I numeri naturali ed il teorema di ricorsione

Domenico Luminati

10 gennaio 2002

1 I numeri naturali: gli assiomi di Peano

Ricordiamo gli assiomi (dovuti a Peano) che descrivono la struttura dei numeri naturali.

Assioma 1.1. $0 \in \mathbb{N}$

Assioma 1.2. $\mathrm{succ} : \mathbb{N} \to \mathbb{N}$ è una funzione iniettiva

Assioma 1.3. $\forall n \in \mathbb{N} \quad \mathrm{succ}(n) \neq 0$

Assioma 1.4 (di induzione). se $A \subseteq \mathbb{N}$ è un sottinsieme tale che

1. $0 \in A$
2. $\forall n \in \mathbb{N} \quad (n \in A \implies \mathrm{succ}(n) \in A)$

allora $A = \mathbb{N}$.

Proposizione 1.5. *Sia $n \in \mathbb{N}$, $n \neq 0$ allora esiste un unico $m \in \mathbb{N}$ tale che* $\mathrm{succ}(m) = n$. *Tale m viene chiamato il* predecessore *di m.*

Dimostrazione. Avendo l'esistenza, l'unicità segue immediatamente dall'iniettività di succ.

Supponiamo per assurdo che esista un $m \neq 0$ tale che $\mathrm{succ}(n) \neq m$ per ogni n, allora sia $A = \mathbb{N} - \{m\}$. Chiaramente $0 \in A$, in quanto $m \neq 0$. Se $n \in A$, allora $succ(n) \neq m$ e quindi $succ(n) \in A$. Ma allora $A = \mathbb{N}$, e questa è una contraddizione. ❑

L'assioma di induzione fornisce una potente tecnica di dimostrazione di proposizioni indicizzate sui naturali.

2 Il principio di induzione (prima forma)

Teorema 2.1 (prima forma dell'induzione). *Sia $P(n)$ una famiglia di proposizioni indicizzate su $\mathbb{N}$ e si supponga che*

1. $P(0)$ sia vera

2. *per ogni* $n \in \mathbb{N}$ $P(n) \implies P(succ(n))$

allora $P(n)$ *è vera per ogni* $n \in \mathbb{N}$

Dimostrazione. Sia $A = \{n \mid P(n) \text{ è vera}\}$, allora $0 \in A$ e se $n \in A$ allora vale $P(n)$, quindi vale $P(\text{succ}(n))$ ossia anche $succ(n) \in A$, quindi per l'assioma di induzione (1.4) $A = \mathbb{N}$. ❏

3 Il teorema di ricorsione

Al momento i naturali sembrano essere una struttura molto povera, non vi è definita né la somma né il prodotto e nemmeno la relazione d'ordine (poter dire quando due numeri sono uno più grande dell'altro). Per poter dare queste definizioni è necessario dimostrare il seguente

Teorema 3.1 (di ricorsione). *Sia* X *un insieme,* $h : \mathbb{N} \times X \to X$ *una funzione e* $c \in X$*. Esiste una unica funzione* $f : \mathbb{N} \to X$ *tale che:*

$$\begin{aligned} f(0) &= c && (1) \\ f(\text{succ}(n)) &= h(n, f(n)) \quad \forall n \in \mathbb{N} && (2) \end{aligned}$$

Dimostrazione. Cominciamo con il provare l'unicità di una tale f. Supponiamo che f e g verifichino le due proprietà e proviamo che allora $f(n) = g(n)$ per ogni $n \in \mathbb{N}$. Usiamo l'induzione. Per $n = 0$ la proposizione è vera, infatti dato che sia f che g verificano 1, si ha che $f(0) = c = g(0)$.

Supponiamo che $f(n) = g(n)$. f verifica la (2) e quindi $f(\text{succ}(n)) = h(n, f(n))$, ma anche g verifica la (2) quindi $g(\text{succ}(n)) = h(n, g(n))$. Dato che, per ipotesi di induzione, $f(n) = g(n)$, allora

$$f(\text{succ}(n)) = h(n, f(n)) = h(n, g(n) = g(\text{succ}(n)).$$

Proviamo ora l'esistenza. Per definizione di funzione, quello che si cerca è un insieme $f \subseteq \mathbb{N} \times X$ tale che:

$$\forall n \in \mathbb{N} \quad \exists \text{ unico } x \in X : (n, x) \in f \qquad (3)$$

e, traducendo in termini di appartenenza le richieste (1) e (2)

$$\begin{aligned} (0, c) \in f & \qquad (4) \\ \forall n \in \mathbb{N} \quad (x, n) \in f \implies (\text{succ}(n), h(n, x)) \in f & \qquad (5) \end{aligned}$$

Sia $\Omega = \{Z \subseteq \mathbb{N} \times X \mid Z \text{ verifica (4) e (5)}\}$, quello che dobbiamo trovare è un elemento di Ω che sia una funzione.

