LA MATEMATICA FA PER TE?

INTRODUZIONE ALLA
MATEMATICA UNIVERSITARIA

STEFANO COSTA

Il fronte e il retro della copertina sono la rappresentazione grafica di alcune iterazioni del frattale di Cantor (*"Cantor set"*)

Preambolo

Questo libro nasce con il desiderio di chiarire cosa sia davvero la matematica e cosa significhi studiarla. Purtroppo alle superiori, per via delle poche ore, non si trasmette agli studenti la vera essenza della materia, che diventa quasi esclusivamente studio di esercizi e successiva ripetizione degli stessi. Questa vuole essere un'introduzione, un primo sguardo al mondo matematico universitario e vuole dare un'idea di come si studi alla facoltá di matematica riportando i primi argomenti (che non richiedono preparazione di alcun tipo). Il tema centrale, che fa da filo conduttore, é il concetto di insieme, concetto fondante in matematica. Verranno date diverse definizioni e mostrate alcune dimostrazioni, principale argomento nello studio universitario, per poi spiegare la costruzione dei numeri e infine, l'argomento piú difficile, verranno dimostrati i criteri di divisibilitá. L'ordine dei capitoli é tale da presentare una difficoltá crescente negli argomenti, ma é stato originariamente scelto in modo da trasmettere la struttura sequenziale dello studio della matematica, il quale si sviluppa su conoscenze precedentemente acquisite, che quindi devono essere sufficientemente radicate. Non intendo dire che per entrare in facoltá sia necessario essere usciti da un liceo (sicuramente torna utile, questo é certo), ma che lo studio debba essere giornaliero e intrapreso fin dal primo giorno.
Se non é tutto chiaro alla prima lettura non c'é da allarmarsi: il formalismo matematico, la principale causa di disorientamento nelle nuove matricole, é una questione di forma mentis che si acquisisce anche con l'esperienza. Ognuno ha i propri tempi per imparare e il mio consiglio é sfruttare questo libro per mettersi alla prova con i primi argomenti (non necessariamente intuitivi) trattati all'universitá dedicandoci tutto il tempo necessario. La scelta di portare i primi argomenti trattati é utile ovviamente perché sono i piú semplici, ma anche perché non necessitano di conoscenze pregresse, quindi quello che imparerete in questo libro é esattamente quello che imparereste nei primi giorni di universitá.

Indice

Preambolo **i**

1 Simboli matematici **1**
1.1 Lista di simboli 2

2 Insiemi **3**
2.1 Definizioni 3
2.2 Operazioni tra insiemi 7
2.3 Dimostrazioni 11
2.3.1 Uguaglianza tra insiemi 12
2.3.2 Commutativitá dell'unione tra insiemi 13
2.3.3 Associativitá dell'unione tra insiemi 14
2.3.4 Dimostrazione: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. 15
2.3.5 Leggi di De Morgan 17
2.3.6 Prima dimostrazione per contraddizione 19
2.3.7 Seconda dimostrazione per contraddizione 20

3 Costruzione dei numeri **21**
3.1 Numeri naturali 22
3.1.1 Operazioni sui naturali 24
3.2 Numeri interi 26
3.2.1 Operazioni sugli interi 28
3.3 Numeri razionali 29
3.3.1 Operazioni sui razionali 29
3.4 Numeri irrazionali o reali 31
3.4.1 Operazioni sui reali 37
3.5 Numeri complessi 39
3.5.1 Operazioni sui complessi 39

4 Criteri di divisibilitá **40**
4.1 Anello dei resti 41
4.1.1 Somma 43
4.1.2 Prodotto 46
4.2 Dimostrazione dei criteri di divisibilitá 47
4.2.1 Criterio di divisibilitá per 3 47
4.2.2 Criterio di divisibilitá per 5 48
4.2.3 Criterio di divisibilitá per 7 49

5 Fonti e bibliografia **52**

1 Simboli matematici

Una parte molto importante della matematica é il suo linguaggio che, diversamente da altre lingue e idiomi, consente "solo" di dare definizioni e dimostrazioni. Alle scuole superiori non si usa che una piccola parte del linguaggio matematico senza approfondire il tema e spesso si usano semplificazioni per rendere la materia meno pesante.
La matematica, peró, é nota per la sua universalitá, quindi l'indipendenza da qualunque idioma, e per la rigorositá, cioé per non lasciare spazio a cattive interpretazioni, ed é quindi necessario un linguaggio ben strutturato e completo per rispettare queste due proprietá.
A dimostrare l'importanza dell'universalitá del linguaggio sono i molteplici teoremi risultato di collaborazioni tra grandi matematici di nazionalitá diversa che diedero luce ad importanti risultati che tuttora portano il nome dei loro creatori, come i noti teoremi di Heine-Cantor, di Bolzano-Weierstrass, di Borel-Heine...
Ma non basterebbe solo l'indipendenza dalle lingue nel linguaggio matematico: senza un rigido formalismo questa non sarebbe rigorosa. Basta pensare ad un banale esempio: cosa intendiamo con "cinque piú due diviso tre"? Intendiamo $5 + \frac{2}{3}$ oppure $\frac{5+2}{3}$?
Risulta dunque chiaro che i simboli matematici, per quanto possano risultare noiosi a prima vista, siano un importante punto di partenza per lo studio della matematica.
Nel libro verranno introdotti i simboli piú utilizzati e verranno spiegati mano a mano che compariranno sia con spiegazioni che attraverso esempi del loro utilizzo. Nella pagina successiva viene riportata una lista riassuntiva dei simboli usati con una breve spiegazione del loro significato.

1.1 Lista di simboli

Simboli logici

$\Rightarrow$	Implicazione, se é vero l'argomento a sinistra allora é vero anche quello a destra
$\Leftrightarrow$	Equivalenza, l'argomento a sinistra é logicamente equivalente all'argomento a destra
$\forall$	Per ogni
$\in$	Appartiene a
$\notin$	Non appartiene a
$\exists$	Esiste
$\vee$	Or, oppure
$\wedge$	And, e

Simboli insiemistici

$\mathbb{N}$	Numeri naturali $\{0, 1, 2, ...\}$
$\mathbb{Z}$	Numeri interi $\{..., -2, -1, 0, 1, 2, ...\}$
$\mathbb{Q}$	Numeri razionali $\{..., -\frac{2}{3}, 0, \frac{1}{2}, ...\}$
$\mathbb{R}$	Numeri reali $\{\sqrt{2}, \pi, ...\}$
$\mathbb{C}$	Numeri complessi $\{i = \sqrt{-1}, 1 + i, 2 + 2i, ...\}$
$\emptyset$	Insieme vuoto
$\subset$	Relazione di sottoinsieme, l'insieme a sinistra é sottoinsieme di quello a destra
$\not\subset$	L'insieme a sinistra non é sottoinsieme di quello a destra
$\setminus$	Sottrazione tra insiemi
$\cup$	Unione di insiemi
$\cap$	Intersezione di insiemi

Altri simboli usati

$\mid$	Divide: *a divide b* lo scrivo $a \mid b$
$\nmid$	Non divide: *a non divide b* lo scrivo $a \nmid b$
$\sim$	In relazione con

2 Insiemi

2.1 Definizioni

In matematica gli insiemi sono tra gli oggetti piú semplici e intuitivi da cui partire, nonostante la teoria degli insiemi sia tra le piú importanti: la teoria *assiomatica* degli insiemi é infatti la branca della matematica che sta alla base della matematica stessa. É da questa teoria che si danno le definizioni di numero e di funzione (oltre che delle loro proprietá) risultando fondamentale nell'idealizzare la rigorositá dimostrativa. Nonostante ció la teoria degli insiemi é straordinariamente complessa ed é una branca molto di nicchia per pochi specialisti, citando il mio professore di analisi: "Per quanto importante sia la teoria degli insiemi, é da piú di 40 anni che insegno e non ho mai avuto bisogno di usarla..."
L'insiemistica é il primo tema affrontato all'universitá perché il concetto stesso di insieme é un concetto 'primitivo', cioé che non deriva da altre nozioni piú elementari.

