Il principio di induzione e i numeri naturali.

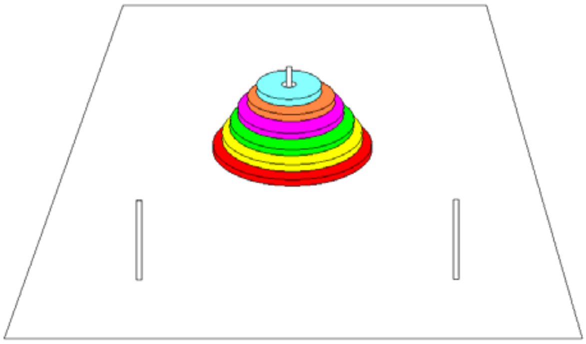
Il principio di induzione è un potente strumento di dimostrazione, al quale si ricorre ogni volta che si debba dimostrare una proprietà in un numero infinito di casi.

Un enunciato non rigorosamente preciso ma espressivo è il seguente:

Se una proprietà P_n vale per $n=1$ e se dalla validità di P_n si può dedurre quella di P_{n+1}, allora P_n vale per ogni intero n.

In formule: $P_1 \,\&\, \forall n (P_n \Rightarrow P_{n+1}) \Rightarrow \forall n \; P_n$.

Il modo migliore (o uno dei modi migliori) per introdurre il principio di induzione è la *Torre di Hanoi*. Si tratta di un gioco costituito da tre pioli, in uno dei quali sono disposti dei dischi bucati di grandezza decrescente.



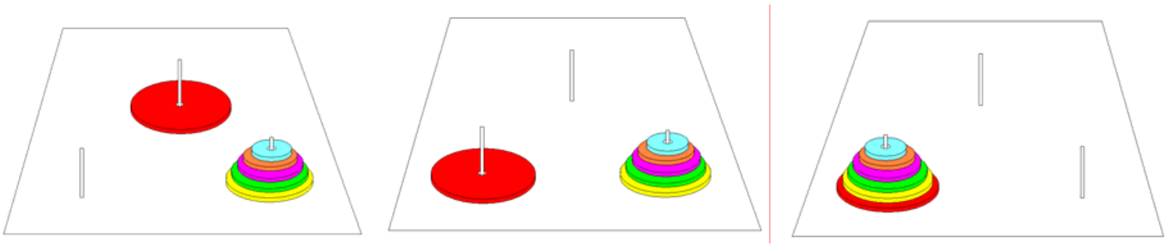
Il gioco consiste nello spostare tutti i dischi su uno dei pioli vuoti, con le seguenti regole:

1. Si può spostare un solo disco alla volta,
2. Il disco spostato si può mettere su uno spazio vuoto o sopra un disco più grande; non è consentito mettere un disco grande su uno più piccolo.

Ci si può chiedere se lo spostamento è sempre possibile, quale che sia il numero dei dischi. La risposta è positiva, e si può ragionare così:

Supponiamo di saper spostare secondo le regole, diciamo cinque dischi[1]. Se ora dobbiamo spostare sei dischi, cominciamo a spostare i cinque dischi superiori senza muovere mai quello grande in basso, la cui presenza non dà fastidio perché essendo il più grande di tutti è come se non ci fosse. Alla fine di questo primo passo, avremo il disco grande sul piolo di partenza e i cinque dischi più piccoli in uno degli altri due pioli, diciamo in quello di destra. A questo punto spostiamo il disco grande sul piolo di sinistra, e infine riportiamo i cinque dischi piccoli sopra il grande.

[1] Notiamo che possiamo scegliere noi se mandarli sul piolo di destra o su quello di sinistra; infatti se sappiamo spostare i cinque dischi sul piolo di destra, basta invertire tutte le mosse (come se guardassimo il gioco allo specchio) e i dischi passeranno sul piolo di sinistra.



Ora quello che abbiamo fatto per sei dischi lo possiamo rifare per qualsiasi altro numero di dischi, ad esempio per diciassette: se sappiamo come spostare sedici dischi, potremo spostarne anche diciassette: spostiamo prima i sedici dischi più piccoli, cosa che per ipotesi sappiamo fare, poi il diciassettesimo più grande, e poi di nuovo i sedici piccoli.

Ricapitolando, se è possibile spostare un certo numero di dischi, è anche possibile spostarne uno di più.

