Appunti di Metodi Algebrici per l'Informatica

Federico Zotti

2° A.A. 2024-25, 1° Semestre
03 Mar 2025

Università degli Studi di Milano - Bicocca
CdL Informatica

Prof. Marina Avitabile

Indice

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 $\mathbb{Z}_{n_o}$ 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
- $\forall n > n_0, p(n-1)$ vera $\Rightarrow p(n)$ 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
- $\forall n > n_0, p(m)$ vera $\forall n_0 \leq m < n \Rightarrow p(n)$ vera

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

Esempio:

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

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

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

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

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

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

Esempio:

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

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

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

- **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 $x_0 \in X$.

$$\mathcal{P}(X) = A \cup B$$
$$A = \{Y \subseteq X \mid x_0 \in Y\}$$
$$B = \{Z \subseteq X \mid x_0 \neg \in Z\}$$
$$A \cap B = ? \to = \emptyset$$

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.

$$f : A \to B \text{ (biiettiva)}$$
$$Y \to Y \setminus \{x_0\}$$
$$f^{-1} : Z \to Z \cup \{x_0\}$$

Dunque

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

3. Algoritmo della divisione

Esempio:

$23 \text{ diviso } 3 \to 23 = 3 \cdot 7 + 2 \to 7 \text{ quoziente; } 2 \text{ resto}$

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 $n < 0 \to -n > 0$, 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

$$0 \leq r_1 < m \to -m \leq -r_1 < 0 \Rightarrow 0 \leq \underbrace{m - r_1}_{r} < m$$

  - 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

$$0 \leq r_1 \leftarrow m \to m \leq -r_1 < 0 \Rightarrow 0 \leq \underbrace{-m - r_1}_{r} \leftarrow m$$

Dimostrazione dell'unicità per assurdo:

Supponiamo che sia

$$\begin{aligned} n &= mq + r & 0 &\leq r < |m| \\ n &= mq_1 + r_1 & 0 &\leq r_1 < |m| \end{aligned}$$

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

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

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 impropri** 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

  $$\begin{gathered}\exists c \in \mathbb{Z} \text{ t.c. } b = ac \\ \exists d \in \mathbb{Z} \text{ t.c. } a = bd\end{gathered}$$

  Sostituisco la seconda nella prima $b = bcd$

  $$\begin{gathered}b(1 - cd) = 0 \qquad b \neq 0 \\ 1 - cd = 0 \\ cd = 1 \begin{cases} \Rightarrow c = 1 = d \Rightarrow a = b \\ \Rightarrow c = -1 = d \Rightarrow a = -b \end{cases}\end{gathered}$$

- **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

  $$\begin{gathered}c|a \Rightarrow \exists h \in \mathbb{Z} \text{ t.c. } a = ch \\ c|b \Rightarrow \exists i \in \mathbb{Z} \text{ t.c. } b = ci\end{gathered}$$

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

  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 Bezout**).

4.1. Algoritmo di Euclide

Sia $a \geq b$. Eseguo le divisioni

$$\begin{aligned} & a = bq_1 + r_1 && 0 \leq r_1 < b \\ \text{Se } r_1 \neq 0 \quad & b = r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\ \text{Se } r_2 \neq 0 \quad & r_1 = r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\ & \vdots \end{aligned}$$

Essendo la successione dei resti una successione strettamente decrescente di interi non negativi, dopo un numero finito di divisioni trovo resto 0.

Suppongo che sia $r_k = 0$:

- Se $k = 1$: $r_1 = 0 \quad a = bq_1 \quad d = b$
- Se $k > 1$: affermo che $d = r_{k-1}$

Dimostrazione:

1. $r_{k-1} \mid a$ e $r_{k-1} \mid b$

   La divisione k-esima mi dice che $r_{k-1} \mid r_{k-2}$.

   Sostituisco il passo (k)in $(k-1)$in e trovo

   $$\begin{aligned} r_{k-3} &= r_{k-1} q_k q_{k-1} + r_{k-1} \\ &= r_{k-1} \underbrace{(q_k q_{k-1} + 1)}_{\overline{q} \in \mathbb{Z}} \end{aligned}$$

   Quindi $r_{k-1} \mid r_{k-3}$. Scrivo $r_{k-3} = \overline{q} r_{k-1}$. Sostituisco in $(k-2)$ e trovo

   $$\begin{aligned} r_{k-4} &= \overline{q} r_{k-1} q_{k-2} + r_{k-1} q_k \\ &= r_{k-1} (\overline{q} q_{k-2} + q_k) \end{aligned}$$

   Proseguo in questo modo e concludo che $r_{k-1} \mid b$ e $r_{k-1} \mid a$.

2. Se $c \in \mathbb{Z}$ con $c \mid a$ e $c \mid b$ allora $c \mid r_{k-1}$.

   So che

   $$\begin{aligned} a &= \overline{a}, \overline{a} \in \mathbb{Z} \\ b &= \overline{b}, \overline{b} \in \mathbb{Z} \end{aligned}$$

   Dunque

   1. $a = bq_1 + r_1 \Rightarrow r_1 = a - bq_1 = c\overline{a} - c\overline{b} q_1 = c\underbrace{\left(\overline{a} - \overline{b} q_1\right)}_{\overline{r_1}} \Rightarrow c \mid r_1 \Rightarrow r_1 = c\overline{r_1}$
   2. $r_2 = b - r_1 q_2 = c\overline{b} - c\overline{r_1} q_2 = c\left(\overline{b} - \overline{r_1} q_2\right) \Rightarrow c \mid r_2$
   3. $\ldots$

Identità di Bezout:

$$
\begin{aligned}
a &= bq_1 + r_1 \quad & r_1 &= a \cdot 1 + b(-q_1) \\
b &= r_1 q_2 + r_2 \quad & r_2 &= b - r_1 q_2 \\
& & &= b - (a - bq_1)q_2 \\
& & &= a(-q_2) + b(1 + q_1 q_2)
\end{aligned}
$$

r_1, r_2 combinazione lineare a coefficienti interi di a e b. Proseguendo in questo modo si trovano $s, t \in \mathbb{Z}$ t.c. $r_{k-1} = as + bt$

Teorema dell'unicità degli MCD:

Se d è un MCD tra a e b, l'unico altro MCD è $-d$.

Dimostrazione:

1. $-d$ è un MCD tra a e b

   Infatti

   1. $-d \mid a$ e $-d \mid b$ perchè $d \mid a$.

      $a = d\overline{a}$, per $\overline{a} \in \mathbb{Z}$ quindi $a = (-d)(-\overline{a})$ con $-\overline{a} \in \mathbb{Z}$.

      Analogamente $-d \mid b$.

   2. Sia $c \in \mathbb{Z}$, $c \mid a$ e $c \mid b$ devono mostrare che $c \mid -d$.

      Sicuramente $c \mid d$, cioè $d = c\overline{d}$,