Insieme: *collezione di elementi*

Prima di dare alcuni esempi di insiemi, visto che si é parlato di teoria *assiomatica* degli insiemi, riporto la definizione di assioma:

Assioma: *Proposizione (matematica) assunta come vera*

La teoria degli insiemi infatti si basa su diversi assiomi sui quali vengono date definizioni e costruzioni. Non verrá approfondito l'argomento, in quanto troppo complesso e diramato. Tornando invece agli insiemi: in matematica per definire un insieme si usano le parentesi graffe (similmente agli array in informatica):

$$\text{Insieme dei numeri pari} : P = \{2, 4, 6, 8, ...\}$$
$$\text{Insieme dei numeri dispari} : D = \{1, 3, 5, 7, 9, ...\}$$

Generalmente i nomi degli insiemi sono formati da una lettera maiuscola. Ci sono degli insiemi particolari in matematica, i piú noti sono $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, gli insiemi dei numeri (verranno approfonditi nel prossimo capitolo), ma un insieme molto importante é:

$$\emptyset = \{\}$$

Cioé l'insieme vuoto. Per quanto banale sembri ha molte caratteristiche che lo rendono uno tra gli insiemi piú importanti, noi lo useremo nella sezione dimostrazioni.
Iniziamo ora a usare i simboli matematici nelle definizioni partendo dall'appartenenza di un elemento ad un insieme: si dice che un elemento x appartiene all'insieme A con i simboli:

$$x \in A$$

Un banale esempio:

$$A = \{1, 2, 3\}$$
$$1 \in A$$

Dunque non ha senso scrivere:

$$x \in \emptyset$$

Perché $\emptyset$ non ha elementi e dire $x \in \emptyset$ significa appunto "*x appartiene a* $\emptyset$". Viene introdotta ora la prima relazione tra insiemi, la relazione di sottoinsieme:

Sottoinsieme: *un insieme B lo diciamo sottoinsieme di A se tutti gli elementi di B appartengono anche ad A. In simboli:* $B \subset A$

Con questa definizione abbiamo un primo assaggio della rigorositá della matematica. Un esempio:

Sia $A = \{1, 2, 3\}$
Sia $B = \{1, 2\}$

Tutti gli elementi di B appartengono a A, quindi B é sottoinsieme di A
Un esempio di insieme non sottoinsieme:

Sia $A = \{1, 2, 3\}$
Sia $B = \{1, 2, 4\}$
Non tutti gli elementi di B appartengono ad A: $4 \notin A$
Quindi B non é sottoinsieme di A

Da notare l'uso del simbolo di appartenenza sbarrato. In matematica quasi sempre sbarrare un simbolo significa l'opposto del significato del simbolo. Il simbolo $\in$ significa "*appartiene a*", quindi $\notin$ significa "*non appartiene a*".
La stessa definizione attraverso la simbologia:

Sottoinsieme: *un insieme B lo diciamo sottoinsieme di A se* $\forall x \in B \Rightarrow x \in A$

La prima parte:

$$\forall x \in B$$

dice di considerare ogni elemento x nell'insieme B. Il simbolo $\forall$ indica infatti "*per ogni*", cioé di considerare ogni elemento dell'insieme.
La notazione:

$$P \Rightarrow B$$

significa che l'evento P scatena l'evento B. Cioé la freccia indica un'implicazione, una traduzione potrebbe essere "allora". Questo tipo di connettori logici sono per altro molto importanti nei test d'ingresso!

Un esempio semplice puó essere:

$$\text{Piove} \Rightarrow \text{ci sono nuvole in cielo}$$

Cioé quando piove sicuramente ci sono nuvole, a parole: "*Se piove* ***allora*** *ci sono nuvole in cielo*". La condizione a sinistra della freccia si dice *sufficiente*, infatti é sufficiente che piova per trovare delle nuvole in cielo, la condizione a destra si dice *necessaria*, infatti é necessario ci siano delle nuvole in cielo per piovere. Da notare che il contrario non é vero:

$$\text{Ci sono nuvole in cielo} \Rightarrow \text{piove}$$

Infatti non é corretto dire "*se ci sono nuvole in cielo* ***allora*** *piove*", non é raro trovare giornate nuvolose senza pioggia.
Sono uguali:

$$\text{Piove} \Rightarrow \text{ci sono nuvole in cielo}$$
$$\text{Ci sono nuvole in cielo} \Leftarrow \text{Piove}$$

Ora possiamo interpretare la definizione di sottoinsieme:

$$\forall x \in B \Rightarrow x \in A$$

A parole: "*Per ogni x che appartiene a B allora x appartiene a A*". Un esempio:

$$A = \{1, 2, 3\}$$
$$B = \{1, 2\}$$

B é sottoinsieme di A perché:

$$1 \in B \wedge 1 \in A$$
$$2 \in B \wedge 2 \in A$$

Ho introdotto il simbolo $\wedge$, che significa *e*, l'*and* logico. Quindi:

$$1 \in B \wedge 1 \in A$$

Significa "*1 appartiene a B e 1 appartiene a A*". Quindi visto che ogni elemento che appartiene a B appartiene anche a A, B é sottoinsieme di A.
Prima di passare alle operazioni con gli insiemi, che ci permetteranno di dare alcune semplici dimostrazioni, siamo in grado di capire un risultato molto importante per la matematica: l'infinitá dei numeri primi.
(Sono sicuro non sia necessario ricordare che un numero primo é un numero divisibile solo per 1 e per se' stesso)
Euclide trova una dimostrazione dell'infinitá dei numeri primi sfruttando gli insiemi (ci sono altre decine di dimostrazioni che usano branche diverse della matematica dalla topologia alla divergenza delle serie...). La dimostrazione é *per assurdo*, cioé suppone che esista un numero finito di numeri primi raggrupati in un insieme e dimostra che esiste sempre un numero primo che non appartiene a quell'insieme.
Nella dimostrazione viene usato un nuovo simbolo: per dire *a divide b* si scrive: $a \mid b$. Al solito, per dire *a non divide b* si scrive $a \nmid b$. Con "*divide*" si intende il piú comune dei significati: 2 divide 4 perché $\frac{4}{2} = 2$, cioé il risultato é un intero, e quindi 2 non divide 3 perché $\frac{3}{2} = 1.5$ dove il risultato non é un intero.

