La ribellione del Numero

π = 3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706798214808651328230664709384460955058223172535940812848111745028410270193852110555964462294895493038196442881097566593344612847564823378678316527120190914564856692346034861045432664821339360726024914127372458700660631558817488152092096282925409171536436789259036001133053054882046652138414695194151160943305727036575959195309218611738193261179310511854807446237996274956735188575272489122793818301194912983367336244065664308602139494639522473719070217986094370277053921717629317675238467481846766940513200056812714526356082778577134275778960917363717872146844090122495343014654958537105079227968925892354201995611212902196086403441815981362977477130996051870721134999999837297804995105973173281609631859502445945534690830264252230825334468503526193118817101000313783875288658753320838142061717766914730359825349042875546873115956286388235378759375195778185778053217122680661300192787661119590921642019893809525720106548586327886593615338182796823030195203530185296899577362259941389124972177528347913151557485724245415069595082953311686172785588907509838175463746493931925506040092770167113900984882401285836160356370766010471018194295559619894676783744944825537977472684710404753464620804668425906949129331367702898915210475216205696602405803815019351125338243003558764024749647326391419927260426992279678235478163600934172164121992458631503028618297455570674983850549458858692699569092721079750930295532116534498720275596023648066549911988183479775356636980742654252786255181841757467289097777279380008164706001614524919217321721477235014144197356854816136115735255213347574184946843852332390739414333454776241686251898356948556209921922218427255025425688767179049460165346680498862723279178608578438382796797668145410095388378636095068006422512520511...

Uno, due ... pochi, tanti

La presenza nei linguaggi più antichi di forme numerali diverse da singolare e plurale suggerisce che la mancanza dei numeri venisse sopperita a livello linguistico.

Il duale

Greco antico, (usato spesso in Omero, poco in Attico, gia perso nelle κοινή alessandrina)

... ὅ ἂν φαίνηται νῷν περί τε τούτων καὶ περὶ τῶν ἄλλων ἄριστον. (Platone, Simposio)

... quello che parrà più giusto a noi in questa e in altre questioni.

Socrate si riferisce a sè e ad Alcibiade (che lo stava "corteggiando") in questo caso "noi" è proprio "noi due" (se fosse stata un'orgia avrebbe usato ἡμῖν invece che νῷν).

Anche l' Accadico (la lingua semitica degli antichi abitanti della Mesopotamia) aveva il duale e da lì è passato all'Arabo

Arabo (duale ancora usato ma confuso col plurale nella lingua parlata) ad esempio

Mujahid	singolare	مجاهد
Mujahidun	plurale nominativo	مجاهدون
Mujahidin	plurale accusativo	مجاهدين
Mujahidan	duale nominativo	مجاهدان

Ebraico, Gaelico, Lingue eschimesi

Lo Sloveno è più complicato c’è anche il numero collettivo.

In altre lingue esisteva anche il triale e il paucale.

Sassi e Pecore

Sorge il problema di CONTARE

un sasso <-> una pecora, due sassi <-> due pecore, ...

Un sasso per ogni pecora (anche senza sapere il nome dei numeri)

Calculus

I numeri cardinali: corrispondenza biunivoca

UNO è la proprietà in comune a tutti gli insiemi con un solo elemento

DUE è la proprietà in comune a tutti gli insiemi con due elementi

...

Una coppia di insiemi ha lo stesso numero di elementi se questi possono essere messi in corrispondenza biunivoca

ZERO è il numero di elementi dell'insieme vuoto. E' un'astrazione apparsa tardi (verso il 1000) ma come sensazione concreta era nota anche agli antichi (essere senza soldi, senza vino, senza marito, senza ragazza, senza testa ...)

Le operazioni sugli insiemi sono difficili da definire e maneggiare.

I numeri ordinali: uno dopo l'altro

Zero, uno, due, tre, quattro, cinque, ...

Il nome dei numeri in forma algoritmica (il concetto di successore)

Anche un bambino può imparare a contare e sa leggere 4.564.965 e dire il suo successore

Operazioni ricorsive, facili da maneggiare, basta saper fare il successore e il predecessore.

