Teoremi di Fondamenti Matematici per l'Informatica

Carlo Ramponi

May 16, 2019

Contents

1 L'ordinamento dei numeri naturali è un buon ordinamento

Enunciato

L'ordinamento dei numeri naturali è un buon ordinamento

Dimostrazione

Supponiamo che l'insieme $A \subseteq \mathbb{N}$ non abbia minimo e proviamo che allora $A = \emptyset$. Chiamiamo B il suo complementare ($B = \mathbb{N} \setminus A$) e dimostriamo per induzione che

$$\forall n \in \mathbb{N} \quad \{0, 1, ..., n\} \subseteq B$$

- $0 \notin A$, altrimenti ne sarebbe il minimo, quindi $0 \in B$ e pertanto $\{0\} \subseteq B$.
- Supponiamo che $\{0, 1, ..., n\} \subseteq B$, allora $0, 1, ..., n \notin A$ e quindi $n+1 \notin A$, altrimenti ne sarebbe il minimo, ma allora $n+1 \in B$ e pertanto $\{0, 1, ..., n, n+1\} \subseteq B$.

Per il principio di induzione di prima forma un insieme con queste proprietà coincide con quello dei numeri naturali ($B = \mathbb{N}$) e quindi $A = \emptyset$

2 Il principio di induzione (seconda forma)

Enunciato

Sia $P(n)$ una famiglia di proposizioni indicate su $\mathbb{N}$ e si supponga che

1. $P(0)$ sia vera
2. $\forall n > 0 (P(k) vera \forall k < n) \Rightarrow P(n) vera$

allora $P(n)$ è vera $\forall n \in \mathbb{N}$

Dimostrazione

Sia $A = \{n \in \mathbb{N} | P(n)$ non è vera $\}$, e supponiamo per assurdo che $A \neq \emptyset$.
Allora per la proprietà di buon ordinamento A ha minimo n.
Chiaramente $n \neq 0$ in quanto $P(0)$ è vera per ipotesi.
Inoltre se $k < n$ allora $k \notin A$ in quanto $n = \min A$, ma allora dalla (2) segue che $P(n)$ è vera e quindi $n \notin A$, contraddicendo il fatto che $n \in A$.

3 La divisione euclidea (esistenza e unicità)

Enunciato

Siano $n, m \in \mathbb{Z}$ con $m \neq 0$, allora esistono unici $q, r \in \mathbb{Z}$ tali che

$$\begin{cases} n = mq + r \\ 0 \leq r < |m| \end{cases}$$

Dimostrazione

- **Esistenza** Supponiamo dapprima che $n, m \in \mathbb{N}$, ed usiamo il principio di induzione della seconda forma su n.

  - Se $n = 0$ basta prendere $q = 0$ e $r = 0$.
  - Supponiamo $n > 0$ e che la tesi sia vera $\forall k < n$. Se $n < m$ basta prendere $q = 0$ e $r = n$, altrimenti sia $k = n - m$, dato che $m \neq 0$, $0 < k < n$, quindi per ipotesi di induzione esistono $q, r \in \mathbb{N}$ tali che
  $$\begin{cases} k = mq + r \\ 0 \leq r < |m| \end{cases}$$

  ma allora $n = k + m = mq + r + m = (q + 1)m + r$.
  Supponiamo ora $n < 0$ e $m > 0$. Allora $-n > 0$ e quindi per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che $-n = mq + r$ e $0 \leq r < m = |m|$. E quindi $n = m(-q) - r$. Se $r = 0$ abbiamo finito, se invece $0 < r < m$ allora $0 < m - r < m = |m|$ e $n = m(-q) - r = m(-q) - m + m - r = m(-1 - q) + (m - r)$.
  Sia infine $m < 0$ allora $-m > 0$, quindi per i due casi precedenti $\exists q, r \in \mathbb{Z}$ tali che $n = (-m)q + r = m(-q) + r$ con $0 \leq r < -m = |m|$

- **Unicità** Supponiamo che $n = mq + r$ e $n = mq' + r'$ con $0 \leq r, r' < m$. Supponiamo che $r' \geq r$, allora $m(q - q') = r' - r$ e quindi passando ai moduli si ha $|m||q - q'| = |r' - r| = r' - r < |m|$, da cui $0 \leq |q - q'| < 1$ e quindi $|q - q'| = 0$ ovvero $q = q'$.
  Ma allora da $mq + r = mq' + r'$ segue che anche $r = r'$.

