Metodi Matematici per l'Informatica - Dispensa 15
(a.a. 22/23, I canale)

Docente: Lorenzo Carlucci (`lorenzo.carlucci@uniroma1.it`)

1 Induzione

Come abbiamo visto una dimostrazione per induzione consta di due parti fondamentali:

> **Principio di Induzione**
> Vogliamo stabilire una tesi di tipo universale, ossia che per ogni $n \geq 1$ vale una certa proprietà $P(n)$. È sufficiente stabilire i due punti seguenti:
>
> 1. **Base**: Verifichiamo/dimostriamo che la proprietà P vale per $n = 1$.
> 2. **Passo Induttivo**: Consideriamo un generico $n \geq 1$. Assumendo che la proprietà P valga per n, dimostriamo che vale per $n + 1$. Ossia dimostriamo che vale l'implicazione:
>
> $$\text{Se } P(n) \text{ allora } P(n+1).$$

Nel Passo Induttivo, l'ipotesi che valga P per n viene detta *ipotesi induttiva*.

Per giustificare la validità di questo metodo possiamo fare alcune considerazioni.

In primo luogo: tutti i numeri $1, 2, 3, 4, \ldots$ si ottengono partendo da 1 applicando l'operazione di successore, ossia il $+1$. Se sappiamo dimostrare che una certa proprietà P vale di 1 e che la proprietà P viene *trasmessa* da un generico numero $n \geq 1$ al suo successore immediato $n + 1$ è ragionevole concludere che la proprietà P viene trasmessa a tutti i numeri $\{1, 2, 3, 4, \ldots\}$.

Il Principio di Induzione ammette anche una formulazione insiemistica, che otteniamo considerando un sottoinsieme X non vuoto di $\mathbf{N} = \{1, 2, 3, 4, \ldots\}$.

> **Principio di Induzione (versione insiemistica)**
> Se X soddisfa le due proprietà seguenti:
>
> 1. $1 \in X$, e
> 2. Per un generico $n \geq 1$: se $n \in X$ allora $n + 1 \in X$.
>
> Allora è legittimo concludere che $\mathbf{N} \subseteq X$, ossia che X contiene tutti i numeri naturali.

Il Principio di Induzione può giustificarsi un po' più rigorosamente ricorrendo a un principio decisamente più intuitivo. Consideriamo un arbitrario $A \subseteq \mathbf{N}$ non vuoto. Risulta abbastanza intuitivo dedurre che A possiede un elemento minimo, ossia esiste un $a \in A$ tale che per ogni altro $b \in A$, non vale $b < a$.

Chiamiamo questo principio il Principio del Minimo Numero (o Principio del Buon Ordinamento). Vediamo come il Principio di Induzione (per comodità nella sua formulazione insiemistica) si può giustificare in base a questo principio.

Principio del Minimo Numero/Principio del Buon Ordinamento
Ogni sottinsieme non vuoto dei numeri naturali ha un minimo.

Consideriamo un insieme $X \subseteq \mathbf{N}$ che soddisfa le due proprietà: (1) $1 \in X$ e (2) per un generico $n \geq 1$, se $n \in X$ allora $n+1 \in X$. Supponiamo per assurdo che non valga la conclusione del Principio di Induzione: ossia supponiamo che non è vero che $\mathbf{N} \subseteq X$. Dunque l'insieme $A = (\mathbf{N} \setminus X)$ è un sottinsieme non-vuoto di $\mathbf{N}$. Per il Principio del Minimo Numero A contiene un minimo. Sia m il minimo di A. Si osserva che m non può essere 1; dato che $1 \in X$ e $m \notin X$. Dunque $m > 1$ e pertanto $m - 1 \geq 1$ (ossia è ancora un numero naturale). Inoltre dato che m è scelto come il minimo in $\mathbf{N}$ ma non in X, necessariamente $m - 1 \in X$. Ma X soddisfa la proprietà (2) e dunque se $m - 1 \in X$ allora $m \in X$. Abbiamo raggiunto una contraddizione: $m \in X$ e $m \notin X$.

Questa dimostrazione per assurdo stabilisce la validità del Principio di Induzione in base al Principio del Minimo Numero.

Una semplice generalizzazione degli argomenti visti sopra giustifica la seguente versione del Principio di Induzione, che differisce dalla precedente solo per il fatto che il caso base non è 1 ma un arbitrario numero k.

