

CAPITOLO 4: COMBINATORIA ENUMERATIVA

4.1 Il problema fondamentale della combinatoria enumerativa

Sia A un insieme.

DEF La cardinalità di A (scrive $|A|$, o $\#A$)
è il numero di elementi di A .

PROBLEMA FONDAMENTALE della C.E. :

Data una sequenza A_0, A_1, \dots di insiemi finti,
calcolare la successione delle cardinalità $\{|A_i|\}_{i=0,1,\dots}$

Cosa significa "calcolare"?

3 RISPOSTE:

1) Una formula (esempio: $|A_n| = 2^n \forall n \in \mathbb{N}$,
oppure $|A_n| = \sum_{i=0}^n 2^i$)

2) Una ricorsione (esempio: $|A_n| = |A_{n-1}| + |A_{n-2}|$
per $\forall n \geq 2$)

3) Una funzione generatrice. (esempio cioè una
funzione $f: \mathbb{R} \rightarrow \mathbb{R}$, f infinitamente differentiabile
in $x=0$ (all'origine), tale che lo sviluppo in
serie di Taylor di f in $x=0$ è $\sum_{n \geq 0} |A_n| \cdot x^n$
(esempio: $f(x) = \frac{1}{1-x-x^2}$)

E5. calcolare l'inverso moltiplicativo di
 $[28]_{125}$

Se esiste.

Sappiamo dalla teoria che tale inverso moltiplicativo esiste se e solo se

$$(125, 28) = 1.$$

Calcoliamo A.E. con $(125, 28)$:

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

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

$$13 = 6 \cdot 2 + \boxed{1}$$

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

$\Rightarrow (125, 28) = 1 \Rightarrow$ esiste ed è unica inversa moltiplicativa di $[28]_{125}$?

Calcoliamo Bezout:

$$\begin{aligned} 1 &= 13 + (-6 \cdot 2) \\ &= 13 + (-6) \cdot (28 - 2 \cdot 13) \\ &= (13) \cdot 13 + (-6) \cdot 28 \\ &= (13) \cdot (125 + 4 \cdot 28) + (-6) \cdot 28 \\ &= (13) \cdot 125 + (-58) \cdot 28 \end{aligned}$$

Quindi l'id. di Bezout è

$$1 = (13) \cdot 125 + (-58) \cdot 28$$

Pertanto $(-58) \cdot 28 \equiv 1 \pmod{125} \Rightarrow$

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

$$\Rightarrow [-58]_{125} \cdot [28]_{125} = [1]_{125}$$

Quindi l'inverso moltiplicativo di $[28]_{125}$ è

$$[-58]_{125} = [67]_{125}$$

ES. Calcolare le inverse moltiplicative di

$$\begin{bmatrix} 172 \\ 221 \end{bmatrix}_{221} \quad \text{e} \quad \begin{bmatrix} 221 \\ 172 \end{bmatrix}_{172}.$$

Sappiamo dalla teoria che tali I.M. esistono \Leftrightarrow
 $(221, 172) = 1$. e $\cancel{\text{e}} \begin{bmatrix} 221 \\ 172 \end{bmatrix}$

Calcoliamo A.E.

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

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

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

$$25 = 1 \cdot 24 + \underline{1}$$

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

$$\text{Quindi } (221, 172) = 1$$

Calcoliamo Bezout

$$\begin{aligned} 1 &= 25 + (-1) \cdot 24 \\ &= 25 + (-1) \cdot (49 + 25 \cdot 1) \\ &= (2) \cdot 25 + (-1) \cdot 49 \\ &= (2) \cdot (172 + (-3) \cdot 49) + (-1) \cdot 49 \\ &= (2) \cdot (172) + (-7) \cdot 49 \\ &= (2) \cdot 172 + (-7) \cdot (221 + (-1) \cdot 172) \\ &= (-7) \cdot 221 + (9) \cdot 172 \end{aligned}$$

Pertanto l'Id. di Bezout è:

$$1 = (-7) \cdot 221 + (9) \cdot 172$$

$$\text{Quindi } 9 \cdot 172 \equiv 1 \pmod{221} \quad \text{e} \quad (-7) \cdot 221 \equiv 1 \pmod{172}$$

$$\Rightarrow \begin{bmatrix} 9 \\ 221 \end{bmatrix}_{221} \cdot \begin{bmatrix} 172 \\ 221 \end{bmatrix}_{221} = \begin{bmatrix} 1 \\ 221 \end{bmatrix}_{221}$$

e

$$\begin{bmatrix} -7 \\ 172 \end{bmatrix}_{172} \cdot \begin{bmatrix} 221 \\ 172 \end{bmatrix}_{172} = \begin{bmatrix} 1 \\ 172 \end{bmatrix}_{172}$$

Pertanto l'inversa uolteoperativa di

$$\begin{bmatrix} 1 & 7 \\ 2 & 2 \end{bmatrix}_{172} \text{ è } \begin{bmatrix} 9 \\ -1 \end{bmatrix}_{221}$$

e

$$\begin{bmatrix} 2 & 2 \\ 1 & 7 \end{bmatrix}_{172} \text{ è } \begin{bmatrix} -1 \\ 7 \end{bmatrix}_{221} (= \begin{bmatrix} 165 \\ 221 \end{bmatrix}_{172})$$

es $\begin{bmatrix} 1 & 7 \\ 2 & 2 \end{bmatrix}$: S.ano $p, q \in \mathbb{P}$, tali che p e q hanno 3 cifre decimali.

Quante cifre decimali ha il loro prodotto $p \cdot q$

4.2 PROPRIETÀ DI BASE

OSS: Siano A e B due insiemi e $f: A \rightarrow B$,
 f biunivoca. Allora

$$|A| = |B| \quad (\text{A ha lo stesso n° di elementi})$$

DEF: La POTENZA di A alla B è A^B

$$A^B := \{f: B \rightarrow A\}$$

PROP. 4.2.1

Siano A e B insiemi finiti.