4 Codifica dei natuali in base maggiore o uguale a 2

Enunciato

Definizione Sia $b \in \mathbb{N}$, diremo che $n \in \mathbb{N}$ è rappresentabile in base b se esistono numeri $\epsilon_0, \epsilon_1, ..., \epsilon_k \in I_b = \{0, 1, ..., b-1\}$ tali che $n = \epsilon_0 + \epsilon_1 b + \epsilon_2 b^2 + ... + \epsilon_k b^k$.

Sia $b \in \mathbb{N}, b \geq 2$. Allora ogni $n \in \mathbb{N}$ è rappresentabile in modo unico in base b. Ossia esiste una successione $\{\epsilon_i\}_{i \in \mathbb{N}}$ tale che:

1. $\{\epsilon_i$ è definitivamente nulla ($\exists i_0 \in \mathbb{N} : \epsilon_i = 0 \quad \forall i > i_0$)
2. $\epsilon_i \in I_b$ (ossia $0 \leq \epsilon_i < b$) per ogni $i \in \mathbb{N}$
3. $n = \sum_{i=0}^{\infty} \epsilon_i b^i$

e se $\{\epsilon'_i\}_{i \in \mathbb{N}}$ è un'altra tale successione, allora $\epsilon_i = \epsilon'_i \quad \forall i \in \mathbb{N}$

Dimostrazione

Esistenza per induzione su n.

1. Se $n = 0$ basta prendere $\epsilon_i = 0 \quad \forall i \in \mathbb{N}$.
2. Supponiamo ora $n > 0$ e che la tesi sia vera per ogni $k < n$.
   Siano q, r tali che $n = bq + r$ con $0 \leq r < b$. Dato che $b \geq 2$ si ha che $0 \leq q < bq \leq bq + r = n$ e quindi per l'ipotesi di induzione esiste una successione definitivamente nulla $\{\delta_i\}_{i \in \mathbb{N}}$, costituita da interi tali che $0 \leq \delta_i < b \quad \forall i \in \mathbb{N}$ e tale che $q = \sum_{i=0}^{\infty} \delta_i b^i$. Ma allora
   $$n = bq + r = b \sum_{i=0}^{\infty} \delta_i b^i + r = \sum_{i=0}^{\infty} \delta_i b^{i+1} + r = \sum_{i=1}^{\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{\infty} \epsilon_i b^i$$
   dove si è posto $\epsilon_0 = r$ e $\epsilon_i = \delta_{i-1} \quad \forall i > 0$.
   La successione $\{\epsilon_i\}$ è definitivamente nulla, dato che lo è $\{\delta_i\}$ ed inoltre $0 \leq \epsilon_i = \delta_{i-1} < b \quad \forall i > 0$ e $0 \leq \epsilon_0 = r < b$.

Unicità per induzione su n.

