Appunti del corso

Matematiche Elementari da un Punto di Vista Superiore: Aritmetica

tenuto dal Prof. Pietro Di Martino

Università di Pisa - Anno Accademico 2011/2012

Michele Santa Maria

Indice

Introduzione

Questo testo è ricavato dagli appunti da me presi durante il corso *Matematiche Elementari da un Punto di Vista Superiore: Aritmetica*, tenuto dal professor Pietro Di Martino nell'anno accademico 2011/12 all'Università di Pisa.

Nel corso degli appunti ho lasciato come esercizi quelle verifiche che in classe sono state lasciate da fare autonomamente a casa e che risultano prove non troppo complesse o comunque di tipo meccanico. Quegli esercizi che sono stati lasciati e che hanno invece richiesto uno sforzo maggiore li ho riportati come osservazioni dimostrate o esempi.

Prego chiunque legga questo testo di contattarmi nel caso trovasse alcuni errori nel testo (o anche solo per domande/chiarimenti) all'indirizzo mail: msm139@gmail.com

Capitolo 1

L'importanza di $\mathbb{R}$

1.1 Commensurabilità

Una delle domande principali che ci possiamo fare riguardo i numeri è: **Ma perché serve $\mathbb{R}$?**

Questa domanda è tutt'altro che banale, dato che la formalizzazione vera e propria dei numeri reali avviene storicamente molto tardi, addirittura nel 1800, mentre l'uso di numeri interi o frazionari avviene già in popoli arcaici migliaia di anni prima.

La risposta al "perché serve" la si può in realtà trovare in testi molto antichi e deriva dal fatto che esistono grandezze *incommensurabili*, ovvero che non hanno una "misura comune" tra di loro.

Diciamo che due segmenti r e s, di lunghezze rispettivamente $m(r)$ e $m(s)$ sono *commensurabili* se esistono due numeri naturali h e n tali che $m(s) = h\frac{m(r)}{n}$.
Ovvero posso dividere il segmento r in n pezzetti tutti di stessa lunghezza in modo che h pezzetti messi uno accanto all'altro abbiano la stessa misura di s. Chiameremo poi *misura comune* fra r e s il numero $\frac{m(r)}{n}$

All'inizio si credette che tutti i segmenti fossero commensurabili, ma se così fosse non avremmo alcun bisogno dei numeri Reali. Coloro che scoprirono che non tutti i segmenti erano commensurabili furono i matematici dell'antica Grecia, grazie allo studio delle figure geometriche e alla scoperta, con esse, dei primi numeri irrazionali.

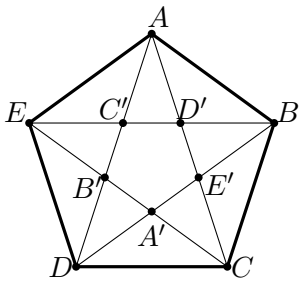
1.2 Incommensurabilità/Irrazionalità

Dati due segmenti di misure a_0 e a_1 (con $a_1 < a_0$) la misura comune veniva cercata con l'**Algoritmo di Euclide** nel modo seguente:
$a_0 = n_1 a_1 + a_2,\ \ a_2 < a_1$
$a_1 = n_2 a_2 + a_3,\ \ a_3 < a_2$
$a_2 = n_3 a_3 + a_4,\ \ a_4 < a_3$
...

L'idea che sta dietro a questo procedimento è che l'algoritmo termina sempre, il che purtroppo non è vero.

La prima idea di irrazionalità (o meglio, di incommensurabilità) non è, come ci si potrebbe aspettare, venuta da $\sqrt{2}$, ma da $\sqrt{5}$, ed è accreditata a **Ippaso Da Metaponto** (**V** AC). Vediamo come:

Prendiamo un pentagono ABCDE:



Nel pentagono abbiamo i triangoli AED e $BE'C$ sono simili, quindi abbiamo la seguente proporzione: $\overline{AD} : \overline{AE} = \overline{BC} : \overline{BE'}$, in cui $\overline{BE'} = \overline{BD} - \overline{DE'} = \overline{BD} - \overline{AE}$.

Possiamo rinominare le lunghezze per ottenere una scrittura più semplice con $\overline{AD} = a_0$ (diagonale), $\overline{AE} = a_1$ (lato), $\overline{BE'} = \overline{BD} - \overline{AE} = a_2 = a_0 - a_1$ (diagonale - lato). In questo modo avremo la proporzione: $a_0 : a_1 = a_1 : a_2$, da cui si ricava

$$\frac{a_0}{a_1} = \frac{a_1}{a_2} \quad \Longleftrightarrow \quad a_0 a_2 = a_1^2$$

Ora quello che vorremmo fare è trovare una catena infinita di uguaglianze, quindi l'idea che ci può venire è di definire una quantità $a_3 = a_1 - a_2$ e verificare se anche per questa vale la relazione

$$\frac{a_1}{a_2} = \frac{a_2}{a_3}$$

Quest'idea in realtà non è casuale: è data dall'osservazione che all'interno del pentagramma disegnato si può trovare un altro pentagramma, e questo processo possiamo portarlo avanti teoricamente fino all'infinito.

Per verificare che la relazione sopra nominata è valida vediamo che

$$\frac{a_1}{a_2} = \frac{a_2}{a_3} \iff a_1 a_3 = a_2^2 \iff a_1^2 - a_1 a_2 = a_2^2 \iff$$

$$\iff a_0 a_2 - a_1 a_2 = a_2^2 \iff (a_0 - a_1) a_2 = a_2^2 \iff a_2^2 = a_2^2$$

Quindi la relazione è vera! Abbiamo allora trovato che

$$\frac{a_0}{a_1} = \frac{a_1}{a_2} = \frac{a_2}{a_3}$$

A questo punto è facile comprendere come continuare: potremo sempre definire una quantità $a_{i+2} = a_i - a_{i+1}$ e creare così una catena infinita del tipo

$$\frac{a_0}{a_1} = \frac{a_1}{a_2} = \frac{a_2}{a_3} = \ldots = \frac{a_i}{a_{i+1}} = \ldots$$

in cui $a_{i+1} < a_i \; \forall i$.

A questo punto se provassimo ad applicare l'algoritmo di Euclide a queste quantità otterremmo:

$a_0 = 1 \cdot a_1 + a_2$
$a_1 = 1 \cdot a_2 + a_3$
$\vdots$
$a_i = 1 \cdot a_{i+1} + a_{i+2}$

Da cui si conclude che *la diagonale e il lato del quadrato non sono commensurabili.*

1.3 $\sqrt{2}$ è Irrazionale

In questo paragrafo sono raccolte molte dimostrazioni diverse dell'irrazionalità di $\sqrt{2}$, che sono state date in momenti diversi durante il corso, ma ho preferito raccogliere tutte in questo capitolo iniziale.

Molte delle dimostrazioni proposte sono abbastanza conosciute e usano metodi che potremmo chiamare "standard", ma ce ne sono altre che si basano su idee molto originali e sono quindi interessanti da leggere e da comprendere.

Teorema. $\sqrt{2}$ *è irrazionale*

Dimostrazione 1: Per assurdo: supponiamo che $\exists p, q \in \mathbb{N}$ coprimi tali che $\sqrt{2} = \frac{p}{q}$.

Allora abbiamo:

$$2 = \frac{p^2}{q^2} \Longrightarrow p^2 = 2q^2 \Longrightarrow p^2 \text{ è pari} \Longrightarrow p \text{ è pari}^1$$

Visto che p è pari mi scrivo $p = 2k$, ed ottengo:

$$4k^2 = p^2 = 2q^2 \Longrightarrow q^2 = 2k^2 \Longrightarrow q^2 \text{ è pari} \Longrightarrow q \text{ è pari}$$

E ciò è assurdo perché li avevo supposti coprimi.

□

Dimostrazione 2: Supponiamo, come prima, che $\exists p, q \in \mathbb{Q}$ coprimi tali che $\sqrt{2} = \frac{p}{q}$. Da ciò ricaviamo che $2q^2 = p^2$.

La grande idea da sfruttare è il passaggio ai moduli: se l'equazione $2q^2 = p^2$ non ha soluzioni in $\mathbb{Z}_n$ non l'avrà nemmeno in $\mathbb{Z}$!

Scegliamo, allora, $\mathbb{Z}_3$, e vediamo se l'equazione di sopra ha soluzioni:

$$\begin{cases} 0^2 \equiv 0\ (3) \\ 1^2 \equiv 1\ (3) \\ 2^2 \equiv 1\ (3) \end{cases} \Longrightarrow \begin{array}{l} \text{l'unica possibilità perché sia vera l'equazione è che } p \equiv q \equiv 0\ (3) \\ \text{ma questo non è possibile perché sono coprimi.} \end{array}$$

□

Dimostrazione 3: Supponiamo, stavolta, che $\exists p, q \in \mathbb{Q}$ non necessariamente coprimi tali che $\sqrt{2} = \frac{p}{q}$, da cui ricavo di nuovo la relazione $2q^2 = p^2$.

Considero l'insieme di tutti i numeri primi a_i che sono contenuti nella fattorizzazione di p o in quella di q, e scrivo i due numeri nel seguente modo:

$$q = \prod_{i=1}^{n} a_i^{\alpha_i} \qquad\qquad p = \prod_{i=1}^{n} a_i^{\beta_i}$$

In cui faccio valere $\alpha_j = 0$ nel caso in cui a_j non sia nella fattorizzazione di q, e lo stesso per quelli di p.

Da queste fattorizzazioni ricavo:

$$2q^2 = p^2 \Longleftrightarrow 2\prod_{i=1}^{n} a_i^{2\alpha_i} = \prod_{i=1}^{n} a_i^{2\beta_i}$$

[1] Attenzione: l'ultima implicazione è meno ovvia delle altre!

Ma l'esponente di 2 per il primo membro è dispari, mentre per il secondo è pari, il che è assurdo.

□

Dimostrazione 4: Dato un qualsiasi polinomio a coefficienti interi, riesco abbastanza facilmente a trovare le radici in $\mathbb{Q}$:

Dato $t(x) = \sum_{i=1}^{n} a_i x^i$, con $a_i \in \mathbb{Z}$, so che $\frac{p}{q}$, con $p, q \in \mathbb{Z}$ coprimi, è radice di $t(x)$ solo se $p|a_0$ e $q|a_n$.

Allora considero il polinomio $t(x) = x^2 - 2$, di cui una radice sappiamo essere $\sqrt{2}$. Se voglio le radici in $\mathbb{Q}$ trovo che: $\frac{p}{q}$ è radice solo se $p|2$ e $q|1$, ovvero se $p = \pm 1, \pm 2$ e $q = \pm 1$.

Ciò vuol dire che le uniche possibili radici razionali sono $\pm 1, \pm 2$, ma $t(x)$ valutato in questi punti non è nullo, quindi $x^2 - 2$ non ha radici razionali.

$$\implies \sqrt{2} \notin \mathbb{Q}$$

□

Dimostrazione 5: Supponiamo, ancora una volta, $\sqrt{2} = \frac{p}{q}$. Se pensiamo a $\sqrt{2}$ come diagonale del quadrato unitario abbiamo di sicuro che $\sqrt{2} > 1 \implies p > q$.

$\implies \exists\, a > 0$ t.c. $p = q + a$.

Da ciò ricavo che $2q^2 = p^2 = (q + a)^2 \implies q^2 = a^2 + 2a \implies q^2 > a^2 \implies q > a$.

Ma allora $\exists\, c > 0$ t.c. $q = a + c$.

Quindi ho $2q^2 = 2(a + c)^2 = p^2 = (2a + c)^2 \implies c^2 = 2a^2 \implies c > a \implies p > q > c > a > 0$.

Dalle relazioni trovate ho che c e a soddisfano $c^2 = 2a^2$, $c > a$ esattamente come succedeva per p e q. Quindi posso rifare tutto il ragionamento con c e a, e creare così una catena infinita discente, il che è assurdo, visto che sono tutti positivi.

□

Facciamo alcune osservazioni sulle dimostrazioni appena fatte:

Le dimostrazioni (1) e (3) sono legate dal **Teorema Fondamentale dell'Aritmetica**, quindi per poterle usare è necessario prima spiegare questo importante principio.

La dimostrazione (5) usa una catena discendente infinita, similmente a come abbiamo fatto nel caso del pentagono del paragrafo precedente.

Le dimostrazioni (3) e (5) non suppongono che p e q siano coprimi, quindi sembrano più generali di altre.

Nella dimostrazione (1) non si capisce bene cosa abbia a che fare la conclusione con la tesi da dimostrare. Inoltre l'enunciato "$\sqrt{2}$ è irrazionale" sembra che non abbia ipotesi, quindi non è chiaro su cosa si vada a fare la dimostrazione per assurdo.

Una interessante conseguenza della dimostrazione (3) è che essa ci dice praticamente che $\mathbb{Q}$ non aggiunge alcuna radice che non fosse già in $\mathbb{N}$.

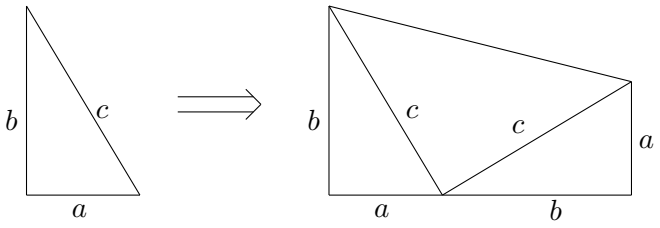
1.4 Il Teorema di Pitagora

Similmente a quanto fatto nel paragrafo precedente riporteremo adesso varie dimostrazioni del **Teorema di Pitagora**.

Teorema. *In un triangolo rettangolo di cateti a e b e ipotenusa c vale la seguente formula:*

$$c^2 = a^2 + b^2$$

Dimostrazione 1: Dato il triangolo rettangolo di lati (a, b, c) costruiamo un trapezio come mostrato in figura:



A questo punto l'area A del trapezio possiamo trovarla in due modi, che dovranno dare poi lo stesso risultato, ovvero:

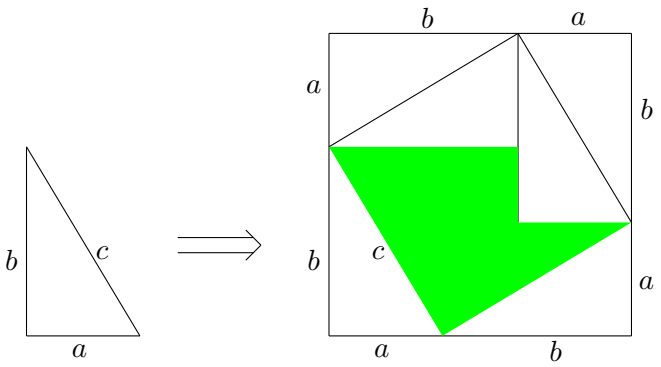
$$A = \begin{cases} \frac{(a+b)^2}{2} \\ \frac{ab}{2} + \frac{ab}{2} + \frac{c^2}{2} \end{cases}$$

Da cui ricavo

$$\frac{(a+b)^2}{2} = ab + \frac{c^2}{2} \quad \Longrightarrow \quad a^2 + b^2 = c^2$$

□

Dimostrazione 2: Dato il triangolo rettangolo di lati (a, b, c) costruiamo come mostrato in figura:



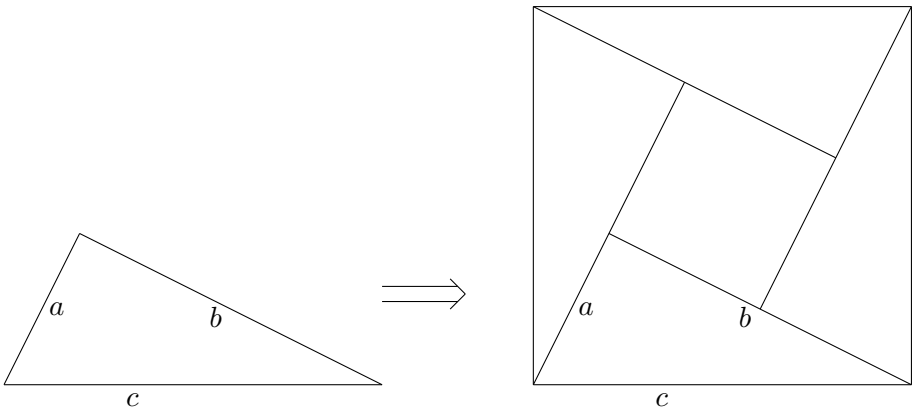
Se osserviamo il poligono colorato all'interno della costruzione possiamo notare che la sua area si può calcolare come l'area del quadrato esterno meno quattro volte l'area del triangolo dato, ovvero $(a+b)^2 - 4\frac{ab}{2} = a^2 + b^2 - ab$.

Ma se ad essa aggiungiamo due volte l'area del triangolo di partenza otteniamo l'area del quadrato interno più piccolo, che è c^2, quindi

$$(a^2 + b^2 - ab) + 2\frac{ab}{2} = c^2 \quad \Longrightarrow \quad a^2 + b^2 = c^2$$

□

Dimostrazione 3: Dato il triangolo rettangolo di lati (a, b, c) costruiamo come mostrato in figura:



In questo caso l'area del quadrato esterno di lato c è uguale a quattro volte l'area del triangolo dato più l'area del quadrato interno di lato $b - a$. Dunque

$$c^2 = 4\frac{ab}{2} + (b-a)^2 = a^2 + b^2$$

□

Capitolo 2

I Numeri Naturali: $\mathbb{N}$

2.1 Definizione di $\mathbb{N}$

Cosa sono i numeri naturali?

Per molti secoli non è stata data una definizione "formale" dei numeri naturali, ma si è più semplicemente detto "a cosa servono": servono a *contare*.

Contare cosa? tutto.