Principio di Induione da k
Se devo dimostrare che per ogni $n \geq k$ vale una proprietà P, è sufficiente stabilire i due fatti seguenti:

1. **Base**: La proprietà P vale per k.
2. **Passo Induttivo**: Consideriamo un generico $n \geq k$. Assumendo che la proprietà P valga per n, dimostriamo che vale per $n+1$. Ossia dimostriamo che vale l'implicazione:

$$\text{Se } P(n) \text{ allora } P(n+1).$$

2 Esempi algebrici

Il Principio di Induzione è valido per qualunque proprietà P con un parametro n. La varietà di queste proprietà è immensa. Vediamo alcuni esempi particolarmente semplici che riguardano proprietà algebriche elementari.

Esempio 1. Consideriamo la somma dei primi n numeri naturali, ossia

$$1 + 2 + 3 + \cdots + n.$$

Questa somma ammette una formula chiusa (detta formula di Gauss), che è

$$\frac{n(n+1)}{2}.$$

Una tipica applicazione dell'Induzione è dimosttrare che per ogni $n \geq 1$, vale la seguente identità algebrica:

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Dimostriamo il caso base.

Base. $n = 1$. Dobbiamo dimostrare che $1 = 1(1+1)/2$. Ovviamente è vero.

Passo Induttivo. Sia $n \geq 1$. Dobbiamo dimostrare che se è vera l'identità

$$1 + 2 + 3 + \cdots + n = n(n+1)/2, \text{ (Ipotesi Induttiva)}$$

allora è vera anche l'identità

$$1 + 2 + 3 + \cdots + n + 1 = (n+1)(n+1+1)/2. \text{ (Tesi).}$$

Il primo passo in una dimostrazione per induzione consiste nel **mettere in evidenza** il caso n all'interno del caso $n+1$. Nel nostro caso dobbiamo evidenziare la presenza della somma

$$1 + 2 + 3 + \cdots + n$$

all'interno della somma

$$1 + 2 + 3 + \cdots + n + 1.$$

Ovviamente la prima è la parte iniziale della seconda: Il caso $n+1$ è:

$$\underbrace{1 + 2 + 3 + \cdots + n}_{\text{Caso } n} + n + 1$$

A questo punto possiamo **applicare l'ipotesi induttiva**. In questo caso ci permette di **sostituire** l'espressione

$$1 + 2 + \cdots + n$$

con

$$n(n+1)/2.$$

Otteniamo dunque:

$$1 + 2 + 3 + \cdots + n + 1 = \underbrace{1 + 2 + 3 + \cdots + n}_{\text{Caso } n} + n + 1 = \underbrace{n(n+1)/2}_{\text{Caso } n} + n + 1.$$

Qui finisce la parte propriamente induttiva dell'argomento. Resta da dimostrare che l'espressione che abbiamo ottenuto, ossia

$$n(n+1)/2 + n + 1$$

coincide con quanto previsto dalla nostra tesi per il Caso $n+1$, ossia con

$$(n+1)(n+2)/2.$$

Verificare questa identità:

$$n(n+1)/2 + n + 1 = (n+1)(n+2)/2$$

è un semplice esercizio di manipolazione algebrica (non ha nulla a che fare con l'induzione), e conclude la dimostrazione.

Esempio 2. Consideriamo la somma dei primi n numeri pari, ossia

$$2 + 4 + 6 + \cdots + 2n.$$

Dimostriamo per induzione che per ogni $n \geq 1$ vale

$$2 + 4 + 6 + \cdots + 2n = n(n+1).$$

Base. $n = 1$. Dobbiamo verificare che la somma dei primi $n = 1$ numeri pari, ossia il solo numero 2 è uguale al risultato della formula $n(n+1)$ con $n = 1$, ossia $1(1+1) = 2$. Anche in questo caso la verifica è ovvia.

Passo Induttivo. Dobbiamo dimostrare la **tesi**, ossia:

$$2 + 4 + 6 + \cdots + 2(n + 1) = (n + 1)(n + 1 + 1),$$

assumendo che sia vera l'**ipotesi induttiva**, ossia:

$$2 + 4 + 6 + \ldots 2n = n(n + 1).$$

Come nell'esempio precedente evidenziamo il caso n nel caso $n + 1$:

$$\underbrace{2 + 4 + 6 + \cdots + 2(n + 1)}_{\text{Caso}n+1} = \underbrace{2 + 4 + 6 + \cdots + 2n}_{\text{Caso}n} + 2(n + 1).$$

L'Ipotesi Induttiva ci permette di sostituire

$$2 + 4 + 6 + \cdots + 2n$$

con

$$n(n + 1).$$

Otteniamo dunque

$$\underbrace{2 + 4 + 6 + \cdots + 2(n + 1)}_{\text{Caso}n+1} = n(n + 1) + 2(n + 1).$$

Resta da colmare algebricamente il gap tra l'espressione appena ottenuta e la parte destra della nostra tesi per il caso $n + 1$, ossia verificare l'identità:

$$n(n + 1) + 2(n + 1) = (n + 1)(n + 2).$$

La dimostrazione è così conclusa.