Teorema dell'infinitá dei numeri primi
Dimostrazione di Euclide

Sia l'insieme finito di numeri primi: $P = \{2, 3, ..., p_n\}$
Supponiamo che p_n sia il piú grande
Definiamo a come il prodotto di tutti i numeri nell'insieme P
$a = 2 \times 3 \times ... \times p_n$
Dimostriamo che *a+1* é primo
Se non fosse primo allora uno dei numeri primi in P dividerebbe *a+1*
cioé uno dei suoi divisori sarebbe diverso da 1 e da se' stesso
Ma $2 \nmid a + 1$: poiché $2 \mid a$
(visto che $a = 2 \times 3 \times 5... \Rightarrow \frac{a}{2} = \frac{2 \times 3 \times 5 \times ...}{2} = 3 \times 5 \times ...$)
si ha che $\frac{a+1}{2}$ ha come resto 1, cioé $2 \nmid a + 1$
Per esempio: $2 \mid 8 \Rightarrow \frac{8+1}{2} = \frac{9}{2} = 4.5$ cioé 4 con resto 1
Ugualmente con il 3: $3 \nmid a + 1$ poiché $3 \mid a$ e $\frac{a+1}{3}$ ha resto 1
Possiamo ripetere il ragionamento con tutti i numeri in P
Visto che nessun numero primo dell'insieme P divide *a+1*
significa che gli unici divisori sono 1 e *a+1*, cioé *a+1* é primo
Visto che $a + 1 > p_n$ nell'insieme P posso aggiungere $a + 1$
Ora basta ripetere il ragionamento con: $P' = \{2, 3, ..., p_n, a + 1\}$
a cui posso aggiungere $b + 1$ con $b = 2 \times 3 \times ... \times p_n \times (a + 1)$
Posso quindi ripetere all'infinito questa aggiunta, ottenendo
che non riesco a definire un insieme finito di numeri primi

Questa prima dimostrazione (probabilmente la prima che abbiate mai visto) é un modo semplice per immergersi nel mondo delle dimostrazioni, tema principale nello studio della matematica. La capacitá di dimostrare un teorema é una caratteristica fondamentale dello studente di matematica ed é la principale differenza tra matematica e le altre facoltá. É uno degli ostacoli piú grandi riuscire a dimostrare proposizioni mai viste, quindi essere in grado di assimilare informazioni e riproporle in modi diversi da come vengono spiegate, ma é una capacitá acquisibile con molto impegno e molta dedizione.

2.2 Operazioni tra insiemi

Vengono introdotte in questo capitolo le 3 principali operazioni tra insiemi. Si tratta di vere e proprie operazioni che invece di lavorare con dei numeri manipolano coppie di insiemi per ottenerne un terzo come risultato. Per quanto possano sembrare basilari, quelle tra insiemi sono operazioni molto importanti e usate in molti ambiti della matematica, primo tra tutti l'ambito dei numeri che, come vedremo nel prossimo capitolo, si definiscono attraverso gli insiemi.
Iniziamo il capitolo con l'**unione** tra insiemi:

Unione tra insiemi: *l'unione dei due insiemi A e B si indica con $A \cup B$ ed é l'insieme formato da tutti gli elementi di A e tutti gli elementi di B a meno di ripetizioni*

Con gli esempi sará piú chiaro:

$$A = \{1, 2, 3\}$$
$$B = \{1, 2, 6, 7\}$$
$$A \cup B = \{1, 2, 3, 6, 7\}$$

É importante notare che non vengono ripetuti due volte gli elementi *1,2*. In generale non ha senso definire un insieme con elementi che si ripetono, sono infatti uguali due insiemi nella forma:

$$\{1, 2, 2\} = \{1, 2\}$$

In simboli:

Unione tra insiemi: $x \in A \cup B \Leftrightarrow x \in A \vee x \in B$

La definizione é in forma: "*x appartiene all'unione di A con B ...*" e poi vengono fornite le condizioni. Spieghiamo ora i nuovi simboli:
Il primo nuovo simbolo é $\Leftrightarrow$, che é un'implicazione ($\Rightarrow$) in due direzioni, e infatti il suo significato é proprio quello dell'implicazione nei due versi:

$P \Rightarrow B$ significa che l'evento P scatena l'evento B
$P \Leftarrow B$ significa che l'evento B scatena l'evento P
$P \Leftrightarrow B$ significa che P scatena B e B scatena P

Un esempio pratico:

a oppure b é pari e l'altro é dispari $\Leftrightarrow a + b$ é dispari

In parole: "*a oppure b é pari e l'altro é dispari é equivalente a chiedere che $a + b$ sia dispari*". Infatti considerando a pari e b dispari (o viceversa) **allora** $a+b$ é effettivamente dispari ($5 + 4 = 9$), questo rende valida l'implicazione $\Rightarrow$; considerando invece una somma nella forma $a + b = c$ con c un numero dispari **allora** a o b deve essere pari e l'altro dispari ($a + b = 9$ casistica: (a, b)=(1,8), (2,7), (3,6), (4,5), (5,4), (6,3), (7,2), (8,1)), che rende valida l'implicazione $\Leftarrow$.

Visto che valgono le due implicazioni nei due versi, cioé che l'argomento a sinistra rende vero quello a destra e viceversa, é possibile dire che i due eventi sono equivalenti, cioé l'avvenire di uno é equivalente all'avvenire dell'altro. Non si puó dire che sia un'equivalenza una semplice implicazione:

$$P \Rightarrow B$$

Poiché abbiamo giá visto in precedenza che l'avvenire di B **non** scatena l'evento P (l'esempio della pioggia), quindi che il fatto che avvenga l'evento B non mi dice nulla sull'evento P
Quindi:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

Si traduce in "*x appartiene a A∪B é equivalente a dire che* $x \in A \vee x \in B$". Il simbolo $\wedge$ é giá comparso in precedenza e indica *and*, mentre $\vee$, quindi un *and* al contrario, indica *or*. In conclusione:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

Significa: "$x \in A \cup B$ *é equivalente a chiedere che* $x \in A$ *oppure (or)* $x \in B$". Dagli esempi:

$$A = \{1, 2, 3\}$$
$$B = \{1, 2, 6, 7\}$$
$$A \cup B = \{1, 2, 3, 6, 7\}$$

Infatti:

$$1 \in A \wedge 1 \in B$$
$$2 \in A \wedge 2 \in B$$
$$3 \in A$$
$$6 \in B$$
$$7 \in B$$

Nell'esempio si ha che $1 \in A$ e $1 \in B$, ma sarebbe bastato che 1 appartenesse a solo uno dei due, non era necessario appartenesse ad entrambi.

La seconda operazione che vediamo é l'**intersezione**:

Intersezione tra insiemi: *l'intersezione di due insiemi A e B si indica con $A \cap B$ ed é l'insieme formato da tutti gli elementi contenuti in A e contenuti in B*

Un esempio:

$$A = \{1, 2, 3\}$$
$$B = \{1, 2, 6, 7\}$$
$$A \cap B = \{1, 2\}$$

Solo 1 e 2 sono contenuti sia in A che in B, quindi $A \cap B$ contiene solo 1 e 2. Un trucchetto mnemonico per ricordare la differenza dei simboli di intersezione e unione, che sono lo stesso simbolo rovesciato, é immaginare l'unione, $\cup$, come un contenitore in cui si "versano" tutti gli elementi dei due insiemi, per cui l'unione é l'insieme di tutti gli elementi dei due insiemi. Ad esclusione, nell'intersezione, $\cap$, non é possibile versare gli elementi quindi é l'insieme degli elementi contenuti contemporaneamente nei due insiemi.
La definizione in simboli:

Intersezione tra insiemi: $x \in A \cap B \Leftrightarrow x \in A \wedge x \in B$

A parole: "$x \in A \cap B$ *é equivalente a chiedere che* $x \in A$ *e* $x \in B$". Quindi la differenza dall'unione é che x deve appartenere ad entrambi gli insiemi. Di nuovo dagli esempi risulta chiara:

$$A = \{1, 2, 3\}$$
$$B = \{1, 2, 6, 7\}$$
$$A \cap B = \{1, 2\}$$
Infatti:
$$1 \in A \wedge 1 \in B$$
$$2 \in A \wedge 2 \in B$$

La terza e ultima operazione é la **differenza**:

Differenza tra insiemi: *la differenza tra due insiemi A e B si indica con $A \setminus B$ ed é l'insieme formato da tutti gli elementi di A che non appartengono a B*

Un esempio:

$$A = \{1, 2, 3, 5\}$$
$$B = \{1, 2, 6, 7\}$$
$$A \setminus B = \{3, 5\}$$

In simboli:

Differenza tra insiemi: $x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B$

Quindi "$x \in A \setminus B$ *é equivalente a dire che* $x \in A$ *e* $x \notin B$". Di fatto é un'operazione di sottrazione degli elementi di B dall'insieme A.