Ma ad un certo punto (in realtà molto tardi, a metà Ottocento) si necessita di una formalizzazione del concetto di $\mathbb{N}$. Per fare ciò **Peano** e **Dedekind** decidono di usare un approccio assiomatico, utilizzando i seguenti enti primitivi:

- il concetto di numero
- la funzione *successore*: $S : \mathbb{N} \longrightarrow \mathbb{N}$
- lo zero

Con cui si definisce $\mathbb{N}$ per mezzo dei seguenti **Assiomi di Peano**:

1. $0 \in \mathbb{N}$
2. $0 \notin S(\mathbb{N})$
3. S è iniettiva
4. Se $\exists\, M \subseteq \mathbb{N}$ tale che $(0 \in M) \wedge (m \in M \Rightarrow S(m) \in M) \Longrightarrow M = \mathbb{N}$

Definizione. Un insieme che verifica la proprietà numero (4) degli Assiomi di Peano si dice *induttivo*

L'ultima proprietà in particolare ci dice che $\mathbb{N}$ non ha sottoinsiemi induttivi propri.

A questo punto sorge spontanea una domanda: ma esiste almeno un insieme che soddisfi tutti questi assiomi?

In realtà l'esistenza di un insieme di questo tipo è equivalente al cosiddetto *Assioma dell'infinito*, che postula l'esistenza di un insieme *infinito*.

Ma a pensarci bene cosa vuol dire *infinito*? Lo definiamo così:

Definizione. Un insieme è detto *infinito* se è in corrispondenza biunivoca con un suo sottoinsieme proprio.

Sul significato di insieme infinito torneremo poi in maniera molto più esaustiva in uno dei capitoli successivi.

Vediamo ora che in effetti postulare l'esistenza di un insieme infinito equivale a postulare l'esistenza di un insieme che soddisfi gli Assiomi di Peano (che chiamiamo per comodità di simboli proprio "$\mathbb{N}$"):

Teorema. $\exists$ A *infinito* $\iff \exists$ $\mathbb{N}$.

Dimostrazione: $\boxed{\Leftarrow}$ $\mathbb{N}$ è infinito poiché è in corrispondenza biunivoca, per esempio, con i numeri pari, che rappresentano un suo sottoinsieme proprio.
$\boxed{\Rightarrow}$ visto che esiste un insieme infinito A abbiamo che $\exists f : A \longrightarrow A$ iniettiva tale che $f(A) \subsetneq A$. Quello che vogliamo fare è "costruire" $\mathbb{N}$:

Prendo[1] $a \in A \setminus f(A)$ e lo chiamo "0".

Considero l'insieme $\mathcal{M} = \{M \subseteq A \mid 0 \in M \text{ e } f(M) \subseteq M\}$. Di sicuro $\mathcal{M} \neq \emptyset$ perchè $A \subseteq \mathcal{M}$, e definisco "$\mathbb{N}$"$=\bigcap_{M \in \mathcal{M}} M$, dove la funzione "successore" è rappresentata da f. □

Nell'insieme dei Numeri Naturali appena definiti è molto utile il **Principio di Induzione**:

$\mathbb{N}$ *non ha sottoinsiemi induttivi propri.*

Questo è uno dei più importanti principi della matematica e può essere utile per dimostrare una proprietà qualsiasi $\mathcal{P}$ basandosi sul seguente ragionamento:

Se chiamo $\mathcal{A} = \{n \in \mathbb{N} \mid \mathcal{P}(n) \text{ è vera } \}$ e riesco a dimostrare che $\mathcal{A}$ è induttivo, allora per il Principio di Induzione ho che $\mathcal{A} = \mathbb{N}$, e dunque la proprietà è valida $\forall n$.

[1] Attenzione! Per fare ciò si necessita dell'Assioma della Scelta!!

2.2 Principio di Induzione

Diamo altre due formulazioni del Principio di Induzione:

$$I_1 = \begin{cases} \mathcal{P}(0) \text{ vera} \\ \forall n(\mathcal{P}(n) \text{ vera } \Rightarrow \mathcal{P}(n+1) \text{ vera}) \end{cases} \quad \Longrightarrow \quad \mathcal{P} \text{ è vera.}$$

$$I_2 = \begin{cases} \mathcal{P}(0) \text{ vera} \\ \forall n(\forall k \leq n \ (\mathcal{P}(k) \text{ vera } \Rightarrow \mathcal{P}(k+1) \text{ vera})) \end{cases} \quad \Longrightarrow \quad \mathcal{P} \text{ è vera.}$$

Possiamo anche dimostrare che le due formulazioni sono equivalenti:

Dimostrazione: $\boxed{I_1 \Rightarrow I_2}$ Basta considerare $\mathcal{Q} = \mathcal{P}(1) \wedge \cdots \wedge \mathcal{P}(n)$, e applicare l'induzione a $\mathcal{Q}$.
$\boxed{I_1 \Leftarrow I_2}$ Sicuramente vera, viste le ipotesi di I_2 rispetto a quelle di I_1. □

Facciamo alcune considerazioni su questo principio:

- è un assioma dell'Aritmetica, non un assioma puramente teorico (come può essere il *ragionamento per assurdo*), quindi non può essere applicato a prescindere dalla teoria.
- non è un metodo per congetturare, ma solo per dimostrare. Questo implica in particolare che devo già avere una teoria da provare.
- può essere usato anche per definire, come vedremo per le operazioni in $\mathbb{N}$.

Esercizio. Provare a dimostrare che $\forall n \in \mathbb{N}$ vale:

$$\sum_{i=1}^{n} i = -\frac{1}{6}n^3 + \frac{3}{2}n^2 - \frac{4}{3}n + 1$$

- Perchè non funziona $\forall n$?
- Per quali n funziona?
- Dove "salta" il passo induttivo?

Esercizio. È vero che il polinomio $n^2 - 79n + 1601$ genera solo numeri primi?
Un polinomio può generare solo numeri primi?

Esercizio. Dimostrare che i *numeri primi di Fermat* $\mathbb{F}_n = 2^{2^n} + 1$ non sono tutti primi.

Esercizio. Determinare il numero massimo di parti in cui n punti scelti in una circonferenza dividono il relativo cerchio quando vengono congiunti a due a due tramite segmenti ($n \geq 2$).

2.2.1 Difficoltà ed Errori

Il principio di Induzione può portarci anche a dimostrazioni assurde se usato in maniera inopportuna, come ad esempio il seguente

Teorema. *Tutti i bambini hanno gli occhi uguali.*

Dimostrazione: Per induzione sul numero di bambini:
$\underline{n = 1}$: c'è solo un bambino, quindi è vera.
$\underline{n \Rightarrow n+1}$: presi $n+1$ bambini so, per ipotesi induttiva, che un qualsiasi sottoinsieme di n di essi ha gli occhi uguali. In particolare questo vale per i primi n e per gli ultimi n, quindi tutti gli $n+1$ bambini hanno gli occhi uguali. □

Esercizio. Cosa c'è che non va in questo teorema? Perchè non si può applicare l'induzione?

Ci sono anche esempi di teoremi giusti, ma il cui caso base è *molto* difficile da dimostrare, come ad esempio il seguente

Teorema (di Piek)**.** *L'area di un poligono privo di lati che si intrecciano e con vertici reticolari (cioè a coordinate intere) è data da:*

$$A = i + \frac{1}{2}c - 1$$

dove i=numero di punti reticolari interni al poligono, c=numeri di punti reticolari sul contorno.

Dimostrazione: per induzione sul numero di lati del poligono:
$\underline{n = 3}$: (**esercizio**)
$\underline{n \Rightarrow n+1}$: dato il poligono $\mathcal{P}$ con n lati, considero una diagonale interna che divida il poligono in $\mathcal{P}_1$ e $\mathcal{P}_2$ di lati $< n$.

Da questa divisione ricaviamo: $A = A_1 + A_2 = (i_1 + \frac{1}{2}c_1 - 1) + (i_2 + \frac{1}{2}c_2 - 1)$.

Valgono, inoltre, queste relazioni:

$$\begin{aligned} i &= i_1 + i_2 + x - 2 \\ c &= c_1 + c_2 - 2x + 2 \end{aligned}$$

dove x rappresenta i punti reticolari sulla diagonale.

Da queste ricaviamo facilmente la tesi: $A = i + \frac{1}{2}c - 1$ □

2.2.2 Maurolico (1575)

Cantor riconosce **Maurolico** come primo fautore del principio di induzione.

Maurolico compila la seguente tabella:

Interi	Pari	Dispari	Triangolari	Quadrati
1	2	1	1	1
2	4	3	3	4
3	6	5	6	9
4	8	7	10	16
5	10	9	15	25
⋮	⋮	⋮	⋮	⋮

E chiama *collaterali* i numeri sulla stessa riga, *precedente* (o *successivo*) un numero che sta nella riga sopra (o sotto) il numero dato.

Con queste definizioni Maurolico riesce a dimostrare alcuni teoremi facendo uso di un ragionamento che sarà poi la base da cui si formalizzerà il vero e proprio Principio di Induzione come noi lo conosciamo (riportiamo solo una delle dimostrazioni):

Teorema. *I numeri dispari sono ottenuti dall'unità e da successive addizioni di 2.*

Teorema. *Ogni intero più il precedente intero è uguale al numero dispari collaterale.*

Dimostrazione: L'intero 2 più l'unità fa l'intero 3, quindi fin qui tutto apposto[2].

Per i casi successivi usiamo il teorema precedente:
5=3+2
7=4+3=5+2
...ed è così possibile continuare fino all'infinito. □

Teorema. *La somma dei primi n dispari è uguale all'n-esimo quadrato.*

Così utilizzato è una forma piuttosto debole e informale rispetto a quello a cui siamo abituati adesso, ma per l'epoca il ragionamento era ben accettato e considerato sufficientemente rigoroso.

2.2.3 Pascal (1654)

In realtà la prima *vera* comparsa dell'induzione è data da **Pascal** nel 1654, che dopo aver definito il *Triangolo Aritmetico* (oggi detto *Triangolo di Pascal*) come quello sottostante:

$$
\begin{array}{ccccccccccc}
 & & & & 1 & & & & & & \\
 & & & 1 & & 1 & & & & & \\
 & & 1 & & 2 & & 1 & & & & \\
 & 1 & & 3 & & 3 & & 1 & & & \\
1 & & 4 & & 6 & & 4 & & 1 & & \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots
\end{array}
$$

[2]Notare che questo è proprio ciò che noi chiameremo "passo base"!

dimostra una proprietà in modo molto più preciso di quanto sia mai stato fatto precedentemente.

Corollario. *In ogni triangolo aritmetico vale la seguente proprietà:*
se due celle sono adiacenti nella stessa riga, allora quella a sinistra sta a quella a destra come il numero di celle a sinistra sta al numero di celle a destra.

Dimostrazione: Per dimostrare questo corollario citiamo le parole di Pascal stesso:

> *Sebbene questa dimostrazione abbia un numero infinito di casi, io darò una piuttosto corta dimostrazione, assumendo due lemmi:*
>
> **Lemma** (che è evidente)**.** *la proposizione è vera nella riga 2*
>
> **Lemma.** *se la proposizione è vera in una riga qualsiasi allora è vera in quella successiva*
>
> *Da questo seguirà che la proposizione è necessariamente vera per tutte le righe:*
> *Nella seconda per il primo lemma, quindi nella terza per il secondo lemma, quindi nella quarta e così via fino all'infinito.*
> *È dunque necessario provare soltanto il secondo lemma. La dimostrazione è basata solo sull'assunzione che la proposizione sia vera nella riga precedente e che ogni cella è uguale alla somma delle due precedenti, che è vero in tutti i casi.*

□

Esercizio. Dimostrare il lemma 2

Osservazione. Sebbene questa sia la prima vera comparsa del principio di induzione come lo conosciamo, dovremo aspettare **De Morgan** (1838) per far si che la procedura già usata da Pascal venga chiamata "Principio di Induzione".

Il tutto verrà poi formalizzato solo da **Peano** (1889) con l'assiomatizzazione di $\mathbb{N}$.

2.3 Operazioni su $\mathbb{N}$

Con il Principio di Induzione definiamo le operazioni su $\mathbb{N}$ a partire da un qualsiasi naturale m:

$$+_m : \mathbb{N} \longrightarrow \mathbb{N} \qquad \begin{cases} +_m(0) = m \\ +_m(S(n)) = S(+_m(n)) \end{cases}$$

$$\cdot_m : \mathbb{N} \longrightarrow \mathbb{N} \qquad \begin{cases} \cdot_m(0) = 0 \\ \cdot_m(S(n)) = \cdot_m(n) + m \end{cases}$$

Invece di scrivere $+_m(n)$ e $\cdot_m(n)$ scriveremo per semplicità $m + n$ e $m \cdot n$, in cui cambia solo la notazione, ma le operazioni sono definite come sopra.

Ma quelle appena date sono buone definizioni? Cioè esistono funzioni del genere? Per rispondere usiamo il seguente

Teorema (di Ricorsione (**Dedekind**, 1888)). *Siano $A \neq \emptyset$, $a \in A$, $g : A \longrightarrow A$. Allora*

$$\exists!\ \varphi : \mathbb{N} \longrightarrow A \text{ tale che } \begin{cases} \varphi(0) = a \\ \varphi \cdot S = g \cdot \varphi \end{cases}$$

Dimostrazione: Dimostriamo innanzitutto l'esistenza di tale funzione, passando poi a dimostrarne l'unicità.

Esistenza: Considero tutti i sottoinsiemi H di $\mathbb{N} \times A$ tali che

$$\begin{cases} (0, a) \in H \\ (n, b) \in H \Longrightarrow (S(n), g(b)) \in H \end{cases}$$

Sicuramente di questi insiemi ne esiste almeno uno perché $\mathbb{N} \times A$ è uno di essi, quindi definiamo $\mathcal{G}$ l'intersezione di tutti questi sottoinsiemi: $\mathcal{G} = \cap H$.

Vorremmo provare che $\mathcal{G}$ è grafico di una funzione $\varphi : \mathbb{N} \longrightarrow A$ tale che $\varphi(0) = a$ e $\varphi \circ S = g \circ \varphi$.

Per fare questo dimostriamo per induzione che $\forall n \in \mathbb{N}\ \ \exists! x \in A$ tale che $(n, x) \in \mathcal{G}$.

$\boxed{n = 0}$ $(0, a) \in H\ \forall H \Longrightarrow (0, a) \in \mathcal{G}$.

Supponiamo per assurdo che $\exists c \in A$ tale che $c \neq a$ e $(0, c) \in \mathcal{G}$.

Ma allora $\mathcal{G} \setminus \{(0, c)\}$ va ancora bene come insieme, quindi $\mathcal{G}$ non è minimale, il che è assurdo perché è l'intersezione di tutti.

$\boxed{n \Rightarrow S(n)}$ So che dato n $\exists! b$ tale che $(n, b) \in \mathcal{G} \Longrightarrow (S(n), g(b)) \in \mathcal{G}$.

Supponiamo di nuovo per assurdo che $\exists c \in A$ tale che $(S(n), c) \in \mathcal{G}$, $c \neq g(b)$. Ma allora di nuovo $\mathcal{G} \setminus \{(S(n), c)\}$ va ancora bene, il che è un assurdo.

Dunque l'esistenza è provata.

Unicità: Supponiamo che $\exists \varphi_1, \varphi_2 : \mathbb{N} \longrightarrow A$ tali che $\varphi_i(0) = a$, $\varphi_i \circ S = g \circ \varphi_i$, e dimostriamo per induzione che queste due funzioni devono coincidere:

$\boxed{n = 0}$ $\varphi_1(0) = a = \varphi_2(0)$, quindi ok.

$\boxed{n \Rightarrow S(n)}$ $\varphi_1(S(n)) = g(\varphi_1(n)) = g(\varphi_2(n)) = \varphi_2(S(n))$, in cui abbiamo usato il passo induttivo nella seconda uguaglianza.

Dunque anche l'unicità è provata. □

Grazie a questo teorema si riescono a dimostrare tutte le proprietà conosciute sulle operazioni di $\mathbb{N}$: associatività, commutatività, etc...

Esercizio. Dimostrare che vale: $a + b = b + a \ \forall a, b \in \mathbb{N}$

Vediamo adesso un'ultimo importantissimo teorema sui Numeri Naturali:

Teorema (di Unicità)**.** *Sia* $(\mathbb{N}', 0', S')$ *una terna soddisfacente gli assiomi di Peano. Allora* $\exists \varphi : \mathbb{N} \longrightarrow \mathbb{N}'$ *bigettiva tale che* $\varphi(0) = 0'$, $S' \cdot \varphi = \varphi \cdot S$

Dimostrazione: Il teorema di ricorsione ci dà tutto apparte la bigettività;

Ma in realtà è del tutto lecito invertire i ruoli di $\mathbb{N}$ ed $\mathbb{N}'$ nel teorema di ricorsione, quindi ho anche la bigettività □

Capitolo 3

Numeri Primi

3.1 Cenni Storici

I numeri primi sono risultati affascinanti già da molti matematici dell'antichità, ma i primi risultati esplicitamente su di esso tardarono molto ad arrivare. Inizialmente questi erano dati solo come pura teoria dei numeri, tant'è che **Tomas Hardy** (1877-1947) disse a tal proposito: "*Sarebbe difficile trovare qualcuno che sia più profondamente appassionato e attratto da qualsiasi cosa di quanto lo sia io per la teoria dei numeri primi*", sostenendo poi che "*La vera matematica è quella che non porta a risultati praticabili*".

Uno dei primi studiosi dei numeri primi è stato **Fermat** (1601-1665), il cosiddetto "Principe dei Dilettanti", passando poi per Padre **Mersenne** che nel 1640 a Parigi smistava le lettere di molti matematici affermati dell'epoca.

Fermat è famoso per aver dato vita a moltissime congetture (alcune vere, altre false) senza darne poi le dimostrazioni, pur sostenendo di averle. Sua è infatti la famosa citazione "*La mirabile dimostrazione di questo fatto purtroppo non rientra nei ristretti margini di questo foglio*".

