POLITECNICO DI MILANO





Problemi e paradossi dell’infinito

Seminari di Cultura Matematica - 29 marzo 2006

Claudio Citrini

Wilhelm Ackerman
(29 marzo 1896 - 24 dicembre 1962)

1928. Funzione di Ackermann

A(x, y, z) = esponenziale iterato

= funzione ricorsiva non primitiva ricorsiva

$A(x,y,0) = x + 1$

$A(x,y,1) = x + y$

$A(x,y,2) = x \cdot y$

$A(x,y,n+1) =$ se $y = 0$, allora 1

se $y = z+1$, allora $A(x, A(x,z,n+1),n)$

Paradossi

Paradosso = parà + doxa = contro l'opinione.

Antinomia = antì + nomos = contro la legge.

Schopenhauer: la verità nasce come paradosso e muore come ovvietà.

Borges: C'è un concetto che corrompe e altera tutti gli altri. Non parlo del male, il cui limitato impero è l'etica; parlo dell'infinito.

Un paradosso classico sugli interi

Galileo (1638):

Salv - […] Se io dirò, i numeri tutti, comprendendo i quadrati e i non quadrati, esser più che i quadrati soli, dirò proposizione verissima: non è così?

Simp - Non si può dir altrimenti.

Salv - Interrogando io di poi, quanti siano i numeri quadrati, si può con verità rispondere, loro esser tanti quante sono le proprie radici, avvenga che ogni quadrato ha la sua radice, ogni radice il suo quadrato, né quadrato alcuno ha più d'una sola radice, né radice alcuna più d'un quadrato solo.

Simp - Così sta.

Salv - Ma se io domanderò, quante siano le radici, non si può negare che elle non siano quante tutti i numeri, …

Albergo di Hilbert.

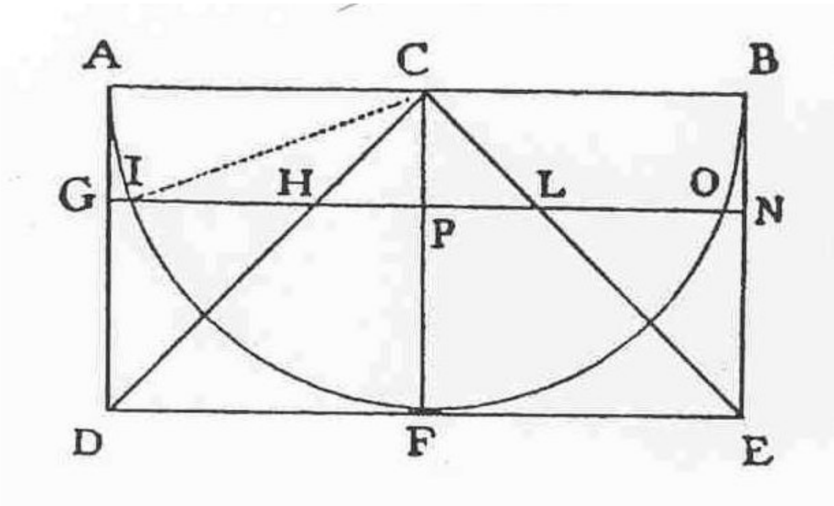
Due paradossi classici sui reali

Pitagora: Incommensurabilità della diagonale e del lato di un quadrato (o pentagono).

Prospettiva: due segmenti di diversa lunghezza contengono lo stesso numero di punti.

Salv - Io non veggo che ad altra decisione si possa venire, che a dire, … in ultima conclusione, gli attributi di eguale maggiore e minore non aver luogo ne gl'infiniti, ma solo nelle quantità terminate.

E però quando il Sig. Simplicio mi propone più linee diseguali, e mi domanda come possa essere che nelle maggiori non siano più punti che nelle minori, io gli rispondo che non ve ne sono né più né manco né altrettanti, ma in ciascheduna infiniti …



Scodella di Galileo

Principio di Cavalieri (… ma già metodo “meccanico” di Archimede)

