

Metodi Algebrici per l'Informatica

Appunti Universitari

1° Semestre, 2° A.A. 2024-25
27 Feb 2025

Università degli Studi di Milano - Bicocca
CdL Informatica
Prof. Marina Avitabile

AUTORE

Federico Zotti

Indice

1. Principio di buon ordinamento	1
2. Principio di induzione	1
2.1. 1° forma	1
2.2. 2° forma	1
3. Algoritmo della divisione	2
4. Massimo Comun Divisore e Algoritmo di Euclide	4
4.1. Algoritmo di Euclide	5

1. Principio di buon ordinamento

Sia $n_0 \in \mathbb{Z}$ e $\mathbb{Z}_{n_0} = \{n \in \mathbb{Z} \mid n \geq n_0\}$

$$\forall \emptyset \neq X \subseteq \mathbb{Z}_{n_0}$$

Ovvero ogni sottoinsieme non vuoto di \mathbb{Z}_{n_0} ammette un minimo.

2. Principio di induzione

2.1. 1° forma

Siano $n_0 \in \mathbb{Z}$, $p(n)$ un enunciato che ha senso $\forall n \geq n_0$.

Se

- $p(n_0)$ è vera
- $\forall n > n_0, p(n-1) \text{ vera} \Rightarrow p(n) \text{ vera}$

Allora $p(n)$ è vera per ogni $n \geq n_0$.

2.2. 2° forma

Siano $n_0 \in \mathbb{Z}$, $p(n)$ un enunciato che ha senso $\forall n \geq n_0$.

Se

- $p(n_0)$ è vera
- $\forall n > n_0, p(m) \text{ vera } \forall n_0 \leq m < n \Rightarrow p(n) \text{ vera}$

Allora $p(n)$ è vera per ogni $n \geq n_0$.

Esempio:

$$p(n) \rightarrow \sum_{k=1}^n k = \frac{n(n+1)}{2}$$

Dimostrare per induzione che $p(n)$ è vera $\forall n \geq 1$.

- **Passo base:** $n_0 = 1$ $p(n)$ è vera.
- **Passo induttivo:** $\forall n > 1, p(n-1) \text{ vera} \Rightarrow p(n) \text{ vera}$.

$$p(n-1) \rightarrow \sum_{k=1}^{n-1} k = \frac{(n-1)n}{2}$$

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

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

Dimostrato $p(n) \forall n \geq 1$.

Esempio:

$$p(n) \rightarrow |X| = n \Leftrightarrow |\mathcal{P}(X)| = 2^n$$

- **Passo base:** $n_0 = 0$

$$|X| = 0 \Leftrightarrow X = \emptyset \Leftrightarrow \mathcal{P}(\emptyset) = \{\emptyset\} \Leftrightarrow |\mathcal{P}(\emptyset)| = 1 = 2^0$$

- **Passo induttivo:** $\forall n > 0$, assumo vera $p(n-1)$ e mostro che $p(n)$ è vera.

X insieme con $|X| = n > 0$ posso scegliere $x_0 \in X$.

$$\mathcal{P}(X) = A \cup B$$

$$A = \{Y \subseteq X \mid x_0 \in Y\}$$

$$B = \{Z \subseteq X \mid x_0 \notin Z\}$$

$$A \cap B = \emptyset$$

Quindi

$$|\mathcal{P}(X)| = |A \cup B| = |A| + |B|$$

$$B = \mathcal{P}(X \setminus \{x_0\}) = 2^{n-1}$$

$$|A| = |B|$$

perchè esiste la funzione f t.c.

$$f : A \rightarrow B \text{ (biiettiva)}$$

$$Y \rightarrow Y \setminus \{x_0\}$$

$$f^{-1} : Z \rightarrow Z \cup \{x_0\}$$

Dunque

$$|\mathcal{P}(X)| = |A| + |B|$$

$$|A| = |B| = 2^{n-1}$$

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

■

3. Algoritmo della divisione

Esempio:

23 diviso 3 $\rightarrow 23 = 3 \cdot 7 + 2 \rightarrow 7$ quoziente; 2 resto

Teorema:

Siano n, m interi $\in \mathbb{Z}$ con $m \neq 0$. Allora esistono e sono unici $q, r \in \mathbb{Z}$ t.c.

1. $n = mq + r$

2. $0 \leq r < |m|$

Osservazione:

- $0 \leq r < |m| \Rightarrow r \neq |m|$
- La seconda condizione garantisce l'unicità di quoziente e resto.

Dimostrazione:

Utilizziamo l'induzione nella seconda forma. Dimostriamo prima l'esistenza di quoziente e resto.

- 1° caso: $n \geq 0$

Fissiamo arbitrariamente m , procediamo per induzione su n .

- Base induzione: $n = 0$ vero con $q = 0; r = 0$.

Se $n < |m|$ vero con $q = 0; r = m$.