Più volte si fa vanto di saper dimostrare importanti risultati, riportiamo ad esempio:

> *Tutti i numeri primi misurano infallibilmente una delle potenze meno uno di qualunque progressione data, e l'espressione della detta potenza è sottomultiplo del numero primo dato meno uno. E questa proposizione è generalmente vera per tutte le progressioni e tutti i numeri primi; della qual cosa vi invierei la dimostrazione se non temessi di dilungarmi troppo.*
>
> Fermat - *Lettera a Berry del 18/10/1640*

Quello di cui parla è il **Piccolo Teorema di Fermat**[1], dimostrato da **Eulero** nel 1736, ovvero quasi un secolo dopo!

[1] L'enunciato in termini moderni si riassume in: $a^{p-1} \equiv 1 \pmod{p}$, e fu chiamato "Piccolo Teorema di Fermat per la prima volta da **Hensel** nel 1913.

Questo importante teorema viene usato come test di non primalità di un numero, ed è il primo test di cui siamo a conoscenza. Un metodo per cercare numeri primi è invece il famoso **Crivello di Eratostene** in cui si scrivono tutti i numeri fino ad un certo k e si iniziano ad individuare i primi a partire dal numero 2 procedendo in modo che ogni volta che si incontra un nuovo numero primo si cancellano tutti i suoi multipli, arrivando così ad avere scritto tutti i numeri primi minori o uguali al k scelto.

La prima lista dei numeri primi fino a 100 risale a **Fibonacci** nel XIII secolo, per poi passare alla lista di primi fino a 750 data da **Cataldi** verso la metà del XVI secolo.

Curiosità sui numeri primi:

- Sono infiniti, e questo fatto è stato dimostrato in decine di modi diversi nell'arco dei secoli da diversi matematici, usando spesso metodi estremamente diversi tra loro.
- Preso un naturale k è sempre possibile k numeri consecutivi non primi; Questa proprietà viene chiamata **Deserto dei Numeri Primi**.
- I numeri primi sembrano disposti nei numeri naturali in maniera caotica, nel senso che non è stato ancora trovato una regola che ne determini l'andamento. Su questo concetto si basa molta parte della crittografia moderna.

3.2 Primi di Fermat

I matematici di tutti i tempi hanno cercato formule di qualsiasi tipo che generassero numeri primi. Una formula molto studiata è stata la formula $p_n = a^n + b$, con $a, b \in \mathbb{N} \setminus \{0\}$.

Se proviamo a studiare questa formula con b=1 troviamo $p_n = a^n + 1$. Per far si che esso sia primo ci serve a pari. Dunque il caso più semplice è $p_n = 2^n + 1$.

Si scopre, però, che vale la seguente proprietà:

Proposizione. *Se n ha un fattore dispari $\Longrightarrow p_n = 2^n + 1$ non è primo*

Dimostrazione: Scrivo $n = 2^k d$, con $d > 1$ dispari, ed ho $p_n = 2^{2^k d} + 1$. Se chiamo $x = 2^{2^k}$ vale $p_n = x^d + 1$, che si può facilmente fattorizzare in $(x + 1)t$, per un certo $t \in \mathbb{N}$.

□

Visto che non devo avere fattori pari l'unica possibilità rimasta è

$$\mathbb{F}_n = 2^{2^n} + 1 \quad \longleftarrow \text{ n-esimo } \textbf{Numero di Fermat}$$

I Numeri di Fermat crescono molto rapidamente di grandezza:

$\mathbb{F}_0 = 3$
$\mathbb{F}_1 = 5$
$\mathbb{F}_2 = 17$
$\mathbb{F}_3 = 257$
$\mathbb{F}_4 = 65537$
$\mathbb{F}_5 = 4294967297$
...

Fermat congetturò che $\mathbb{F}_n$ fosse primo $\forall n$, ma non ne era nemmeno sicuro lui stesso, visto che in una lettera a **Pascal** scrisse (parlando di tale congettura): "*Non vi chiederei di lavorare a questo problema se fossi riuscito da solo a risolverlo*".

La confutazione venne poi da **Eulero**, che nel 1732 dimostrò che $\mathbb{F}_5 = 641 \cdot 6700417$.

Dopo Eulero si è continuata la ricerca di altri Numeri di Fermat, che si è velocizzata moltissimo nel XX secolo grazie all'arrivo dei calcolatori. Ma anche senza l'aiuto di essi si sono dimostrati dei risultati interessanti:

Nel 1880 si è dimostrato che $\mathbb{F}_6$ non è primo, e nel 1909 anche $\mathbb{F}_7$ (ma per i suoi fattori si è dovuto attendere addirittura il 1970!).

Ad oggi siamo arrivati a dimostrare che gli $\mathbb{F}_n$ non sono primi per n fino a 32 (e a trovare sporadicamente dei fattori di altri molto più alti come $\mathbb{F}_{1945}$, $\mathbb{F}_{9448}$, e nel giugno 2011 addirittura di $\mathbb{F}_{2543548}$[2]), e la congettura è diventata che $\mathbb{F}_n$ non è primo $\forall n \geq 5$.

Grazie ai Numeri di Fermat possiamo dimostrare il seguente

Teorema. *I numeri primi sono infiniti.*

Dimostrazione: Dimostriamo innanzitutto per induzione che

$$\prod_{k=0}^{n-1} \mathbb{F}_k = \mathbb{F}_n - 2$$

$\boxed{n = 1}$

$$\prod_{k=0}^{0} \mathbb{F}_k = \mathbb{F}_0 = 3 = 5 - 2 = \mathbb{F}_1 - 2$$

$\boxed{n \Rightarrow n+1}$

$$\prod_{k=0}^{n} \mathbb{F}_k = \left(\prod_{k=0}^{n-1} \mathbb{F}_k\right) \cdot \mathbb{F}_n = (\mathbb{F}_n - 2) \cdot \mathbb{F}_n = \left(2^{2^n} - 1\right) \cdot \left(2^{2^n} + 1\right) =$$

$$= 2^{2^{n+1}} - 1 = \left(2^{2^{n+1}} + 1\right) - 2 = \mathbb{F}_{n+1} - 2$$

[2]Per avere un'idea della grandezza di questi numeri basti pensare che $\mathbb{F}_{21}$ è più grande del numero di particelle contenute nell'universo, e che il fattore primo di $\mathbb{F}_{2543548}$ scoperto a giugno 2011 ha ben 765687 cifre!

Da questo lemma segue che $\forall \mathbb{F}_m, \mathbb{F}_n$, con $m \neq n \implies \mathbb{F}_m, \mathbb{F}_n$ coprimi, poiché se k divide sia $\mathbb{F}_m$ che $\mathbb{F}_n$ k deve dividere anche 2 (visto che posso scrivermi uno dei due come sopra). Allora k è 1 oppure 2; ma non può essere 2 perché i numeri di Fermat sono tutti dispari.

Visto che i Numeri di Fermat sono tutti coprimi tra loro posso prendere un fattore primo da ogniuno di essi, ed avere così un insieme infinito di primi.

□

Potremmo porci una domanda: come ha fatto Eulero nel 1732 a trovare quella fattorizzazione di $\mathbb{F}_5$?

Si sarà messo a provarli tutti uno ad uno? Poco probabile...

In realtà Eulero aveva fatto una grande scoperta nell'ambito dei Numeri di Fermat, che riportiamo di seguito come importante teorema:

Teorema. *Se p è primo allora vale la seguente implicazione:*

$$p|\mathbb{F}_n \quad \implies \quad p \equiv 1 \ mod(2^{n+1})$$

Dimostrazione:

$$p|\mathbb{F}_n = 2^{2^n} + 1 \implies [2^{2^n} + 1]_p = [0]_p$$

In cui indichiamo $[k]_p$ la classe di k in $\mathbb{Z}_p$.

$$[2^{2^n} + 1]_p = [0]_p \implies [2^{2^n}]_p = [-1]_p \implies [2^{2^{n+1}}]_p = [1]_p$$

Ci servono, ora, due grandi idee:

Idea 1: Considero le potenze di 2 modulo p:
In base a ciò che si è appena trovato:

$$[2]_p \neq [2^2]_p \neq ... \neq [2^{2^n}]_p \neq [2^{2^{n+1}}]_p = [1]_p \implies ord([2]_p) = 2^{n+1}$$

Idea 2: Considero $\mathbb{Z}_p^*$ (che sappiamo avere cardinalità $p-1$).
$D := \{[2^i]_p \,|\, i \in \mathbb{N}\} \subsetneq \mathbb{Z}_p^*$ ha esattamente 2^{n+1} elementi.
Definiamo una relazione di equivalenza:

$$[a]_p = [b]_p \Leftrightarrow \exists i, j \text{ tali che } [a]_p = [2]_p^i \cdot [b]_p^j$$

D è una classe di equivalenza per questa relazione. Ho k classi di equivalenza in $\mathbb{Z}_p^*$, ogniuna con cardinalità $= |D| = 2^{n+1}$

$\implies k \cdot 2^{n+1} = p - 1$

□

Come possiamo usare questo teorema? Vorremmo scoprire se $\mathbb{F}_5$ è primo. Ma in virtù di ciò che si è appena dimostrato sappiamo che $p|\mathbb{F}_5 \Longrightarrow p \equiv 1\ (2^6)$, quindi ci scriviamo i primi numeri congrui a 1 modulo 64(=2^6): 1,65,129,193,257,321,385,449,513,577,641,...

Se da questi scartiamo i non primi, quelli che rimangono sono: 193,257,449,577,641,...

Quindi per trovare il fattore 641 Eulero ha dovuto fare solo 5 verifiche!

Esiste in realtà anche un'altro criterio più forte, che restringerebbe ancora di più le scelte, ma lo lasciamo per esercizio agli interessati:

Esercizio. Dimostrare che per $n \geq 2$ vale $p|\mathbb{F}_n \Longrightarrow p \equiv 1\ (2^{n+2})$.

3.3 Primi di Mersenne

Un'altro matematico che ha studiato la formula $p_n = a_n + b$ per cercare numeri primi è **Padre Mersenne**(1588-1648). La scelta che fa lui è diversa da quella fatta da Fermat: decide di provare b=-1.

Con $p_n = a^n - 1$ abbiamo, però, un problema: $a^n - 1 = (a-1) \cdot t$, quindi se vogliamo che sia primo l'unica scelta possibile è prendere $a = 2$.

Quindi abbiamo $p_n = 2^n - 1$.

Ma i problemi non sono finiti, visto che vale la proprietà:

Proposizione. *se n non è primo* $\Longrightarrow p_n = 2^n - 1$ *non è primo.*

Dimostrazione: $n = hk \Longrightarrow p_n = 2^{h \cdot k} - 1 = (2^h)^k - 1 = (2^h - 1)t$

□

L'unica possibilità rimasta è dunque:

$$\mathbb{M}_p = 2^p - 1 \quad \longleftarrow \textbf{Numero di Mersenne}$$

Mersenne sostenne che gli unici **Primi di Mersenne** (cioè Numeri di Mersenne primi) si ottengono per p=2,3,5,7,13,17,19,31,67[3],127,257, ma ciò è in realtà falso poiché anche per p=89,107 si ottengono due Primi di Mersenne, ed inoltre $\mathbb{M}_{257}$ non è primo.

Da notare che $\mathbb{M}_{127}$ ha 39 cifre, ed è rimasto il più grande numero primo trovato fino al 1951. Pur non essendo più il più grande rimane comunque il numero primo più grande trovato senza uso di calcolatori.

Nel 1961 grazie ad un IBM7090 è stato trovato il 19esimo primo di Mersenne, che è $\mathbb{M}_{4253}$ (di 1281 cifre), e nel 1963 all'Università dell'Illinois è stato trovato il 23esimo: $\mathbb{M}_{11213}$ (di ben 3376 cifre)[4].

[3]In realtà $\mathbb{M}_{67}$ è composto, ma si crede sia un'errore di trascrittura, visto che $\mathbb{M}_{61}$ risulta essere davvero primo.

[4]Questa scoperta è stata celebrata in America con un francobollo in onore di Mersenne!

È attivo da alcuni anni il **GIMPS** (Great Internet Mersenne Prime Search) che mette in palio grosse somme di denaro per numeri primi molto alti, e si congettura che i primi di Mersenne siano infiniti.

Usiamo adesso i Numeri di Mersenne per dimostrare

Teorema. *I numeri primi sono infiniti.*

Dimostrazione: supponiamo che siano finiti: chiamo l'insieme dei numeri primi $\mathbb{P}$.
Visto che è finito ammette un elemento massimale: $p = max(\mathbb{P})$.
Considero, allora, $\mathbb{M}_p = 2^p - 1$.
Preso q un fattore primo di $\mathbb{M}_p$ ho:

$$2^p - 1 \equiv 0\ (q) \Longrightarrow 2^p \equiv 1\ (q) \Longrightarrow ord(2)_{\mathbb{Z}_q^*} = p \Longrightarrow p|(q-1) \Longrightarrow p < q$$

Quindi ho $q > p = max(\mathbb{P})$, che è assurdo.

□

3.4 Numeri Perfetti

Definizione. Un numero a si dice *perfetto* se è uguale alla somma dei suoi divisori strettamente minori

$$a = \sum_{d|a, d<a} d$$

Osservazione. (1) Il numero 3, "perfetto" per antonomasia, non è perfetto.
(2) Il primo numero perfetto è 6.

Sant'Agostino scrisse a proposito dei numeri perfetti:

> *Sei è un numero perfetto per sé stesso e non perché Dio creò tutte le cose in sei giorni, è vero piuttosto il viceversa: Dio creò tutte le cose in sei giorni perché sei è un numero perfetto. Rimarrebbe perfetto anche se l'opera dei sei giorni non esistesse.*
>
> Sant'Agostino - *De Civitate Dei*

Il filosofo neopitagorico **Nicomaso di Gerasa** scrisse:

> *Capita che le cose belle e buone siano rare e facilmente contate, mentre le brutte e cattive siano prolifiche, così anche si trova che i numeri abbondanti e difetti sono moltissimi e disordinati, e la loro identificazione non è sistematica, mentre i numeri perfetti sono facilmente contati e disposti in preciso ordine.*

Nota: i numeri abbondanti (o difetti) sono quelli la cui somma dei divisori è maggiore (o minore) del numero stesso.

Gli unici Numeri Perfetti conosciuti sono rimasti a lungo 6,28,496 e 8128. Conoscendone così pochi e non trovandone facilmente altri sono nate molte congetture nell'arco del tempo:

- *Tutti i numeri perfetti terminano alternativamente con 6 e 8.*

  Questa congettura si è poi rivelata falsa, poiché il quinto numero perfetto è 33550336, e il sesto 8589869056.

  Si è anche dimostrato, poi, che non vi è alcuna regolarità sull'ultima cifra dei perfetti, ma che essa deve sempre essere un 6 o un 8.

- *Ricorre un numero perfetto ogni potenza di 10.*

  Anche questa rivelata falsa dalla scoperta del quinto.

- *Ad eccezione del 6 sono tutte somme parziali dei primi dispari al cubo.*

- *Tutti i numeri perfetti sono pari.*

  Questa non è stata ancora provata/confutata, ma si è dimostrato che un perfetto dispari, se esiste, deve avere almeno 29 fattori primi, uno di questi deve essere maggiore di 10^{20}, ed il numero stesso deve essere maggiore di 10^{300}.

Euclide nota una certa regolarità nei numeri perfetti a lungo conosciuti: se scriviamo le loro fattorizzazioni troviamo
$6 = 2 \cdot 3 = 2^1 \cdot (2^2 - 1)$
$28 = 2^2 \cdot 7 = 2^2 \cdot (2^3 - 1)$
$496 = 2^4 \cdot 31 = 2^4 \cdot (2^5 - 1)$
$8128 = 2^6 \cdot 127 = 2^6 \cdot (2^7 - 1)$
Ma allora sarà vero che $2^{(p-1)}(2^p - 1)$ è numero perfetto $\forall p$ primo? In realtà no, visto che $2^{10}(2^{11} - 1)$ non è numero perfetto.

Euclide non si ferma certo qua, e arriva a dimostrare un importante risultato sui numeri perfetti:

> *Se a partire dall'unità si prende un numero a piacere di numeri successivi proporzionali in ragione doppia, fino a che la somma sia un prima, il prodotto di tale numero per l'ultimo numero sarà un numero perfetto.*
>
> Euclide - *Proposizione 36, Libro IX*

Vediamone la dimostrazione.

Teorema. *Dato $n = 2^{t-1}(2^t - 1)$, se $2^t - 1$ è primo $\Longrightarrow$ n è numero perfetto.*

Dimostrazione: Supponiamo che $q = 2^t - 1$ sia primo.

Allora n ha come divisori: 2^i, $2^i q$ al variare di $i = 0, ..., t-1$.

Se sommiamo i divisori trovati:

$$\sum_{i=0}^{t-1} 2^i + 2^i q = \sum_{i=0}^{t-1} 2^i(1+q) = (1+q)\sum_{i=0}^{t-1} 2^i = (1+q)(2^t-1) = 2^t(2^t-1) = 2 \cdot 2^{t-1}(2^t-1) = 2n$$

Quindi la somma di tutti i primi strettamente minori è proprio n.

□

Proprio grazie a questo criterio è stato trovato il quinto numero perfetto $2^{12}(2^{13}-1)$, visto che $2^{13} - 1 = 8191$ è primo.

Eulero dimostra che per i perfetti pari vale anche il viceversa del teorema:

Dimostrazione: Sia n perfetto pari. Fattorizzandolo otteniamo: $n = 2^{p-1}q$, con $p > 1$, q dispari.

Visto che n è perfetto, se indico con $\sigma(n)$ la somma dei suoi divisori ho:

$$2(2^{p-1}q) = 2n = \sigma(n) = \sigma(2^{p-1}q) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q)$$

$$\Longrightarrow \sigma(q) = \frac{2^p q}{2^p - 1} = q + \frac{q}{2^p - 1} \Longrightarrow (2^p - 1)|q$$

Scrivo quindi $q = (2^p - 1)m$.