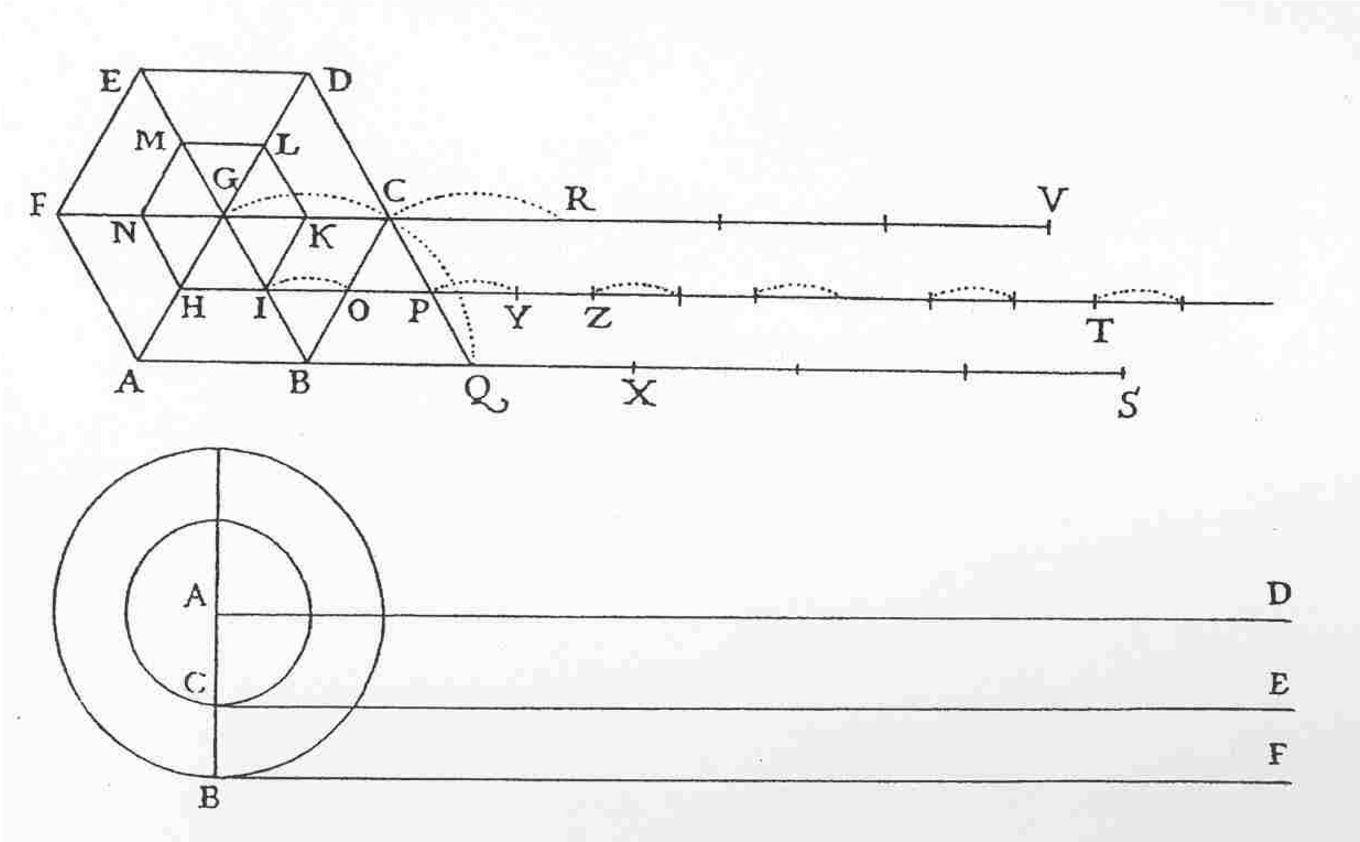
Salv - Or mentre che nella diminuzione de i due solidi si va, sino all’ultimo, mantenendo sempre tra essi la egualità, ben par conveniente il dire che gli altissimi ed ultimi termini di tali menomamenti restino tra di loro eguali, e non l’uno infinitamente maggior dell’altro: par dunque che la circonferenza di un cerchio immenso possa chiamarsi eguale a un sol punto […] li quali perché non si devon chiamare eguali, se sono le ultime reliquie e vestigie lasciate da grandezze eguali?

… ma ricordiamoci che siamo tra gl'infiniti e gl'indivisibili, quelli incomprensibili dal nostro intelletto finito per la lor grandezza, e questi per la lor piccolezza.

Aristotele: Una linea non è costituita di punti. [Phys. IV, 8, 215 b 19]

Galileo
Ruota di Aristotele

il più ammirabil problema che sia da Aristotele messo tra quelli che esso medesimo addimanda ammirandi.



