Teorema cinese del resto.

Siano $b_1, \dots, b_h \in \mathbb{Z}$ $\quad n_1, \dots, n_h \in \mathbb{N} - \{0,1\}$. Se

$\forall i, j \in \{1, 2, \dots, h\}$ $\quad$ M.C.D. $(n_i, n_j) = 1$,

allora il sistema di congruenze lineari

$$(*) \quad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_h \pmod{n_h} \end{cases}$$

ammette soluzioni congrue tra loro $\pmod{R}$, dove

$$R = n_1 \cdot n_2 \cdot \ldots \cdot n_h.$$

Cenno di dim. Siano: $R_1 = \dfrac{R}{n_1} = n_2 \cdot n_3 \cdot \ldots \cdot n_h$

$$R_2 = \frac{R}{n_2} = n_1 \cdot n_3 \cdot \ldots \cdot n_h$$

$$\vdots$$

$$R_h = \frac{R}{n_h} = n_1 \cdot n_2 \cdot \ldots \cdot n_{h-1}$$

Si considerano le congruenze lineari ausiliarie

$(1) \quad R_1 x \equiv b_1 \pmod{n_1}$

$(2) \quad R_2 x \equiv b_2 \pmod{n_2}$

$\vdots \qquad \vdots$

non è un sistema di congruenze lineari

$$\vdots \qquad \vdots \qquad \vdots$$

$$(h) \qquad R_h x \equiv b_h \pmod{n_h}$$

M.C.D.$(R_i, n_i) = 1$ e quindi queste congruenze lineari hanno soluzione: siano

$x_1, x_2, \dots, x_h$ soluzioni delle congruenze lineari (1), (2), ..., (h) rispettivamente.

Allora una soluzione del sistema $(*)$ è

$$\bar{x} = R_1 x_1 + R_2 x_2 + \dots + R_h x_h$$

e tutte le soluzioni sono $\bar{x} + Rh$, $h \in \mathbb{Z}$.

Esercizi.

1. $$\begin{cases} x \equiv \overset{b_1}{7} \pmod{\overset{m_1}{3}} \\ x \equiv \overset{b_2}{5} \pmod{\overset{m_2}{2}} \\ x \equiv \overset{b_3}{4} \pmod{\overset{m_3}{5}} \end{cases}$$

M.C.D.$(3,2) = 1$, M.C.D.$(3,5) = 1$, M.C.D.$(2,5) = 1$

pertanto esistono soluzioni del sistema.

$R = 3 \cdot 2 \cdot 5 = 30 \qquad R_1 = 2 \cdot 5 = 10 \qquad R_2 = 3 \cdot 5 = 15 \qquad R_3 = 2 \cdot 3 = 6$

$R_1 x \equiv b_1 \pmod{n_1}$ $\quad R_2 x \equiv b_2 \pmod{n_2}$ $\quad R_3 x \equiv b_3 \pmod{n_3}$

$10x \equiv 7 \pmod 3$ $\quad \boxed{x_1 = 1}$ è soluzione perché $10 \cdot 1 - 7 = 3$ multiplo di 3

$15x \equiv 5 \pmod 2$ $\quad \boxed{x_2 = 1}$ è soluzione perché $15 \cdot 1 - 5 = 10$ multiplo di 2

$6x \equiv 4 \pmod 5$ $\quad \boxed{x_3 = 4}$ è soluzione perché $6 \cdot 4 - 4 = 20$ multiplo di 5.

$$\bar{x} = R_1 x_1 + R_2 x_2 + R_3 x_3 = 10 \cdot 1 + 15 \cdot 1 + 6 \cdot 4 = 49$$

Tutte le soluzioni $\quad x = 49 + 30h, \quad h \in \mathbb{Z}$

La prima soluzione positiva è 19 (si ottiene per $h = -1$).

Verificare per esercizio che 19 è soluzione delle tre congruenze lineari componenti il sistema.

