8 \quad = \quad 4\alpha - 2c = 0 \\ 27\alpha - 9\alpha - 9c + 18 + 3c = 20 \quad = \quad 18\alpha - 6c = 2 \end{cases}$$

$$\begin{cases} \alpha = \frac{1}{2}c \\ 9c - 6c = 2 \quad c = \frac{2}{3} \\ b = -\frac{3}{6} - \frac{4}{6} + \frac{12}{6} = \frac{5}{6} \end{cases}$$

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

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

Esercizio. Trovare una formula chiusa per

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

Proviamo a calcolare la somma intera abbiamo

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

Pertanto

$$\begin{aligned} \sum_{i=0}^n \sum_{j=0}^m 3^{i+j} &= \sum_{i=0}^n 3^i \frac{3^{m+1} - 1}{3 - 1} = \\ &= 3^0 \cdot \frac{3^{m+1} - 1}{2} + \dots + 3^n \cdot \frac{3^{m+1} - 1}{2} = \frac{3^{m+1} - 1}{2} \cdot \sum_{i=0}^n 3^i \stackrel{(5.1.1)}{=} \\ \frac{3^{m+1} - 1}{2} \cdot \frac{3^{n+1} - 1}{2} &= \frac{(3^{m+1} - 1)(3^{n+1} - 1)}{4} \end{aligned}$$

Esercizio. 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 5.3.1 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 di dividere

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

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

Per il teorema del confronto

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

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

Es [+] la relazione  $\theta$  su  $\mathbb{R}_{>0}$  è una relaz. di equivalenza

Es trovare una formula chiusa per

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

Il prodotto interno è

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

Pertanto

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

Esercizio. Trovare la formula chiusa per

$$\sum_{i=0}^n \sum_{j=0}^{n-i} (n-j)$$

la somma interna è

$$\begin{aligned} \sum_{j=0}^{n-i} (n-j) &= n + (n-1) + (n-2) + \dots + i = \\ &= (1 + 2 + \dots + n) - (1 + 2 + \dots + (i-1)) \\ &= \binom{n+1}{2} - \binom{i}{2} \end{aligned}$$

Oppure

$$\begin{aligned} \sum_{j=0}^{n-i} (n-j) &= \sum_{j=0}^{n-i} n - \sum_{j=0}^{n-i} j = \underbrace{n+n+\dots+n}_{n-i+1} - \binom{n-i+1}{2} = \\ &= n(n-i+1) - \binom{n-i+1}{2} = \\ &= (n-i+1)\left(n-\frac{n-i}{2}\right) = \\ (n-i+1) \frac{n+i}{2} &= \frac{n^2 + ni - ni - i^2 + ni}{2} = \frac{n^2 + n}{2} - \binom{i}{2} \end{aligned}$$

Pertanto

$$\begin{aligned} \sum_{i=0}^n \sum_{j=0}^{n-i} (n-j) &= \sum_{i=0}^n \left( \binom{n+1}{2} - \frac{i(i-1)}{2} \right) = \\ (n+1) \binom{n+1}{2} - \sum_{i=0}^n &\left( \frac{i^2}{2} - \frac{i}{2} \right) \end{aligned}$$

**Esercizio.** Siano  $f(n) = \log_2(n)$  e  $g(n) = \log_{10}(n)$   $\forall n \in \mathbb{P}$   
 Quale delle relazioni  $\circ, O, \Omega, \Theta, \cong$  valgono  
 tra  $f$  e  $g$ ?

Sappiamo che

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

abbiamo

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

quindi  $f \neq o(g)$  e  $f \neq g$ . Similmente

$$\lim_{n \rightarrow +\infty} \frac{g(n)}{f(n)} \neq 1$$

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

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

$$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)} \neq 0$$

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

$\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)}$  è un numero

$f = \Theta(g)$  e  $g = \Theta(f)$ . Infine (s.6.7)  $f = \omega(g)$  e  $g = \omega(f)$   
 (perché  $f = O(g) \Leftrightarrow g = \omega(f)$ ).

Es. Siano  $f, g: \mathbb{N} \rightarrow \mathbb{R}_{>0}$  definite da

$$f(n) = 2 + \cos\left(\frac{\pi n}{2}\right) : g(n) = 2 + \sin\left(\frac{\pi n}{2}\right) \quad \forall n \in \mathbb{N}$$

Quali relazioni tra  $O, \Omega, \Theta, \cong$  valgono tra  $f$  e  $g$ ?

abbiamo:

n	1	2	3	4	5	6	7	8	...
$f(n)$	2	1	2	3	2	1	2	3	...
$g(n)$	3	2	1	2	3	2	1	2	...

quindi  $\lim_{n \rightarrow +\infty} \frac{f(n)}{g(n)}$  non esiste  $\Rightarrow f \neq g$   
 $\Rightarrow f \neq o(g)$

$\Rightarrow g \neq o(f)$

v2 ore ass.  
 $|f(n)| \leq 3 \leq 3 \cdot |g(n)| \quad \forall n \in \mathbb{P} \Rightarrow f = O(g)$   
 $\Rightarrow g = O(f)$