Bernhard Bolzano (1781 - 1848)

Paradossi dell'infinito (1851)

Chiamiamo "insieme" un aggregato che concepiamo in modo tale che sia indifferente la disposizione delle sue parti…

Bernhard Bolzano (2)

Possibilità di insiemi infiniti in atto (proposizioni: A; A è vera; È vero che A è vera, ecc.).

Non vale la contestazione che “un insieme infinito non può venir risolto in un tutto unico, né può essere colto nella sua totalità dal pensiero. E’ un errore derivato dalla falsa opinione che, per pensare a un tutto costituito da determinati oggetti … ci si debba essere formate delle rappresentazioni di ciascuno di tali oggetti preso singolarmente. Non è affatto così: posso pensare l’insieme … degli abitanti di Praga senza formarmi una rappresentazione separata di ciascuno di essi.”

Bernhard Bolzano (3)

…Notevolissima caratteristica che si può presentare nella relazione tra due insiemi,quando entrambi siano infiniti, e che, anzi, a dire il vero, si presenta sempre, ma che fino ad oggi…è stata trascurata.

In primo luogo è possibile formare delle coppie… (= corrispondenza biunivoca).

In secondo luogo è nello stesso tempo possibile che uno dei due insiemi contenga l'altro come semplice parte…

Es.: 5y = 12x dà corrispondenza tra [0, 5] e [0,12].

Bernhard Bolzano (4)

L’aspetto paradossale … sorge unicamente dal fatto che quella relazione … è certamente sufficiente, nel caso in cui i due insiemi siano finiti, a stabilirne la perfetta uguaglianza per quanto riguarda la molteplicità delle loro parti.

Può quindi sembrare che ciò debba accadere anche nel caso in cui i due insiemi siano infiniti…

Ma tale necessità non esiste, perché la ragione per la quale ciò accade per tutti gli insiemi finiti sta appunto nella loro finitezza…

Dedekind:

Un insieme si dice infinito se può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

Un insieme si dice finito se non è infinito!

Bernhard Bolzano (5)

Serie “di Grandi” :

$x = 1 - 1 + 1 - 1 + 1 - \ \ldots = ?$

$x = \ 1 \ - (1 - 1 + 1 - 1 + \ldots) \ = 1 - x$, da cui $x = 1/2$,

Ma anche $x = (1 - 1) + (1 - 1) + \ldots = 0 \ + 0 + \ldots = 0$

E pure $x \ = 1 + (-1 + 1) + (-1 + 1) + \ldots = 1 + 0 + 0 + \ldots = 1$.

$x = 1 - 2 + 4 - 8 + 16 - \ldots = ?$

$= 1 - 2\,(1 - 2 + 4 - 8 + \ldots) = 1 - 2\,x$, da cui $x = \ 1/3$,

Ma anche $x = 1 + \ (-2 + 4) + (-8 + 16) + \ldots = 1 + 2 + 8 + 32 + \ldots$

Oppure $x \ = (1 \ - 2) + (4 - 8) + \ \ldots = -1 - 4 - \ldots$

Sono “espressioni prive di un riferimento obiettivo”.

Teorema di Riemann - Dini

Una serie convergente ma non assolutamente convergente può essere riordinata in modo da assumere come somma un numero S scelto ad arbitrio (o divergere a + o – infinito).

Es.: $1 - 1/2 + 1/3 - 1/4 + 1/5 - 1/6 + \ldots = \log 2.$

Prendendo p termini positivi e q negativi la somma vale

$S = \log 2 + 1/2 \log (p/q).$

Georg Cantor
(S. Pietroburgo 3 marzo 1845 - Halle 6 giugno 1918)

1872: definizione di R

1872 e 1883: insieme di Cantor

1873: R non numerabili

1877: corrispondenza (biunivoca) segmento - quadrato

1879-84: teoria degli insiemi (cardinali e ordinali transfiniti)

Insiemi numerabili

Una successione di successioni è ancora una successione.

I numeri razionali sono tanti quanti i naturali.