Addizione

$$\begin{cases} a+0=a, \\ a+b=(a+1)+(b-1), \quad b>0 \end{cases}$$

Moltiplicazione

$$\begin{cases} a\times 1=a, \\ a\times b=a(b-1)+a, \quad b>1 \end{cases}$$

Elevamento a potenza

$$\begin{cases} a^0=1\,, & a>0 \\ a^b=a^{b-1}\times a, & b>0 \end{cases}$$

La matematica è una costruzione o una scoperta?

Difatti la proposizione: “il secondo e il terzo numero presi insieme fanno il quinto numero” è vera per arbitrio di quelli che per loro volontà e secondo la legge del linguaggio hanno chiamato un certo numero secondo e un altro terzo, un altro ancora quinto della serie; la legge è un ordine del legislatore; e l’ordine è una dichiarazione di volontà. (Hobbes)

successore(successore(zero)) più successore(successore(successore(zero)) fa

successore(successore(successore(successore(successore(zero)))))

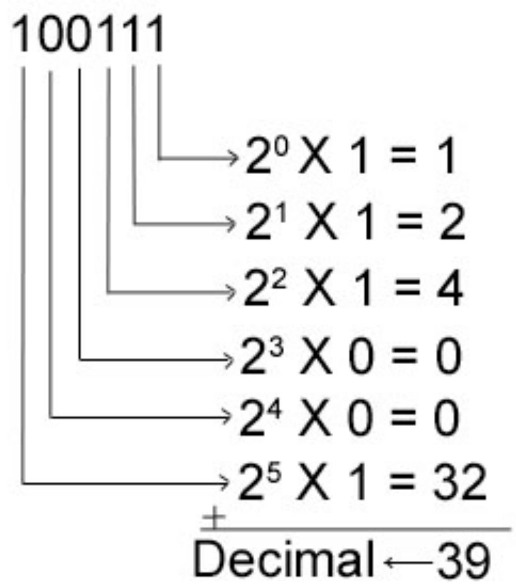
succ(succ(0)) + succ(succ(succ(0) = succ(succ(succ(succ(succ(0)))))

2+3 = 5

(il concetto è lo stesso sia che lo leggiate in italiano o tedesco o in francese)

La scelta dei nomi è libera ma il teorema è bloccato

Il concetto di codifica



Codifica binaria dei numeri interi

Praticamente tutta la cultura si basa sulla codifica

- nomi - parole come codifica di concetti,
- segni come codifica di parole
- bit come codifica di stringhe
- stringhe come codifica di parole - numeri - concetti - immagini - oggetti

Gödelizzazione

Si tratta di una codifica effettiva che porta a far corrispondere un insieme contabile con i numeri naturali. Vediamo due semplici esempi.

Codifica delle stringhe

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
λ	**A**	**B**	**AA**	**AB**	**BA**	**BB**	**AAA**	**AAB**	**ABA**	**ABB**	**BAA**	**BAB**	**BBA**	**BBB**	**AAAA**

Codifica delle coppie

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
(0,0)	(0,1)	(1,0)	(0,2)	(1,1)	(2,0)	(0,3)	(1,2)	(2,1)	(3,0)	(0,4)	(1,3)	(2,2)	(3,1)	(4,0)	(0,5)

$$
\begin{array}{cccccc}
(0,0) & (0,1) & (0,2) & \cdots & (0,n) & \cdots \\
(1,0) & (1,1) & (1,2) & \cdots & (1,n) & \cdots \\
(2,0) & (2,1) & (2,2) & \cdots & (2,n) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
(n,0) & (n,1) & (n,2) & \cdots & (n,n) & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{array}
$$

Numeri naturali ed estensioni

Isomorfismo tra ordinali e cardinali finiti $\rightarrow$ Numeri interi naturali

0	cardinalità dell'insieme vuoto	0	$\emptyset$
1	gli insiemi con un elemento	il successore di 0	$\{\emptyset\}$
2	gli insiemi con 2 elementi	il successore di 1	$\{0,1\}=\{\emptyset,\{\emptyset\}\}$
3	gli insiemi con 3 elementi	il successore di 2	$\{0,1,2\}=\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}$

Visione costruttiva ed esistenziale

Visione insiemistica - esistenziale.

Estensione dei numeri dai naturali ai complessi per chiusura rispetto a classi di operazioni.

- Numeri naturali. (chiusura rispetto al successore)

  0, 1, 2, 3, 4, ...