Mostriamo che q è primo:

$$q = (2^p - 1)m \Longrightarrow 1, q, m, (2^p - 1)|q$$

$$\Longrightarrow q + \frac{q}{2^p - 1} = \sigma(q) \geq 1 + q + (2^p - 1) + m$$

$$\text{ma } m = \frac{q}{2^p - 1} \Longrightarrow m = 1 \Longrightarrow q \text{ ha come unici divisori 1 e } q$$

$$\Longrightarrow q = 2^p - 1 \text{ primo}$$

□

Abbiamo usato, nell'arco della dimostrazione, una proprietà non dimostrata che lasciamo per esercizio:

Esercizio. Provare che se MCD(a,b)=1 $\Longrightarrow \sigma(ab) = \sigma(a)\sigma(b)$.

3.5 Infinità dei Numeri Primi

Abbiamo già visto alcune dimostrazioni che i numeri primi sono infiniti, in questo capitolo ne proporremmo altre di vario tipo, anche molto diverse tra loro.

1 ***Eulero I:*** Sia $x \in \mathbb{R}$[5], e definiamo $\pi(x)$ il numero di primi minori o uguali ad x. Chiamo $\mathbb{P}$ l'insieme dei numeri primi, e supponiamo di indicizzare i primi in ordine crescente $p_1 < p_2 < ....$ Sappiamo che

$$\log(x) = \int_1^x \frac{1}{t} dt$$

Se approssimiamo per eccesso il valore dell'integrale con la comma delle aree dei rettangoli di base $[n, n+1]$ e altezza $\frac{1}{n} \forall x \in [n, n+1]$ vale:

$$\log(x) \leq 1 + \frac{1}{2} + ... + \frac{1}{n} \leq \sum_{m \in \mathcal{A}} \frac{1}{m}, \quad \mathcal{A} := \{t \in \mathbb{N} \mid \exists p \leq x \text{ primo t.c. } p|t\}$$

Grazie al teorema Fondamentale dell'Aritmetica abbiamo che

$$\sum_{m \in \mathcal{A}} \frac{1}{m} = \prod_{p \in \mathbb{P}, p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

Dunque, tornando all'approssimazione del logaritmo, vale

$$\log(x) \leq \sum_{m \in \mathcal{A}} \frac{1}{m} = \prod_{p \in \mathbb{P}, p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right) = \prod_{p \in \mathbb{P}, p \leq x} \frac{1}{1 - \frac{1}{p}} = \prod_{p \in \mathbb{P}, p \leq x} \frac{p}{p-1} =$$

$$= \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

A questo punto abbiamo finito poiché

$$\infty = \lim_{x \to \infty} \log(x) \leq \lim_{x \to \infty} (\pi(x) + 1) \quad \Longrightarrow \quad \pi(x) \longrightarrow \infty, \text{ per } x \to \infty$$

□

2 ***Eulero II:*** Consideriamo la serie geometrica

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}$$

Vale che

$$\prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \sum_{n=1}^{\infty} \frac{1}{n} = \infty \quad \Longrightarrow \quad |\mathbb{P}| = \infty$$

□

[5] Da notare che usciamo da $\mathbb{Z}$, cosa che non si fa quasi mai parlando di numeri primi!

3 ***Erdos:*** Dimostreremo che

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$$

Da cui si potrà quindi dedurre due cose:

$$|\mathbb{P}| = \infty \qquad\qquad \sum_{n=1}^{\infty} \frac{1}{n} = \infty$$

Supponiamo per assurdo che non valga l'ipotesi:

$$\sum_{p\in\mathbb{P}} \frac{1}{p} \lneq \infty \Longrightarrow \exists k \in \mathbb{N} \text{ t.c. } \sum_{i>k+1} \frac{1}{p_i} < \frac{1}{2}$$

Chiamo, allora, $\{p_1, ..., p_k\}$ i "primi piccoli" e $\{p_{k+1}, p_{k+2}, ...\}$ i "primi grandi".

Fissato $N \in \mathbb{N}$, chiamo $\mathcal{N}_G := \{m \in \mathbb{N} \mid m \leq N, \exists i \text{ t.c. } p_{k+i}|m\}$, e $\mathcal{N}_p := \{m \in \mathbb{N} \mid m \leq N, p_i|m \ \forall i \leq k\}$. Se denotiamo con n_G ed n_p le loro cardinalità dovrà necessariamente valere che $N = n_G + n_p$.

Quanti sono gli $n \leq N$ che hanno un fattore primo grande p_j (con $j \geq k+1$)?

Sono la parte intera di $\frac{N}{p_j}$. Si ha quindi la maggiorazione:

$$n_G \leq \sum_{j\geq k+1} \left\lfloor \frac{N}{p_j} \right\rfloor \leq \sum_{j\geq k+1} \frac{N}{p_j} = N \sum_{j\geq k+1} \frac{1}{p_j} < \frac{N}{2}$$

D'altra parte, dato $n \in \mathcal{N}_p$ supponiamo di scriverlo come $a_n^2 - b_n$, con b_n libero da quadrati. b_n deve essere prodotto di primi piccoli, con esponente 1, e di questi ce ne sono esattamente 2^k; quindi altrwttante possibilità per b_n. Invece per a_n possiamo dire che $a_n \leq \sqrt{n} \leq \sqrt{N}$.

Da queste stime ottengo $n_p \leq 2^k\sqrt{N}$, quindi per k abbastanza grande

$n_p,\ n_G < \frac{1}{2} \quad \Longrightarrow \quad n_p + n_G < N$, che è assurdo.

□

4 ***Saidak (2005):*** Cerco una successione infinita di coprimi: sappiamo che preso $n > 1$ vale che $MCD(n, n+1) = 1$.

Scelgo, quindi, la successione così formata:
$N_1 = n$
$N_2 = n(n+1) = N_1(N_1+1)$
$N_3 = N_2(N_2+1)$

$N_4 = N_3(N_3 + 1)$
...
In tal modo abbiamo che N_k ha sempre k fattori primi.

□

5 ***Furstemberg (1955):*** Scelgo $a, b \in \mathbb{Z}$, $b > 0$, e definisco $\mathcal{N}_{a,b} = \{a + bn \mid n \in \mathbb{Z}\}$.

Definiamo una topologia: $\mathcal{O}$ è aperto se è vuoto oppure se $\forall a \in \mathcal{O}\ \exists b > 0$ t.c. $\mathcal{N}_{a,b} \subseteq \mathcal{O}$.[6]

Osserviamo che ogni aperto (non banale) di questa topologia è sicuramente infinito, e che un insieme $\mathcal{N}_{a,b}$ è sia aperto che chiuso! Aperto perché contiene se stesso, ma anche chiuso perché complementare di un aperto:

$$\mathcal{N}_{a,b} = \left(\bigcup_{i=1}^{b-1} \mathcal{N}_{a+i,b}\right)^c$$

Adesso possiamo notare che $\forall n \in \mathbb{Z} \setminus \{-1, 1\}\ \exists p$ primo t.c. $p|n \implies \mathcal{N}_{0,p}$. Quindi $\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p\in\mathbb{P}} \mathcal{N}_{0,p}$.

Allora supponiamo per assurdo che $\mathbb{P}$ sia finito;

$$\implies \mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p\in\mathbb{P}} \mathcal{N}_{0,p} \text{ è chiuso (proprio perché è insieme finito)}$$

$$\implies \{-1, 1\} \text{ è aperto}$$

Ma ogni aperto era infinito!

□

[6] Si riesce facilmente a dimostrare che questa è effettivamente una topologia usando "minimo comune multiplo" e "massimo comun divisore" nel modo giusto, provate!

Capitolo 4

L'Infinito

4.1 Cenni Storici

Durante tutta la storia si sono avuti due tipi di "infinito":

- Infinito **potenziale**: è l'infinità dei numeri primi, ovvero preso un numero finito comunque grande posso sempre raggiungerne uno più grande;
- Infinito **in atto**: è l'infinità "vera", quella del segmento continuo.

Ma l'esistenza dell'infinito in atto è stata provata molto tardi, con **Cantor**($\sim$1850) (ed accettata veramente ancor più tardi!). Fino a quell'epoca ci sono stati dibattiti e lunghe discussioni da parte di grandi matematici di ogni tempo.

Aristotele(384-322 ac) dice più volte che "*è impossibile che l'infinito sia in atto*", e aggiunge:

> *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 - *Generazione degli Animali*

Archimede(287-212 aC) arriva addirittura a limitare il numero dei granelli di sabbia di tutto il mondo per provare l'impossibilità di un infinito in atto con $\Omega^{\Omega^{\Omega}}$, in cui Ω indica la *miriade*, considerata dai Greci come la massima cifra[1].

Non solo i Greci si sono addentrati in questo ambito, **San Tommaso** scrive:

[1] La parola "Miriade" deriva da due parole greche,*Myriàs* e *àdos*, che significano "insieme di 10.000"; Tale numero equivaleva, quindi, a 10.000 unità.

> *Come Dio, beché abbia una potenza infinita, non può creare qualcosa di increato perché ciè farebbe coesistere cose contraddittorie, così non può creare qualcosa di assolutamente infinito*
>
> San Tommaso - *Somma Theologiae*

Solo nel XVII Secolo iniziano veramente i primi dubbi, con scienziati di grande calibro come **Galileo Galilei** che scrive:

> *Infiniti essere tutti i numeri, infiniti i quadrati, infinite le loro radici, né la moltitudine dei quadrati essere minore di quella di tutti i numeri, né questa maggiore di quella. Ed in ultima conclusione gli attributi di maggiore e minore non aver luogo negli infiniti, ma solo nelle quantità terminate*
>
> Galileo Galilei - *Discorso e Dimostrazioni Matematiche Intorno a Due Nuove Scienze (1638)*

Bolzano pone, nel 1851, alcuni quesiti molto importanti nel trattato *I Paradossi dell'Infinito* tra cui le domande "*Se [a,b] è un intervallo della retta contenuto in [a,c], i punti di [a,b] sono meno di quelli di [a,c]?*", oppure "*I numeri tra 0 e 5 sono meno dei numeri tra 0 e 12?*".

Arriviamo poi ad una vera e propria considerazione dell'infinito in atto con **Hilbert**(1862-1943) che scrive "*trattiamo i punti di un segmento come un insieme che si presenta a noi allo stato di totalità compiuta. Si chiama infinito* ***attuale*** *questo tipo di infinito*".

Il passo finale è fatto da **Cantor**, che analizza gli infiniti nello stesso modo in cui si fa con il finito!

Una volta definito un insieme A *finito* se esiste una corrispondenza biunivoca tra A e $\mathbb{N}_n := \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$, il passo successivo (che possiamo considerare geniale) fatto da Cantor è quello di definire l'equipotenza tra insiemi di qualsiasi grandezza nello stesso modo: A è *equipotente* a B se esiste una corrispondenza biunivoca tra di loro.

Grazie a questo modo di pensare del tutto nuovo e rivoluzionario si aprono le "porte dell'infinito" per il matematico tedesco, che analizza quali possono essere le diverse "grandezze" nell'infinito, partendo dal "numerabile" $|\mathbb{N}| := \aleph_0$ ed arrivando al "continuo" $|\mathbb{R}|$.

4.2 Il Finito

Potremmo prendere come definizione di insieme infinito la negazione del "finito", ma allora ci serve una definizione formale per il concetto che vogliamo negare:

Definizione. A si dice *finito* se $\exists n \in \mathbb{N}$, $\exists f : A \to \mathbb{N}_n$ biunivoca. E in questo caso si dirà che A ha *cardinalità* n: $|A| = n$.

Dove $\mathbb{N}_n := \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$.

Sorge a questo punto un problema: è una buona definizione?
Cioè può mai capitare che A finito sia in corrispondenza con $\mathbb{N}_n$ e anche con $\mathbb{N}_m$?
In realtà no, e ce lo dice il seguente importante teorema:

Teorema (Principio dei Cassetti)**.** $n > m \Longrightarrow \nexists f : \mathbb{N}_n \to \mathbb{N}_m$ *iniettiva*

Dimostrazione: Per induzione su m:
$\underline{m = 0}$: $\mathbb{N}_0 = \emptyset$, quindi è vero perchè $\nexists f : \mathbb{N}_n \to \emptyset$.
$\underline{m \Rightarrow m + 1}$: se $n > S(m) \Rightarrow P(n) > m$ (in cui P è la funzione "predecessore").
Supponiamo per assurdo che $\exists \varphi : \mathbb{N}_n \to \mathbb{N}_{S(m)}$ iniettiva.

- se $\varphi(n) = S(m)$ ho finito perché $f|_{\mathbb{N}_{P(n)}} : \mathbb{N}_{P(n)} \to \mathbb{N}_m$ è iniettiva, ma per ipotesi induttiva $\nexists f : \mathbb{N}_{P(n)} \to \mathbb{N}_m$ iniettiva.
- se $\varphi(n) = a \neq S(m)$ considero $\tau : \mathbb{N}_{S(m)} \to \mathbb{N}_{S(m)}$ trasposizione che scambia a con $S(m)$. La trasposizione τ è bigettiva, quindi la composizione con φ è la funzione: $\tau \cdot \varphi : \mathbb{N}_n \to \mathbb{N}_{S(m)}$, che è iniettiva, e mi riconduco al caso sopra.

□

Esercizio. Dimostrare che $\mathbb{N}_{S(m)} = \mathbb{N}_m \cup S(m)$

Dal Principio dei cassetti si ricavano moltissimi corollari utili

Corollario. *Se $\exists f : A \to \mathbb{N}_n$ bigettiva, allora A non è in corrispondenza biunivoca con nessun $\mathbb{N}_m$, con $m \neq n$.*

Corollario. *Due insiemi finiti X e Y hanno la stessa cardinalità se e solo se $\exists f : X \to Y$ bigettiva*

Corollario. *Siano X e Y finiti con cardinalità m ed n $(m > n)$. Allora*
$\nexists f : X \to Y$ iniettiva

Corollario. *X finito, $Y \subseteq X \Longrightarrow |Y| \leq |X|$.*
Inoltre vale $Y \subsetneq X \Longrightarrow |Y| \lneq |X|$

Corollario. *Se X, Y finiti ed $\exists f : X \to Y$, $g : Y \to X$ iniettive, allora $\exists h : X \to Y$ bigettiva*

Lasciamo adesso una serie di problemi legati al Principio dei Cassetti, di difficoltà variabile:

1. Sul tavolo getto 15 fazzoletti con misura e forma diverse in modo da coprire tutta la superficie. Dimostra che si possono scegliere 8 fazzoletti da togliere in modo che $\frac{7}{15}$ del tavolo rimangano coperti.

2. Dimostrare che tra 51 punti scelti in un quadrato unitario ne esistono almento 3 che sono in un quadrato di lato $\frac{1}{5}$ (oppure anche in un cerchio di raggio $\frac{1}{7}$.

3. I 123 abitanti di un paese hanno come somma delle età 3813 anni. Dimostrare che ne esistono 100 la cui somma delle età è almeno 3100.

4. Siano $a_1, ..., a_n$ numeri reali, e sia $S = \sum_{i=1}^{n} \frac{a_i}{n}$. Dimostrare che $\forall k \in \{1, ..., n\} \exists$ k indici $i_1, ..., i_k$ e k indici $j_1, ..., j_k$ tali che valga:
$$\sum_{l=1}^{k} a_{i_l} \geqslant kS \qquad \sum_{l=1}^{k} a_{j_l} \leqslant kS$$

5. Data una superficie bianca rettangolare (8x16m), viene spruzzata della vernicie a caso per una superficie totale di 12m^2. Siamo sicuri che esistano due punti a distanza 1m di colore diverso? Perchè?

6. Dimostrare che esistono potenze intere di 29 che finiscono con "001".

7. Su una circonferenza butto colore rosso a caso, stando attento a colorare meno della metà della circonferenza stessa. Dimostrare che esistono due punti antipodali non colorati.

8. Dimostrare che presi 1000 interi qualsiasi ne esistono sempre due la cui somma o la cui differenza è un multiplo di 1997.

4.3 L'Infinito Numerabile

Definizione. Un insieme A si dice *infinito* se non è finito

Cosa vuol dire questa definizione?

Possiamo riscriverla nel modo seguente: A è *infinito* se $\forall m \in \mathbb{N}^+ \nexists f : A \to \mathbb{N}_m$ bigettiva.

Proposizione. $\mathbb{N}$ *è infinito*

Vediamo due dimostrazioni:

Dimostrazione: (1) Sappiamo già che non esistono funzioni iniettive da $\mathbb{N}_n$ in $\mathbb{N}_m$ se $n > m$.

Se esistesse una funzione $f : \mathbb{N} \to \mathbb{N}_m$ bigettiva potrei considerare $f|_{S(m)} : \mathbb{N}_{S(m)} \to \mathbb{N}_m$ che è iniettiva, il che porta ad un assurdo.

□

Dimostrazione: (2) Noi sappiamo che se A è finito allora A non è in corrispondenza biunivoca con nessun suo sottoinsieme proprio.

Da ciò ricaviamo che $\mathbb{N}$ non può essere finito, perchè di funzioni bigettive tra $\mathbb{N}$ e un suo sottoinsieme proprio ne trovo praticamente quante ne voglio.

□

Proposizione. $\forall \mathcal{X}$ *insieme infinito* $\exists f : \mathbb{N} \to X$ *iniettiva.*

Dimostrazione: $\mathcal{X} \neq \emptyset \Longrightarrow \exists^2 x_0 \in \mathcal{X}$
Visto che $\mathcal{X}$ è infinito $\Longrightarrow \mathcal{X}_1 = \mathcal{X} \setminus \{x_0\} \neq \emptyset \Longrightarrow \exists x_1 \in \mathcal{X}_1$
Visto che $\mathcal{X}_1$ è infinito $\Longrightarrow \mathcal{X}_2 = \mathcal{X}_1 \setminus \{x_1\} \neq \emptyset \Longrightarrow \exists x_2 \in \mathcal{X}_2$
[...] Proseguendo in questo modo posso creare una funzione $f : \mathbb{N} \to \mathcal{X}$ tale che $f(n) = x_n$, che è iniettiva.