Sia $f = \bigcap_{Z \in \Omega} Z$. Dato che f è l'intersezione di tutti gli elementi di Ω, necessariamente

$$\forall Z \in \Omega \quad f \subseteq Z \qquad (6)$$

Proviamo ora che $f \in \Omega$.

f verifica la proprietà (4). Infatti $(0, c) \in Z$ per ogni $Z \in \Omega$, quindi $(0, c) \in \bigcap_{Z \in \Omega} Z = f$.

f verifica la proprietà (5). Se $(n, x) \in f$ allora $(n, x) \in Z$ per ogni $Z \in \Omega$, ma allora dato che ogni $Z \in \Omega$ verifica la (5), $(\mathrm{succ}(n), h(x, n)) \in Z$ per ogni $Z \in \Omega$ e quindi $(\mathrm{succ}(n), h(x, n)) \in \bigcap_{Z \in \Omega} Z = f$.

Per concludere resta da provare che f verifica la (3). Procediamo per induzione su n. Sia $n = 0$. Abbiamo già visto che $(0, c) \in f$. Supponiamo per assurdo che esista $(0, d) \in f$ con $d \neq c$, e sia $f' = f - \{(0, d)\}$. Chiaramente $(0, c) \in f'$ e se $(n, x) \in f' \subseteq f$ allora $(\mathrm{succ}(n), h(n, x)) \in f$, ma allora, per il terzo assioma di Peano (1.3), $\mathrm{succ}(n) \neq 0$ per ogni $n \in \mathbb{N}$ e quindi $(\mathrm{succ}(n), h(n, x)) \neq (0, d)$, pertanto $(\mathrm{succ}(n), h(n, x)) \in f'$. Quindi $f' \in \Omega$, ma ciò contraddice la (6) perché $f \not\subseteq f'$.

Supponiamo la tesi vera per n. Sia x l'unico elemento tale che $(n, x) \in f$, dato che f verifica la (5), allora $(\mathrm{succ}(n), h(n, x)) \in f$. Supponiamo per assurdo che anche $(\mathrm{succ}(n), e) \in f$ con $e \neq h(n, x)$ e si ponga $f' = f - \{(\mathrm{succ}(n), e)\}$. Proviamo che anche in questo caso $f' \in \Omega$ e si avrà, come prima, un assurdo. Dal terzo assioma di Peano segue che $(0, c) \neq (\mathrm{succ}(n), e)$ e quindi, dato che $(0, c) \in f$ allora $(0, c) \in f'$. Se $(i, z) \in f' \subseteq f$ allora $(\mathrm{succ}(i), h(i, z)) \in f$. Si hanno due casi: $i \neq n$ oppure $i = n$. Se $i \neq n$ allora, per l'iniettività di succ (assioma 1.2) si ha che $(\mathrm{succ}(i), h(i, z)) \neq (\mathrm{succ}(n), e)$ e quindi $(\mathrm{succ}(i), h(i, z)) \in f'$. Se invece $i = n$ allora $(i, z) = (n, z) \in f$ e quindi, per ipotesi di induzione, l'unicità di x implica che $z = x$. Dato che $h(n, x) \neq e$,

$$(\mathrm{succ}(i), h(i, z)) = (\mathrm{succ}(n), h(n, x)) \in f'.$$

Questo conclude la dimostrazione. ❑

4 Le operazioni sui naturali

Il teorema di ricorsione permette di definire la somma il prodotto di numeri naturali.

Definizione 4.1. Dato $n \in \mathbb{N}$ si definisce ;la funzione $m \mapsto n + m$ ricorsivamente nel seguente modo:

$$\begin{aligned} n + 0 &= n \\ n + \mathrm{succ}\, m &= \mathrm{succ}\, n + m \end{aligned}$$

ed analogamente si definisce il prodotto $m \mapsto nm$:

$$\begin{aligned} n0 &= 0 \\ n(m + 1) &= nm + n \end{aligned}$$

Osservazione 4.2. Se si chiamo $1 = succ(0)$, allora per ogni $n \in \mathbb{N}$ si ha che $\mathrm{succ}(n) = n + 1$, infatti dalla definizione di + si ha che

$$n + 1 = n + \mathrm{succ}(0) = \mathrm{succ}(n + 0) = \mathrm{succ}(n)$$

D'ora in poi non scriveremo più $\mathrm{succ}(n)$ ma $n+1$.