- Interi relativi (chiusura rispetto alla differenza)

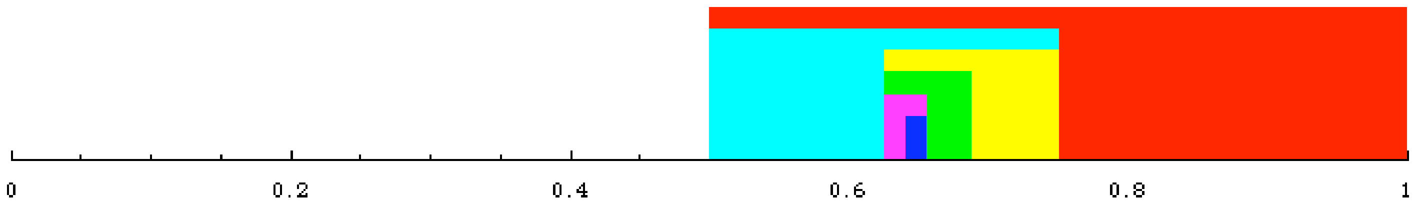
  -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, ...

- Numeri razionali (chiusura rispetto alla divisione)

  0, 1, 1/2, 11/3, 5/6, 12/37, ...

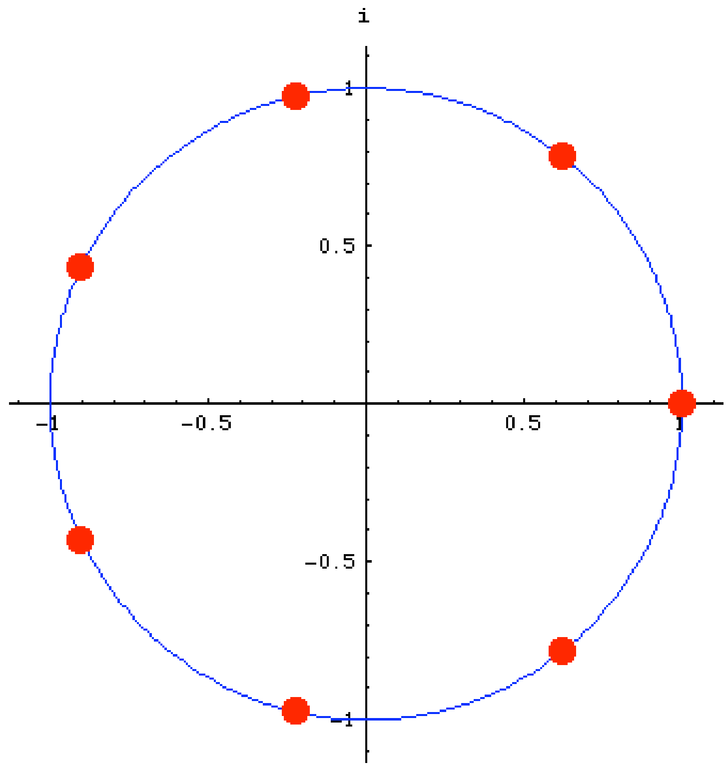
- Numeri reali (corrispondenza biunivoca con i punti della retta)

  0.101001...



- Numeri complessi (chiusura rispetto alla estrazione di radice)

$x^7 - 1 = 0$



Le radici settime dell'unità nel piano complesso

Nel piano complesso vale il Teorema fondamentale dell'Algebra: ogni equazione polinomiale di grado n ha n soluzioni.

Costruzione operativa (informatica)

- Naturali
- Relativi -> Naturale + segno
- Razionali -> {Relativo, Naturale-{0}}
- Reali -> Rappresentazione binaria infinita
- Complessi -> {Reale, Reale}