1	2	5	10	17
4	3	6	11	18
9	8	7	12	19
16	15	14	13	20
25	25	23	22	21

R: non numerabili

Data una enumerazione (ipotetica) di tutti i reali di [0,1):

$x_1 = 0,\mathbf{7}538220122\ldots$

$x_2 = 0,2\mathbf{4}52900628\ldots$

$x_3 = 0,46\mathbf{4}9913467\ldots$

$x_4 = 0,123\mathbf{8}6419\ldots$

…

costruiamo un numero reale y

$y = 0,\mathbf{5267\ldots}$

che è diverso da tutti gli x_n. Dunque y non fa parte della successione!

Dopo aver enumerato tutti i reali esprimibili mediante frasi della lingua italiana, ottenendo una enumerazione dei "Numeri di Richard", consideriamo il numero N definito dalla frase:

N = "il numero reale la cui n-esima cifra decimale è 1 se l'n-esima cifra decimale dell'n-esimo numero di di Richard non è 1, e la cui n-esima cifra decimale è 2 se l'n-esima cifra decimale dell'n-esimo numero di di Richard è 1".

Metodo diagonale di Cantor

corrispondenza (biunivoca) segmento - quadrato

x = 0,***75301289225***…

y = 0,***45380399823***…

(x, y) corrisponde a t = 0,***7455330810238998922235*** …

e viceversa.

Il trucco di tenere i 9 consecutivi assieme alla prima cifra seguente, come in ***99892***

serve ad evitare il 9 periodico, garantendo la rappresentazione unica dei numeri come allineamenti decimali.

corrispondenza (continua)
segmento - quadrato

Curva di Peano (1890): Existe complexo de ordine *n*, vel puncto in spatio ad *n* dimensiones, functio continuo de variabile reale, vel de tempore, tale que trajectoria de puncto mobile ple toto spatio.

Id es, existe linea continuo, que transi per omne puncto de plano…

Insieme ternario di Cantor

E' perfetto = coincide col suo derivato

E' in nessun luogo denso

Ha la potenza del continuo

Ha misura nulla

E' autosimilare con dimensione frattale $\log_3 2$

Scala del diavolo di Vitali

E’ continua

E’ costante a tratti sul complementare dell’insieme di Cantor

E’ derivabile quasi ovunque, con derivata 0

Non è l’integrale della sua derivata

teoria di Zermelo-Fraenkel (primi assiomi)

(AE) Assioma di estensione: Insiemi uguali sono elementi degli stessi insiemi.

(ASo) Assioma di sostituzione: per ogni insieme s e per ogni predicato binario F(x,y) “funzionale in x su s” * esiste l' insieme t i cui elementi sono tutti e soli gli associati di tutti gli elementi x di s rispetto a F(x,y).

* = che associa a ogni x di s al più un y:

$(\forall x)(\forall y)(\forall z)\ ((x \in s) \wedge F(x,y) \wedge F(x,z)) \Rightarrow (y=z))$

(AP) Assioma delle potenze: per ogni insieme s esiste l' insieme t $= \wp(s)$ i cui elementi sono tutti e soli i sottoinsiemi di s.

(AU) Assioma della somma (unione): per ogni insieme s esiste l' insieme t i cui elementi sono tutti e soli gli elementi di tutti gli elementi di s.

(AI) Assioma di infinità: esiste un insieme W tale che $\varnothing \in W$, e se $x \in W$ allora $(x \cup \{x\}) \in W$.

(AR) Assioma di regolarità: ogni insieme non vuoto x ha un elemento y tale che x e y non hanno elementi in comune.

commenti

(AP)

$\wp(X)$ l'insieme delle parti di X

$\wp(X) = 2^X$ = insieme delle funzioni da X in $\{0, 1\}$

$R = 2^N$ = {insieme delle successioni di cifre binarie}

(AI)

e costruzione dei naturali N

$\varnothing$

$(\varnothing \cup \{\varnothing\})$

$(\varnothing \cup \{\varnothing\} \cup \{\{\varnothing\}\})$

teoria di Zermelo-Fraenkel (indipendenza e consistenza degli assiomi)

G' = {(AE), (ASo), (AP), (AU)} G = {G', (AI)}

G' = è un sistema consistente di assiomi, ciascuno indipendente dagli altri.

Gödel: è impossibile dimostrare la consistenza di G.

(IF) Ipotesi fondamentale: G è consistente.