- Passo induttivo: Sia allora $n \geq |m|$. Per induzione suppongo l'esistenza vera per tutti gli interi t con $0 \leq t < n$. So che $n \geq |m|$ quindi $n - |m| \geq 0$ e $n - |m| < n$ perchè $|m| \neq 0$.

$$t = n - |m|$$

$\exists q_1, r_1 \in \mathbb{Z}$ con

1. $n - |m| = mq_1 + r_1$
2. $0 \leq r_1 < |m|$

1. equivale ad $n = |m| + mq_1 + r_1$

- Se $m > 0$: $n = m(q_1 + 1) + r_1 \Rightarrow q = q_1 + 1; r = r_1$
- Se $m < 0$: $n = m(q_1 - 1) + r_1 \Rightarrow q = q_1 - 1; r = r_1$

- 2° caso: $n < 0$

Se $n < 0 \rightarrow -n > 0$, quindi posso utilizzare il primo caso con $-n$.

$\exists q_1, r_1 \in \mathbb{Z}$ con

1. $-n = mq_1 + r_1$
2. $0 \leq r_1 < |m|$

dunque $n = -mq_1 - r_1 = -mq_1 - |m| + |m| - r_1$.

- Se $m > 0$: $n = -mq_1 - m + m - r_1 \Rightarrow q = -q_1 - 1; r = |m| - r_1$.

Devo verificare che $0 \leq r < m$, so che

$$0 \leq r_1 < m \rightarrow -m \leq -r_1 < 0 \Rightarrow 0 \leq \underbrace{m - r_1}_r < m$$

- Se $m < 0$: $n = -mq_1 + m - m - r_1 \Rightarrow q = -q_1 + 1; r = -m - r_1$.

Devo verificare che $0 \leq r \leftarrow m$, so che

$$0 \leq r_1 \leftarrow m \rightarrow m \leq -r_1 < 0 \Rightarrow 0 \leq \underbrace{-m - r_1}_r \leftarrow m$$

Dimostrazione dell'unicità per assurdo:

Supponiamo che sia

$$n = mq + r \quad 0 \leq r < |m|$$

$$n = mq_1 + r_1 \quad 0 \leq r_1 < |m|$$

Supponiamo che $r \geq r_1$. Risulta $r - r_1 = m(q_1 - q)$.

Passiamo ai moduli: $|r - r_1| = r - r_1 = |m| \cdot |q_1 - q|$.

So che $0 \leq r - r_1 < |m|$

$$|m||q_1 - q| < |m| \rightarrow 0 \leq |q_1 - q| < 1 \Rightarrow |q_1 - q| = 0 \Rightarrow q_1 = q \Rightarrow r_1 = r$$

4. Massimo Comun Divisore e Algoritmo di Euclide**Divisibilità:**

Siano $a, b \in \mathbb{Z}$ t.c. $a = bc$. Allora dico che b divide a (a è un multiplo di b) e scrivo $b \mid a$.

Dato $a \in \mathbb{Z}, a \neq 0, \pm 1 \mid a; \pm a \mid a$, ovvero $\pm 1, \pm a$ sono **divisore improprio** di a .

Se esiste $b \in \mathbb{Z}, b \mid a$ con $b \neq \pm 1, b \neq \pm a$ allora b è un **divisore proprio** di a .

- **Fatto 1:** $a, b \in \mathbb{Z}$.

Se $a \mid b$ e $b \mid a$ allora $a = \pm b$.

Infatti

$$\exists c \in \mathbb{Z} \text{ t.c. } b = ac$$

$$\exists d \in \mathbb{Z} \text{ t.c. } a = bd$$

Sostituisco la seconda nella prima $b = bcd$

$$b(1 - cd) = 0 \quad b \neq 0$$

$$1 - cd = 0$$

$$cd = 1 \begin{cases} \Rightarrow c = 1 = d \Rightarrow a = b \\ \Rightarrow c = -1 = d \Rightarrow a = -b \end{cases}$$

- **Fatto 2:** $a, b, c \in \mathbb{Z}$.

Se $c \mid a$ e $c \mid b$ allora $c \mid ax + by, \forall x, y \in \mathbb{Z}$.

Infatti

$$c \mid a \Rightarrow \exists h \in \mathbb{Z} \text{ t.c. } a = ch$$

$$c \mid b \Rightarrow \exists i \in \mathbb{Z} \text{ t.c. } b = ci$$

$$\forall x, y \in \mathbb{Z} \quad ax + by = chx + ciy = c(\underbrace{hx + iy}_{\in \mathbb{Z}})$$

Concludo che $c \mid ax + by$.

Dunque se $c \mid a$ e $c \mid b$ allora c divide ogni combinazione lineare a coefficienti interi di a e b .

MCD:

Siano $a, b \in \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$.

Si dice **massimo comune divisore tra a e b** ogni intero che soddisfa le seguenti proprietà:

- $d \mid a$ e $d \mid b$
- $\forall c \in \mathbb{Z}$, con $c \mid a, c \mid b$ allora $c \mid d$

d è un MCD tra a e b . Tutti e soli i divisori di d coincidono con i divisori comuni tra a e b .

Teorema esistenza di un MCD:

$\forall a, b \in \mathbb{Z}$, con $a > 0$ e $b > 0$, esiste un MCD d tra a e b .

Inoltre esistono $s, t \in \mathbb{Z}$ t.c. $d = as + bt$ (**Identità di Bézout**).

4.1. Algoritmo di Euclide