2.3 Dimostrazioni

Le dimostrazioni sono una parte che uno studente di matematica non puó non capire. Sono proprio le dimostrazioni a caratterizzare la formalitá e rigorositá della materia, permettendone lo sviluppo e consentendole di rivoluzionare la scienza nel corso dei secoli. Riuscire a spiegare come dimostrare una qualunque proposizione é un compito irraggiungibile in poche pagine, quello in cui spero di riuscire, invece, é trasmettere la forma di una dimostrazione attraverso la sua struttura logica che si compone di formulazione di ipotesi, applicazione delle definizioni e, nelle dimostrazioni piú difficili, l'intuizione per chiudere la dimostrazione. In questa sezione verranno spiegate alcune semplici dimostrazioni tali da riutilizzare le definizioni viste finora (che consiglio di capire bene) e i simboli introdotti, in modo da riuscire a maneggiare con una certa facilitá questi (pochi e semplici) argomenti trattati finora.
Voglio che sia chiaro che nello studio della matematica l'attivitá principale é proprio dimostrare assunti. Non é mia intenzione spaventare chi non riesce a capire le dimostrazioni piú difficili di questo libro: questa sezione serve anche a mostrare cosa si studia all'universitá, in modo da chiarire le idee per chi fosse interessato a proseguire gli studi di questa materia.
Visto che non é un testo universitario e siete quindi liberi di non ricordare qualche simbolo, vi ricordo la lista riassuntiva a pagina 2.

2.3.1 Uguaglianza tra insiemi

Partiamo da un grande classico: le dimostrazioni ovvie. Posso assicurare che non c'é niente di piú difficile di dimostrare cose assolutamente ovvie. Basta pensare a 1+1=2: é un uguaglianza che conoscono tutti ma che quasi nessuno sa dimostrare.
Parlando di uguaglianza tra due insiemi: due insiemi sono uguali se hanno gli stessi elementi, ma un modo piú agevole per definirlo é:

$$A = B \Leftrightarrow A \subset B \wedge B \subset A$$

Ricordando che $\Leftrightarrow$ significa che quello che c'é a sinistra implica quello che c'é a destra e viceversa, é necessario dividere la dimostrazione in due passaggi:

$$(1)\ A = B \Rightarrow A \subset B \wedge B \subset A \quad \text{e} \quad (2)\ A = B \Leftarrow A \subset B \wedge B \subset A$$

Dimostazione (1) : $A = B \Rightarrow A \subset B \wedge B \subset A$
Vogliamo dimostrare che da $A = B$ é possibile ottenere $A \subset B \wedge B \subset A$. Cioé consideriamo $A = B$ tra le ipotesi, cioé la consideriamo un'affermazione vera, e dimostriamo $A \subset B \wedge B \subset A$. Dalla definizione di sottoinsieme:

"*un insieme B lo diciamo sottoinsieme di A se tutti gli elementi di B appartengono anche a A*"

Sappiamo che sicuramente tutti gli elementi di A appartengono anche a B (visto che sono insiemi uguali da ipotesi e quindi hanno gli stessi elementi), quindi che A é sottotinsieme di B, ugualmente tutti gli elementi di B appartengono anche a A, quindi B é sottotinsieme di A. Abbiamo quindi dimostrato che $B \subset A$ e $A \subset B$, che é quello che dovevamo dimostrare.

Dimostrazione (2) : $A = B \Leftarrow A \subset B \wedge B \subset A$
Consideriamo $A \subset B \wedge B \subset A$ tra le ipotesi, quindi supponiamo che sia vera, e dimostriamo che $A = B$, cioé che i due insiemi hanno gli stessi elementi. Un altro modo per dire che due insiemi abbiano gli stessi elementi é chiedere che ogni elemento di A appartenga anche a B e che ogni elemento di B appartenga anche a A. Ma noi sappiamo che $A \subset B$, quindi che ogni elemento di A appartiene anche a B, e che $B \subset A$, quindi che ogni elemento di B appartiene anche a A, che é esattamente quello che dovevamo dimostrare.

Dimostrando le due implicazioni abbiamo concluso la dimostrazione.
L'equivalenza tra $A = B$ e $A \subset B \wedge B \subset A$ é molto importante e ci servirá nelle altre dimostrazioni.

2.3.2 Commutativitá dell'unione tra insiemi

Dimostriamo ora la **proprietá commutativa** per l'operazione di unione tra insiemi. Vogliamo dimostrare:

$$A \cup B = B \cup A$$

É probabile che risulti ovvia al lettore, ma cerchiamo di dare una dimostrazione rigorosa attraverso le definizioni e i simboli. Stiamo cercando di dimostrare un'uguaglianza tra insiemi, ci appelliamo quindi alla dimostrazione precedente e cerchiamo di dimostrare:

$$(1)\ A \cup B \subset B \cup A \quad \text{e} \quad (2)\ B \cup A \subset A \cup B$$

sapendo appunto che é equivalente a dire $A \cup B = B \cup A$

Dimostrazione (1) : $A \cup B \subset B \cup A$

Vogliamo dimostrare, dalla definizione di sottoinsieme, che ogni elemento in $A \cup B$ appartiene anche all'insieme $B \cup A$. Consideriamo x un generico elemento in $A \cup B$:

$$x \in A \cup B$$

Dalla definizione di $A \cup B$, sappiamo che:

$$x \in A \vee x \in B$$

Dobbiamo dimostrare che $x \in B \cup A$ cioé che $x \in B \vee x \in A$. Abbiamo ottenuto $x \in A \vee x \in B$ ma l'ordine in cui si scrive l'appartenenza di x non importa, cioé sono equivalenti:

$$x \in A \vee x \in B \qquad x \in B \vee x \in A$$

Quindi ora sappiamo $x \in B \vee x \in A$, che dalla definizione di unione é equivalente a $x \in B \cup A$ che era quello che volevamo dimostrare.

Viene introdotta ora la scrittura dei passaggi logici. Quello che abbiamo scritto finora lo possiamo compattare in questo modo:

$$x \in A \cup B \Leftrightarrow^{(a)} x \in A \vee x \in B \Leftrightarrow^{(b)} x \in B \vee x \in A \Leftrightarrow^{(c)} x \in B \cup A$$

Il passaggio *(a)* segue dalla definizione di unione tra insiemi:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$

Il passaggio *(b)* possiamo scriverlo perché abbiamo visto che $x \in A \vee x \in B$ é **uguale** a $x \in B \vee x \in A$, questa uguaglianza mi permette di usare $\Leftrightarrow$.
Il passaggio *(c)* segue di nuovo dalla definizione dell'unione tra insiemi.
Rileggendo i passaggi:

$x \in A \cup B$ **equivale a** $x \in A \vee x \in B$ **equivale a** $x \in B \vee x \in A$ **equivale a** $x \in B \cup A$

I passaggi sono equivalenti tra loro quindi otteniamo che $x \in A \cup B$ é **equivalente** a $x \in B \cup A$, quindi che gli elementi che appartengono a $A \cup B$ appartengono anche a $B \cup A$, che era quello che volevamo dimostrare. In realtá il fatto che siano equivalenti dice anche il viceversa, cioé che ogni elemento che appartiene a $B \cup A$ appartiene anche a $A \cup B$, dimostrando anche la (2). Possiamo quindi concludere la dimostrazione.