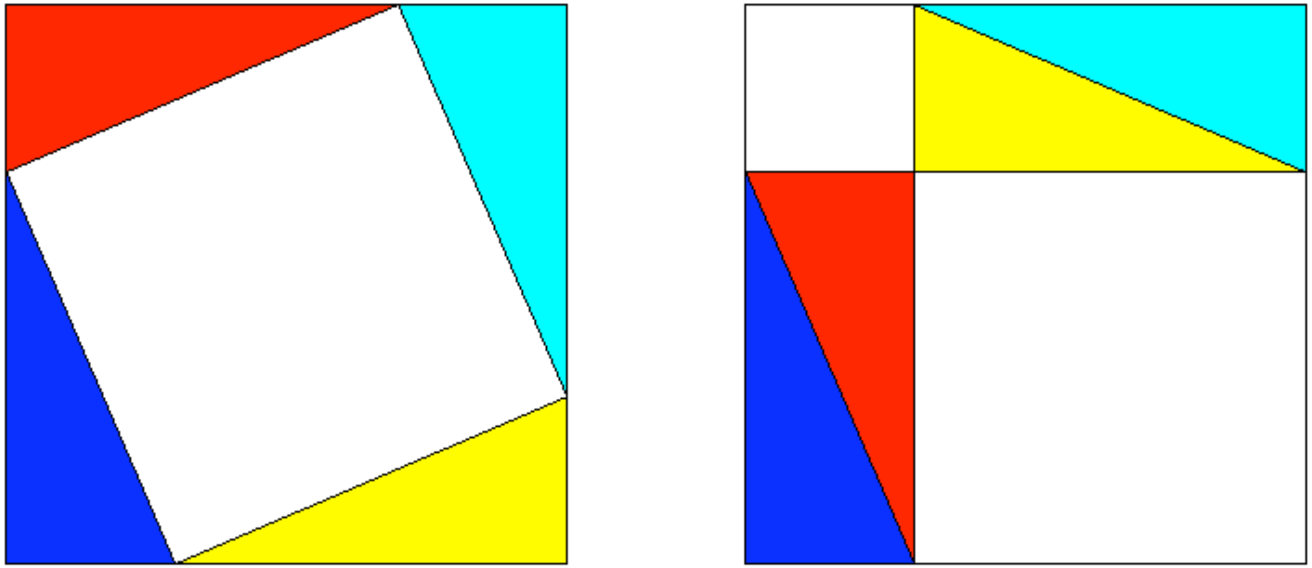
Omomorfismi tra elementi corrispondenti

- 1+2 = 3
- (+1) + (+2) = (+3)
- 1/1 +2/1 = 3/1
- 1.0 + 2.0 = 3.0
- (1+ 0 i) + (2+0 i) = (3+ 0 i)

I matematici possono ignorare i tipi, gli informatici no.

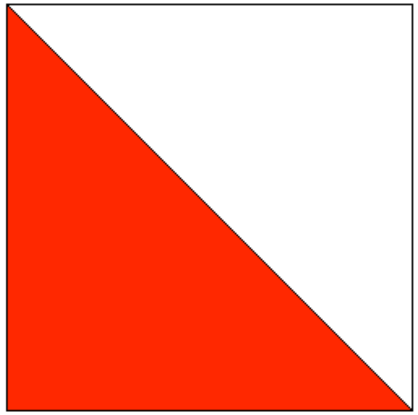
I numeri irrazionali: numeri reali non esprimibili come rapporto di interi

Teorema di Pitagora in forma “visiva”, (concentriamoci sul triangolo rosso)



Il quadrato costruito sull’ipotenusa è uguale alla somma dei quadrati costruiti sui cateti.

Grazie al Teorema di Pitagora si dimostra che il rapporto tra la diagonale e il lato del quadrato è uguale alla radice di due ($d^2 = l^2 + l^2$ -> $d^2 = 2l^2$ -> $(d/l)^2 = 2$)



I pitagorici avevano identificato il numero con la geometria; l'esistenza dei rapporti incommensurabili (conseguenza del Teorema di Pitagora) annullò questa identificazione. L'esistenza dei numeri irrazionali contraddiceva non solo le convinzioni filosofiche dei pitagorici, ma metteva anche in crisi il concetto di infinito della filosofia greca; non c'è da meravigliarsi perciò del fatto che fu proibito ai membri della setta di rivelare ad altri queste scoperte considerate blasfeme e sconcertanti, ma Ippaso da Metaponto divulgò il segreto.

Proclo, a questo proposito, in uno scolio del X libro degli elementi scrive:

> I pitagorici narrano che il primo divulgatore di questa teoria fu vittima di un naufragio; e parimenti si riferivano alla credenza secondo la quale tutto ciò che è irrazionale, completamente inesprimibile e informe, ama rimanere nascosto; e se qualche anima si rivolge ad un tale aspetto della vita, rendendolo accessibile e manifesto, viene trasportata nel mare delle origini, ed ivi flagellata dalle onde senza pace.