Di qui segue che possiamo spostare quanti dischi vogliamo. Infatti un disco sappiamo spostarlo senza problemi. Dato che è possibile spostare un disco, potremo spostarne due. Ma allora possiamo spostarne tre. E quindi anche quattro. Dunque anche cinque, e poi sei, eccetera.

Ma siamo proprio sicuri che con questo eccetera riusciamo a coprire tutti i numeri? Chi ci dice che qualche numero non sgusci via senza che possiamo mai raggiungerlo? Certo, il numero cinquantaquattro con un po' di pazienza riusciamo a raggiungerlo: possiamo spostare un disco, quindi ne possiamo spostare due, quindi tre, e dopo un po' di tempo arriveremo a 54. Ma se dovessimo spostarne un numero un po' più grande, diciamo 87235491098467657682659852194987546283519? Riusciremmo a contare fino a raggiungerlo?

Il principio di induzione (un principio, ricordiamolo, non un teorema) ci dice che sì, contando un numero dopo l'altro raggiungiamo tutti i numeri senza eccezione. Di conseguenza, possiamo spostare quanti dischi vogliamo.

Avendo tempo. Perché per spostare n dischi da un piolo a un altro occorrono 2^n-1 mosse. Anche questo si può dimostrare per induzione. Infatti è vero per $n=1$ (per spostare un disco basta una mossa). Supponiamo ora che per n dischi ci vogliano 2^n-1 mosse. Quante ce ne vorranno per spostarne $n+1$? Bisogna prima spostare n dischi piccoli lasciando in pace il più grande, e per questo occorrono 2^n-1 mosse; poi si sposta il grande (1 mossa) e infine di nuovo gli n piccoli (2^n-1 mosse). In totale $2^n-1+1+2^n-1$ mosse, cioè $2\times2^n-1=2^{n+1}-1$ mosse. In conclusione, se per spostare n dischi ci vogliono 2^n-1 mosse, per $n+1$ dischi ne occorrono $2^{n+1}-1$. Si può dunque applicare il principio di induzione, e concludere la dimostrazione.

Ad esempio, per spostare 64 dischi occorrono $2^{64}-1$ mosse, cioè 18.446.744.073.709.551.615 mosse. Se si fa una mossa al secondo, ci vorranno 584.546.491.649 anni, 58 giorni, 14 ore, 56 minuti e 15 secondi, secondo più secondo meno. Provare per credere.

Dopo questa introduzione, torniamo alla storia.

Quando nel suo *Arithmetices principia* Peano introduce i numeri naturali:

1. 1 è un numero,

2. Il successivo di un numero è un numero,
3. 1 non è successivo di nessun numero,
4. Se i successivi di due numeri sono uguali, anche i due numeri sono uguali,
5. Se un insieme $A \subseteq N$ contiene il numero 1 e il successivo di ogni suo elemento, allora $A = N$,

il principio di induzione non è che uno degli assiomi che determinano N. Appena però si prosegue la lettura, si vede immediatamente che, benché tutti gli assiomi siano essenziali per caratterizzare il sistema dei numeri naturali, il quinto gioca un ruolo centrale nella definizione delle operazioni con i numeri e nella dimostrazione delle proprietà relative.

Gli assiomi riguardano una sola operazione: il passaggio da un numero intero a al successivo, che indicheremo con $S(a)$. Occorrerà dunque definire a partire da essa le operazioni con i numeri (in particolare la somma e il prodotto) e dimostrarne le principali proprietà.

Cominciamo con la somma. Per sommare ad a il numero 1, basterà prendere il successivo di a: $a + 1 = S(a)$. La somma di due numeri interi a + b è più complicata. Intuitivamente, si può pensare di sommare successivamente ad a tante unità quante sono contenute in b; ossia, partendo da a, di ripetere b volte l'operazione di passaggio al successivo:

$$a + b = S(S(. . . S(a)) . . .) \ \ b \text{ volte.}$$

I puntini fanno pensare che la definizione non sia così esplicita come sarebbe necessario: qualcosa è lasciata sottintesa. In genere, ogni volta che in una formula compaiono dei puntini, c'è un uso implicito del principio di induzione. E infatti la definizione più corretta della somma fa appunto uso di questo assioma:

Definizione 1 (Somma) La somma $a+b$ di due numeri naturali a e b è definita dalle relazioni seguenti:

$$a + 1 = S(a)$$
$$a + (b + 1) = (a + b) + 1 = S(a+b). \quad \text{(A)}$$

A questa definizione Peano aggiunge una nota esplicativa:

> Questa definizione si deve leggere così: se a e b sono numeri, e se a+b è un numero [cioè se è stato definito], ma $a+(b+1)$ non è stato ancora definito, allora $a + (b + 1)$ significa il numero che segue $a + b$.