2.3.3 Associativitá dell'unione tra insiemi

Un'altra proprietá ovvia dell'unione tra insiemi é l'associtativitá, cioé:

$$(A \cup B) \cup C = A \cup (B \cup C)$$

Nuovamente useremo la prima dimostrazione sull'uguaglianza dimostrando che $(A \cup B) \cup C$ é sottoinsieme di $A \cup (B \cup C)$ e viceversa. Dimostreremo quindi che ogni elemento che appartiene a $(A \cup B) \cup C$ appartiene a $A \cup (B \cup C)$ e viceversa e per farlo sfrutteremo $\Leftrightarrow$ cioé le equivalenze.
Sappiamo dalla definizione di unione:

$$x \in (A \cup B) \cup C \Leftrightarrow x \in (A \cup B) \vee x \in C$$

La definizione dice infatti: $x \in P \cup Q \Leftrightarrow x \in P \vee x \in Q$, se sostituisco $P = A \cup B$ ottengo $x \in (A \cup B) \cup Q \Leftrightarrow x \in (A \cup B) \vee x \in Q$.
Ora possiamo di nuovo sfruttare la definizione di unione e scrivere:

$$x \in (A \cup B) \vee x \in C \Leftrightarrow x \in A \vee x \in B \vee x \in C$$

Se adesso sfrutto la definizione di unione con $x \in B \vee x \in C$ ottengo:

$$x \in A \vee x \in B \vee x \in C \Leftrightarrow x \in A \vee (x \in B \cup C)$$

Di nuovo dalla definizione di unione:

$$x \in A \vee (x \in B \cup C) \Leftrightarrow x \in A \cup (B \cup C)$$

Riassumendo:

$$x \in (A \cup B) \cup C \Leftrightarrow x \in (A \cup B) \vee x \in C \Leftrightarrow x \in A \vee x \in B \vee x \in C$$
$$\Leftrightarrow x \in A \vee (x \in B \cup C) \Leftrightarrow x \in A \cup (B \cup C)$$

Quindi: $x \in (A \cup B) \cup C \Leftrightarrow x \in A \cup (B \cup C)$, quindi che un elemento che apparteniene a $(A \cup B) \cup C$ apparteniene anche a $A \cup (B \cup C)$ e, visto che vale l'equivalenza, cioé $\Leftrightarrow$, anche il viceversa. Questo mi dice che $(A \cup B) \cup C$ é sottoinsieme di $A \cup (B \cup C)$ e viceversa, quindi che sono uguali.

2.3.4 Dimostrazione: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

A partire da questa dimostrazione iniziamo a vedere enunciati meno ovvi. Ancora, per dimostrare l'uguaglianza tra insiemi basta dimostrare che l'insieme a sinistra é sottoinsieme dell'insieme a destra e viceversa:
(1) $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$ e (2) $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$

Dimostrazione (1): $A \cup (B \cap C) \subset (A \cup B) \cap (A \cup C)$

Dobbiamo dimostrare che $A \cup (B \cap C)$ é sottoinsieme di $(A \cup B) \cap (A \cup C)$, quindi dimostriamo che ogni elemento di $A \cup (B \cap C)$ appartiene anche a $(A \cup B) \cap (A \cup C)$. Applicando la definizione di unione:

$$x \in A \cup (B \cap C) \Leftrightarrow x \in A \vee x \in B \cap C$$

Applicando invece la definizione di intersezione:

$$x \in A \vee x \in B \cap C \Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$$

Cioé x appartiene a A oppure x appartiene a B e C. Dobbiamo dimostrare che x appartiene a $(A \cup B) \cap (A \cup C)$. Sappiamo:

$$x \in A \vee (x \in B \wedge x \in C)$$

In cui compare un $\vee$, cioé un *oppure*, quindi siamo di fronte a due casi: $x \in A$ e $(x \in B \wedge x \in C)$ e ci dobbiamo assicurare che in entrambi si abbia $x \in (A \cup B) \cap (A \cup C)$.

Caso 1: $x \in A$

Possiamo scrivere:

$$x \in A \Rightarrow x \in A \cup B$$

Cioé se x appartiene a A allora appartiene anche a $A \cup B$, che é l'insieme degli elementi contenuti in A oppure in B. In questo caso non é possibile usare "$\Leftrightarrow$", in quanto l'affermazione $x \in A \Leftarrow x \in A \cup B$ é errata. Per dimostrare che non vale, come é usuale in matematica, si porta un controesempio: non possiamo dire $x \in A \Leftarrow x \in A \cup B$ perché possiamo considerare un elemento $x \in B$, il quale appartiene a $A \cup B$ ma non appartiene a A, quindi non posso dire "*ogni elemento di* $A \cup B$ *appartiene anche a* A".

Ugualmente:

$$x \in A \Rightarrow x \in A \cup C$$

Dobbiamo dimostrare che $x \in (A \cup B) \cap (A \cup C)$, dalla definizione di intersezione ricordiamo:

$$x \in (A \cup B) \cap (A \cup C) \Leftrightarrow x \in (A \cup B) \wedge x \in (A \cup C)$$

Cioé per dire che $x \in (A \cup B) \cap (A \cup C)$ mi basta avere che $x \in (A \cup B)$ e contemporaneamente $x \in (A \cup C)$, che é esattamente quello che abbiamo trovato poco sopra. Riassumendo:

$$x \in A \Rightarrow x \in (A \cup B) \wedge x \in (A \cup C) \Leftrightarrow x \in (A \cup B) \cap (A \cup C)$$

Caso 2: $x \in B \wedge x \in C$
Di nuovo dalla definizione di unione abbiamo:

$$x \in B \Rightarrow x \in A \cup B$$
$$x \in C \Rightarrow x \in A \cup C$$

Trovato dunque che $x \in A \cup B \wedge x \in A \cup C$, per la definizione di intersezione vale $x \in (A \cup B) \cap (A \cup C)$, che era quello che dovevo dimostrare.

Dimostrazione (2): $(A \cup B) \cap (A \cup C) \subset A \cup (B \cap C)$
La dimostrazione é fondamentalmente uguale:

$$x \in (A \cup B) \cap (A \cup C) \Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$$

Cioé "*x appartiene a A* ***oppure*** *B* ***e*** *x appartiene a A* ***oppure*** *C*". Identifichiamo ora 4 casi per via dei 2 *or*:

Caso 1	$x \in A \wedge x \in A$ (o semplicemente $x \in A$)
Caso 2	$x \in A \wedge x \in C$
Caso 3	$x \in B \wedge x \in A$
Caso 4	$x \in B \wedge x \in C$

Caso 1-2-3:
Nei casi 1, 2 e 3 abbiamo che $x \in A$, questo ci basta per dimostrare che $x \in A \cup (B \cap C)$, in quanto é l'insieme degli elementi in A oppure in $B \cap C$.

Caso 4: $x \in B \wedge x \in C$
Anche questo mi basta per affermare che $x \in A \cup (B \cap C)$, in quanto é l'insieme degli elementi in A oppure in $B \cap C$.