$\Rightarrow g = \Omega(f)$

$\Rightarrow f = \Omega(g)$

$\Rightarrow g = \Theta(f)$

$\Rightarrow f = \Theta(g)$

pertanto

ED. Calcolare il minimo  $k \in \mathbb{P}$  tale che  
 $\ln(n!) = O(n^k)$ .  
dobbiamo capire quanto rapidamente  $\ln(n!)$   
 $\rightarrow +\infty$  per  $n \rightarrow +\infty$ abbiamo che

$$\ln(n!) = \sum_{i=1}^n \ln(i)$$

poiché  $\ln(x)$  è monotona crescente e  
continua per  $x > 0$ abbiamo che (S. 3, 1)  
 $\ln(1) + \int_1^n \ln(x) dx \leq \sum_{i=1}^n \ln(i) \leq \ln(n) + \int_n^n \ln(x) dx$

ma

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

pertanto

$$n \ln(n) - n + 1 \leq \ln(n!) \leq \ln(n) + n \ln(n) - n + 1$$

$$1 \leq \frac{\ln(n!)}{n \ln(n)} \leq 1$$

concludendo

$$\ln(n!) \approx n \ln(n)$$

ma  $n \ln(n) \neq O(n)$  (se lo fosse  $\exists c \in \mathbb{R}_{>0}$ , e  
 $N \in \mathbb{P}$  tali che  $n \ln(n) \leq c \cdot n$  se  $n \geq N$ . assurdo).

mentre  $n \ln(n) = O(n^2)$  (perché  $n \ln(n) \leq n^2 \forall n \in \mathbb{P}$ )

Quindi:  $K=2$  per  $n \ln(n)$  e per  $\ln(n!)$ ?

poiché  $\frac{\ln(n!)}{n \ln(n)} \rightarrow 1$  per  $n \rightarrow +\infty$

$$\Rightarrow \exists N \in \mathbb{P} \text{ tale che } \frac{1}{2} \leq \frac{\ln(n!)}{n \ln(n)} \leq \frac{3}{2}$$

Se  $n \geq N$ , m2 allora

$$\ln(n!) \leq \frac{3}{2} n \ln(n) \leq \frac{3}{2} n^2$$

Se  $n \geq N \Rightarrow \ln(n!) = O(n^2)$ .

è vero che  $\ln(n!) = O(n)$ ? se lo fosse

$$\Rightarrow \exists c \in \mathbb{R}_{>0} \text{ e } \exists N \in \mathbb{P} \text{ tali che } \ln(n!) \leq c \cdot n$$

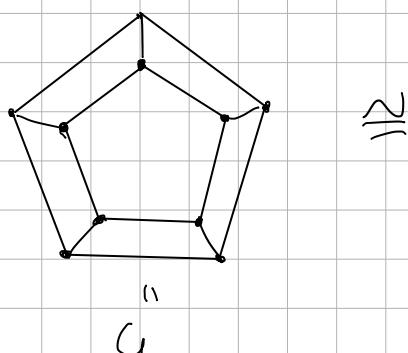
Se  $n \geq N$ , m2 allora

$$n \ln(n) \leq 2 \ln(n!) \leq 2c \cdot n$$

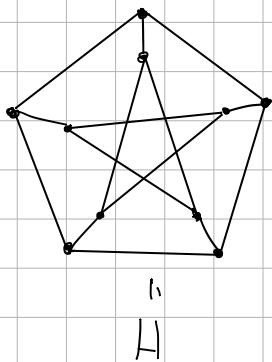
Se  $n \geq N$ , assurdo, quindi  $\ln(n!) \neq O(n)$ .

pertanto  $K=2$  per  $\ln(n!)$ .

ED.



$\cong$



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

ED. Si<sub>2</sub>  $G = (V, E)$  dove  $V := \binom{[n]}{2} \cup \binom{[n]}{3}$  ( $n \in \mathbb{N}$ )

e dove

$$\{X, Y\} \in E \iff \begin{cases} X \subseteq Y \\ Y \subsetneq X \end{cases} \quad \forall x, y \in V, X \neq Y$$

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

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

$$\begin{cases} \{\{1, 3\}, \{1, 3, 4\}\} \in E \\ \{\{1, 3\}, \{1, 4, 5\}\} \notin E \end{cases}$$

$G$  è legato nei gradi?

Si<sub>2</sub>  $x \in V$ , Si<sub>2</sub>  $x = \{a, b\}$  ( $a, b \in [n]$ ) ( $a \neq b$ )

$$\begin{aligned} d(X) &:= |\{Y \in V_2 : \{X, Y\} \in E\}| \\ &= |\{Y \in \binom{[n]}{3} : X \subseteq Y\}| \\ &= |\{Y \in \binom{[n]}{3} : |Y| = 3, \{a, b\} \subseteq Y\}| \\ &= n - 2 \end{aligned}$$

Si<sub>2</sub>  $y \in V_2$ , Si<sub>2</sub>  $y = \{a, b, c\}$  ( $a, b, c \in [n]$ ,  $a, b, c$  distinti). Allora

$$\begin{aligned} d(Y) &:= |\{X \in V_1 : \{X, Y\} \in E\}| \\ &= |\{X \in \binom{[n]}{2} : X \subseteq Y\}| \\ &= |\{X \in [n] : |X| = 2, X \subseteq Y\}| \\ &= |\{X \subseteq \{a, b, c\} : |X| = 2\}| = \binom{3}{2} = 3 = \binom{3}{2} \\ &\quad (4.2) \end{aligned}$$

Quindi se  $n \geq 5$

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

C'è quindi legge a 2 dei gradi se  $n \geq 5 \Rightarrow$

$\Rightarrow$  esiste un <sup>(6.22)</sup>accoppiamento di  $V_1$  in  $V_2$  se

$$n \geq 5$$