Allora:

$$1) |A \times B| = |A| \cdot |B| \quad (\text{La cardinalità del prodotto cartesiano di } A \text{ e } B \text{ è uguale al prodotto delle cardinalità di } A \text{ e la card. di } B)$$

$$2) |A^B| = |A|^{|B|}$$

$$3) |A \cup B| = |A| + |B| - |A \cap B|$$

D14 Chiara

[es [2-]: Quanti numeri di cellulare ci sono in Italia? (cioè ≠ cifre. Ogni cifra tra 0 e 9)]

[es. [1-]: Quanti numeri di cellulare ci sono in Italia che non cominciano con la cifra "0"?]

4.3 COEFFICIENTI BINOMIALI

Sia $n \in \mathbb{N}$. Ricordiamo che

$$[n] := \{1, 2, \dots, n\}.$$

PROP. 4.3.1

Sia $n \in \mathbb{N}$. Allora

$$|\mathcal{P}([n])| = 2^n$$

(La cardinalità
dell'insieme potenza
di n è uguale a 2^n)

DIM

Sia $\varphi: \mathcal{P}([n]) \rightarrow \underbrace{[2] \times [2] \times \dots \times [2]}_n$

Dobbiamo dimostrare che la funzione sia biequivoca.

Definiamo ponendo

$$\varphi(A) \stackrel{\text{def}}{=} (a_1, \dots, a_n)$$

↓
un sottoinsieme
dei numeri da
1 a n

→ n numeri (sono 1 o 2,
dalla funzione
definita prima)

Dove

$$a_i \stackrel{\text{def}}{=} \begin{cases} 2, & \text{se } i \in A \\ 1, & \text{se } i \notin A \end{cases}$$

Per $\forall i \in [n]$ e per $\forall A \subseteq [n]$

(ad esempio $\varphi(\emptyset) = (1, 1, 1, \dots, 1)$),

$\varphi([n]) = (2, 2, 2, \dots, 2)$ poiché dentro di sottoinsieme,
se $n=7$ e $A = \{2, 3, 6\} \Rightarrow \varphi(A) = (1, 2, 2, 1, 1, 2, 1)$

↑
1 non
è in A
A
↑
2 è in A
A
↑
3 è in A
A
↑
4
5
6
7

Affora φ è biunivoca \Rightarrow

$$|\mathcal{P}(\mathbb{I}_n)| = \left| \underbrace{\mathbb{I}_2 \times \dots \times \mathbb{I}_2}_{n} \right|_{(4.2.1)} = |\mathbb{I}_2|^n = 2^n$$

Sia A un insieme e sia $n \in \mathbb{N}$.

Poniamo

$$\binom{A}{n} \stackrel{\text{def}}{=} \{B \subseteq A : |B| = n\}$$

(detto "A binomiale n ")

Esempio

$$A = \{a\}, n = 2. \quad \text{Affora}$$

$$\binom{\{a\}}{2} = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$$

Sia $n \in \mathbb{N} \setminus \{0\}$

DEF Il coefficiente binomiale di grado n è

$$\binom{x}{n} \stackrel{\text{def}}{=} \frac{x(x-1)\dots(x-n+1)}{n!}$$

Se $n \in \mathbb{P}$

$$\text{se } n=0 \rightarrow \binom{x}{0} \stackrel{\text{def}}{=} 1$$

$$\text{se } n < 0 \rightarrow \binom{x}{n} \stackrel{\text{def}}{=} 0$$

OSS

$$\binom{x}{n} \in \mathbb{Q}[x]$$

OSS

Se $n \in \mathbb{P}$ affora

$$\binom{x}{n} = \binom{x-1}{n-1} + \binom{x-1}{n-2}$$

esempio

$$\begin{array}{ccccccc} & & & 1 & & & \\ & & & 1 & 1 & & \\ & & & 1 & 2 & 1 & \\ & & & 1 & 3 & 3 & 1 \\ & & & 1 & 4 & 6 & 4 & 1 \\ & & & 1 & 5 & 10 & 10 & 5 & 1 \\ & & \vdots \end{array}$$

(Il numero in riga n e in posizione $k+1$ è $\binom{n}{k}$)

PROP A.3.2 :

Sia $n \in \mathbb{N}$. Allora

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

DIM Per induzione su $n \geq 0$

Chiaro che $n \leq 1$.

Sia $n \geq 2$. Allora

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

$$\left(\binom{n-1}{n} = 0 \right) \Rightarrow \sum_{k=0}^{n-1} \binom{n-1}{k} x^k + \sum_{k=0}^{n-1} \binom{n-1}{k-1} x^k$$

$$\left(\binom{n-1}{k-1} = 0 \right) \Rightarrow \sum_{k=0}^{n-1} \binom{n-1}{k} x^k + \sum_{k=0}^{n-1} \binom{n-1}{k-1} x^k$$

$$= \sum_{k=0}^{n-1} \left[\binom{n-1}{k} + \binom{n-1}{k+1} \right] \times k$$

$$= \sum_{k=0}^n \binom{n}{k} \times k$$

PROP. 4.3.3 :

Siano $n, k \in \mathbb{N}$, $0 \leq k \leq n$.

Allora

$$\left| \binom{n}{k} \right| = \binom{n}{k}$$

DIM Induzione su $n \geq 0$

Faccio se $n \leq 1$.

Sia $n \geq 2$.

Se $k = 0$, allora

$$\left| \binom{n}{0} \right| = \left| \{ \emptyset \} \right| = 1 = \binom{n}{0} \Rightarrow \text{OK}$$

Se $k \geq 1$, allora

$$\binom{n}{k} = \left\{ A \in \binom{[n]}{k} : n \notin A \right\} \cup \\ \left\{ A \in \binom{[n]}{k} : n \in A \right\}.$$

ma

$$\left\{ A \in \binom{[n]}{k} : n \notin A \right\} = \binom{[n-1]}{k}$$

Inoltre, la funzione

$$\psi : \left\{ A \in \binom{[n]}{k} : n \in A \right\} \xrightarrow{\text{def}} \binom{[n-1]}{k-1}$$

definita da $\psi(A) := A \setminus \{n\}$ è una biunivoca.
(la funzione $B \mapsto B \cup \{n\}$ è e' inversa).