2.3.5 Leggi di De Morgan

Nell'ambito dell'algebra booleana (dove i "numeri" possono assumere il valore "*vero*" oppure "*falso*") le leggi di De Morgan ci danno alcune relazioni tra i connettori *and* e *or* (Non é importante conoscere o essere pratici con l'algebra booleana: delle leggi di De Morgan c'é anche una versione insiemistica). Usando la notazione $not(p) = \neg p$:

Leggi di De Morgan

Algebra booleana:

$$\neg(p \wedge q) = \neg p \vee \neg q$$
$$\neg(p \vee q) = \neg p \wedge \neg q$$

In termini insiemistici:

$$(1):\ A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$$
$$(2):\ A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$$

Dimostrazione (1): $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Dalla definizione di sottrazione tra insiemi:

$$x \in A \setminus (B \cap C) \Leftrightarrow x \in A \wedge x \notin B \cap C$$

Ora abbiamo un passaggio importante:

$$x \notin B \cap C \Leftrightarrow x \notin B \vee x \notin C$$

Questo segue dalla definizione di intersezione:

$$x \in B \cap C \Leftrightarrow x \textit{ appartiene a } B \textbf{ e } x \textit{ appartiene a } C$$

Cioé deve appartenere ad entrambi, quindi é chiaro che se la x non appartiene a B o anche se non appartiene a C non puó appartenere a $B \cap C$. Segue appunto che:

$$x \notin B \cap C \Leftrightarrow x \notin B \vee x \notin C$$

Cioé "x ***non*** *appartiene a* $B \cap C$ *é equivalente a* x ***non*** *appartiene a* B *oppure* ***non*** *appartiene a* C". Metto insieme:

$$x \in A \wedge x \notin B \cap C \Leftrightarrow x \in A \wedge (x \notin B \vee x \notin C)$$

Di nuovo abbiamo un *or*, $\vee$, quindi dividiamo i casi e usiamo la definizione di sottrazione tra insiemi:

Caso 1 $\quad x \in A \wedge x \notin B \Leftrightarrow x \in A \setminus B$
Caso 2 $\quad x \in A \wedge x \notin C \Leftrightarrow x \in A \setminus C$
Caso 3 $\quad x \in A \wedge x \notin B \wedge x \notin C \Leftrightarrow x \in A \setminus B \wedge x \in A \setminus C$

Dobbiamo dimostrare che i 3 casi sono equivalenti a $x \in (A \setminus B) \cup (A \setminus C)$, ma dalla definizione di unione sappiamo che:

$$x \in (A \setminus B) \cup (A \setminus C) \Leftrightarrow x \in (A \setminus B) \vee x \in (A \setminus C)$$

Cioé "*x appartiene a* $(A \setminus B) \cup (A \setminus C)$ *é equivalente a chiedere che x appartiene a* $(A \setminus B)$ *oppure x appartiene a* $(A \setminus C)$", che é esattamente quello che ci dicono i 3 casi: nel caso 1 abbiamo che $x \in (A \setminus B)$, nel caso 2 che $x \in (A \setminus C)$ e nel caso 3 abbiamo $x \in (A \setminus B) \wedge (A \setminus C)$, quindi viene sempre soddisfatta l'equivalenza. Riassumendo:

$$x \in A \setminus (B \cap C) \Leftrightarrow x \in A \wedge x \notin B \cap C \Leftrightarrow x \in A \wedge (x \notin B \vee x \notin C)$$

$$\Leftrightarrow \begin{cases} \text{Caso 1: } x \in A \wedge x \notin B \Leftrightarrow x \in A \setminus B \\ \text{Caso 2: } x \in A \wedge x \notin C \Leftrightarrow x \in A \setminus C \\ \text{Caso 3: } x \in A \wedge x \notin B \wedge x \notin C \Leftrightarrow x \in A \setminus B \wedge x \in A \setminus C \end{cases}$$

$$\Leftrightarrow x \in (A \setminus B) \cup (A \setminus C)$$

Dimostrazione (2): $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

La dimostrazione é analoga: dimostriamo che é equivalente appartenere a $A \setminus (B \cup C)$ e appartenere a $(A \setminus B) \cap (A \setminus C)$. Dalla definizione di sottrazione tra insiemi:

$$x \in A \setminus (B \cup C) \Leftrightarrow x \in A \wedge x \notin (B \cup C)$$

Di nuovo un'osservazione su $x \notin (B \cup C)$:

$$x \notin (B \cup C) \Leftrightarrow x \notin B \wedge x \notin C$$

Segue dalla definizione di unione: $x \in B \cup C \Leftrightarrow x \in B \vee x \in C$, quindi per non appartenere a $B \cup C$ é necessario non appartenere né a B né a C. Mettendo insieme:

$$x \in A \wedge x \notin (B \cup C) \Leftrightarrow x \in A \wedge x \notin B \wedge x \notin C$$

Ricaviamo dalla definizione di sottrazione tra insiemi:

$$x \in A \wedge x \notin B \wedge x \notin C \Leftrightarrow x \in (A \setminus B) \wedge x \in (A \setminus C)$$

Dalla definizione di intersezione:

$$x \in (A \setminus B) \wedge x \in (A \setminus C) \Leftrightarrow x \in (A \setminus B) \cap (A \setminus C)$$

Riassumendo:

$$x \in A \setminus (B \cup C) \Leftrightarrow x \in A \wedge x \notin (B \cup C) \Leftrightarrow x \in A \wedge x \notin B \wedge x \notin C$$
$$\Leftrightarrow x \in (A \setminus B) \wedge x \in (A \setminus C) \Leftrightarrow x \in (A \setminus B) \cap (A \setminus C)$$

2.3.6 Prima dimostrazione per contraddizione

Finora abbiamo visto "dimostrazioni dirette", cioé a partire dalle ipotesi abbiamo trovato dei passaggi che ci permettessero di dimostrare la tesi. É possibile peró dimostrare una proposizione in modo "indiretto" con un metodo chiamato *dimostrazione per contraddizione*. É un metodo semplice che permette di saltare molti passaggi: si tratta di *assumere* che la proposizione sia falsa e dimostrare che non é una proposizione corretta, cioé che porta ad una contraddizione. In questo modo dimostriamo che la proposizione iniziale non puó essere falsa, quindi deve essere vera. Dimostriamo per contraddizione:

$$(A \setminus B) \cap (B \setminus A) = \emptyset$$

($\emptyset$ é l'insieme vuoto) Assumiamo che la proposizione sia falsa:

$$(A \setminus B) \cap (B \setminus A) \neq \emptyset$$

E dimostriamo che non é possibile.

La non-uguaglianza ci dice che $(A \setminus B) \cap (B \setminus A)$ é un insieme con almeno un elemento, visto che é diverso dall'insieme vuoto. Quindi deve esistere almeno un certo x che appartenga all'insieme, in simboli:

$$\exists x \in (A \setminus B) \cap (B \setminus A)$$

Il simbolo $\exists$ significa "*esiste*". Sappiamo dalla definizione di intersezione:

$$x \in (A \setminus B) \cap (B \setminus A) \Leftrightarrow x \in (A \setminus B) \wedge x \in (B \setminus A)$$

E dalla definizione di sottrazione tra insiemi:

$$x \in (A \setminus B) \Leftrightarrow x \in A \wedge x \notin B$$
$$x \in (B \setminus A) \Leftrightarrow x \in B \wedge x \notin A$$

Quindi dalla prima affermazione si ottiene $x \in A$ mentre dalla seconda $x \notin A$ e, visto che devono valere contemporaneamente poiché si ha un *and* ($\wedge$), otteniamo un'assurditá. Questa é la *contraddizione* che stavamo cercando. Visto che l'affermazione $(A \setminus B) \cap (B \setminus A) \neq \emptyset$ non puó essere vera altrimenti porta a una contraddizione, deve valere l'opposto, cioé deve valere:

$$(A \setminus B) \cap (B \setminus A) = \emptyset$$

Quindi cosí abbiamo dimostrato in modo indiretto la proposizione.