2. $\begin{cases} 3x \equiv 4 \pmod 5 \\ 2x \equiv 4 \pmod 3 \end{cases}$

Una soluzione di $3x \equiv 4 \pmod 5$ è 3 perché $3 \cdot 3 - 4 = 5$ multiplo di 5

$x = 3 + 5h \quad (h \in \mathbb{Z})$ $\qquad \underbrace{x \equiv 3 \pmod 5}$

Una soluzione di $2x \equiv 4 \pmod 3$ è 2 perché $2 \cdot 2 - 4 = 0$ multiplo di 3

$x = 2 + 3k \quad (k \in \mathbb{Z})$ $\qquad \underbrace{x \equiv 2 \pmod 3}$

Il sistema si scrive come $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 3 \end{cases}$

e questo può essere risolto utilizzando il Teorema cinese del resto.

$R = 5 \cdot 3 = 15 \qquad R_1 = 3 \qquad R_2 = 5$

$3x \equiv 3 \pmod 5$ $\qquad \boxed{x_1 = 1}$ è soluzione perché $3 \cdot 1 - 3 = 0$ multiplo di 5

$5x \equiv 2 \pmod 3$ $\qquad \boxed{x_2 = 1}$ è soluzione perché $5 \cdot 1 - 2 = 3$ multiplo di 3.

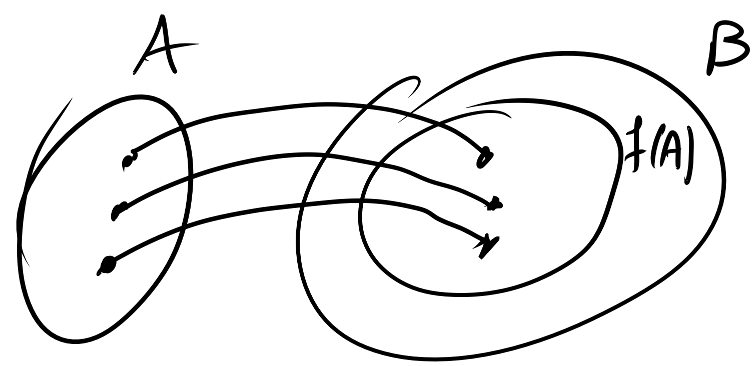
$\bar{x} = R_1 x_1 + R_2 x_2 = 3 \cdot 1 + 5 \cdot 1 = 8$

tutte le soluzioni $\quad x = 8 + 15t \qquad t \in \mathbb{Z}$.

CALCOLO COMBINATORIO

Principio dei cassetti. Sia A un insieme finito e sia $B \subset A$. Allora $|B| \leq |A|$ e $|B| = |A| \Leftrightarrow B = A$.

Osserv. Siano A, B insiemi, A finito; sia inoltre
$$f : A \to B$$
una funzione iniettiva. Allora $|f(A)| = A$.



$$f(A) = \{ y \in B \, : \, \exists x \in A \text{ tale che } f(x) = y \} = \{ f(x) \, : \, x \in A \}$$

Esempio $\quad A = \{1, 2, 3, 4, 5, 6\}$

$\quad B = \mathbb{N}$

$$f : A \to B \quad \forall x \in A \quad f(x) = 2x$$

$$f(A) = \{2, 4, 6, 8, 10, 12\} \subset \mathbb{N}$$

Esercizio Verificare che nella città di Bari ci sono almeno due persone che hanno lo stesso numero di capelli.

Una persona può avere al massimo 200.000 capelli inoltre gli abitanti di Bari sono 360.000.

Supponiamo che non ci siano due persone abitanti di Bari che abbiano lo stesso numero di capelli.

Siano $A = \{0, 1, \ldots, 200.000\} \subset \mathbb{N}$

B = insieme degli abitanti di Bari

sia $g : B \longrightarrow A$

$x \longmapsto$ numero dei capelli di x

se non ci sono due persone che hanno lo stesso numero di capelli, allora g è iniettiva

$$\forall x, y \in B \qquad x \neq y \Rightarrow g(x) \neq g(y)$$

$$|g(B)| = |B| = 360.000 \leq |A| = 200.000$$

principio dei cassetti

contraddizione.

poiché $g(B) \subseteq A$ per il principio dei cassetti

$$360.000 = |g(B)| \leq |A| = 200.000$$

contraddizione perché $200.000 < 360.000$.