□

Questa proposizione ci dice, praticamente, che $\mathbb{N}$ è *il più piccolo infinito*, visto che per ogni insieme infinito posso trovare un sottoinsieme con stessa cardinaltà di $\mathbb{N}$.

Ma allora sorge spontanea una domanda: esistono altri insiemi infiniti "più grandi" di $\mathbb{N}$? A questa domanda risponderemo nella prossima sezione, dopo il prossimo importante teorema:

Teorema. *Ogni insieme infinito $\mathcal{X}$ può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio*

Dimostrazione: prendiamo la funzione $f : \mathbb{N} \to \mathcal{X}$ iniettiva (che so esistere per il teorema precedente).

Quello che voglio fare è costruire $g : \mathcal{X} \to \mathcal{X}$ iniettiva ma non surgettiva. Definisco, allora, questa nuova funzione a pezzi:

$$g(x) = \begin{cases} f(S(f^{-1}(x))) & \text{se } x \in f(\mathbb{N}) \\ x & \text{se } x \in X \setminus f(\mathbb{N}) \end{cases}$$

Così definita g è iniettiva, ma non può essere surgettiva perché $f(0)$ non stà nell'immagine di g.

□

Visto il teorema appena dimostrato possiamo dare un'altra definizione equivalente di insieme infinito:

Definizione. Un insieme A si dice *infinito* se è in corrispondenza biunivoca con un suo sottoinsieme proprio[3].

[2] Attenzione: Assioma della Scelta in atto!

[3] Questa seconda definizione di insieme infinito è dovuta a Cantor!

Definizione. Si dice che A e B sono *equipotenti*, o che hanno "stessa cardinalità", se $\exists f : A \to B$ bigettiva.

Quando due insiemi A e B sono equipotenti si scrive $|A| = |B|$.

Definizione. Un insieme A equipotente con $\mathbb{N}$ si dice *numerabile*.

Diamo un simbolo alla cardinalità "numerabile": $|\mathbb{N}| = \aleph_0$.

Osservazione. L'equipotenza è una relazione di equivalenza.

Gli insiemi di cardinalità "numerabile" sono molto importanti, poiché per moltissimo tempo si è creduto che fosse l'unico tipo di infinito.

Com'è possibile? In realtà si può comprendere bene questo problema se si analizzano i risultati seguenti:

Proposizione. *Qualunque sottoinsieme A non finito di $\mathbb{N}$ è numerabile.*

Dimostrazione: Definisco $f : \mathbb{N} \to A$ bigettiva in maniera induttiva:
$f(0) = min(A)$
$f(S(n)) = min(A \setminus \{f(0), ..., f(n)\})$

□

Proposizione. *L'unione disgiunta di un insieme finito A e di un insieme numerabile B è numerabile.*

$$\aleph_0 + m = \aleph_0 \quad \forall m \in \mathbb{N}$$

Dimostrazione: Viste le ipotesi abbiamo che:
$|A| = m < \infty \Longrightarrow \exists h : A \to \mathbb{N}_m$ bigettiva.
$|B| = \aleph_0 \Longrightarrow \exists g : B \to \mathbb{N}$ bigettiva.
Allora definisco la mia funzione $f : A \sqcup B \to \mathbb{N}$ a pezzi:

$$f(x) = \begin{cases} h(x) - 1 & \text{se } x \in A \\ g(x) + m & \text{se } x \in B \end{cases}$$

□

Osservazione. Sapendo che l'equipotenza è una relazione di equivalenza potevamo dimostrare la proposizione precedente anche dimostrando che $|N \sqcup B| = |\mathbb{N}|$.

Proposizione. *Il prodotto cartesiano tra un insieme finito i uno numerabile è numerabile*

$$\aleph_0 \cdot m = \aleph_0 \quad \forall m \in \mathbb{N}$$

Dimostrazione: Definiamo

$$\begin{array}{ccc} f : \mathbb{N} & \longrightarrow & \mathbb{N} \times \mathbb{N}_m \\ n & & (q, r+1) \end{array}$$

con q, r dati dalla divisione euclidea: $n = q \cdot m + r$, $0 \leq r < m$.

□

Proposizione. *L'unione disgiunta di numerabili è numerabile*

$$\aleph_0 + \aleph_0 = \aleph_0$$

Dimostrazione: Possiamo dividere i naturali in pari e dispari, ed abbiamo:
$|\mathbb{P}| = \aleph_0$, $|\mathbb{D}| = \aleph_0$
$id : \mathbb{P} \sqcup \mathbb{D} \to \mathbb{N}$ bigettiva.

□

Proposizione. *Il prodotto cartesiano tra numerabili è numerabile*

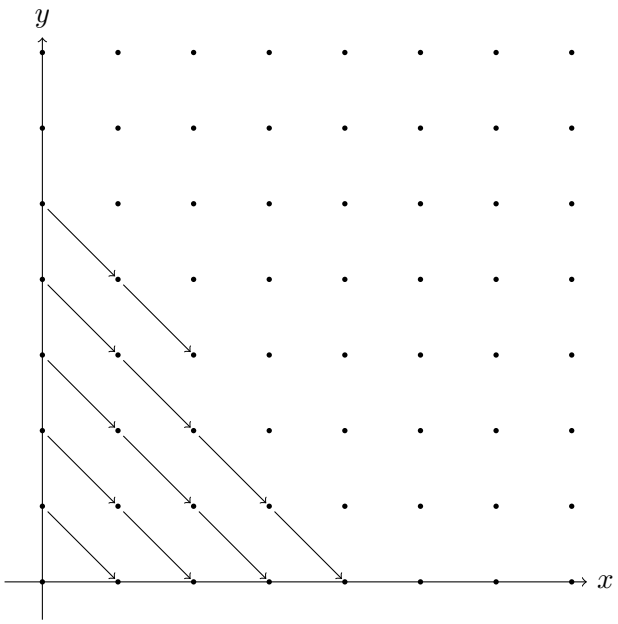
$$\aleph_0 \cdot \aleph_0 = \aleph_0$$

Dimostrazione: Devo trovare una funzione bigettiva $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

Un'altro modo per vedere la cosa è che dobbiamo trovare un modo per "numerare" tutti i punti interi del primo quadrante del piano. Come potremmo fare?

In realtà ci sono moltissimi modi possibili, ma uno di quelli più semplici è venuto in mente a Cantor con il suo "Metodo Diagonale", dando la seguente numerazione:
$(0,0) \longrightarrow 0$
$(0,1) \longrightarrow 1$
$(1,0) \longrightarrow 2$
$(0,2) \longrightarrow 3$
$(1,1) \longrightarrow 4$
$(2,0) \longrightarrow 5$
...

Il nome si comprende meglio se si usa una figura per capire in che modo vengono ordinati i punti:



□

Esercizio (*)**.** Riesci a trovare una formula per la funzione usata qua sopra?

Tutti questi risultati, in particolare, ci dimostrano anche che $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$. È dunque difficile trovare un insieme che sia "più che numerabile"!. Allora dove possiamo cercare insiemi più grandi di $\mathbb{N}$?

4.4 Altri Infiniti

Dati due insiemi A e B (sia finiti che non), si dice che A ha cardinalità minore o uguale di B se $\exists f : A \to B$ iniettiva. E si scrive $|A| \leq |B|$.

Inoltre vale $|A| \lneq |B|$ se $|A| \leq |B|$ e $\nexists f : A \to B$ surgettiva.

È un ordinamento? Devono valere le seguenti proprietà:

- riflessiva: $|A| \leq |A|$
- antisimmetrica: $|A| \leq |B|, |B| \leq |A| \implies |A| = |B|$
- transitiva: $|A| \leq |B|, |B| \leq |C| \implies |A| \leq |C|$

La dimostrazione delle buone proprietà non è affatto banale, in particolare per dimostrare il secondo punto ci serve un teorema molto importante:

Teorema (**Cantor-Berstein**)**.** *Se* $\exists f : A \to B, g : B \to A$ *iniettive* $\implies \exists \lambda : A \to B$ *bigettiva*

Dimostrazione: Date le due funzioni f, g mi costruisco λ come segue:

Definiamo x *capostipite* di y se x non sta né nell'immagine di f né nell'immagine di g, e se y è raggiunto da x tramite iterazioni di f e g.

A questo punto ci definiamo degli insiemi a partire dalle funzioni date:

$$\begin{array}{ll} A_\infty = \{x \in A \,|\, x \text{ non ha capostipite}\} & B_\infty = \{x \in B \,|\, x \text{ non ha capostipite}\} \\ A_A = \{x \in A \,|\, x \text{ ha capostipite in } A\} & B_A = \{x \in B \,|\, x \text{ ha capostipite in } A\} \\ A_B = \{x \in A \,|\, x \text{ ha capostipite in } B\} & B_B = \{x \in B \,|\, x \text{ ha capostipite in } B\} \end{array}$$

Con questi insiemi definiamo la nostra funzione $\lambda : A \to B$ bigettiva

$$\lambda(x) = \begin{cases} f(x) & \text{se } x \in A_\infty \cup A_A \\ g^{-1}(x) & \text{se } x \in A_B \end{cases}$$

□

È un ordinamento totale? È vero che $\forall A, B$ vale $|A| \leq |B|$ opp $|B| \leq |A|$? <u>si</u>, per il seguente teorema:

Teorema (di **Hartags**(1874-1943))**.** *Dati due insiemi $A, B \neq \emptyset$ è sempre vero che $\exists f : A \to B$ iniettiva, oppure $\exists f : B \to A$ iniettiva.*

Dimostrazione: Considero le terne: $\{(X, f, Y)\} = \mathcal{H}$, in cui $X \subseteq A$, $Y \subseteq B$, $f : X \to Y$ bigettiva.

Sicuramente $\mathcal{H} \neq \emptyset$ perché $[(\{a\}, f, \{b\}) \mid f(a) = b] \in \mathcal{H}$ (si può fare poiché $A, B \neq \emptyset$).

Definire una relazione d'ordine in $\mathcal{H}$.

$$(X_1, f_1, Y_1) \leq (X_2, f_2, Y_2) \iff \begin{array}{l} X_1 \subseteq X_2 \\ Y_1 \subseteq Y_2 \\ f_2|_{X_1} = f_1 \end{array}$$

E con essa dimostriamo adesso che ogni catena in $\mathcal{H}$ ammette maggiorante:

Data una catena $(X_1, f_1, Y_1) \leq (X_2, f_2, Y_2) \leq ...$ definiamo

$$\mathcal{X} = \bigcup_i X_i \quad \mathcal{Y} = \bigcup_i Y_i \quad \mathcal{F}(x) = f_i(x) \text{ se } x \in X_i$$

$$\implies (\mathcal{X}, \mathcal{F}, \mathcal{Y}) \text{ è un maggiorante.}$$

Se ogni catena ammette un maggiorante posso usare il **lemma di Zorn**[4] ed avere così un elemento $(\mathcal{S}, g, \mathcal{T})$ *massimale* per $\mathcal{H}$.

[4]Il **lemma di Zorn** dice che se X è un insieme non vuoto su cui è definita una relazione d'ordine parziale "$\leq$" tale che ogni sua catena possiede un maggiorante, allora contiene almeno un elemento massimale.

Supponiamo per assurdo che in questo elemento massimale $\mathcal{S} \neq A$, $\mathcal{T} \neq B$.

$$\Longrightarrow \exists a \in A \backslash \mathcal{S},\ \exists b \in B \backslash \mathcal{T} \Longrightarrow (\mathcal{S}, g, \mathcal{T}) \leq (\mathcal{S} \cup \{a\}, \widehat{g}, \mathcal{T} \cup \{b\}),\ \widehat{g}(x) = \begin{cases} b & \text{se } x = a \\ g(x) & \text{altrimenti} \end{cases}$$

Ma $(\mathcal{S}, g, \mathcal{T})$ era massimale, il che porta ad un assurdo.

Rimangono quindi due possibilità:
$\mathcal{S} = A \Longrightarrow g : A \to B$ iniettiva
$\mathcal{T} = B \Longrightarrow g^{-1} : B \to A$ iniettiva

□

Ma esiste qualcosa di non numerabile? si: $|\mathbb{N}| < |\mathbb{R}|$.

Dimostrazione: Vediamo perché con vari passaggi:
Passo 1: $|\mathbb{R}| = |(0,1)|$
Questo primo passaggio è il più semplice.
Basta trovare una funzione bigettiva $f : \mathbb{R} \to (0,1)$.
Una delle tante che possiamo prendere è

$$f(x) = \frac{1}{\pi}(arctg(x) + \frac{\pi}{2})$$

Passo 2: $\nexists f : (0,1) \to \mathbb{N}$ bigettiva
Questo lo facciamo per assurdo: supp $\exists f : \mathbb{N} \to (0,1)$ bigettiva.
Allora posso "enumerare" l'intervallo (0,1):
$\forall \alpha,\ \beta \in (0,1) \Rightarrow \exists n, m \in \mathbb{N}$ tali che $f(n) = \alpha,\ f(m) = \beta$.

Visto che li posso "enumerare" ho:
$\alpha_1 = 0, \alpha_1^{(1)} \alpha_1^{(2)} \alpha_1^{(3)} ...$
$\alpha_2 = 0, \alpha_2^{(1)} \alpha_2^{(2)} \alpha_2^{(3)} ...$
$\alpha_3 = 0, \alpha_3^{(1)} \alpha_3^{(2)} \alpha_3^{(3)} ...$
[...]
in cui $\alpha_i^{(j)}$ rappresentano le cifre dopo la virgola dei vari α_i.

A questo punto posso costruire un numero reale che sta in (0,1) ma non sta nell'immagine $f(\mathbb{N})$ nel seguente modo:
prendo $\beta = 0, \beta_1 \beta_2 \beta_3 ...$ tali che $\beta_i \neq \alpha_i^{(i)} \forall i$.
Visto che $\beta \notin f(\mathbb{N}) \Longrightarrow f$ non è surgettiva.

Abbiamo quindi mostrato che $|\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{N}| < |\mathbb{R}|$.

□

La cardinalità di $\mathbb{R}$ si dice *continua.*

Adesso sappiamo che $|\mathbb{N}| < |\mathbb{R}|$, ma non sappiamo ancora "quanto è più grande". Per fare questo vediamo prima alcuni risultati che ci permetteranno di caratterizzare la grandezza di $\mathbb{R}$.

Teorema. $\forall$ *insieme* $\mathcal{X}$ *vale* $|\mathcal{X}| < |\mathcal{P}(\mathcal{X})|$, *in cui* $\mathcal{P}(\cdot)$ *indica l'insieme delle parti.*

Dimostrazione: Si trova facilmente una funzione $f : \mathcal{X} \to \mathcal{P}(\mathcal{X})$ iniettiva: $f(x) = \{x\}$. Da ciò abbiamo che $|\mathcal{X}| \leq |\mathcal{P}(\mathcal{X})|$.

Per l'altra disuguaglianza dimostriamo che $\nexists f : \mathcal{X} \to \mathcal{P}(\mathcal{X})$ surgettiva. Supponiamo per assurdo che esista;

Se tale funzione esiste costruiamo un sottoinsieme di $\mathcal{P}(\mathcal{X})$ che porti ad un assurdo:
$\mathcal{Y} := \{x \in \mathcal{X} \mid x \notin f(x)\}$
Visto che f è surgettiva $\exists z \in \mathcal{X}$ tale che $f(z) = \mathcal{Y}$.

Domanda: $z \in \mathcal{Y}$?
se $z \in \mathcal{Y} \Longrightarrow z \notin f(z) = \mathcal{Y} \Longrightarrow$ assurdo.
se $z \notin \mathcal{Y} \Longrightarrow z \in f(z) = \mathcal{Y} \Longrightarrow$ assurdo.

□

Siamo ora pronti per dimostrare che $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$:

Dimostrazione: La dimostrazione di questo fatto si divide in tre fasi:

Passo 1: $|\mathbb{R}| = |(0,1)|$ (già fatto)

Passo 2: $|\mathcal{P}(X)| = |\mathcal{F}_X := \{f : X \to \{0,1\}\}|$

Sto cercando una funzione $\phi : \mathcal{P}(X) \to \mathcal{F}_X$ bigettiva. Definisco, allora, $\phi(X) = \Theta_X$, in cui Θ_X è la funzione indicatrice dell'insieme X ($\Theta_X(x) = 1 \Leftrightarrow x \in X$, altrimenti $\Theta_X(x) = 0$).

ϕ iniettiva: $\phi(X) = \phi(Y) \Longrightarrow \Theta_X = \Theta_Y \Longrightarrow X = Y$;

ϕ surgettiva: $\forall f \in \mathcal{F}_X$ basta prendere $A = f^{-1}(\{1\})$.

Passo 3: $|(0,1)| = |\mathcal{F}_{\mathbb{N}}|$

Presa $\varphi \in \mathcal{F}_{\mathbb{N}}$ gli associo $0, \varphi(1)\varphi(2)\varphi(3)... \in (0,1)$.

Ho una funzione fa $\mathcal{F}_{\mathbb{N}}$ a (0,1) $\Longrightarrow |\mathcal{F}_{\mathbb{N}}| \leq |(0,1)|$.

Ora l'altra disuguaglianza: preso $a \in (0,1)$, me lo riscrivo in base 2 (stando attendo a non avere scritture periodiche: $0,0\overline{1} = 0,1$) e gli associo la funzione

$f_a(n) = a_n$ (l'n-esima cifra di a in base 2) $\Longrightarrow |(0,1)| \leq |\mathcal{F}_{\mathbb{N}}|$

$\Longrightarrow |(0,1)| = |\mathcal{F}_{\mathbb{N}}|$

Dai tre punti appena dimostrati abbiamo che $|\mathbb{R}| = |(0,1)| = |\mathcal{F}_{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|$.