Pertanto

$$\left| \left\{ A \in \binom{[n]}{k} : n \in A \right\} \right| = \left| \binom{[n-1]}{k-1} \right|$$

Quindi

$$\left| \binom{[n]}{k} \right| = \left| \left\{ A \in \binom{[n]}{k} : n \notin A \right\} \right| + \left| \left\{ A \in \binom{[n]}{k} : n \in A \right\} \right|$$

$$= \left| \binom{[n-1]}{k} \right| + \left| \binom{[n-1]}{k-1} \right|$$

(x Induzione)

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

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

COR. 4.3.4

Sia $n \in \mathbb{N}$. Allora

$$\left| \left\{ A \subseteq [n] : |A| \text{ e' pari} \right\} \right| = \left| \left\{ A \subseteq [n] : |A| \text{ e' dispari} \right\} \right|$$

DIM

Basta porre $x = -1$ in 4.3.2

[es [2] Sia $n \in \mathbb{N}$. Trova una bizione tra questi due insiemi]

$$\left\{ A \subseteq [n] : |A| \text{ è par.} \right\} \text{ e } \left\{ A \subseteq [n] : |A| \text{ è dispari} \right\}$$

G.4 Il principio di inclusione - esclusione

Sappiamo che

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (*)$$

Se A e B sono insiemi finiti.

Siano A, B, C insiemi finiti. Ricorda

$$\begin{aligned} |A \cup B \cup C| &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &\stackrel{(*)}{=} |A| + |B| - |A \cap B| + |C| - |(A \cap C) \cup (B \cap C)| \\ &\stackrel{(*)}{=} |A| + |B| + |C| - |A \cap B| - (|A \cap C| + |B \cap C|) \\ &\quad - |(A \cap C) \cap (B \cap C)| \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + \\ &\quad + |A \cap B \cap C| \end{aligned}$$

Siano A_1, A_2, \dots, A_n insiemi finiti ($n \in \mathbb{N}$).

Dato $T \subseteq [n]$, $T = \{t_1, \dots, t_r\}$, poniamo

$$A_T \stackrel{\text{def}}{=} A_{t_1} \cap \dots \cap A_{t_r}$$

$$(\text{esempio: } A_{\{1, 5, 6\}} = A_1 \cap A_5 \cap A_6)$$

Nello stesso modo che per $n=3$ si dimostra:

TEO 4.4.1 (Principio di inclusione - esclusione) :

Siano A_1, \dots, A_n insiemi finiti. Allora

$$|A_1 \cup \dots \cup A_n| = \sum_{\substack{T \subseteq [n] \\ T \neq \emptyset}} (-1)^{|T|-1} \cdot |A_T|$$

TEO. : Sia $n \in \mathbb{N}$ e sia $n = p_1^{a_1} \cdots p_e^{a_e} < \infty$ la sua decomposizione in numeri primi

($\Rightarrow p_1, \dots, p_e, a_1, \dots, a_e \in \mathbb{N}$, p_1, \dots, p_e primi distinti).

Allora

$$\Phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_e}\right)$$

esercizio: costruire un sistema di codifica RSA
usando i primi $p = 47$ e $q = 83$.
Inoltre, codificare e decodificare un
messaggio

Abbiamo

$$n = 47 \cdot 83 = 3901$$

Inoltre

$$\varphi(n) = (p-1)(q-1) = 46 \cdot 82 = 3772$$

Dobbiamo ora trovare $e \in \mathbb{P}$ tale che

$$(e, \varphi(n)) = 1$$

($3772 = 46 \cdot 82 = 23 \cdot 2 \cdot 41 \cdot 2$) prendiamo $e = 127$
($\Rightarrow (127, 3772) = 1$)

Dobbiamo ora calcolare l'inversa moltiplicativa di $[e] = [127]$
 $\varphi(n) = 3772$.

Usiamo A.E.

$$\begin{aligned} 3772 &= 29 \cdot 127 + 89 \\ 127 &= 1 \cdot 89 + 38 \\ 89 &= 2 \cdot 38 + 13 \\ 38 &= 2 \cdot 13 + 12 \\ 13 &= 1 \cdot 12 + \underline{\underline{1}} \\ 12 &= 12 \cdot 1 + 0 \end{aligned}$$

Quindi $(127, 3772) = 1$

Calcoliamo Bezout:

$$\begin{aligned}
 f &= 13 + (-1) \cdot 12 \\
 &= 13 - (-1) \cdot (38 + (-2) \cdot 13) \\
 &= (3) \cdot (13) + (-1) \cdot 38 \\
 &= (3) (82 + (-2) \cdot 38) + (-1) \cdot 38 \\
 &= (-7) \cdot 38 + (3) \cdot 89 \\
 &= (-7) \cdot (12f + (-1) \cdot 89) + (3) \cdot 89 \\
 &= (-7) \cdot 12f + (10) \cdot 89 \\
 &= (-7) \cdot 12f + (10) \cdot (3f + 2 + (-29) \cdot 12f) \\
 &= (-29f) \cdot 12f + (10) \cdot 3f + 2
 \end{aligned}$$

Quindi l'ID di Bezout è:

$$f = (-29f) \cdot 12f + (10) \cdot 3f + 2$$

Pertanto è inverso moltiplicativo di $\begin{bmatrix} 12f \\ 3f + 2 \end{bmatrix}$ e

$$\begin{bmatrix} -29f \\ 3f + 2 \end{bmatrix} = \begin{bmatrix} 3975 \\ 3772 \end{bmatrix}$$

Concludendo

$$d = 3975$$

Quindi pubblichiamo

$$n = 3901, e = 12f$$

Teniamo segreti

$$p = 47, q = 83, d = 3975.$$

Codifichiamo un messaggio

$$m = 3 \quad (\Rightarrow (m, n) \Rightarrow (3, 3901) = 1 \Rightarrow \text{OK})$$

Dobbiamo calcolare

$$\begin{bmatrix} \tilde{m} \end{bmatrix}_n = \begin{bmatrix} m^e \end{bmatrix}_n = \begin{bmatrix} 3^{12f} \end{bmatrix}_{3901}$$