1. Se $n = 0 = \sum_i \epsilon_i b^i$ allora ogni addendo della somma, essendo non negativo, deve essere nullo e quindi $\epsilon_i = 0 \quad \forall i \in \mathbb{N}$

2. Supponiamo ora $n > 0$ e che l'espressione in base b sia unica per tutti i numeri $k < n$. Sia n tale che $n = \sum_{i=0}^{\infty} \epsilon_i b^i = \sum_{i=0}^{\infty} \epsilon_i' b^i$, allora possiamo scrivere

$$n = b \sum_{i=1}^{\infty} \epsilon_i b^{i-1} + \epsilon_0 = b \sum_{i=1}^{\infty} \epsilon_i' b^{i-1} + \epsilon_0'$$

ma per l'unicità della divisione euclidea si ha che $\epsilon_0 = \epsilon_0'$ e $q = \sum_{i=1}^{\infty} \epsilon_i b^{i-1} = \sum_{i=1}^{\infty} \epsilon_i' b^{i-1}$. Come prima $q < n$ e quindi per ipotesi induttiva si ha anche che $\epsilon_i = \epsilon_i' \quad \forall i \geq 1$

5 Il massimo comun divisore

Enunciato

Definizione Dati due interi $n, m \in \mathbb{Z}$ non entrambi nulli, si dice che d è un *massimo comun divisore tra n e m* se:

1. $d|n$ e $d|m$ (è un divisore)
2. Se $c|n$ e $c|m$ allora $c|d$ (è il massimo)

Proposizione Se d e d' sono due *massimi comun divisori tra n ed m* allora $d' = \pm d$.
Dimostrazione d è un divisore comune di n e m, quindi poichè d' è un massimo comun divisore di ha che $d|d'$. Scambiando i ruoli di d e d' si ha allora che anche $d'|d$ e quindi si ha che $d' = \pm d$.
Definizione Diremo che d è il massimo comun divisore di n e m se è un massimo comun divisore positivo. La proposizione precedente ci garantisce che se esiste un massimo comun divisore esso è unico.

Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli, allora esiste il *massimo comun divisore tra n ed m.*

Dimostrazione

Esistenza Si consideri l'insieme

$$S = \{s \in \mathbb{Z} | s > 0, \exists x, y \in \mathbb{Z} : s = nx + my\}$$

$S \neq \emptyset$ dato che $nn + mm > 0$ (visto che n ed m non sono entrambi nulli).
Sia ora

$$d = nx + my = \min S$$

dimostriamo che d è il massimo comun divisore:
Se $c|n$ e $c|m$ allora $n = ck$ e $m = ch$, quindi $d = nx + my = ckx + chy = c(kx + hy)$, ossia $c|d$.
Dimostriamo ora che $d|n$:
consideriamo la divisione euclidea tra n e d, ossia $n = dq + r$ con $0 \leq r < d$, se $r > 0$, allora $r = n - dq = n - (nx + my)q = n(1 - qx) + (-m)y \in S$. Ciò è assurdo perchè $r < d$ e $d = \min S$. Quindi $r = 0$ ossia $d|n$. In modo del tutto analogo si prova che $d|m$.

6 Il minimo comune multiplo

Enunciato

Definizione Dati due interi $n, m \in \mathbb{Z}$ si dice che M è un *minimo comune multiplo di n ed m* se:

1. $n|M$ e $m|M$ (è un multiplo)
2. se $n|c$ e $m|c$ allora $M|c$ (è il minimo)

Come nel caso del massimo comun divisore di dimostra che due minimi comuni multipli sono uguali a meno del segno e quindi si chiama *il minimo comune multiplo* quello positivo (è quindi unico)

Siano $n, m \in \mathbb{Z}$ non entrambi nulli, allora esiste il *minimo comune multiplo tra n e m.*

Dimostrazione

Esistenza Sia

$$M = \frac{nm}{(n, m)} = n'm'(n, m)$$

dove si è posto

$$\begin{cases} n = n'(n, m) \\ m = m'(n, m) \end{cases}$$

Chiaramente allora $M = nm' = n'm$ e quindi $n|M$ e $m|M$.
Se $n|c$ e $m|c$ allora $(n, m)|c$ e quindi posto $c = c'(n, m)$ si ha che $n'|c'$ e $m'|c'$.
Dato che $(n', m') = 1$, si ha che $n'm'|c'$ e quindi che $M = n'm'(n, m)|c'(n, m) = c$.