□

Definizione. Dati due insiemi A, B definiamo $B^A := \{f : A \to B\}$

Proposizione. $|A^{B\times C}| = |(A^B)^C|$

Dimostrazione: $A^{B\times C} = \{f : B \times C \to A\}$
$(A^B)^C = \{h : C \to \{g : B \to A\}\}$
definiamo, allora, la seguente funzione bigettiva $\phi(f) = h$, tale che $h(c) = f|_{B\times\{c\}}$.

□

Esercizio. Dimostrare che le successioni reali hanno la cardinalità del continuo.

Svolgimento: $|\mathbb{R}^{\mathbb{N}}| = |\{f : \mathbb{N} \to \mathbb{R}\}| = |\{f : \mathbb{N} \to \{g : \mathbb{N} \to \{0,1\}\ \}\}| = |2^{\mathbb{N}\times\mathbb{N}}| = |2^{\mathbb{N}}| = |\mathbb{R}|$.

Esercizio. Contare le funzioni reali continue.

Svolgimento: $|\{f : \mathbb{R} \to \mathbb{R} \text{ continue}\}| = |\{f : \mathbb{Q} \to \mathbb{R}\}| = |\{f : \mathbb{N} \to \mathbb{R}\}| = |\mathbb{R}|$.

Esercizio. Contare tutte le funzioni reali.

Svolgimento: $|\{f : \mathbb{R} \to \mathbb{R}\}| = |\{0,1\}^{\mathbb{N}\times\mathbb{R}}| = |\{0,1\}^{\mathbb{R}}| = |\mathbb{R}^{\mathbb{R}}| = |\mathcal{P}(\mathbb{R})|$.

Esercizio. Dimostrare che $|\mathbb{R}^m| = |\mathbb{R}|\ \forall m \in \mathbb{N}$

Svolgimento: Usiamo di nuovo il processo diagonale di Cantor: associamo ad ogni punto
$(x_1; \cdots ; x_m) = (0, x_1^{(1)}x_1^{(2)}x_1^{(3)}.. ; \cdots ;\ 0, x_m^{(1)}x_m^{(2)}x_m^{(3)}..) \ \in\ (0,1)^m$
il punto $0, x_1^{(1)}x_2^{(1)}..x_m^{(1)}x_1^{(2)}x_2^{(2)}..x_m^{(2)}... \ \in\ (0,1)$
Con questo abbiamo: $|\mathbb{R}^m| = |(0,1)^m| = |(0,1)| = |\mathbb{R}|$.

Esercizio. Dato V spazio vettoriale su $\mathbb{R}$ dimostrare i seguenti fatti:

1. Se V ha dimensione finita $\implies |V| = |\mathbb{R}|$;
2. Se V ha dimensione numerabile $\implies |V| = |\mathbb{R}|$;
3. Se V ha dimensione continua $\implies |V| = |\mathcal{P}(\mathbb{R})|$.

Capitolo 5

Estensioni Numeriche: $\mathbb{Z}$

5.1 Introduzione alle Estensioni

Le motivazioni per cui si cercano delle estensioni sono principalmente due:

1. **Applicativo:** definire grandezze che non sono misurabili con il "vecchio" sistema numerico;

2. **Teorico:** riuscire ad eseguire operazioni che nel "vecchio" sistema non sono possibili.

Nel caso del passaggio $\mathbb{N} \longrightarrow \mathbb{Z}$ la motivazione applicativa viene fuori dalla ricerca di una scala unica per misurare crediti e debiti, quindi dalla necessità di definire le grandezze "negative".

La motivazione teorica è, invece, poter risolvere equazioni di questo tipo:

$$10 + x = 3$$

che in $\mathbb{N}$ è sicuramente insolubile.

Hankel (nel 1800) analizza il concetto di "estensione numerica" dicendo che esso consta di due tappe:

1. Attribuire il significato di *numero* a simboli o sistemi di simboli che non rappresentano numeri nel "vecchio" insieme;

2. Definire proprietà dell'uguaglianza, dell'ordinamento e delle operazioni fondamentali dell'aritmetica in modo che si conservino le proprietà formali del "vecchio" insieme. (**Criterio di Permanenza delle Proprietà Formali**)

Ma quali sono le proprietà formali he vogliamo mantenere?
Sicuramente non tutte. Dobbiamo fare una scelta.

Villani, nel suo libro *Cominciamo da Zero*, propone una scaletta per verificare di aver raggiunto gli scopi che ci siamo prefissati con l'estensione voluta (nel nostro caso $\mathbb{Z}$):

1. Dotare $\mathbb{Z}$ (il nuovo insieme) della struttura di ordine e si definiscono le operazioni in modo che ristrette a $\mathbb{N}$ (il vecchio insieme) "siano uguali" alle vecchie operazioni;
2. Verificare quali proprietà continuano a valere e quali no;
3. Verificare se è stato raggiunto lo scopo applicativo;
4. Verificare se è stato raggiunto lo scopo teorico.

Una volta fatte le verifiche da lui proposte siamo sicuri di avere esattamente l'estensione che stavamo cercando.

5.2 Cenni Storici

Attenzione: i numeri negativi che noi oggi usiamo con molta disinvoltura sono stati accettati molto tardi nell'occidente, e con grande difficoltà.

L'approccio che noi usiamo oggi in matematica prevede questa scala di estensioni:

$$\mathbb{N} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R}$$

ma l'approccio "storico" che è avvenuto è il seguente:

$$\mathbb{N} \longrightarrow \mathbb{Q}^{+} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{R}$$

in cui $\mathbb{Z}$ compare solo come sottoinsieme dei razionali (positivi e negativi).

L'equazione $10+x = 3$ è stata considerata insolubile per molti secoli perchè "illogica": è impossibile e impensabile *aggiungere* qualcosa a 10 ed ottenere 3.

I **Maestri D'Abaco** (all'incirca a metà del 1500) stabiliscono (o scoprono?) le regole per fare i conti tra debiti e crediti, ma non accettano i numeri negativi come veri e propri *numeri*, tant'è che li chiamano "falsi"[1]

Nelle società orientali i numeri negativi sono stati accettati molto prima che da noi. Già nel VI secolo d.C. **Brahmagupta** definisce le regole per moltiplicare e sommare numeri sia negativi che positivi. Le sue opere verranno poi tradotte in latino solo nel XVI secolo d.C., e portate così in occidente.

Addirittura un accenno viene fatto da **Diofanto**, che scrive:

[1]Per enfatizzare la differenza tra i numeri positivi (considerati veri *numeri*) e i numeri negativi i Maestr D'Abaco introducono anche una differenza di colore tra le due scale usate per fare i conti: i numeri positivi vengono scritti in blu, mentre quelli negativi in rosso. Da ciò nascerà il detto "andare in rosso", legato a crediti/debiti.

il prodotto di due termini tolti deve essere aggiunto

in cui si annuncia la regola fondamentale[2]: $(-a) \cdot (-b) = +ab$.

5.3 Sulla Regola dei Segni

> *Il mio entusiasmo per la matematica era basata principalmente sul mio orrore per l'ipocrisia. L'ipocrisia come la vedevo io era mia zia Serafie, Madam Vignon e i loro preti. Nella mia opinione l'ipocrisia non era possibile in matematica.[...] Che stupore allora per me scoprire che nessuno poteva spiegarmi com'accadeva che meno per meno fa più! Non solo nessuno mi spiegava questa difficoltà (ed è sicuramente spiegabile perchè conduce a verità), ma ciò che era peggio essi la spiegavano su ragioni che erano evidentemente lontane da essere chiare a loro stessi.*
>
> Stendhal - *Vita di Henry Brulard*

La confusione descritta da Stendhal nei matematici è dovuta alla convinzione di molti che la regola dei segni vada "dimostrata". Non è così: la regola dei segni è una *definizione*.

Le operazioni su $\mathbb{Z}$ vengono definite nel modo che conosciamo perchè si vogliono preservare le proprietà delle operazioni che avevo su $\mathbb{N}$ (commutativa, distributiva) e l'identità "1".

Ma è proprio necessario definire le operazioni (cioè la regola dei segni) in questo modo? Chi ci dice che non sia possibile definirla in altro modo pur mantenendo inalterate le proprietà richieste?

Esercizio. Dimostrare che l'unico modo di mantere le proprietà sopra elencate è di definire le operazioni du $\mathbb{Z}$ come tutti le conosciamo.

5.4 Costruzione Formale di $\mathbb{Z}$

L'idea per la formalizzazione di $\mathbb{Z}$ come lo conosciamo è di indicare un numero qualsiasi (positivo o negativo) come una coppia di naturali, la cui "sottrazione"[3] dà come risultato il numero stesso.

Da ciò introduciamo formalmente

$$\mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{N}\}/_\sim$$

[2]Attenzione: è vero che Diofanto aveva compreso la fondamentale regola che *meno per meno fa più*, ma non considera mai numeri negativi in sé. Il suo interesse è per le operazioni del tipo $(a - c) \cdot (b - d)$, in cui si avrà sempre $a > c, b > d$.

[3]Attenzione: il termine "sottrazione" è usato in modo improprio, visto che nei naturali non è possibile farla sempre!

dove la relazione di equivalenza è data da

$$(a,b) \sim (c,d) \iff a+d = b+c$$

Domanda: cosa rappresenta questa relazione di equivalenza sul piano $\mathbb{N} \times \mathbb{N}$?

Abbiamo quindi adesso una definizione di $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/_\sim$. Definiamo su di esso le operazioni che volgiamo:

- $(a,b) \oplus (c,d) := (a+c, b+d)$

  Osservazione. La somma così definita è compatibile con la relazione di equivalenza "$\sim$".

  Osservazione. Essendo $\mathbb{N}$ un semigruppo additivo abeliano $\Rightarrow$ $\mathbb{Z}$ sarà un gruppo additivo abeliano

- $(a,b) \odot (c,d) := (ac+bd, ad+bc)$

  Esercizio. Dimostrare che è una buona definizione.

Essendo $\mathbb{Z}$ un'estensione di $\mathbb{N}$ vogliamo che in $\mathbb{Z}$ esista una copia *isomorfa* di $\mathbb{N}$, e la troviamo facilmente come immagine della funzione

$$\begin{array}{rcl} i : \mathbb{N} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & [(n,0)] \end{array}$$

Esercizio. Dimostrare che i è un morfismo iniettivo.

Con le operazioni sopra definite abbiamo che $(\mathbb{Z}, \oplus, \odot)$ è il più piccolo *dominio di integrità* contenente $\mathbb{N}$.

L'unica cosa che manca è l'ordinamento, che definiamo nel seguente modo:

$$a \leq b \Leftrightarrow b + (-a) \in \mathcal{N}$$

In cui indichiamo con $\mathcal{N}$ la copia isomorfa ad $\mathbb{N}$ contenuta in $\mathbb{Z}$ (che da ora in poi indicheremo più semplicemente con lo stesso simbolo $\mathbb{N}$).

5.5 Terne Pitagoriche e Teorema di Fermat

Un importante risultato che vale la pena di approfondire è il famoso **Teorema di Fermat**. Per arrivare ad esso partiamo dall'inizio: le *Terne Pitagoriche*.

Nei triangoli rettangoli la forma sul lato che sottende l'angolo retto (ipotenusa) è uguale alle forme sui lati che comprendono l'angolo retto (cateti)

Euclide - *Elementi, Libro VI*

Nella precedente citazione **Euclide** enuncia il famoso **Teorema di Pitagora**, che fornisce un modo concreto per costruire triangoli rettangoli senza alcun bisogno di misurare effettivamente gli angoli interni. Da ciò nascono le *Terne Pitagoriche*:

Definizione. (a, b, c) si dice *Terna Pitagorica* se vale $a^2 + b^2 = c^2$.

Facciamo alcune osservazioni:

Osservazione.
1. Riconoscere tutti i diversi triangoli rettangoli interi equivale a trovare tutte le terne pitagoriche.
2. Se (a, b, c) è terna pitagorica $\Longrightarrow$ (ak, bk, ck) è terna pitagorica $\forall k \in \mathbb{N}$, ma i triangoli formati dalle due terne pitagoriche sono equivalenti.
3. Le terne pitagoriche sono infinite.

Definizione. (a, b, c) si dice terna pitagorica *primitiva* (*t.p.p*) se MCD(a, b, c)=1.

Le terne pitagoriche primitive sono importanti perché sono quelle che forniscono triangoli rettangoli non equivalenti.

Osservazione. Se $(2n - 1)$ è un quadrato $\Longrightarrow$ $(n - 1, \sqrt{2n - 1}, n)$ è t.p.p.

Dimostrazione:

$$n^2 = \sum_{i=1}^{n} 2n - 1 = \overbrace{1 + 2 + \cdots + (2n - 3)}^{(n-1)^2} + (2n - 1)$$

□

Per classificare le t.p.p è utile fare un ragionamento sulla parità possibile dei suoi elementi (nei casi significativamente differenti):
$(P, P, P) \longrightarrow$ no, perchè con 3 pari non è primitiva;
$(P, P, D) \longrightarrow$ no, perchè somma di pari è pari;
$(P, D, P) \longrightarrow$ no, perchè somma di pari e dispari è dispari
$(D, D, D) \longrightarrow$ no;
$(D, P, D) \longrightarrow$ si, ad esempio $(3, 4, 5)$;
$(D, D, P) \longrightarrow$ no (è possibile fare ragionamenti "modulo 4" per cui si elimina uesta possibilità).

Un risultato fondamentale per classificare le t.p.p è il seguente

Proposizione.

$$(a,b,c)\ t.p.p \quad \iff \quad \begin{cases} c = m^2 + n^2 \\ a = m^2 - n^2 \quad con\ MCD(m,n) = 1 \\ b = 2mn \end{cases}$$

Dimostrazione: $\boxed{\Leftarrow}$

$$\begin{cases} c^2 = m^4 + 2m^2n^2 + n^4 \\ a^2 = m^4 - 2m^2n^2 + n^4 \\ b^2 = 4m^2n^2 \end{cases} \implies a^2 + b^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = c^2$$
$$\Downarrow$$
$$(a,b,c)\ \text{t.p.p}$$

$\boxed{\Rightarrow}$ Sappiamo che uno fra a e b è pari; supponiamo b pari: $b = 2s$.

Inoltre ho che $4s^2 = b^2 = c^2 - a^2 = (c-a)(c+a)$, quindi entrambi i fattori devono essere pari:

$(c-a) = 2x$, $(c+a) = 2y$, tali che $x = m^2$, $y = n^2$, MCD(x,y)=1.[4]

Da tutto ciò ricaviamo:

$$\begin{cases} c - a = 2x = 2m^2 \\ c + a = 2y = 2n^2 \\ s^2 = xy = m^2n^2 \end{cases} \implies \begin{cases} c = m^2 + n^2 \\ a = m^2 - n^2 \\ b = 2mn \end{cases}$$

□

Esercizio. Quanti punti razionali stanno sulla circonferenza unitaria?[5]

Siamo dunque pronti ad enunciare il famoso

Teorema (di Fermat)**.** *Non ci sono soluzioni intere (non banali) dell'equazione*

$$a^n + b^n = c^n,\ n \geq 2$$

Osservazione. Per dimostrarlo basta provare che è vero per $a, b, c \in \mathbb{N}^+$, poichè:

- se n è pari: $a^n = (-a)^n$
- se n è dispari: se $(-a,-b,-c)$ è soluzione, allora anche (a,b,c) è soluzione.

[4] Si riesce a formalizzare bene questi passaggi usando il teorema fondamentale dell'Aritmetica, provate!

[5] *Hint:* se le terne (a,b,c) sono infinite, lo saranno anche quelle $(\frac{a}{c}, \frac{b}{c}, 1)$. Cosa ci dice questo?

Esattamente con le stesse considerazione del caso $n = 2$ si dimostra che la parità deve essere del tipo (P, D, D).

Inoltre Fermat stesso osservò che, visto che ogni interno ≥ 3 è divisibile o per 4 o per un primo dispari, allora per dimostrare il teorema basterà dimostrarlo per $n = 4$ oppure $n = p$ (primo dispari).

La dimostrazione completa del teorema di Fermat è stata data da **A. Wiles** nel 1994 ed è molto complessa, ma già Fermat aveva dimostrato un caso particolare. Vediamo allora la dimostrazione di questo caso:

Dimostrazione: $\boxed{n = 4}$ La dimostrazione si basa sulla concatenazione di tre affermazioni:
1) Se esiste una soluzione in $\mathbb{N}^+$ di $a^4 + b^4 = c^2$ allora esistono $x, y, w \in \mathbb{N}^+$ tali che $x^4 + y^4 = w^2$ e $w < c$;
2) Allora ne deduciamo che non esiste soluzione in $\mathbb{N}^+$ di $a^4 + b^4 = c^2$.
3) Qundi non esiste soluzione in $\mathbb{N}^+$ di $a^4 + b^4 = c^4$.

Dimostrando quindi la prima di queste cose la dimostrazione è conclusa. Partiamo dal fatto che (a^2, b^2, c) è una terna pitagorica, quindi sappiamo che valgono le relazioni:

$$\begin{cases} a^2 = m^2 - n^2 \\ b^2 = 2mn \\ c^2 = m^2 + n^2 \end{cases} \implies m^2 = a^2 + n^2 \implies (a, n, m) \text{ è una terna pitagorica}$$

$$\implies \begin{cases} a = r^2 - s^2 \\ n = 2rs \\ m = r^2 + s^2 \end{cases}$$

ma $m \cdot \frac{n}{2} = b^2$ è un quadrato $\implies m$ è quadrato e $\frac{n}{2}$ è quadrato.
ma $\frac{n}{2} = rs$, e $\frac{n}{2}$ è quadrato $\implies r, s$ sono quadrati.
$\implies w^2 = m = r^2 + s^2 = t^4 + u^4 \implies w < c$ □

Capitolo 6

Estensioni Numeriche: $\mathbb{Q}$

6.1 Cenni Storici

Il primo accenno alle frazioni si trova già nel **Papiro di Rhind** (1800 a.C.), che contiene alcuni problemi risolubili con l'uso di esse[1].