Abbiamo qui un esempio di definizione ricorsiva. Intuitivamente, la prima relazione definisce la somma a + b per b = 1; la seconda ci dice che se essa è definita per b, lo è anche per b + 1. Di conseguenza, la somma è definita per ogni numero b.

Veniamo ora brevemente alle principali proprietà della somma.

Teorema 1 (Proprietà associativa) Per ogni terna di numeri a, b e c si ha
$$(a + b) + c = a + (b + c). \quad \text{(B)}$$

Dimostrazione. La (B) è vera per $c = 1$; infatti in questo caso non è altro che la (A). Supponiamo ora che sia vera per c e dimostriamola per $c + 1$. Si ha

$(a + b) + (c + 1) =_{(A)} [(a + b) + c] + 1 =_{(B)} [a + (b + c)] + 1 =_{(A)} a + [(b + c) + 1] =_{(A)} a + [b + (c + 1)].$

Per il principio di induzione, la (B) vale allora per ogni c, e il teorema è dimostrato.

Per la proprietà commutativa bisognerà procedere in due tappe.

Lemma 1. Per ogni intero a si ha $a + 1 = 1 + a$. (C)

Dimostrazione. La (C) è vera per $a = 1$. Se supponiamo che sia vera per a, si ha

$(a + 1) + 1 =_{(C)} (1 + a) + 1 =_{(A)} 1 + (a + 1)$

e il lemma è dimostrato.

Teorema 2 (Proprietà commutativa della somma.) Per ogni coppia di numeri naturali a e b risulta

$$a + b = b + a. \quad \text{(D)}$$

Dimostrazione. Per il lemma precedente la (D) è vera per $b = 1$. Supponiamo ora che sia vera per b, e dimostriamola per $b + 1$. Si ha

$a + (b + 1) =_{(A)} (a + b) + 1 =_{(D)} (b + a) + 1 =_{(A)} b + (a + 1) =_{(C)} b + (1 + a) =_{(B)} (b + 1) + a$

e la (D) è dimostrata per $b+1$. Per il principio di induzione, la (D) varrà allora per ogni b.

Veniamo ora al prodotto. Anche per questa operazione occorrerà dare una definizione ricorsiva:

Definizione 2 (Prodotto) Il prodotto ab di due numeri naturali è definito dalle relazioni:

$$a \cdot 1 = a$$
$$a(b + 1) = ab + a. \quad \text{(E)}$$

Teorema 3 (Proprietà distributiva) Risulta

$$(a + c)b = ab + cb. \quad \text{(F)}$$

Dimostrazione. Per $b = 1$ la (F) segue dalla definizione precedente. Supponiamo che valga per b e dimostriamola per $b + 1$. Si ha

$(a + c)(b + 1) =_{(E)} (a + c)b + a + c =_{(F)} ab + cb + a + c =_{(D)} ab + a + cb + c =_{(E)} a(b + 1) + c(b + 1).$

La (F) vale dunque per $b + 1$, e il teorema è dimostrato.

Lemma 2. Si ha $1 \cdot a = a$.

Dimostrazione. La relazione è valida per $a = 1$. Supponiamo che valga per a; si ha allora

$$1 \cdot (a + 1) = 1 \cdot a + 1 = a + 1$$

e dunque vale anche per $a + 1$.

Dal lemma precedente e dalla (F) segue che

$$ba + a = ba + 1 \cdot a =_{(F)} (b + 1)a.$$

Teorema 4 (Proprietà commutativa del prodotto) Per ogni a e b in N risulta

$$ab = ba. \quad (G)$$

Dimostrazione. Per il lemma precedente e la definizione di prodotto, la (G) vale per $b = 1$. Supponiamo ora che valga per b; si ha

$$a(b + 1) =_{(E)} ab + a =_{(G)} ba + a = (b + 1)a$$

e quindi vale per $b + 1$. Per il principio di induzione, essa vale per ogni b.

In maniera analoga si può definire la potenza a^b mediante le relazioni $a^1 = a$, $a^{b+1} = a^b a$. Lasciamo al lettore la dimostrazione delle proprietà

$$a^{b+c} = a^b a^c$$
$$(ab)^c = a^c b^c$$
$$(a^b)^c = a^{bc}.$$