Secondi altri Ippaso fu semplicemente buttato a mare con una pietra al collo ...

I numeri algebrici

La radice di 2 è solo un esempio di numero irrazionale algebrico. E’ infatti soluzione dell’equazione $x^2-2 = 0$.

Le soluzioni reali di equazioni polinomiali a coefficienti interi sono detti numeri algebrici.

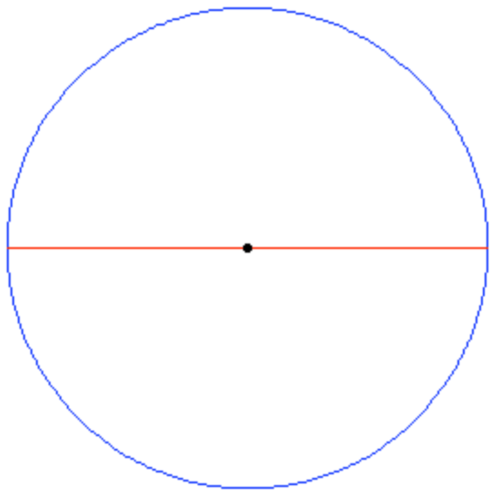
I numeri trascendenti

I numeri irrazionali non algebrici non sono esprimibili in termini finiti neppure in modo implicito.

Pigreco

$\pi = 3.141592653589793238462643383279502884197169399375105820974944592\ldots$

rapporto tra circonferenza e diametro



La costante e di Eulero

e = 2.71828182845904523536028747135266249775724709369995957496696...

è più difficile da definire di π ma non meno importante.

$$e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$$

oppure

$$e = 1 + \frac{1}{2} + \frac{1}{2 \times 3} + \frac{1}{2 \times 3 \times 4} + \ldots$$

vale anche la relazione fondamentale

$$\frac{d}{dx} e^x = e^x$$

La relazione “divina” di Eulero lega e, π e i (la radice quadrata di -1)