Abbiamo che $127 = 64 + 32 + 16 + 8 + 4 + 2 + 1$.

ma

$$\left[\begin{smallmatrix} 3^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 9 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 3^4 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 81 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 3^8 \\ 3901 \end{smallmatrix} \right] = \left(\left[\begin{smallmatrix} 3^4 \\ 3901 \end{smallmatrix} \right] \right)^2 = \left[\begin{smallmatrix} 81^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 6561 \\ 3901 \end{smallmatrix} \right] =$$

~~$$\left[\begin{smallmatrix} 11660 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2660 \\ 3901 \end{smallmatrix} \right]$$~~

$$\left[\begin{smallmatrix} 3^{16} \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2660^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3087 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 3^{32} \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3087^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3327 \\ 3901 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 3^{64} \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3327^2 \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 1792 \\ 3901 \end{smallmatrix} \right]$$

Quindi

$$\begin{aligned} \left[\begin{smallmatrix} \tilde{n} \\ 3901 \end{smallmatrix} \right] &= \left[\begin{smallmatrix} 3^{127} \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 3^{64} \\ 3901 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 3^{32} \\ 3901 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 3^{16} \\ 3901 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 3^8 \\ 3901 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 3^4 \\ 3901 \end{smallmatrix} \right] \cdot \left[\begin{smallmatrix} 3^2 \\ 3901 \end{smallmatrix} \right] \\ &\quad \cdot \left[\begin{smallmatrix} 3 \\ 3901 \end{smallmatrix} \right] = \\ &= \left[\begin{smallmatrix} 247 \\ 3901 \end{smallmatrix} \right] \end{aligned}$$

concedendo

$$\left[\begin{smallmatrix} \tilde{n} \\ 3901 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 247 \\ 3901 \end{smallmatrix} \right]$$

Decodifichiamo \tilde{n} . Dobbiamo calcolare

$$\left[\begin{smallmatrix} \tilde{n}^d \\ n \end{smallmatrix} \right] = \left[\begin{smallmatrix} 247^{3475} \\ 3901 \end{smallmatrix} \right]$$

Abbiamo che

$$3475 = 2048 + 1024 + 256 + 128 + 16 + 2 + 1$$

ma

$$\left[\begin{smallmatrix} 247^2 \\ 3921 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2494 \\ 1842 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 247^4 \\ 2494^2 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2494^2 \\ 1842^2 \end{smallmatrix} \right]$$

$$\left[\begin{smallmatrix} 247^8 \\ 2494^4 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 1842^2 \\ 2985 \end{smallmatrix} \right]$$

$$\vdots \quad \vdots \quad \vdots$$
$$\left[\begin{smallmatrix} 247^{128} \\ 2494^{2048} \end{smallmatrix} \right] = \left[\begin{smallmatrix} 1842^2 \\ 2873 \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2873 \\ 2926 \end{smallmatrix} \right]$$

Quindi

$$\left[\begin{smallmatrix} 247^{3975} \\ 2494^{3975} \end{smallmatrix} \right] = \left[\begin{smallmatrix} 2926 \\ 2873 \end{smallmatrix} \right] \left[\begin{smallmatrix} 3861 \\ 3516 \end{smallmatrix} \right] \left[\begin{smallmatrix} 2873 \\ 1626 \end{smallmatrix} \right] \cdot$$

$$\cdot \left[\begin{smallmatrix} 2494 \\ 247 \end{smallmatrix} \right] =$$

$$= \left[\begin{smallmatrix} 3 \\ 1 \end{smallmatrix} \right]_{3921}$$

DIH

$$\Phi(n) = n - \left| \left\{ 1 \leq i \leq n : (i, n) \geq 2 \right\} \right| \text{ ma}$$

$$\left\{ 1 \leq i \leq n : (i, n) \geq 2 \right\} = A_1 \cup \dots \cup A_r \text{ dove}$$

$$A_j = \left\{ 1 \leq i \leq n : p_j | i \right\} \quad \forall j = 1, \dots, r$$

(se $(i, n) \geq 2 \Rightarrow \exists p \in \mathbb{P}$, p primo tale che $p | n$ e $p | i$
 $\Rightarrow p | (p_1^{\alpha_1} \dots p_r^{\alpha_r})$ e $p | i \Rightarrow p = p_j$ per qualche
 $1 \leq j \leq r$ e $p | i$)

Applichiamo il principio di Inclusione-Eclusione:

S.i.a

$$T = \{e_1, \dots, e_k\} \subseteq [r]. \text{ Dobbiamo calcolare}$$

$$|A_T| = |A_{e_1} \cap \dots \cap A_{e_k}|$$

ma

$$A_{e_1} \cap \dots \cap A_{e_k} = \left\{ 1 \leq i \leq k : p_{e_1} | i, \dots, p_{e_k} | i \right\} =$$

$$= \left\{ 1 \leq i \leq k : (p_{e_1} \dots p_{e_k}) | i \right\}$$

$$= \left\{ p_{e_1} \dots p_{e_k}, 2(p_{e_1} \dots p_{e_k}), \dots, \right.$$

$$\left. \left(\frac{n}{p_{e_1} \dots p_{e_k}} \right) p_{e_1} \dots p_{e_k} \right\}$$

Pertanto

$$|A_T| = \frac{n}{p_{e_1} \dots p_{e_k}}$$

Quindi per a.g. 1

$$\left| \left\{ 1 \leq i \leq n : (i, n) \geq 2 \right\} \right| = \prod_{\substack{T \subseteq [n] \\ T \neq \emptyset}} (-1) \cdot \frac{n}{p_{t_1} \dots p_{t_n}} =$$

$T = \{t_1, \dots, t_k\}$
 $T \neq \emptyset$

dim per $t=3$

$$= -n \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_n} \right) + n$$

4.5 COMPOSIZIONI

Siano $n, k \in \mathbb{N}$

def: una composizione di n in k parti è una sequenza $(a_1, \dots, a_k) \in \mathbb{N}^k$ tale che

$$a_1 + \dots + a_k = n$$

$$(\text{dae } \mathbb{N}^k = \underbrace{\mathbb{N} \times \dots \times \mathbb{N}}_k)$$

esempio: le composizioni di $n=3$ in $k=3$ parti sono:

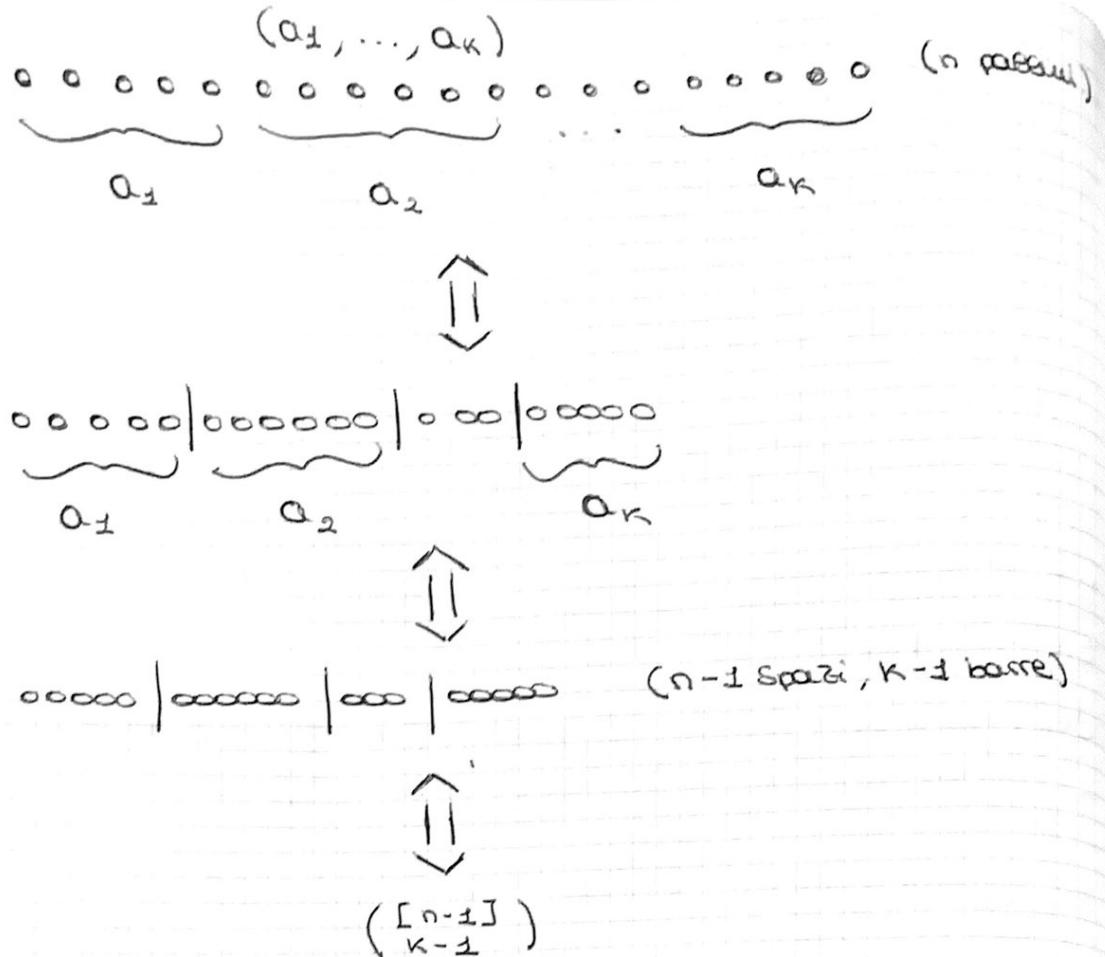
$$(2, 1, 1), (2, 2, 1), (1, 2, 2), (3, 1, 1), (1, 3, 1), \\ (1, 1, 3)$$

prop. 4.5.1

Siano $n, k \in \mathbb{N}$. Allora ci sono $\binom{n-1}{k-1}$ composizioni di n in k parti

dim:

costruiamo una bizione tra composizioni di n in k parti e $\binom{[n-1]}{k-1}$:

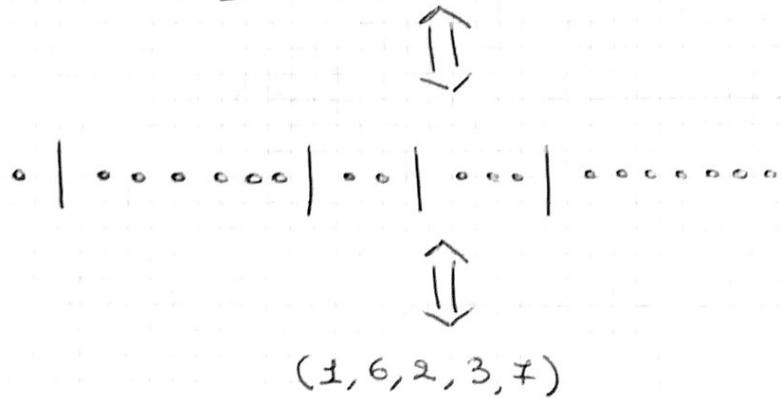


esempio:

$$n=19, k=5$$

Sia $S = \{1, 7, 9, 12\}$ e $(\binom{[18]}{4})$. Allora

$$\{1, 7, 9, 12\} \leq [18]$$



def : una composizione debole (di n in K parti) è
una sequenza (a_1, \dots, a_K) e $\sqsubset \mathbb{N}^K$
tale che $(!)$

$$a_1 + \dots + a_K = n$$

Prop. 4.5.2

c'sono $\binom{n+k-1}{k-1}$ composizioni deboli di n in K parti

dim:

da funzione

$$(a_1, \dots, a_K) \longmapsto (a_1+1, \dots, a_K+1)$$

è una biezione tra composizioni deboli di n in K parti e composizioni di $n+k$ in k parti. Segue quindi da 4.5.1.