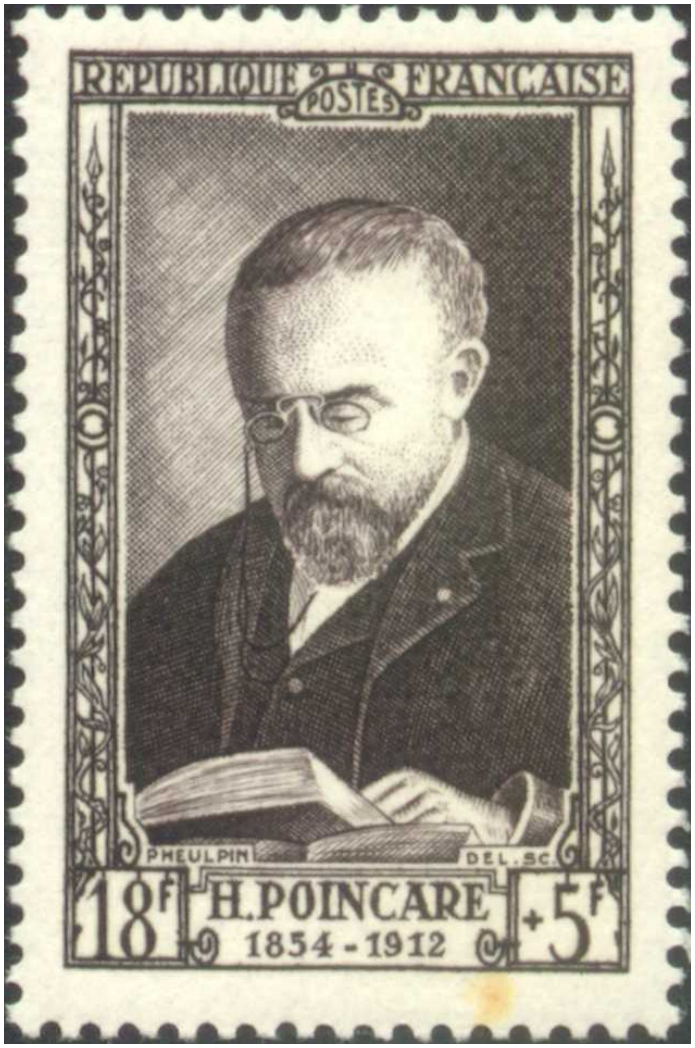
Dio esiste perché la matematica è non contraddittoria, e il diavolo esiste perché non possiamo dimostrarlo. (H. Weyl)

Gödel: (AR) è consistente con G.

Gentzen: dimostrazione per induzione transfinita della non contraddittorietà dell'aritmetica.

Galileo: … un esempio della più solenne fallacia che sia tra tutte le fallacie, cioè quella che prova *ignotum per ignotius*.

H. Poincaré (1854-1912)



Voilà purquoi les axiomes de M. Zermelo ne sauraient me satisfaire. Non seulement ils ne me semblent pas évidents, mais quand on me demandera s'ils sont exemptes de contradiction, je ne saurai que répondre.

L'auteur a cru éviter le paradoxe du plus grand cardinal, en s'interdisant toute spéculation en dehors de l'enceinte d'une Menge bien close; il a cru éviter le paradoxe de Richard … .

Mais s'il a bien fermé sa bergerie, je ne suis pas sûr qu'il n'y a pas enfermé le loup.

[Dernières Pensées]

Assioma della scelta

Sia X un insieme non vuoto, e sia $\wp(X)$ l'insieme delle parti di X; allora esiste un'applicazione f : $\wp(X) \to X$ tale che per ogni $Y \neq Ø$, $Y \in \wp(X)$ si ha che $f(Y) \in Y$.

f "sceglie" da ogni Y un suo elemento.

Un insieme non misurabile (Vitali)

$E = [0, 1)$

$x' \sim x$ se $x' - x \in Q$.

Da ogni classe di equivalenza $[x]$ “scegliamo” un rappresentante x_0, ottenendo un insieme di scelta E_0.

Se $r \in Q$, definiamo i traslati di E_0 come

$E_r = \{y : y = x_0 + r \ (\mathrm{mod}\ 1),\ x_0 \in E_0\}$.

Se E_0 fosse misurabile, tutti gli E_r avrebbero la stessa misura.

Ma $E = \cup_r E_r$, e per il teorema della additività numerabile dovrebbe essere $m(E) = 1 = \Sigma_r\, m(E_r) = \Sigma_r\, m(E_0)$,

impossibile sia che sia $m(E_0) = 0$, sia che $m(E_0) > 0$.