In casi come i precedenti è comune utilizzare dei simboli di sommatoria per abbreviare le somme e avere maggior rigore. Per esempio, la somma $1 + 2 + 3 + \cdots + n$ si abbrevia con il simbolo $\sum_{i=1}^{n} i$ (sommatoria). Questa espressione va letta come un *for*: per ogni valore di i da 1 a n, aggiungo un termine $+i$. Abbiamo

$$\sum_{i=1}^{1} i = 1, \sum_{i=1}^{2} i = 1 + 2, \sum_{i=1}^{3} = 1 + 2 + 3, etc.$$

Per convenzione si ha $\sum_{i=1}^{0} i = 0$ (somma di nessun termine). In generale abbiamo

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n + 1).$$

Analogamente la somma dei primi n numeri pari, $2 + 4 + 6 + \cdots + 2n$ si abbrevia con $\sum_{i=1}^{n} 2 \cdot i$. In generale una espressione di tipo $\sum_{i=1}^{n} f(i)$, dove f è una funzione $f : \mathbf{N} \to \mathbf{N}$ è una abbreviazione della somma iterata dei termini $f(i)$ per i che varia da 1 a n, ossia

$$f(1) + f(2) + \cdots + f(n).$$

Variazioni di questa notazione includono diversi punti di partenza per il conteggio, e.g. $\sum_{i=4}^{n} f(i)$ abbrevia $f(4) + f(5) + \cdots + f(n)$. In modo analogo un'espressione del tipo $\prod_{i=k}^{n} f(i)$ (con $k \leq n$) abbrevia il prodotto dei termini $f(i)$ per i che va da k a n.

Usando queste notazioni gli esempi visti sopra si presentano così:

Dimostrare che per ogni $n \geq 1$ vale

$$\sum_{i=1}^{n} i = n(n+1)/2,$$

e: dimostrare che per ogni $n \geq 1$ vale

$$\sum_{i=1}^{n} 2 \cdot i = n(n+1).$$

Lo svolgimento del primo con simboli di produttoria ha l'aspetto seguente. **Base.** Per $n = 1$ dobbiamo verificare che $\sum_{i=1}^{1} i = 1 \cdot (1+1)$; il che è ovvio perché $\sum_{i=1}^{1} i$ è la somma a un termine 1.

Il **Passo Induttivo** si presenta così: Consideriamo il caso $n+1$, che riguarda la sommatoria $\sum_{i=1}^{n+1} i$. Evidenziamo in questa espressione il caso n:

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i \right) + (n+1).$$

Per Ipotesi Induttiva:

$$\left(\sum_{i=1}^{n} i \right) + (n+1) = n(n+1)/2 + (n+1).$$

Per algebra

$$n(n+1)/2 + (n+1) = (n+1)(n+2)/2.$$

Esercizio 1. *Dimostrare per induzione: per ogni $n \geq 1$*

$$\sum_{i=1}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}.$$

Esempio 3. Dimostrare che per ogni $n \geq 1$, $6^n - 1$ è divisibile per 5.

Base. $n = 1$: Dobbiamo dimostrare che $6^1 - 1$ è divisibile per 5. Ovvio.

Passo Induttivo. Sia $n \geq 1$. Assumiamo l'ipotesi induttiva, ossia che la proprietà vale per n: $6^n - 1$ è divisibile per 5. Dimostriamo che vale per $n+1$, ossia che $6^{n+1} - 1$ è divisibile per 5.

Evidenziamo il caso n nel caso $n+1$:

$$6^{n+1} - 1 = (6^n - 1) \cdot 6 + 5.$$

A questo punto invochiami l'ipotesi induttiva, che ci assicura che $6^n - 1$ è divisibile per 5. La dimostrazione si conclude con semplici considerazioni algebriche: se $6^n - 1$ è divisibile per 5 (ossia è uguale a $5j$ per qualche j), allora $(6^n - 1) \cdot 5$ è divisibile per 5 (è $5 \cdot j \cdot 6$). Inoltre 5 è ovviamente divisibile per 5. Dunque la somma di $(6^n - 1) \cdot 5$ e 5 è divisibile per 5 (è $5(j \cdot 6 + 1)$). Questo conclude la dimostrazione.

Esercizio 2. *Dimostrare per induzione: per ogni $n \geq 0$, $n \cdot (n^2 + 5)$ è divisibile per 6.*

Esempio 4. Dimostrare che per ogni $n \geq 0$ vale $n < 2^n$. Procediamo per induzione.

Base. $n = 0$. La verifica è banale: $0 < 2^0 = 1$.