Anche i Greci usavano le frazioni, ma non le concepivano come "numeri", bensì come rapporti tra *veri* numeri per indicare grandezze geometriche.

La concezione di frazione come vero e proprio "numero" avverrà solo molto più tardi: alla fine del 1800.

6.2 Costruzione Formale di $\mathbb{Q}$

Proprio come era stato fatto per $\mathbb{N} \longrightarrow \mathbb{Z}$ anche stavolta le motivazioni sono sia di tipo applicativo che teorico.

La motivazione applicativa è quella di misurare oggetti che non sono multipli interi dell'unità di misura prefissta.

La motivazione teorica è, invece, poter risolvere equazioni di questo tipo:

$$a \cdot x = b, \, \forall a, b \in \mathbb{Z}$$

che in $\mathbb{Z}$ risultano ancora insolubili.

Definizione. chiamo $\mathcal{F} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, \, b \neq 0\}$ l'insieme delle *frazioni*

Però si nota che nelle frazioni vale

$$\frac{m}{n} = \frac{m \cdot c}{n \cdot c} \quad \forall c$$

[1]Gli antichi Egizi avevano una concezione della matematica molto radicata, tanto che essa era addirittura considerata come una serie di *"norme per investigare nella Natura e per conoscere tutto ciò che esiste, ogni mistero, ogni segreto"!*

Quindi introduciamo sulle frazioni una relazione di equivalenza[2]:

$$\mathbb{Q} = \mathcal{F}/_{\sim}\ , \quad \frac{a}{b} \sim \frac{c}{d} \Longleftrightarrow a \cdot d = c \cdot b$$

Esercizio. Cosa rappresentano le classi di equivalenza nel piano $\mathbb{Z} \times \mathbb{Z}$?

Introduciamo le operazioni e la nozione di ordine sul nostro nuovo insieme:

- **Somma:**
$$\frac{a}{b} \oplus \frac{c}{d} = \frac{ad + bc}{bd}$$
Perchè la somma è stata definita in questo buffo modo? Non potevamo più semplicemente dire $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$?
Ebbene no, non potevamo. Le motivazioni sono molte, ad esempio con la definizione "semplice" (ma sbagliata) avremmo avuto:
$$\frac{1}{2} \oplus \frac{1}{2} = \frac{2}{4} = \frac{1}{2}$$
che non è proprio quello che ci aspettiamo...[3]

Esercizio. Per quali razionali è vero che $\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$?

Esercizio. Quand'è che la somma "semplice" risponde ad una vera esigenza di calcolo?[4] Perchè può succedere?

- **Prodotto:**
$$\frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd}$$

Visto che $\mathbb{Q}$ è estensione di $\mathbb{Z}$ vogliamo che accada, proprio come era accaduto nell'estendere $\mathbb{N}$ in $\mathbb{Z}$, che esista all'interno di $\mathbb{Q}$ una copia *isomorfa* di $\mathbb{Z}$. Ancora una volta il ragionamento che si fa per trovarla è molto simile a quello già fatto per gli interi:

$$\begin{array}{rcl} i : \mathbb{Z} & \longrightarrow & \mathbb{Q} \\ n & \longmapsto & \frac{n}{1} \end{array}$$

Esercizio. Dimostrare che i è un morfismo iniettivo

Osservazione. Una piccola osservazione che vale la pena di fare è che noi siamo partiti con l'idea di voler risolvere tutte le equazioni del tipo: $ax = b$ con $a, b \in \mathbb{Z}$, ma quello che abbiamo raggiunto è un risultato ben più ampio: possiamo adesso risolvere tutte le equazioni del tipo: $ax = b$ con $a, b \in \mathbb{Q}$!

---

[2] Che è esattamente la stessa cosa che si è fatto con gli interi per risolvere il problema dei "troppi" rappresentanti per uno stesso numero!

[3] Sapresti trovare altre motivazioni?

[4] *Hint:* se una squadra vince 7 partite su 15 all'andata e 3 su 15 al ritorno quante partite in tutto a vinto?

Vediamo un'ultima questione su ciò che abbiamo costruito: perchè non diamo significato ad una scrittura del tipo $\frac{a}{0}$? Perchè $\nexists 0^{-1}$?

In linea di massima potremmo anche definire un simbolo per l'inverso di 0, ma poi cosa succederebbe?

Definiamo $0^{-1} = \bigstar$, con le seguenti proprietà:

- $0 \cdot \bigstar = 1$
- $a \cdot \bigstar = \bigstar \quad \forall a \neq 0$
- $a + \bigstar = \bigstar \quad \forall a \in \mathbb{Q}$

Allora vale

$$\begin{cases} (a \cdot 0) \cdot \bigstar = 0 \cdot \bigstar = 1 \\ a \cdot (0 \cdot \bigstar) = a \cdot 1 = a \end{cases} \qquad \Longrightarrow \quad (a \cdot 0) \cdot \bigstar \neq a \cdot (0 \cdot \bigstar)$$

il che non ci rende affatto soddisfatti.

6.3 Numeri Universo

Visto che adesso consideriamo le frazioni abbiamo anche la *scrittura decimale* di un numero razionale, ovvero

$$\frac{a}{c} = \sum_{i=1}^{\infty} q_i \cdot 10^{-1}$$

in cui i numeri q_i rappresentano i quozienti della divisione euclidea di a su c.

La scrittura decimale di un numero può essere finita (nel qual caso i q_i saranno uguali a zero da un certo punto in poi) o anche infinita, ma vale un risultato molto importante:

Proposizione. *Ogni numero razionale ha una scrittura decimale finita o periodica*

Questo ci dice che non può esserci una scrittura infinita senza ripetizioni di alcun tipo!

Esercizio. Dimostrare la proposizione[5]

Definiamo ora dei numeri molto particolari

Definizione. un numero α si dice *numero universo* se la sua scrittura decimale contiene tutte le sequenze finite di cifre possibili

[5] *Hint:* se facendo le divisioni con resto ritrovo un risultato già trovato, cosa succede?

Osservazione. Per la proposizione precedente sicuramente i numeri universo sono irrazionali

Il primo (e più facile) numero universo che si riesce ad immaginare è probabilmente:

$$0,12345678910111213141516171718192021222324252627...$$

chiamato *numero di* ***Champernowne***.

Sui numeri universo sono in corso ancora delle congetture, ad esempio:

1. tutti i numeri universo sono trascendenti;
2. π è un numero universo.

Una cosa certa è, invece, che le potenze di 2 scritte di seguito formano qualsiasi cifra finita, dal quale si ricava che $0,1248163264128...$ è un numero universo.

Domanda: l'insieme dei numeri universo è chiuso per somma?
No, perchè se $0,a_1a_2a_3...$ è un numero universo, allora lo sarà anche $0,(9-a_1)(9-a_2)(9-a_3)...$, ma la loro somma ci dà esattamente $0,999999...$, che non è un numero universo.

Lascio da dimostrare una proposizione molto facile

Proposizione. *Ogni numero universo contiene tutte le cifre finite un numero infinito di volte*

Capitolo 7

Estensioni Numeriche: $\mathbb{R}$

7.1 Cenni Storici

La scoperta di numeri non razionali era già stata fatta dai **Pitagorici** nel VI secolo Avanti Cristo. Essi infatti consideravano tutti i tipi di grandezze (anche la diagonale del quadrato), ma limitavano i rapporti numerici alle sole grandezze commensurabili per evitare che l'Algoritmo di Euclide desse luogo a processi infiniti.

Eudosso (∼408-355 AC) introduce una teoria delle proporzioni che non fa più riferimento al numero, ma solo alle grandezze geometriche. Se le grandezze sono incommensurabili egli dice che "si può parlare implicitamente del loro rapporto" stabilendo anche un ordine[1] fra questi rapporti grazie al **Principio di Esaustione**: il rapporto di due grandezze a e b è *uguale* (o *nella stessa poporzione*) al rapporto tra due grandezze A e B se vale che

$$\forall m, n \in \mathbb{N} \quad \text{vale che} \quad \begin{array}{l} ma < nb \iff mA < nB \\ ma = nb \iff mA = nB \\ ma > nb \iff mA > nB \end{array}$$

Durante i secoli che arrivano fino alla fine del Medioevo in occidente si ha un completo blocco dello sviluppo della scienza, e di conseguenza della Matematica, dovuto a diversi fattori: la religiosità boicottava apertamente il sapere scientifico, molti erano convinti che gli antichi greci avessero scoperto praticamente tutto.

Lo sviluppo riprenderà quindi poi nel 1500 con gli scambi commerciali, che impongono nuove necessità matematiche nella vita di molti cittadini. Principalmente in questo periodo abbiamo due motivi per lo sviluppo: il primo riguarda il fatto che gli scambi commerciali (e quindi inevitabilmente anche culturali) avvenivano anche con popolazioni che avevano una conoscenza matematica molto più avanzata di quella occidentale, basti pensare a i popoli arabi che ripresero il sapere scientifico dell'antica Grecia e lo

[1] "*Egual relazione tra coppie di grandezze" [cit].*

ampliarono con nuove scoperte. Il secondo motivo è che compare un'unità di misura unica (il denaro) che è svincolata dalla geometria, e quindi totalmente astratta.

Dopo questo iniziale sviluppo di tipo commerciale iniziano a venire fuori problemi più astratti che richiedono soluzioni numeriche per equazioni di terzo o quarto grado, in cui l'astrazione gioca quindi un ruolo fondamentale e ci si slaccia dalla semplice necessità pratica.

Nella risoluzione di equazioni di terzo e quarto grado vengono quindi fuori radici quadrate, cubiche e così via, ma non erano ancora stati considerati esplicitamente numeri non razionali, dunque mancava sia la concezione che la notazione necessaria. Questa difficoltà è facilmente superata con l'approssimazione di un qualsiasi irrazionale, che è sempre possibile grazie alla densità dei razionali. Dunque a questo livello i numeri reali semplicemente non servono.

Nella seconda metà del 1500 inizia lo sviluppo del calcolo algebrico grazie a **Viète** (1540-1603) che distacca totalmente il concetto di numero dal contesto pratico e commerciale.

Ma la vera svolta si ha solo con la nascita del calcolo infinitesimale (differenziale e integrale) a cavallo tra il 1600 e il 1700 grazie a **Leibniz** e **Newton**. Riportiamo una interessante citazione a tal proposito:

> *Dagli irrazionali sono nate le quantità impossibili e immaginarie, la cui natura è molto strana, ma la cui utilità non è discutibile.*
>
> Leibniz

Ma in questo ambito si riscontrarono moltissimi problemi teorici, anche se la spinta iniziale fu così travolgente che i matematici del tempo svilupparono moltissime teorie e risultati senza preoccuparsi delle fondamenta su cui questi si basavano.

Abel fu uno dei primi ad accorgersi e a meravigliarsi della poca fondatezza del "Calcolo", e fu tra coloro che spinsero la comunità dei matematici a cercare di sistemare i fondamenti teorici di tutta la matematica nella seconda metà del 1800.

Nel frattempo durante il 1800 **Cauchy** e **Weierstrass** incontrano molti problemi nello sviluppo della teoria dei limiti, e credono che tali problemi nascano proprio dalla non formalizzazione dei numeri reali.

Seguendo queste conclusioni nel 1872 escono ben quattro articoli diversi di formalizzazione dei reali: uno che si basa sulla costruzione dei reali come limiti di **Successioni di Cauchy**, dovuto a **Cantor**; uno legato al **Teorema degli Zeri** di **Bolzano**; uno basato sull'idea delle **Sezioni Razionali** di **Dedekind**; uno dovuto a **Méray**.

Studiando questi diversi approcci per formalizzare $\mathbb{R}$ i matematici compresero che era necessaria una formalizzazione prima di $\mathbb{Q}$, per la quale serve la formalizzazione di $\mathbb{N}$, che si avrà dunque nell'arco del 1900.

7.2 Costruzione Formale di $\mathbb{R}$

7.2.1 Sezioni di Dedekind

Un possibile modo per definire $\mathbb{R}$ è quello usato da **Dedekind**(1872): le *sezioni*.

Definizione. Dati $\alpha \subset \mathbb{Q}$, $\beta \subset \mathbb{Q}$, definiamo una *Sezione di* $\mathbb{Q}$ come la coppia (α, β) tale che

- $\alpha \cup \beta = \mathbb{Q}$
- $\alpha \neq \emptyset$, $\beta \neq \emptyset$
- $\forall a \in \alpha$ e $\forall b \in \beta$ vale che $a < b$

Data la sezione (α, β) vale sicuramente uno dei seguenti:

1. α ha un massimo e β ha un minimo
2. α ha un massimo e β non ha un minimo
3. α non ha un massimo e β ha un minimo
4. α non ha un massimo e β non ha un minimo

In realtà si può facilmente notare che il primo caso non si potrà mai verificare, visto che se α ha un massimo a e β ha un minimo b ho che $\frac{a+b}{2}$ è un razionale che non sta in nessuno dei due, il che è assurdo perché la loro unione deve essere tutto $\mathbb{Q}$.

Una volta definite le sezioni potremmo definire i numeri reali con una relazione di equivalenza sulle sezioni, in modo analogo a quello fatto per la costruzione di $\mathbb{Z}$ a partire dalle coppie di naturali.

Per evitare tutto ciò useremo un'altro approccio: quello di **Cantor**, che riesce a definire $\mathbb{R}$ senza passare dalla relazione di equivalenza!

Come fa? Definendo in modo leggermente diverso le sezioni:

Definizione. β si dice *Sezione di* $\mathbb{Q}$ se valgono i seguenti fatti:

- $\beta \neq \emptyset$, $(\mathbb{Q} \setminus \beta) \neq \emptyset$
- $r \in \beta$, $s \in \mathbb{Q}$ t.c. $r < s \Longrightarrow s \in \beta$
- β <u>non</u> ha minimo

Cioè quello che facciamo è semplicemente esplicitare solo l'insieme "destro" delle sezioni definite da Dedekind, tanto l'altro sarà il suo complementare per forza, per completare tutto $\mathbb{Q}$.

Identifico, allora, i reali proprio come le sezioni di razionali: $\mathbb{R} = \mathcal{S}_C$ (sezioni di Cantor).

Avendo creato un'estensione dobbiamo, come sempre, controllare che al suo interno vi sia una copia isomorfa del "vecchio" insieme:

$$\begin{array}{rccc} \varphi: & \mathbb{Q} & \longrightarrow & \mathbb{R} \\ & q & \longmapsto & \{x \in \mathbb{Q} \mid x > q\} \end{array}$$

La φ così definita è iniettiva poiché $q_1 > q_2 \Longrightarrow q_1 \in (\varphi(q_2) \setminus \varphi(q_1))$.

Osservazione. β è razionale $\Longleftrightarrow \beta^c$ ha un massimo

Teorema. $\mathbb{Q} \subsetneq \mathbb{R}$

Dimostrazione: Ci basta trovare una sezione che sia reale ma non razionale.

Tra le tante possibili una è: $\beta = \{x \in \mathbb{Q} \mid x \geq 0,\ x^2 > 2\}$ che è una sezione, ma non è razionale.

□

Cosa ha $\mathbb{R}$ che non aveva $\mathbb{Q}$?

Una cosa importantissima, l'**Assioma di Continuità**:

> *Se una partizione di tutti i punti della retta è tale che ogni punto di una classe sta a sinistra di ogni punto dell'altra, allora vi è uno ed un solo punto dal quale questa decomposizione della retta è prodotta.*
>
> *La proprietà della retta espressa da questo principio non è che un'assioma, ed è solo sotto forma di questo assioma che riconosciamo alla retta la sua continuità.*
>
> Dedekind

Osservazione. Per ogni q in $\mathbb{Q}$ esiste una sezione che ha q come elemento separatore. Ma non è vero che per ogni sezione di $\mathbb{Q}$ trovo un razionale separatore. Le sezioni per cui accade ciò saranno gli "irrazionali".

Definiamo ora l'ordine su $\mathbb{R}$:

$$\beta \leq \alpha \iff \alpha \subseteq \beta$$

Cioè mi riporto all'ordinamento insiemistico "$\subseteq$" che già conosco. Proprio grazie al fatto che mi sono riportato ad un ordinamento già precedentemente conosciuto vale che "$\leq$" così definito è un ordinamento ben definito (cioè valgono le proprietà riflessiva, antisimmetrica e transitiva).[2]

Osservazione. $\varphi : \mathbb{Q} \longrightarrow \mathbb{R}$ rispetta l'ordinamento appena definito, poiché vale: $q_1 \leq_{\mathbb{Q}} q_2 \Longrightarrow \varphi(q_1) \leq_{\mathbb{R}} \varphi(q_2)$.

Una volta definito in questo modo l'ordinamento valgono alcuni teoremi molto interessanti che andiamo a dimostrare, dopo aver introdotto un paio di nuove definizioni:

Definizione. Un ordinamento su un insieme $\mathcal{X}$ si dice *totale* se $\forall a, b \in \mathcal{X}$ con $a \neq b$ vale $a < b$ oppure $b < a$.

Definizione. Un ordinamento su un insieme $\mathcal{X}$ si dice *completo* se ogni sottoinsieme inferiormente (o superiormente) limitato di $\mathcal{X}$ ammette estremo inferiore (o superiore).

Teorema. *"$\leq_{\mathbb{R}}$" è un ordinamento totale.*

Dimostrazione: Devo dimostrare che $\forall \alpha, \beta \in \mathbb{R},\ \alpha \neq \beta \Longrightarrow \alpha < \beta$ oppure $\beta < \alpha$, dunque:

Supponiamo che $\exists a \in \beta \setminus \alpha$. Visto che non sta in $\alpha \Longrightarrow a \in \overline{\alpha}$.