Paradosso di Banach-Tarski

Paradosso di Banach-Tarski (1)

Equidecomponibilità: è la relazione di equivalenza X ~ Y così definita:

X è equidecomponibile con Y se esistono n sottoinsiemi disgiunti X_k di X e n rototraslazioni r_k tali che $X = \cup X_k$ e $Y = \cup r_k (X_k)$.

Paradosso di Banach-Tarski: Ogni palla B in R^3 è equidecomponibile con due suoi sottoinsiemi U e V propri e disgiunti.

($B = U \cup V$, $U \cap V = \emptyset$, ma anche $U \sim B \sim V$)

ovvero in gergo: Ogni palla in R^3 è "paradossale per isometrie".

Forma forte:

due qualsiasi insiemi di dotati di punti interni sono equidecomponibili.

Paradosso di Banach-Tarski (2)

Decomposizioni paradossali.

G = gruppo che agisce su un insieme X.

Def.: $E \subset X$ si dice G - paradossale se, per m, n interi positivi esistono sottoinsiemi disgiunti di E, U_i, $1 \le i \le m$, V_k, $1 \le k \le n$, ed altrettanti elementi g_i , h_k di G, tali che

$E = (\cup U_i) \cup (\cup V_k)$, ma anche $E = \cup g_i(U_i)$ ed $E = \cup h_k(V_k)$

F = gruppo libero di rango n = gruppo (non commutativo) generato da n elementi indipendenti.

Nessun prodotto non banale si riduce all'identità.

Possiamo ritenere tutte le "parole" di F ridotte, eliminando le coppie di xx^{-1} consecutivi.

Paradosso di Banach-Tarski (3)

Passo 1 Un gruppo libero F di rango 2 è F - paradossale.

W(x) = l'insieme delle parole (ridotte) che finiscono a sinistra (= iniziano) con x.

$F = \{ 1 \} \cup W(a) \cup W(a^{-1}) \cup W(b) \cup W(b^{-1})$

$F = W(a) \cup aW(a^{-1})$ cioè $g_1 = 1$, $g_2 = a$,

(infatti $aW(a^{-1})$ contiene tutte le parole che NON cominciano per a)

e analogamente $F = W(b) \cup b\,W(b^{-1})$

Paradosso di Banach-Tarski (4)

Passo 2 Esistono due rotazioni {a, b} di SO(3) indipendenti.

Passo 3 (Hausdorff). Esiste un sottoinsieme numerabile D della superficie sferica S^2 tale che $(S^2 \setminus D) \sim (S^2 \setminus D) \cup (S^2 \setminus D)$.

Dim.: dato il sottogruppo F (libero) di rotazioni indipendenti, di rango 2, generato da a e b, sia

D = {punti fissi per una rotazione $r \neq 1$ di F}:

D è numerabile, come lo è F.

Sia $p \in S^2 \setminus D$: orbita di p è $F(p) = \{q \mid q = r(p), \text{ con } r \in F\}$.

Due orbite o sono disgiunte o coincidono $\Rightarrow$

F(p) sono classi di equivalenza e generano una partizione di $S^2 \setminus D$.

Paradosso di Banach-Tarski (5)

Da ogni orbita scegliamo (con Assioma Scelta!) un rappresentante, e sia M il loro insieme. Poniamo:

$U_1 = W(a)M$, $U_2 = W(a^{-1})M$,

$V_1 = W(b)M$, $V_2 = W(b^{-1})M$, $\Rightarrow$

$S^2 \setminus D = U_1 \cup U_2 \cup V_1 \cup V_2$, con unione disgiunta, ma anche

$S^2 \setminus D = U_1 \cup aU_2$ $\qquad$ $S^2 \setminus D = V_1 \cup bV_2$

Passo 4 (di assorbimento): D numerabile $\subset S^2 \Rightarrow S^2 \sim S^2 \setminus D$

dunque S è paradossale.

Passo 5: B è paradossale (per omotetia).

Assioma della scelta (variazioni)

Lemma di Zorn: Sia P un insieme parzialmente ordinato tale che ogni suo sottoinsieme $\neq \emptyset$ totalmente ordinato ammetta un confine superiore. Allora P ha almeno un elemento massimale.

Teorema del buon ordinamento: Ogni insieme può essere bene ordinato.

Teorema di Hausdorff: Ogni insieme parzialmente ordinato ha un sottoinsieme parzialmente ordinato massimale.