2.3.7 Seconda dimostrazione per contraddizione

Una dimostrazione per contraddizione un pó piú complessa consiste nel dimostrare:

$$(A \cup B) \subset X \wedge (X \setminus B) \subset (X \setminus A) \Rightarrow A \subset B$$

Supponiamo l'opposto:

$$(A \cup B) \subset X \wedge (X \setminus B) \subset (X \setminus A) \Rightarrow A \not\subset B$$

Come abbiamo giá detto: barrare un simbolo nega il suo significato, quindi $\not\subset$ significa "*non é sottoinsieme*". Dobbiamo dimostrare che questa affermazione porta ad una contraddizione.
Visto che é una implicazione, cioé $\Rightarrow$, abbiamo tra le ipotesi $(A \cup B) \subset X$ e $(X \setminus B) \subset (X \setminus A)$ e stiamo supponendo *per assurdo* che vale $A \not\subset B$. Cerchiamo una contraddizione considerando un elemento x in A tale che non appartenga a B: visto che $A \not\subset B$ e dalla definizione di sottoinsieme sappiamo che $A \subset B \Leftrightarrow \forall x \in A \Rightarrow x \in B$, deve esistere un elemento in A che non appartenga a B, altrimenti A sarebbe un sottoinsieme di B. Quindi prendiamo un x tale che:

$$x \in A \wedge x \notin B$$

Sappiamo anche:

$$x \in A \Rightarrow x \in A \cup B$$

Ora abbiamo $x \in A \cup B$ e l'ipotesi $(A \cup B) \subset X$, mettendo insieme ricaviamo:

$$(A \cup B) \subset X \wedge x \in A \cup B \Rightarrow x \in X$$

dalla definizione di sottoinsieme. Riassumendo:

$$x \in X \wedge x \in A \wedge x \notin B$$

Da cui ricavo

$$x \in X \wedge x \notin B \Leftrightarrow x \in X \setminus B$$

Tra le ipotesi abbiamo $(X \setminus B) \subset (X \setminus A)$ da cui ricavo, per la definizione di sottoinsieme:

$$x \in X \setminus B \Rightarrow x \in X \setminus A$$

E dalla definizione di sottrazione tra insiemi:

$$x \in X \setminus A \Leftrightarrow x \in X \wedge x \notin A$$

Che é l'assurdo che cercavamo poiché abbiamo assunto all'inizio $x \in A$ e ora abbiamo trovato $x \notin A$, che é una contraddizione. Avendo trovato che $(A \cup B) \subset X \wedge (X \setminus B) \subset (X \setminus A) \Rightarrow A \not\subset B$ é falsa sappiamo che deve valere il suo opposto, cioé deve essere vero:

$$(A \cup B) \subset X \wedge (X \setminus B) \subset (X \setminus A) \Rightarrow A \subset B$$

3 Costruzione dei numeri

Vedremo in questo capitolo la costruzione insiemistica di tutti i tipi di numero definendone anche le operazioni di somma e prodotto. Abbiamo giá detto in precedenza che la teoria degli insiemi é fondante per la matematica proprio perché é da questa che nasce la definizione di numero, ma non sorprende sapere che se il primo utilizzo dei numeri naturali risale a circa 30.000 anni fa per semplici conti, le prime definizioni e costruzioni nacquero recentemente: dal 1700 in poi.
É naturale ritrovare nel mutare delle necessitá dell'uomo il motivo della nascita delle diverse classi di numero: i naturali e gli interi furono i primi a nascere per poter eseguire conti, i razionali per esprimere grandezze in funzione di altre grandezze, mentre reali e complessi, i piú recenti, per colmare le avanzate necessitá di calcolo.
L'evolvere dei numeri ha avuto come conseguenza matematica la nascita di teoremi specifici, di cui una parte si studia nel primo corso di algebra universitario il cui tema é l'*algebra degli interi*, che tratta importanti teoremi dei numeri interi, appunto, e, per farvi capire che questa "specializzazione" non é limitante, va ad approfondire alcune proprietá dei numeri primi, la costruzione delle terne pitagoriche e la dimostrazione del piccolo teorema di Fermat.
La costruzione delle varie classi di numeri parte dalla definizione insiemistica dei numeri naturali per poi espandersi alle altre classi, definendo una struttura concentrica. Questo implica che i numeri interi ($\{..., -1, 0, 1, ...\}$) comprendono anche i numeri naturali, i numeri razionali ($\{\frac{1}{2}, \frac{3}{5}...\}$) comprendono anche gli interi e quindi anche i naturali e cosí via.

3.1 Numeri naturali

Innanzitutto con numeri naturali si intende:

$$\mathbb{N} = \{0, 1, 2, 3, ...\}$$

Tra i matematici c'é il famoso litigio per la presenza o meno dello zero nei numeri naturali ma in questo libro, ignorando questi battibecchi, supporremo che 0 sia naturale.

Ci sono diverse costruzioni dei numeri naturali, viene spiegata quella di Von Neumann, la cui costruzione parte proprio dallo zero, che viene definito come:

$$0 = \{\} = \emptyset$$

É piuttosto naturale partire dalla definizione di 0, poiché fornisce il punto di partenza, una sorta di unitá di misura, su cui basare la definizione degli altri numeri.

Come possiamo ora ampliare la definizione a tutti i numeri? Una caratteristica dei numeri naturali é che tutti i numeri **tranne lo zero** hanno un predecessore. Allora per ogni numero (tranne lo zero) é sufficiente dare una definizione che si basa sul numero precedente. Cioé si definisce il "*Successore di a*" come:

$$S(a) = a \cup \{a\}$$

Cioé il successore di un certo a lo definisco come l'unione (perché stiamo lavorando con insiemi!) tra a e $\{a\}$. Attenzione: con a intendiamo l'insieme a, mentre con $\{a\}$ intendiamo invece prendere l'insieme che definisce a e metterlo tra parentesi rendendolo un elemento. Prendiamo in esempio l'insieme $\emptyset$: sono insiemi diversi $\emptyset = \{\}$ e $\{\emptyset\} = \{\{\}\}$, dove nel secondo, visto che $\emptyset$ figura tra le parentesi graffe, $\emptyset$ é un elemento dell'insieme. Facciamo un esempio:

$$0 = \emptyset = \{\}$$
$$1 = S(0) = 0 \cup \{0\} = \emptyset \cup \{0\} = \{0\} = \{\emptyset\} = \{\{\}\}$$

Si definisce quindi 1 come il *successore* di 0. Da notare che $\emptyset \cup \{0\}$ é l'insieme $\{0\}$ in quanto $\emptyset$ é l'insieme vuoto, perció quando consideriamo l'unione tra i due, che é l'insieme composto dagli elementi dei due insiemi, abbiamo a sinistra gli elementi dell'insieme vuoto, $\emptyset$, che non ha elementi, e a destra gli elementi dell'insieme $\{0\} = \{\emptyset\}$ che ha come elemento $0 = \emptyset = \{\}$.