Esercizio 4.1. Si provi che per ogni $n \in \mathbb{N}$ si ha $0+n=n$ e $1+n=n+1$ ossia $1+n=\mathrm{succ}(n)$.

Esercizio 4.2. Si provi che per ogni $n \in \mathbb{N}$ si ha $0 \cdot n = 0$ e $1 \cdot n = n \cdot 1 = n$..

Esercizio 4.3. Si provino le usuali proprietà (i.e. associativa, commutativa, distributiva) della somma e del prodotto di numeri naturali.

5 L'ordinamento dei naturali

Con la somma si può definire la nozione di ordinamento dei numeri naturali.

Definizione 5.1. Siano $n, m \in \mathbb{N}$ diremo che $n \leq m$ se esiste $k \in \mathbb{N}$ tale che $m = n + k$.

Osservazione 5.2. Si può vedere $\leq$ come un sottinsieme di $\mathbb{N} \times \mathbb{N}$ e precisamente $\leq = \{(n,m) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N} : n+k=m\}$. E quindi $\leq$ è una relazione sui naturali e quello che abbiamo definito come significato di $n \leq m$ è effettivamente lo stesso che dire $(n,m) \in \leq$.

Si può dimostrare la seguente

Proposizione 5.3. *Valgono le seguenti proprietà:*

1. $\forall n \in \mathbb{N} \quad n \leq n$.
2. $\forall n, m \in \mathbb{N} \quad (n \leq m$ *e* $m \leq n \implies n = m$
3. $\forall n, m, k \in \mathbb{N} \quad (n \leq m$ *e* $m \leq k \implies n \leq k$
4. $\forall n, m \in \mathbb{N} \quad n \leq m$ *o* $m \leq n$.

Dimostrazione. La dimostrazione è lasciata per esercizio agli studenti volonterosi. I punti che richiedono maggiore attenzione sono il secondo e il quarto. ❑

6 Soluzioni proposte

Soluzione dell'esercizio 4.1 Proviamo la prima. Procediamo per induzione su n. Se $n=0$ allora dalla definizione si ha che $0+0=0$. Supponiamo che $0+n=n$ allora

$$0 + \mathrm{succ}(n) = \mathrm{succ}(0+n) = \mathrm{succ}(n).$$

Proviamo la seconda. Per induzione su n. Per definizione $1+0=1=\mathrm{succ}(0)$. Supponiamo che $1+n=\mathrm{succ}(n)$, allora

$$1 + \mathrm{succ}(n) = \mathrm{succ}(1+n) = \mathrm{succ}(\mathrm{succ}(n))$$

e quindi anche in questo caso, si ha la tesi. ❑

Soluzione dell'esercizio 4.2 Proviamo la prima. Procediamo per induzione su n. Se $n = 0$ allora dalla definizione si ha che $0 \cdot 0 = 0$. Supponiamo che $0 \cdot n = 0$ allora

$$0 \cdot \mathrm{succ}(n) = (0 \cdot n) + 0 = 0 + 0 = 0.$$

Proviamo la seconda. Che $n \cdot 1 = n$ segue dal fatto che

$$n \cdot 1 = n \cdot 0 + n = 0 + n = n$$

L'altra uguaglianza la proviamo per induzione su n. Per definizione $1 \cdot 0$. Supponiamo che $1 \cdot n = n$, allora

$$1 \cdot \mathrm{succ}(n) = 1 \cdot n + 1 = n + 1 = \mathrm{succ}(n).$$

e quindi anche in questo caso, si ha la tesi. ❏

Soluzione dell'esercizio 4.3 Proviamo soltanto l'associatività della somma. Dobbiamo provare che per ogni $n, m, k \in \mathbb{N}$ si ha che $(n+m)+k = n+(m+k)$. Procediamo per induzione su k. Se $k = 0$ dalla definizione si ha $(n+m)+0 = n+m$ e anche $n+(m+0) = n+(m) = n+m$. Supponiamo la tesi vera per k e proviamola per $\mathrm{succ}(k)$.

$$\begin{aligned}(m+n)+\mathrm{succ}(k) &= \mathrm{succ}((m+n)+k) = \mathrm{succ}(m+(n+k)) = \\ & m+\mathrm{succ}(n+k) = m+(n+\mathrm{succ}(k))\end{aligned}$$

❏