Ogni spazio vettoriale ha una base.

Ogni prodotto infinito di insiemi non vuoti è non vuoto.

Teorema di Hartogs: Due insiemi possono sempre essere confrontati (legge di tricotomia).

Assioma della scelta (fine)

Goedel (1938): (AS) consistente con gli altri assiomi di ZF

Cohen (1963): (AS) indipendente dagli altri assiomi di ZF

Alternative?

Solovay: (assioma di misurabilità): ogni insieme è misurabile

Ipotesi del continuo
Ipotesi generalizzata del continuo

$c = 2^{\aleph_0}$ = cardinalità dei reali

$c = \aleph_1$?

(IC): $\aleph_1 = 2^{\aleph_0}$.

(IGC): $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$.

Gödel: (IGC) consistente con G

Cohen: (AS) non implica né (IC) né (IGC) e neppure i loro contrari

Sierpinski: (IGC) implica (AS)

Solovay: (IC) non implica (AS);

Solovay: (IC) e (AS) non implicano (IGC)

Le serie di Goodstein (1)

Sviluppo di un numero n in base k = rappresentazione di n mediante un “polinomio” nella “variabile” k,

a coefficienti < k

ed esponenti qualsiasi.

$$266 = 2^8 + 2^3 + 2^1$$

Sviluppo di un numero n in base k iterata =

rappresentazione mediante un “polinomio” in k, con esponenti ancora espressi come polinomi.

Ha coefficienti ed esponenti < k

$$266 = 2^{2^{2+1}} + 2^{2+1} + 2$$

Le serie di Goodstein (2)

Dilatazione $d_k(n)$: sostituire k+1 a k in ogni occorrenza

$$d_2(266) = 3^{3^{3+1}} + 3^{3+1} + 3$$

Successione di Goodstein di seme n:

$g_1(n)$ = n (in base 2 iterata)

e per ricorrenza, per k > 1:

$g_k(n) = d_k(g_{k-1}(n)) - 1$

$$G_2(266) = 3^{3^{3^1+1}} + 3^{3^1+1} + 2.$$

Le serie di Goodstein (3)

$g_4(2) = 0$, $g_6(3) = 0$, ma

$g_1(4) = 4$,

$g_2(4) = d_2(2^2) - 1 = 3^3 - 1 = 26$,

$g_3(4) = d_3(2 \cdot 3^2 + 2 \cdot 3 + 2) - 1 = 2 \cdot 4^2 + 2 \cdot 4 + 2 - 1 = 41$,

$g_4(4) = d_4(2 \cdot 4^2 + 2 \cdot 4 + 1) - 1 = 2 \cdot 5^2 + 2 \cdot 5 + 1 - 1 = 60$,

$g_5(4) = d_5(2 \cdot 5^2 + 2 \cdot 5) - 1 = 2 \cdot 6^2 + 2 \cdot 6 - 1 = 83$,

eppure raggiunge lo zero dopo $3 \cdot 2^{402653211} - 2$ passaggi,

un numero che ha “solo” centotrentamilioni di cifre in scrittura decimale.

E siccome $g_2(266)$ ha 38 cifre, $g_3(266)$ ne ha 616, $g_4(266)$ ne ha circa 10000…

la successione raggiunge lo stesso lo zero!

<u>Teorema di Goodstein (1944)</u>:

Qualsiasi sia il numero iniziale n scelto, la successione di Goodstein $g_k(n)$ assume in un numero finito di passi il valore zero.

La dimostrazione di questo teorema fa uso degli ordinali transfiniti, mediante una "superdilatazione" in cui si mette ω al posto di k.

$$D_2(266) = \omega^{\omega^{\omega+1}} + \omega^{\omega+1} + \omega$$

e del fatto che ogni successione strettamente decrescente di ordinali raggiunge lo zero in un numero finito di passi.

Teorema di Kirby – Paris (1981)

È impossibile dimostrare il teorema di Goodstein per ricorsione.

... e infine per rintracciarmi ...

… e ricevere la copia powerPoint di queste diapositive ...

Claudio Citrini

Dipartimento di matematica “F. Brioschi”

del Politecnico di Milano

claudio.citrini@polimi.it

fds.mate.polimi.it

… mentre se volete rintracciarmi in libreria:

(per scrivermi su questi argomenti mettete nel subject “i-mail”)