Passo induttivo. Sai $n \geq 1$. Assumiamo l'ipotesi induttiva, ossai $n < 2^n$. Dimostriamo la tesi, ossia $n + 1 < 2^{n+1}$. Evidenziare il caso n nel caso $n+1$ è in questo caso estremamente banale:

$$\underbrace{n+1}_{\text{Caso } n+1} = \underbrace{n}_{\text{Caso } n} +1.$$

Dall'ipotesi induttiva e dalle proprietà di $<$ e di $+1$ abbiamo:

$$\text{Se } n < 2^n \text{ allora } n+1 < 2^n + 1.$$

Dato che $1 \leq 2^n$ per ogni n, abbiamo

$$n + 1 < 2^n + 1 \leq 2^n + 2^n = 2^{n+1}.$$

Abbiamo così ottenuto la tesi.

Esempio 5. Dimostrare che per ogni $n \geq 5$ vale $n^2 < 2^n$.

Base. $n = 5$. Verifichiamo che $5^2 < 2^5$. Ovvio.

Passo Induttivo. Sia n generico ≥ 5. Assumiamo l'ipotesi induttiva:

$$n^2 < 2^n.$$

Dimostriamo la tesi:

$$(n + 1)^2 < 2^{n+1}.$$

Evidenziamo il caso n nel caso $n + 1$:

$$\underbrace{(n + 1)^2}_{\text{Caso } n+1} = \underbrace{n^2}_{\text{Caso} n} + 2n + 1.$$

Applicando l'ipotesi induttiva otteniamo

$$(n + 1)^2 < 2^n + 2n + 1$$

Per semplici considerazioni algebriche osserviamo

$$2^n + 2n + 1 \leq 2^n + n^2.$$

Abbiamo di nuovo il Caso n all'interno di questa espressione (n^2): possiamo applicare di nuovo l'Ipotesi Induttiva ottenenedo:

$$2^n + 2n + 1 \leq 2^n + n^2 + 1 < 2^n + 2^n.$$

Dato che $2^n + 2^n = 2^{n+1}$ concatenando le diseguaglianze abbiamo la tesi desiderata per $n + 1$:

$$(n + 1)^2 < 2^{n+1}.$$

Questo conclude la dimostrazione.

(NB: Abbiamo usato in questa dimostrazione almeno un'altra diseguaglianza che può anch'essa dimostrarsi per induzione: $2n + 1 \leq n^2$. Ci serve per $n \geq 5$. Per esercizio dimostrarla per induzione. Qual è il minimo n a partire dal quale è vera?)

Esercizio 3. *Dimostrare per induzione: per ogni* $n \geq 1$*:*

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Esempio 6. Abbiamo già dimostrato che un insieme di n elementi ha 2^n sottinsiemi. Ne diamo ora una dimostrazione per Induzione. La nostra tesi è, più precisamente, la seguente: Per ogni $n \geq 0$, per ogni insieme A di n elementi, il numero dei sottinsiemi di A (ossia il numero di elementi del suo insieme potenza $\mathcal{P}(A)$) è 2^n.

Il Caso Base è $n = 0$. Dobbiamo dimostrare che la tesi vale, ossia: Ogni insieme A di 0 elementi possiede 2^0 sottinsiemi. Dato che l'unico insieme di 0 elementi è l'insieme vuoto, $\emptyset$, basta considerare i suoi sottinsiemi. L'unico sottinsieme dell'insieme vuoto è l'insieme vuoto, dunque la tesi è dimostrata.

Per il Passo Induttivo ragioniamo così. Assumiamo la tesi per un generico $n \geq 0$. Consideriamo un insieme A arbitrario di $n + 1$ elementi. Dato che $n \geq 0$ abbiamo $n + 1 \geq 1$. Dunque A contiene almeno un elemento.

Scegliamo un elemento $a \in A$ qualunque. I sottinsiemi di A sono di due tipi (esclusivi): quelli che contengono a e quelli che non lo contengono. Quelli che non lo contengono possono vedersi come l'aggunta di a ad un sottinsieme di $A \setminus \{a\}$, o più precisamente come l'unione $S \cup \{a\}$ di un sottinsieme S di $A \setminus \{a\}$ e $\{a\}$. Dato che $A \setminus \{a\}$ ha n elementi posso applicare l'Ipotesi Induttiva (che vale *per ogni* insieme con n elementi) e concludere che il numero di sottinsiemi di $A \setminus \{a\}$ è 2^n. I restanti sottinsiemi di A sono quelli di forma $S \cup \{a\}$ con S sottinsieme di $A \setminus \{a\}$ dunque sono tanti quanti i sottinsiemi di $A \setminus \{a\}$. Ancora l'Ipotesi Induttiva mi dice che sono 2^n. Dunque i sottinsiemi di A sono in totale $2^n + 2^n = 2^{n+1}$.