Principio di inclusione-esclusione.

Siano A, B, C insiemi finiti. Allora

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

Se $C = \emptyset$ caso di 2 insiemi:

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

che vuol dire

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

Esercizio. In una classe di 25 studenti

5 studiano musica

15 praticano calcio

12 " nuoto

3 praticano nuoto e studiano musica

2 " calcio " " "

7 " " " nuoto

1 pratica calcio, nuoto e studia musica

Stabilire quanti studenti praticano una attività extrascolastica

M = insieme degli studenti che studiano musica $|M| = 5$

C = " " " " praticano calcio $|C| = 15$

N = " " " " " nuoto $|N| = 12$

$|M \cap C| = 2$ $|M \cap N| = 3$ $|C \cap N| = 7$ $|M \cap C \cap N| = 1$

$$|M \cup C \cup N| = |M| + |N| + |C| - |M \cap C| - |M \cap N| - |C \cap N| + |M \cap C \cap M$$

$$= 5 + 15 + \cancel{12} - \cancel{2} - \cancel{3} - \cancel{7} + 1 = 21.$$

Def. Siano $k, n \in \mathbb{N}^*$. Si dice disposizione con ripetizioni di k oggetti di classe n una n-pla ordinata con ripetizioni dei k oggetti: si tratta quindi di una parola lunga n formata da k oggetti.

Osserv. In sostanza una disposizione con ripetizioni può essere considerata una funzione di un insieme di cardinalità n in un insieme di cardinalità k (modello delle parole)

Prop. Siano $n, k \in \mathbb{N}^*$. Il numero delle disposizioni semplici di k oggetti di classe n è k^n.

Dim.

$$\underbrace{\begin{matrix} \sqcup & \sqcup & \cdots & \sqcup \\ k & k & \cdots & k \end{matrix}}_{n\text{-volte}}$$

Posso quindi costruire una n-pla con k oggetti in $k \cdot k \cdot \ldots \cdot k = k^n$ modi.

Osserv. Il numero delle funzioni di un insieme di cardinalità n in un insieme di cardinalità k è k^n.

Esempio: A insieme $|A| = 3$ B insieme $|B| = 4$

l'insieme delle funzioni di A in B ha cardinalità $4^3 = 64$.

Osserv. Siano A, B insiemi. Si pone

$$B^A = \{ f : A \to B \} = \text{insieme delle funzioni di } A \text{ in } B.$$

Se A e B sono finiti $|B^A| = |B|^{|A|}$.

Conseguenza: Sia A insieme finito, $|A| = n$. Allora

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

Esempi

$\lvert A\rvert = 0$	$\lvert\mathcal{P}(A)\rvert = 2^0 = 1$
$\lvert A\rvert = 1$	$\lvert\mathcal{P}(A)\rvert = 2^1 = 2$
$\lvert A\rvert = 2$	$\lvert\mathcal{P}(A)\rvert = 2^2 = 4$
$\lvert A\rvert = 3$	$\lvert\mathcal{P}(A)\rvert = 2^3 = 8$
$\vdots$	

Def. Sia A insieme. $\forall B \subset A$ si può considerare la funzione caratteristica di B $f_B : A \longrightarrow \{0,1\}$

Sia $B \subset A$.

$\forall x \in A \qquad x \in B \vee x \notin B$

si pone $\qquad f_B(x) = \begin{cases} 1 & x \in B \\ 0 & x \notin B. \end{cases}$

Esempi: 1. $f_\emptyset : A \to \{0,1\} \qquad \forall x \in A \quad x \notin \emptyset$

$\forall x \in A \quad f_\emptyset(x) = 0$

$f_\emptyset$ = funzione costante di costante valore 0

2. f_A = " " " " " 1.

3. $A = \{1,2,3,4\} \qquad B = \{2,4\}$

$f_B : A \longrightarrow \{0,1\} \qquad f_B(1) = 0 \quad f_B(2) = 1$

$f_B(3) = 0 \quad f_B(4) = 1.$