4.6. coefficienti multinomiali

Siano $n, k \in \mathbb{N}$ e sia (a_1, \dots, a_k) una composizione di n in k parti.

def Il coefficiente multinomiale (a_1, \dots, a_k) è
il numero di modi di assegnare ogni $i \in [n]$
ad una di k categorie c_1, \dots, c_k in modo che
 a_j numeri vengono assegnati a c_j ($\forall j = 1, \dots, k$)

esempio:

$$n = 4, \quad k = 3, \quad (a_1, a_2, a_3) = (1, 2, 1)$$

3	[1, 2]	[4]
2	[1, 3]	[4]
2	[1, 4]	[3]
1	[2, 3]	[4]
1	[2, 4]	[3]
1	[3, 4]	[2]

[4]	[1, 2]	[3]
[4]	[1, 3]	[2]
[3]	[2, 4]	[2]
[4]	[2, 3]	[1]
[3]	[2, 4]	[1]
[2]	[3, 4]	[1]

↓

$$\binom{4}{1, 2, 1} = 12$$

Prop. 4.6.1

Sia (a_1, \dots, a_k) una composizione di n in k parti.

Allora

$$(a_1, \dots, a_k) = \frac{n!}{a_1! \dots a_k!}$$

dim

Possiamo scegliere i numeri da mettere in categoria

C_1 in $\binom{n}{a_1}$ modi: rimangono $n-a_1$ numeri.

Possiamo scegliere quegli da mettere in C_2 in $\binom{n-a_1}{a_2}$ modi: rimangono $n-a_1-a_2$ numeri.

Possiamo scegliere quegli da mettere in C_3 in $\binom{n-a_1-a_2}{a_3}$ modi: rimangono $n-a_1-a_2-a_3$ numeri.

Analogo modo, si arriva a $n-a_1-a_2-\dots-a_{k-1}$

Possiamo scegliere quegli da mettere in C_k in $\binom{n-a_1-\dots-a_{k-1}}{a_k}$ modi.

Concludendo

$$\begin{aligned} (a_1, \dots, a_k) &= (\binom{n}{a_1}) (\binom{n-a_1}{a_2}) \dots (\binom{n-a_1-a_2-\dots-a_{k-1}}{a_k}) \\ &= \frac{n!}{a_1! \dots a_k!} \end{aligned}$$

Sia $S = \{s_1, \dots, s_n\}$ un insieme finito.

def: un multinsieme M su S è una funzione $S \rightarrow \mathbb{N}$, se $x \in S \Rightarrow v(x)$ si dice multiplicità di x in M .

La cardinalità di M è

$$|M| = \sum_{x \in S} v(x)$$

Scritto $M = \{s_1^{v(s_1)}, \dots, s_n^{v(s_n)}\}$ oppure

$$M = \underbrace{\{s_1, \dots, s_1\}}_{v(s_1)}, \underbrace{\{s_2, \dots, s_2\}}_{v(s_2)}, \underbrace{\{s_3, \dots, s_3\}}_{v(s_3)}$$

Intuitivamente, un multinsieme è un insieme "con ripetizioni".

esempio:

$$K = \left\{ 1^4, 2^0, 3^2, 4^4 \right\} = \begin{matrix} \text{posso scrivere} \\ \downarrow \\ \left\{ 1, 1, 1, 1, \cancel{2}, 3, 3, 4, 4, 4, 4 \right\} \end{matrix}$$

è un multinsieme su $[a]$ di cardinalità 10 ($\nu: [a] \rightarrow \mathbb{N}$ è definita da $\nu(1) = 4, \nu(2) = 0, \nu(3) = 2, \nu(4) = 4$)

Siano $n \in \mathbb{P}$ e $K \in \mathbb{N}$.

def: Il coefficiente binomiale «girato» (o storto) (twisted binomial coefficient) è il numero di multinsiemi su $[n]$ di cardinalità K , scritto $\left(\begin{smallmatrix} n \\ K \end{smallmatrix} \right)$

oss: La funzione

$$\left\{ 1^{a_1}, 2^{a_2}, \dots, n^{a_n} \right\} \rightarrow (a_1, a_2, \dots, a_n)$$

è una biezione tra (multinsiemi su $[n]$ di cardinalità K) e (composizioni deboli di K in n parti).

Quindi, per 4.5.2:

$$\left(\begin{smallmatrix} n \\ K \end{smallmatrix} \right) = \binom{K+n-1}{n-1}$$

Prop. 4.6.2

Sia $n \in \mathbb{P}$. Allora

$$\frac{1}{(1-x)^n} = \sum_{k \geq 0} \left(\begin{smallmatrix} n \\ k \end{smallmatrix} \right) x^k$$

dim:

Abbiamo che

$$\left(\frac{d}{dx} \right)^k ((1-x)^{-n}) \Big|_{x=0} = (-1)^k (-n)(-n-1) \cdots (-n-(k-1))$$

Quindi

$$\begin{aligned} \frac{1}{k!} \left(\frac{d}{dx} \right)^k ((1-x)^{-n}) &= \cancel{\frac{n(n+1)\cdots(n+k-1)}{k!}} \\ &= \binom{n+k-1}{k} = \binom{n+k-1}{n-1} = \\ &= \binom{n}{k} \end{aligned}$$

Sia $M = \{1^{a_1}, \dots, n^{a_n}\}$ un multinsieme su $[n]$.

def: una permutazione di m è un ordinamento
lineare degli elementi di M .

Poniamo

$$S(M) = \{ \text{permutezioni di } M \}$$

esempio: Sia $M = \{1^2, 2^2, 3^2\} = \{1, 2, 2, 3\}$.

Allora

$$\begin{aligned} S(M) = \{ &2213, 2231, 2123, 2321, \cancel{2113}, \\ &2132, 2312, 1232, 3212, 1322, \\ &3122, \cancel{1223}, 3221. \end{aligned}$$

prop. 4.6.3 :

Sia $H = \{1^{a_1}, \dots, n^{a_n}\}$ un multinsieme su $[n]$.

Allora

$$|S(H)| = \binom{n}{a_1, \dots, a_n}$$

dove $n \stackrel{\text{def}}{=} a_1 + \dots + a_n$.

dim : c'è una bizione tra $S(H)$ e i modi di
assegnazione assegnare ogni $i \in [n]$ ad
una di n categorie in modo che a_j numeri
vengono assegnati a categoria C_j
($\forall 1 \leq j \leq n$).