$$e^{-i\pi} = -1$$

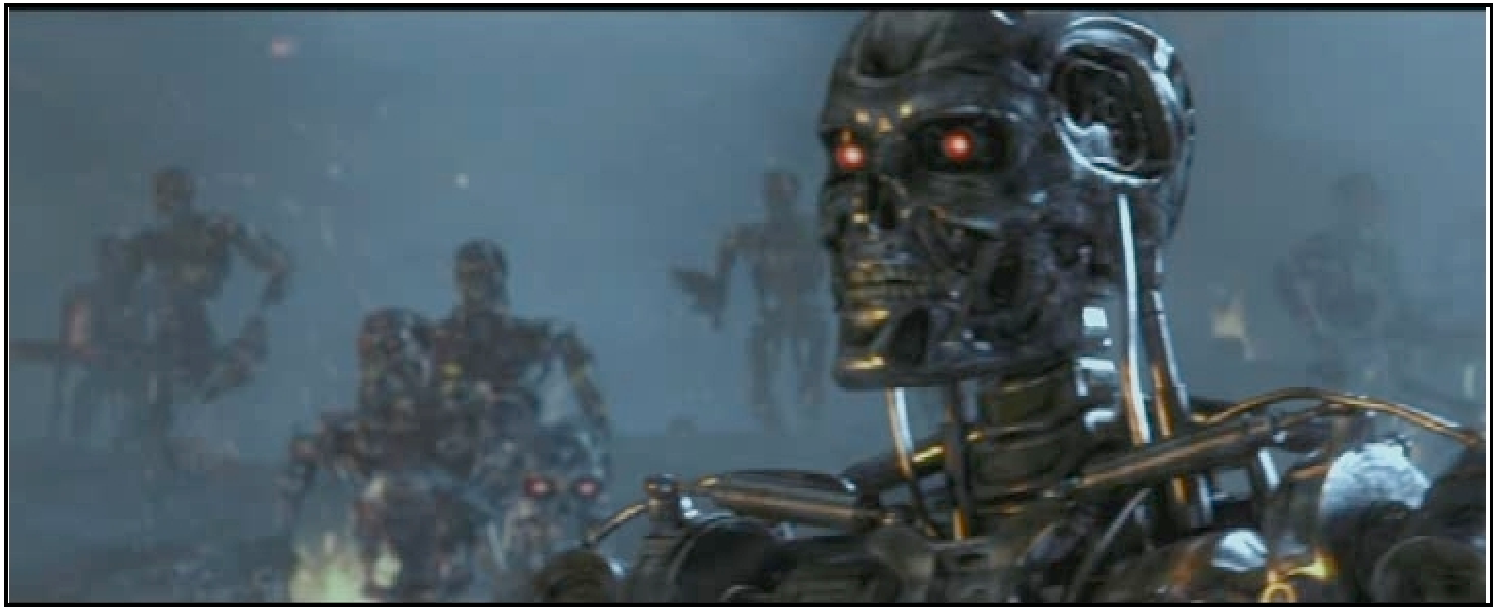
Paradossi numerici

Paradosso di Berry

`Il più piccolo intero non definibile con meno di 62 caratteri`

Questa definizione ha esattamente 61 caratteri!

Come le macchine di Terminator anche le formule si ribellano al loro creatore.



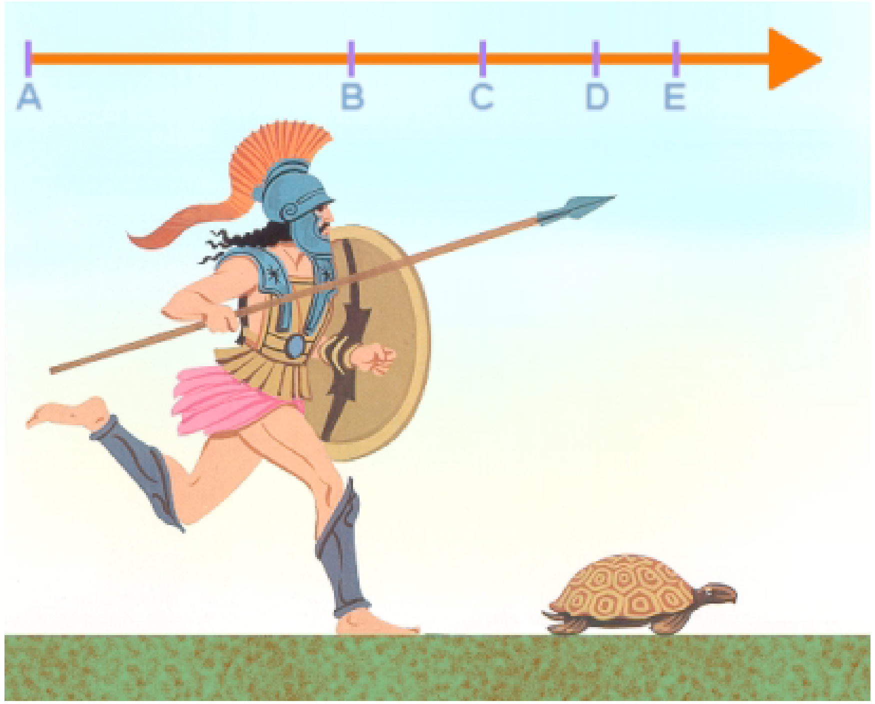
Infinito e Infiniti

Il concetto di infinito è sempre stato difficile da digerire e porta in sé molte sorprese.

Horror infiniti nella filosofia classica

- Achille e la tartaruga (paradosso di Zenone)

Achille non raggiungerà mai la tartaruga, se questa ha un vantaggio! Achille infatti dovrà prima di tutto raggiungere il punto in cui si trovava la tartaruga al momento della partenza. Questa però si sarà a questo punto spostata in un altro punto più avanti, sia pure di poco. Achille dovrà quindi raggiungere questa nuova posizione, mentre di nuovo la tartaruga avrà compiuto però un nuovo piccolo passo… e così all’infinito.



- Infinito in potenza (dimostrazione di Euclide che non esiste il massimo primo)

I numeri primi sono quei numeri che non possono essere scomposti in prodotto di fattori minori

A = {2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... 37,... 317, ...}.

I numeri primi sono il materiale attraverso cui dalla moltiplicazione, si costruiscono tutti i numeri (Teorema fondamentale della Aritmetica). Per esempio si ha 666=2 3 3 37. Ogni numero che non è primo è divisibile per almeno un numero primo (tipicamente per molti). Dimostriamo che esistono infiniti numeri primi e cioè che la successione A non termina mai.