Allora $\forall s \in \alpha \Rightarrow a < s$, ed inoltre $a \in \beta \Longrightarrow s \in \beta \Longrightarrow \alpha \subset \beta$ □

Teorema. *"$\leq_{\mathbb{R}}$" è un ordinamento completo.*

Dimostrazione: Supponiamo di avere $\mathcal{A} \subseteq \mathbb{R}$ inferiormente limitato.

Dovendo trovare un estremo inferiore un ottimo candidato è: $\beta = \bigcup_{\alpha \in \mathcal{A}} \alpha$. Sarà davvero l'estremo inferiore che cerchiamo?

Preso γ tale che $\gamma < \alpha\ \forall \alpha \in \mathcal{A}$ sicuramente vale, per costruzione di β, che $\gamma \subset \beta$, quindi è proprio lui. □

Osservazione. Nella dimostrazione del teorema avremmo dovuto dimostrare che il β preso in considerazione è effettivamente un taglio, ma lo lasciamo come esercizio, visto che le verifiche sono quelle della definizione.

Teorema (Completezza di Dedekind)**.** *Ogni sezione di numeri reali individua un numero reale.*

[2] Potrebbe essere un buon allenamento provarle comunque!

Dimostrazione: Cerco $\psi : \mathbb{R} \longrightarrow \{\text{Tagli di } \mathbb{R}\}$ che sia surgettiva.

Preso $\mathcal{A}$ taglio di $\mathbb{R}$ per definizione di taglio si ha che $\mathcal{A}$ è inferiormente limitato, quindi possiamo definire $\gamma = \inf(\mathcal{A})$ e a questo punto la funzione la possiamo costruire come:

$$\psi(\gamma) = \{x \in \mathbb{R} \,|\, \gamma < x\} = \mathcal{A}$$

□

Abbiamo costruito $\mathbb{R}$ a partire da $\mathbb{Q}$ e abbiamo ottenuto un insieme con molte proprietà, tra cui la seguente importante:

Osservazione. $\mathbb{Q}$ è denso in $\mathbb{R}$

Dimostrazione: Voglio che $\forall \alpha, \beta \in \mathbb{R}$ tc $\alpha < \beta$ $\exists q \in \mathbb{Q}$ tc $\alpha < q < \beta$.

Ma $\alpha < \beta \Longrightarrow \beta \subsetneq \alpha$, quindi prendo $q \in \alpha \setminus \beta$ ed ho che:

$\beta \subsetneq \varphi(q) = \{x \in \mathbb{Q} \,|\, q < x\} \subsetneq \alpha$, che è equivalente a dire $\alpha < q < \beta$ □

Ciò che ci manca di definire adesso sono le operazioni nel nostro nuovo insieme, dunque facciamolo:

⊕ ***Somma:***

$$\forall \alpha, \beta \in \mathbb{R} \qquad \alpha + \beta := \{r + s \,|\, r \in \alpha, s \in \beta\}$$

Esercizio. Dimostrare che l'operazione appena definita rispetta i seguenti tre punti:
1) è ben definita (cioè se la somma è un taglio);
2) si "comporta bene" su $\mathbb{Q}$ (cioè se $\varphi(q_1 +_{\mathbb{Q}} q_2) = \varphi(q_1) +_{\mathbb{R}} \varphi(q_2)$);
3) $+_{\mathbb{R}}$ è compatibile con $\leq_{\mathbb{R}}$ (cioè se $\alpha < \beta \Rightarrow \forall \gamma \in \mathbb{R}\ \gamma + \alpha < \gamma + \beta$).

Teorema. $(\mathbb{R}, +)$ *è un gruppo abeliano con* $\varphi(0)$ *come elemento neutro.*

Dimostrazione: Dato $\alpha \in \mathbb{R}$ definiamo $-\alpha := \{-x \in \mathbb{Q} \mid x \in \overline{\alpha},\ x \neq \max(\overline{\alpha})\}$

Dimostriamo che $\alpha + (-\alpha) = \varphi(0)$ con la doppia inclusione:

$\boxed{\subseteq}$ $\forall a, b \in \alpha + (-\alpha) \Rightarrow a - b > 0 \Rightarrow a - b \in \varphi(0)$.

$\boxed{\supseteq}$ $a \in \varphi(0) \Rightarrow a > 0$, allora prendo $t \in \alpha, s \in \overline{\alpha} \Rightarrow 0 < t - s < a$. Visto che $t - s \in \alpha + (-\alpha) \Rightarrow a \in \alpha + (-\alpha)$.

□

⊗ ***Moltiplicazione:*** Se definiamo l'operazione nel modo analogo a quello fatto per la somma, ovvero: $\forall \alpha, \beta \in \mathbb{R} \quad \alpha \cdot \beta := \{r \cdot s \,|\, r \in \alpha, s \in \beta\}$ scopriamo che il prodotto

appena definito è un taglio solo se $\alpha, \beta > 0$.

Allora quello che facciamo è definire la moltiplicazione per i positivi in questo modo:

$$\forall \alpha, \beta \in \mathbb{R}^+ \qquad \alpha \cdot \beta := \{r \cdot s \,|\, r \in \alpha, s \in \beta\}$$

E poi proseguire come abbiamo fatto per $\mathbb{Z}$:

$$\forall \alpha \in \mathbb{R} \quad \exists \beta, \gamma \in \mathbb{R}^+ \text{ tc } \alpha = \beta + (-\gamma)$$

$$\implies \text{definiamo} \quad \forall \alpha, \beta \in \mathbb{R} \quad \alpha \cdot \beta := (\alpha_1 \cdot \beta_1) - (\alpha_2 \cdot \beta_1) - (\alpha_1 \cdot \beta_2) + (\alpha_2 \cdot \beta_2)$$

$$\text{dove} \qquad \alpha = \alpha_1 - \alpha_2 \quad \beta = \beta_1 - \beta_2$$

Come per le altre volte lasciamo per esercizio di dimostrare le proprietà dell'operazione appena definita. É utile osservare che, avendo definito tutto a partire da elementi positivi per le proprietà "classiche" che dovremo dimostrare ci possiamo limitare ad analizzare il caso di elementi di questo tipo.

Esercizio. Dimostrare che l'operazione appena definita rispetta i seguenti tre punti:
1) è ben definita (cioè se $\alpha \cdot \beta$ è un taglio);
2) si "comporta bene" su $\mathbb{Q}$ (cioè se $\varphi(q_1 \cdot_{\mathbb{Q}} q_2) = \varphi(q_1) \cdot_{\mathbb{R}} \varphi(q_2)$);
3) $\cdot_{\mathbb{R}}$ è compatibile con $\leq_{\mathbb{R}}$ (cioè se $\alpha < \beta \Rightarrow \forall \gamma \in \mathbb{R}\ \gamma \cdot \alpha < \gamma \cdot \beta$);
4) il prodotto definito non dipende dai rappresentati scelti per α e β.

Analogamento a quanto fatto per la somma è possibile dimostrare:

Teorema. $(\mathbb{R}, +, \cdot)$ *è un campo con* $\varphi(1)$ *come elemento neutro moltiplicativo.*

Adesso che abbiamo definito anche le operazioni del nuovo insieme possiamo dimostrare un importante risultato:

Teorema. $\mathbb{R}$ *è archimedeo*[3].

Dimostrazione: L'idea è partire dal dimostrare che $\mathbb{N}$ non è limitato su $\mathbb{R}$, e poi è fatta perché un qualsiasi elemento di $\mathbb{R}$ potrà essere superato da un apposito elemento di $\mathbb{N}$.

Supponiamo $\mathbb{N}$ limitato $\mathbb{R}$.
Chiamo $\mathcal{M} = \{$ insieme dei maggioranti di $\mathbb{N}\}$.
Visto che $\mathbb{N}$ è limitato $\exists c$ estremo inferiore di $\mathcal{M}$.
Per definizione di estremo inferiore so che $\exists n \in \mathbb{N}$ tc $n \in (c-1, c)$.
Allora prendo $n + 1 \in \mathbb{N} \implies n + 1 > c \implies$ Assurdo $\square$

[3]Ricordiamo che *archimedeo* significa che $\forall x, y \in \mathbb{R}^+ \ \exists n \in \mathbb{N}$ tc $nx > y$

7.2.2 Successioni di Cauchy

Quello presentato nel paragrafo precedente non è l'unico modo in cui sono stati pensati i numeri Reali. Anzi, ce ne furono molti nell'arco degli studi matematici, e nei prossimi paragrafi ne proporremo alcuni tra i più noti.

Come fece Dedekind anche altri matematici (**Cantor**, **Meray**) cercano di costruire i numeri reali partendo da un diverso progetto, iniziato da **Cauchy**: vedere i reali come limiti di successioni razionali "particolari" (quelle che poi prenderanno il nome proprio di *successioni di Cauchy*).

Cauchy aveva un grosso problema: se una successione razionale converge a qualcosa di irrazionale vuol dire che, considerata solo nel suo insieme di appartenenza, non converge. Questo implica, in particolare, che non posso sapere chi sia quel numero a cui essa si avvicina indefinitamente.

La grande idea di Cantor e Meray è stata di definire un numero reale non come il limite di una data successione razionale, ma come la successione stessa!

Se definiamo $\mathcal{F}$:=$\{$successioni di Cauchy razionali$\}$ dobbiamo cercare di definire un ordine e delle operazioni in questo insieme:

$\{a_n\} \geq 0 \iff \exists q \in \mathbb{Q}^+$ tale che da un certo punto in poi "per quasi ogni" $n > k$ vale $a_n \geq q$ (in cui "quasi ogni" vuol dire che quelli che non lo fanno sono in numero finito).

Operazioni: $\{a_n\}+\{b_n\}:=\{a_n+b_n\}$
$\{a_n\}\cdot\{b_n\}:=\{a_n\cdot b_n\}$

Ora abbiamo un nuovo insieme. Visto che è un'estensione dell'insieme $\mathbb{Q}$ dobbiamo trovare una "copia" di quest'ultimo all'interno del nuovo "$\mathbb{R}$":

$$\begin{array}{rccl} \varphi: & \mathbb{Q} & \longrightarrow & \mathcal{F} \\ & q & \longmapsto & \{a_n\} \text{ t.c. } a_n = q \ \underline{\forall n} \end{array}$$

Definizione. Una *Successione Razionalmente Convergente* è una successione che converge ad un numero razionale.

Sappiamo bene che vale il teorema:

Teorema. *Ogni successione razionalmente convergente è di Cauchy*

Osservazione. Non è vero il viceversa!

Esempio. Un esempio possibile è la famosa *Sezione Aurea*:

$$\begin{cases} a_0 = 1 \\ a_{n+1} = 1 + \frac{1}{1+a_n} \end{cases}$$

Ora che abbiamo il nostro nuovo "$\mathbb{R}$" dobbiamo risolvere un problema: preso un irrazionale posso trovare tantissime successioni razionali che ci convergono! Come possiamo fare? Il modo più classico è chiaramente definire una relazione di equivalenza.

$$\mathbb{R} = \mathcal{F}/_{\sim} \quad \{a_n\} \sim \{b_n\} \Leftrightarrow |a_n - b_n| = c_n \longrightarrow 0$$

Oltretutto una volta definito così il nostro insieme abbiamo subito il seguente teorema, molto usato in Analisi:

Teorema. *In $\mathcal{F}/_{\sim}$ una successione è convergente se e solo se è di Cauchy.*

Osservazione. $\mathcal{F}/_{\sim}$ è in corrispondenza biunivoca con le sezioni.

7.2.3 Allineamenti Decimali

Definizione. Si dice *allineamento decimale* una funzione $f : \mathbb{N} \longrightarrow \mathbb{Z}$ tale che

$$f(0) \in \mathbb{Z} \qquad f(n) \in \{0, 1, \ldots, 9\}\ \forall n > 0$$

Gli allineamenti decimali vengono rappresentati sotto la forma $f(0), f(1)f(2)\ldots$.

Definizione. Dato un allineamento decimale f chiamiamo *troncamento di f* la successione di Cauchy definita come

$$\{a_n\} = \left\{ \sum_{i=0}^{n} \frac{f(i)}{10^i} \right\}$$

Teorema. *Siano $\{a_n\}$, $\{b_n\}$ due troncamenti di f e g rispettivamente, con $f \neq g$. Allora i due troncamenti sono equivalenti se e solo se $\exists\, k \in \mathbb{N}$ tale che*

1. $f(n) = g(n)\ \forall n < k$
2. $f(k) = 1 + g(k)$
3. $f(n) = 0$ *e* $g(n) = 9\ \forall n > k$

Teorema. *Ogni successione di Cauchy è equivalente ad una successione di Cauchy in corrispondenza con un allineamento decimale.*

Con questi risultati abbiamo una corrispondenza tra l'insieme definito nel paragrafo precedente usando le successioni di Cauchy e gli allineamenti decimali, ovvero:

$$\mathcal{F}/_{\sim} = \{\text{Allineamenti Decimali}\}/_{\sim'}$$

In cui la relazione $\sim'$ è quella definita nel teorema riportato sopra.

Ma in effetti con questo approccio ci sono un po' di problemi da risolvere.

Ad esempio quali sono gli allineamenti decimali che rappresentano i numeri razionali?

In questo caso la soluzione, facendo un po' di conti, si trova: i numeri razionali sono rappresentati da allineamenti decimali finiti o periodici. Ma la soluzione non è poi così semplice ed ha richiesto storicamente diversi sforzi per essere trovata.

Ma i problemi non sono finiti qua: che ordinamento metto nel mio insieme?

Il primo che ci può venire in mente è quello lessicografico, ma purtroppo con questo ordinamento risulterebbe $1 = 0,\overline{9}$, che va contro la relazione di equivalenza definita poco fa.

Esercizio. Provare a definire un ordinamento sull'insieme ora costruito e verificare se questo mantiene la relazione d'ordine.

7.3 Assioma di Completezza

La completezza di $\mathbb{R}$ è un concetto fondamentale della matematica, e come accade spesso in casi come questo i matematici nell'arco del tempo hanno trovato molte forme equivalenti di dire che $\mathbb{R}$ è completo. Ne riportiamo quattro tra la principali:

Completezza di Dedekind: Data una sezione (A, B) esiste un unico elemento separatore.

Completezza di Cauchy: Ogni successione di Cauchy converge.

Completezza per Intervalli: Ogni successione di intervalli incapsulati la cui misura tende a zro ha un unico punto nell'intersezione.

Esistenza dell'Estremo Superiore: Dato A superiormente limitato esiste $\sup A$.

Capitolo 8

Problemi di MEPVS: Aritmetica

1. Stabilire per quali $n \in \mathbb{N}$ è possibile dividere un quadrato in esattamente n quadrati.

2. Dimostrare che un polinomio non può generare solo numeri primi (cioè che valutato in numeri interi non restituisce solo numeri primi, ad esempio $n^2-79n+1601$ genera numeri primi fino a $n = 80$).

3. È vero che $\forall n \in \mathbb{N}$ vale $\sum_{i=1}^{n} i = -\frac{1}{6}n^3+\frac{3}{2}n^2-\frac{4}{3}n+1$? Se no, per quali n funziona?

4. Determinare quali numeri naturali si possono scrivere come somma di k numeri naturali consecutivi (con $k \geq 2$).

5. Determinare il massimo numero di parti in cui n punti, scelti su una circonferenza, dividono il relativo cerchio, quando vengono congiunti due a due mediante corde.

6. Dimostrare che la somma in $\mathbb{N}$ è commutativa.

7. Dimostrare che per $n \geq 2$ si ha che: $p|\mathbb{F}_n \Rightarrow p \equiv 1 \pmod{2^{n+2}}$ (dove $\mathbb{F}_n$ indica l'ennesimo numero di Fermat).

8. Definamo $\sigma(n) = \sum_{d|n,d\neq 1} d$. Dimostrare che dati $a, b \in \mathbb{N}$ vale che: *MCD(a,b)=1* $\implies \sigma(ab) = \sigma(a)\sigma(b)$.

9. Dimostrare che vale $\mathbb{N}_{S(m)} = \mathbb{N}_m \bigcup S(m)$ (in cui abbiamo definito $\mathbb{N}_m = \{n \in \mathbb{N} \,|\, n < m\}$, e con $S(\cdot)$ il successore).

10. Gettiamo su un tavolo 15 fazzoletti con misura e forma diverse in modo da coprirlo tutto. Dimostrare che si possono scegliere 8 fazzoletti da togliere in modo che ameno i $\frac{7}{15}$ del tavolo rimangano coperti.

11. Dimostrare che tra 51 punti scelti in un quadrato unitario ne esistono almeno 3 che sono in un cerchio di raggio $\frac{1}{7}$.

12. I 123 abitanti di un paese hanno come somma delle età 3813 anni. Dimostrare che ne esistono 100 la cui somma delle età è almeno 3100.

13. Data una superficie bianca rettangolare di misura 8x16 metri vengono spruzzati di vernice blu a casaccio 12 m^2. Siamo sicuri che esistono due punti a distanza 1 metro di colore uguale? E di colore diverso?

14. Esistono potenze intere di 29 che finiscono con le cifre "001"?

15. Su una circonferenza butto del colore rosso a caso colorando meno della metà della circonferenza stessa. Dimostrare che esistono 2 punti antipodali non colorati.

16. Per quali $a, b, c, d \in \mathbb{Z}$ vale $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{b+d}$?

17. Provare che $\frac{r}{p} < \frac{s}{q} \Longrightarrow \frac{r}{p} < \frac{r+s}{p+q} < \frac{s}{q}$.

18. Scrivere un algoritmo per passare da una frazione alla sua rappresentazione decimale.

19. Dimostrare che gli allineamenti decimali corrispondenti ai numeri razionali possono essere solo finiti o periodici.

20. Per conoscere *esattamente* l'n-esima cifra decimale di $\alpha + \beta$ e di $\alpha \cdot \beta$ quante cifre di α e β (numeri decimali anche infiniti) devo conoscere?