Definiamo Definita da

$$x_1, x_2, x_3, \dots, x_n \in S(H)$$



$$\left(\begin{array}{l} i \in [n] \text{ è assegnato} \\ a_i C_j \quad (1 \leq j \leq n) \end{array} \Leftrightarrow x_i = j \right)$$

esempio: Sia $H = \{1^5, 2^3, 3^1, 4^2, 5^5\}$

e sia $1534112451251255 \stackrel{(1)(2)(3)(4)}{\dots} \stackrel{(10)}{\in} S(H)$

$$\begin{array}{ccccc} 10 & 13 & 14 & & \\ \boxed{156} & \boxed{711} & \boxed{3} & \boxed{48} & \boxed{2912} \\ 1 & 2 & 3 & 4 & 5 \end{array}$$



(il n°1 va in scatola 1
il n°2 va in scatola 5
(il 3 si trova in pos. 2)

4.7 ENUMERAZIONE PRATICA: Poker

$$52 \text{ carte} : \quad 4 \text{ semi} \times 13 \text{ valori} \\ = \quad \left\{ \text{C, Q, F, P} \right\} \quad \left\{ 1, 2, \dots, 10, J, Q, K \right\}$$

Quante "mani" ci sono?

$$\binom{52}{5} = \frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 26 \cdot 51 \cdot 10 \cdot 49 \cdot 4 = \\ = 2\ 598\ 960$$

Quante "mani" sono un full?

FULL = 3 carte di uguale valore +
2 carte di uguale valore

full \leftrightarrow (valore delle tris, seme mancante, valore della coppia, seme della coppia)

$$\Rightarrow 13 \times 4 \times 12 \times \binom{9}{2} = \\ = 13 \times 4 \times 12 \times 6 = 3744$$

Quante "mani" sono un poker?

POKER = 4 carte di uguale valore

poker \leftrightarrow (valore delle poker, valore della carta rimanente, seme della carta rimanente)

$$\Rightarrow 13 \times 12 \times 4 = 624$$

Quante "mani" sono un colore?

CALORE = 5 carte dello stesso seme

colore \leftrightarrow (seme delle carte , 5 valori)

$$\Rightarrow 4 \times \binom{13}{5} =$$

$$= \frac{4 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9^3}{5 \cdot 4 \cdot 3 \cdot 2} =$$

$$= 13 \cdot 12 \cdot 11 \cdot 3 = 5148$$

Quante "mani" sono una doppia coppia?

DOPPIA COPPIA = 2 carte dello stesso valore + 2 carte dello stesso valore (diverso)

doppia coppia \leftrightarrow (valore delle I coppie , semi delle I coppie , valore delle II coppie , semi delle II coppie)

(valore delle ultime carte , semi delle ultime carte)

$$\Rightarrow 13 \times \binom{4}{2} \times 12 \times \binom{9}{2} \times 11$$

$$\times 4 = 247104$$

= 247104

ERRATO!

Motivo: NON è una biezione!

Esempio:

$$\begin{array}{c} \{2C, 2Q, QP, QF, FC\} \leftrightarrow (2, \{C, Q\}, C, \{P, F\}, F, C) \\ \Downarrow \qquad \qquad \qquad \neq \\ (4, \{P, F\}, 2, \{C, Q\}, I, C) \end{array}$$

Una codifica corretta è:

doppia coppia \leftrightarrow (valore della coppia , valore della coppia con valore più basso , valore della coppia con valore più alto)
valore della coppia rimanente , valore della coppia rimanente)

13 su 48
scagliano 2

$$\Rightarrow \binom{13}{2} \times \binom{4}{2} \times \binom{4}{2} \times 11 \times 4 = \\ = 123552$$

- [es. [1+]: Quante "mani" sono un tris ?]
- [es. [1+]: Quante "mani" sono una coppia ?]

4.8 RICORSIONI LINEARI A COEFFICIENTI COSTANTI

TEO. 4.8.1 (Teorema fondamentale dell'algebra)

Siano $a_0, \dots, a_d \in \mathbb{R}$ ($d \in \mathbb{N}$).
 $a_d \neq 0$.

Allora $\exists d_1, \dots, d_r \in \mathbb{C}$ e $\exists d_1, \dots, d_s \in \mathbb{N}$
tali che

$$d_1 + \dots + d_s = d$$

e

$$a_0 + a_1 x + \dots + a_d x^d = a_d (x - d_1)^{d_1} \dots (x - d_s)^{d_s}$$

DIM ONESSA.

def. : I numeri d_1, \dots, d_d si dicono le radici del nostro polinomio $a_0 + a_1 x + \dots + a_d x^d$.

Ie numero d_i si dice la multiplicità di d_i
 $(\forall i = 1, \dots, r)$

PROP. 4.8.2 (Ruffini) :

Sia $P(x) \in \mathbb{R}[x]$ e $\alpha \in \mathbb{C}$. Allora

$$P(\alpha) = 0 \iff (x - \alpha) \mid P(x).$$

DIM è nota.

per dimostrare

$(A(x) \mid B(x)) \iff \exists C(x) \in \mathbb{R}[x] \text{ tale che } B(x) = A(x) \cdot C(x)$

Sia $f : \mathbb{N} \rightarrow \mathbb{R}$.

def. : f soddisfa una RICORSIONE LINEARE A COEFFICIENTI COSTANTI se esistono
 $a_0, \dots, a_{d-1} \in \mathbb{R}$ ($d \in \mathbb{N}$) tali che

$$f(n+d) = a_{d-1} \cdot f(n+d-1) + \dots + a_1 \cdot f(n+1) + a_0 \cdot f(n) \quad (*)$$

$\forall n \in \mathbb{N}$.

EURISTICA (e idea) :

Calcolando i primi valori si nota che $f(n)$ cresce esponenzialmente.

Sia $\lambda \in \mathbb{C}$ tale che $f(n) = \lambda^n$ per $\forall n \in \mathbb{N}$.