Supponiamo che A abbia fine e che {2, 3, 5, …, p} rappresenti la successione completa dei numeri primi (per cui p risulta il massimo numero primo). Con questa ipotesi consideriamo il numero q definito dalla formula q = (2 3 5 … p)+1. E' evidente che q non è divisibile per nessuno dei numeri 2, 3, 5,…, p, perché il resto della divisione per ognuno di questi numeri sarà sempre 1. Ma, allora o q stesso è un numero primo, oppure esso è divisibile per qualche primo che supera tutti quelli di A. Questo contraddice l'ipotesi che non esista un numero primo maggiore di p, e perciò l'ipotesi che A abbia fine è falsa.

N.B. Euclide non cerca di dimostrare che i primi sono infiniti ma che non ne esiste uno più grande di tutti gli altri

- Infinito in atto (un segmento di retta con infiniti punti)

  E' impossibile che l'infinito sia in atto (Aristotele)

  La natura evita ciò che è infinito poiché l'infinito è privo di quella completezza e finalità verso cui la natura è costantemente tesa (Aristotele)

  Dio non può creare qualcosa di assolutamente infinito (Tommaso d'Aquino)

Gli scolastici non ammettevano una successione infinita di cose una più grande dell'altra (quello che segue è un elegantissimo esempio di latino medievale).

> Nam potest cogitari esse aliquid quod non possit cogitari non esse; quod maius est quam quod non esse cogitari potest. Quare si id quo maius nequit cogitari, potest cogitari non esse: id ipsum quo maius cogitari nequit, non est id quo maius cogitari nequit (Anselmo, Proslogion, cap III).

> > Infatti si può pensare che esista qualcosa che non si può pensare non esistente; ma questo è maggiore di ciò che si può pensare non esistente. Dunque, se ciò di cui non può pensarsi nessuna cosa maggiore può essere pensato non esistente, ciò di cui non può pensarsi nessuna cosa maggiore non è ciò di cui non può pensarsi nessuna cosa maggiore.

Anselmo aveva il concetto di max ma non quello di sup.

Una definizione di Infinito

Un insieme è infinito se può essere messo in corrispondenza biunivoca con una sua parte propria

Esempio: i numeri interi sono esattamente tanti quanti i numeri pari

```
1  2  3  4  5  6  7  8  9 10 11 12 ...
2  4  6  8 10 12 14 16 18 20 22 24 ...
```

Potenza del numerabile

La cardinalità degli insiemi che si possono mettere in corrispondenza biunivoca con gli interi.

E' importante distinguere tra numerabile e algoritmicamente numerabile

- i programmi che terminano sono algoritmicamente numerabili
- i programmi che non terminano sono numerabili ma non algoritmicamente numerabili

Potenza del Continuo

I numeri reali non sono numerabili. Dimostrazione diagonale, per assurdo.

Usiamo la rappresentazione decimale e supponiamo di averli ordinati

```
1   0,2823066470938446095505822317253594081284 81...
```

1 0,282306647093844609550582231725359408128481...

2 0,385211055596446229489549303819644288109756...

3 0,560827785771342757789609173637178721468440...

...

n 0,5 ... 719310100031378387528865875332083 8...

...

Costruiamo un numero che ha nella i-esima posizione una cifra diversa dalla i-esima cifra dell'i-esimo numero (escludendo 0 e 9). e

0,371 ... 1 ...

Tale numero è irrazionale, ammette una rappresentazione unica e non è nella lista perché differisce di almeno una cifra da tutti quelli enumerati.

Esempi di insiemi numerabili

- I numeri naturali
- Gli interi relativi, i numeri razionali, i numeri algebrici;
- Le stringhe su un alfabeto finito,
- I programmi, i teoremi, le dimostrazioni
- I possibili racconti

Esempi di insiemi con la potenza del continuo

- I numeri reali, i numeri trascendenti
- I punti di un segmento, di una retta, gli angoli, i quadrati.
- I punti del piano, dello spazio, di uno spazio n-dimensionale
- Le funzioni dagli interi a {0,1}; le funzioni dagli interi agli interi
- I possibili linguaggi

Numeri cardinali transfiniti