Abbiamo che $f(n)$ è soluzione di (*) se e solo se

$$\lambda^{n+d} = a_{d-1} \lambda^{n+d-1} + \dots + a_1 \lambda^{n+1} + a_0 \lambda^n$$

cioè solo se

$$\lambda^d = a_{d-1} \cdot \lambda^{d-1} + \dots + a_1 \lambda + a_0$$

cioè solo se λ è radice di

$$x^d - a_{d-1} x^{d-1} - \dots - a_1 x - a_0 = 0 \quad (**)$$

def : (**) si dice EQUAZIONE CARATTERISTICA della ricorsione (*)

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

Sì chiede

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

Sia X questo insieme.

Notiamo che

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

Dove

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

$$A_2 := \left\{ \quad = \quad = \quad = : x_2 = x_3 = x_4 \right\}$$

:

$$A_5 := \left\{ \quad = \quad = \quad = : x_5 = x_6 = x_7 \right\}$$

Applichiamo I.-E.. Abbiamo:

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

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

ma

$$\begin{aligned}
|A_1| &= \left| \left\{ (x_1, \dots, x_5) \in [0,9]^5 : x_1 = x_2 = x_3 \right\} \right| \\
&\stackrel{\text{przy 3 wadach}}{=} \underbrace{10 \cdot 10 \cdot 10}_{\text{a wadach indep.}} \cdot 10^5
\end{aligned}$$

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

Poi

$$\begin{aligned}
|A_1 \cap A_2| &= \left| \left\{ (x_1, \dots, x_5) \in [0,9]^5 : x_1 = x_2 = x_3 = x_4 \right\} \right| \\
&= 10^4
\end{aligned}$$

$$\begin{aligned}
|A_1 \cap A_3| &= \left| \left\{ (x_1, \dots, x_5) \in [0,9]^5 : x_1 = x_2 = x_3 = x_4 = x_5 \right\} \right| \\
&= 10^3
\end{aligned}$$

$$\begin{aligned}
|A_1 \cap A_4| &= \left| \left\{ \quad = \quad = \quad = : x_1 = x_2 = x_3 = x_4 = x_5 = x_6 \right\} \right| \\
&= 10^3
\end{aligned}$$

$$\begin{aligned}
|A_1 \cap A_5| &= \left| \left\{ \quad = \quad = \quad = : x_1 = x_2 = x_3, x_5 = x_6 = x_7 \right\} \right| \\
&= 10^3
\end{aligned}$$

$$|A_2 \cap A_3| = |\{ \dots : x_2 = x_3 = x_4 = x_5 \}| = 10^4$$

$$|A_2 \cap A_4| = |\{ \dots : x_2 = x_3 = x_4 = x_5 = x_6 \}| = 10^3$$

$$|A_2 \cap A_5| = |\{ \dots : x_2 = x_3 = x_4, x_5 = x_6 = x_7 \}| = 10^3$$

$$|A_3 \cap A_4| = |\{ \dots : x_3 = x_4 = x_5 = x_6 \}| = 10^4$$

$$|A_3 \cap A_5| = |\{ \dots : x_3 = x_4 = x_5 = x_6 = x_7 \}| = 10^3$$

$$|A_4 \cap A_5| = |\{ \dots : x_4 = x_5 = x_6 = x_7 \}| = 10^4$$

$$|A_1 \cap A_2 \cap A_3| = |\{ \dots : x_1 = x_2 = x_3 = x_4 = x_5 \}| = 10^3$$

$$|A_1 \cap A_2 \cap A_4| = 10^2$$

$$|A_1 \cap A_2 \cap A_5| = |\{(c, a, c, a, b, b, b) : c, b \in [0, 9]\}| = 10^2$$

$$|A_3 \cap A_4 \cap A_5| = 10^2$$

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

$$|A_1 \cap A_4 \cap A_5| = 10^2$$

$$|A_2 \cap A_3 \cap A_4| = 10^3$$

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

$$|A_2 \cap A_4 \cap A_5| = 10^2$$

$$|A_3 \cap A_4 \cap A_5| = 10^3$$

$$|A_1 \cap A_2 \cap A_3 \cap A_4| = 10^2$$

$$|A_1 \cap A_2 \cap A_3 \cap A_5| = 10$$

$$|A_1 \cap A_2 \cap A_4 \cap A_5| = 10$$

$$|A_1 \cap A_3 \cap A_4 \cap A_5| = 10$$

$$|A_2 \cap A_3 \cap A_4 \cap A_5| = 10^2$$

$$|A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| = 10$$

concluendo

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5| &= 5 \cdot 10^5 - (10^4 + 10^3 + 10^3 + 10 \\ &\quad + 10^4 + 10^3 + 10^3 + 10^4 + 10^3 + 10^4) + \\ &\quad + (10^3 + 10^2 + 10^2 + 9 \cdot 10^2 + 2 \cdot 10^3 + 10) - \\ &\quad - (\cancel{10} + 2 \cdot 10^2 + 3 \cdot 10) + 10. \end{aligned}$$

Pertanto

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

TEO. 4.8.3 :

Sia $f: \mathbb{N} \rightarrow \mathbb{R}$ e siano $a_0, \dots, a_{d-1} \in \mathbb{R}$ ($d \in \mathbb{P}$) tali che:

$$f(n+d) = a_{d-1} f(n+d-1) + \dots + a_1 f(n+1) + a_0 f(n) \quad (*)$$

Per $\forall n \in \mathbb{N}$.

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

$$\text{DEG}(P_i) \leq d_i - 1 \quad \forall i = 1, \dots, r$$

e

$$f(n) = \prod_{i=1}^r P_i(n) \cdot (x_i)^{d_i} \quad \forall n \in \mathbb{N}$$

Dove - $x_1, \dots, x_r \in \mathbb{C}$ sono le radici dell'eq. caratteristica della ricorrenza $(*)$

- $d_1, \dots, d_r \in \mathbb{P}$ sono le molteplicità di x_1, \dots, x_r rispettivamente

DM Omessa.

Io succo da te stesso. E' se ho la macchina ho fatto.