Continuando con i numeri:

$$0 = \emptyset = \{\}$$
$$1 = \{0\} = \{\emptyset\} = \{\{\}\}$$
$$2 = S(1) = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\} = \{\{\}, \{\{\}\}\}$$

Anche qui definiamo il 2 come il successore di 1, ottenendo che $2 = \{0, 1\}$ che riscriviamo: $2 = \{\{\}, \{\{\}\}\}$.

É facile intuire che il pattern si ripete:

$$0 = \emptyset = \{\}$$
$$1 = \{0\} = \{\emptyset\} = \{\{\}\}$$
$$2 = \{0,1\} = \{\emptyset, \{\emptyset\}\} = \{\{\}, \{\{\}\}\}$$
$$3 = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{\{\}, \{\{\}\}\ , \{\{\}, \{\{\}\}\}\}$$
$$n = n-1 \cup \{n-1\} = \{0,1,...,n-1\} = \{\{\}, \{\{\}\}, ...\}$$

Con questa definizione un numero n é un insieme di n elementi, cioé gli n insiemi corrispondenti agli n numeri tra 0 e $n-1$, ed é possibile notare:

$$n \leq m \Leftrightarrow n \subset m$$

Cioé "*n é minore di m é equivalente a dire che n é un sottoinsieme di m*" (ricordando che un numero é un insieme). Infatti se consideriamo ad esempio $m = 4$, sappiamo che $4 = \{0,1,2,3\}$ e quindi che i numeri minori di 4 sono effettivamente contenuti nell'insieme 4 per come lo abbiamo definito, cioé che é **equivalente** chiedere che un certo numero n sia contenuto nell'insieme 4 e che $n \leq 4$.
Si usa $\leq$ invece di $<$ poiché un insieme é sottoinsieme di se' stesso. Dalla definizione:

"*un insieme B lo diciamo sottoinsieme di A se tutti gli elementi di B appartengono anche ad A*"

É chiaro che un insieme A ha gli stessi elementi di se' stesso, quindi é un sottoinsieme di se' stesso. É quindi chiaro che scrivere l'enunciato nella forma:

$$n < m \Leftrightarrow n \subset m$$

sarebbe sbagliato. A parole: "$n < m$ *é equivalente a dire* $n \subset m$" ma non sarebbe corretto, in quanto é possibile trovare un insieme n tale per cui vale $n \subset m$ ma per cui non vale $n < m$, ed é l'insieme m stesso, da cui segue che non é un'equivalenza ($\Leftrightarrow$) visto che l'implicazione "$\Leftarrow$" non vale.

3.1.1 Operazioni sui naturali

Restano da definire le operazioni di somma e prodotto. Visto che i numeri sono definiti come insiemi, é naturale definire le operazioni tra numeri come operazioni tra insiemi.
Nella somma partiamo definendo un'operazione ovvia:

$$a + 0 = a$$

e definiamo la somma tra due numeri come:

$$a + S(b) = S(a + b)$$

Dove con $S(a)$ intendiamo il successore di a. Vediamo un esempio per chiarire:

$$1 + 1 = 1 + S(0) = S(1 + 0) = S(1) = 2$$
$$1 + 3 = 1 + S(2) = S(1 + 2) = S(3) = 4$$

Nel primo esempio ci ritroviamo a calcolare $S(1 + 0)$, dove la somma $1 + 0$ risulta ovvia seguendo dalla prima definizione che abbiamo dato, mentre nel secondo ci ritroviamo $S(1 + 2)$ e potrebbe essere contestato il risultato $1 + 2 = 3$ in quanto stiamo cercando di definire proprio questa operazione di somma. La contestazione é sensata, poiché, volendo essere rigorosi, dovrei prima mostrare che $1 + 2 = 3$ per essere in grado di dire che $S(1 + 2) = S(3)$ e quindi $1 + 3 = 4$. Fortunatamente $1 + 2 = 3$:

$$1 + 2 = 1 + S(1) = S(1 + 1) = S(2) = 3$$

Di nuovo, per essere rigorosi dovrei mostrare che $1 + 1 = 2$, ma risparmio i conti in quanto lo abbiamo giá mostrato con il primo esempio.
Questa verifica dei conti a ritroso si chiama "*metodo induttivo*" o "*induzione*", é un metodo che assicura che questa operazione funzioni con tutti i numeri naturali a partire da un passo *elementare*, nel nostro caso $a+0 = a$. Non viene approfondito il funzionamento, ma concettualmente funziona come é stato mostrato: ci si assicura che i passaggi a ritroso siano sempre corretti.
La definizione di moltiplicazione é analoga, si parte quindi da un passo elementare:

$$a \times 0 = 0$$

E si procede definendo il prodotto tra due numeri sfruttando di nuovo il successore:

$$a \times S(b) = (a \times b) + a$$

Diamo degli esempi:

$$3 \times 1 = 3 \times S(0) = (3 \times 0) + 3 = 0 + 3 = 3$$
$$4 \times 2 = 4 \times S(1) = (4 \times 1) + 4 = 4 + 4 = 8$$

Anche qui le moltiplicazioni 3×0 e 4×1 tra parentesi dovrei verificarle per accertarne la correttezza e fare si che il metodo induttivo mi certifichi la corretta definizione della moltiplicazione. Risparmio i calcoli assicurandovi che la definizione é corretta.

Nell'ambito della correttezza delle operazioni ho introdotto vagamente il *metodo induttivo* perché é grazie a quello che é possibile verificare che la somma e il prodotto sono operazioni "*ben definite*", termine matematico che indica la rigorositá della definizione dell'operazione, su cui, quindi, si possono costruire teoremi e proprietá varie. Nelle prossime costruzioni verrá spiegato come si verifica la buona definizione delle operazioni con altri tipi di numero, essendo questa proprietá da verificare in modi diversi in base alla situazione

3.2 Numeri interi

Con numeri interi si intende:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

La costruzione dei numeri interi si appoggia ai numeri naturali, definendo un numero intero come una coppia di numeri naturali nella forma:

$$(a, b)$$

É necessario ora capire con quale regola associamo ad ogni numero intero una coppia di numeri naturali, ed é molto semplice: ad un certo numero intero n é associata una coppia di numeri (a, b) tali per cui $n = a - b$. Quindi:

$$5 = (5, 0)$$
$$-3 = (0, 3)$$
$$0 = (0, 0)$$

Ma nasce un problema: la scrittura di un numero intero come coppia di numeri naturali non é unica:

$$-3 = (0, 3) = (1, 4) = (10, 13) = ...$$

Per risolvere questo problema é necessario introdurre il concetto di *classe d'equivalenza*:

Classe di equivalenza: *Data una relazione (di equivalenza), la classe di equivalenza di un certo elemento a é l'insieme di elementi in relazione con a e si denota con* $[a]$

Questa definizione fa paura la prima volta che si legge ma con alcune spiegazioni diventa banale. Il primo passo é capire cosa si intende con *relazione*: possiamo dire che una relazione é una o piú regole che si applicano ad uno o piú elementi (Non ho creato lo specchietto perché non é una definizione rigorosa, é infatti una semplificazione che risparmia un bel pó di noie matematiche). Per come é stata data la regola di associazione tra un numero n e una coppia (a, b), diciamo che (a, b) é in relazione con un certo n se vale appunto $a - b = n$. In simboli:

$$(a, b) \sim n \Leftrightarrow a - b = n$$

Il simbolo $\sim$ significa proprio "*in relazione con*". A parole: "(a, b) *é in relazione con* n *é* ***equivalente*** *a dire che* $a - b = n$".
Quindi la classe di equivalenza di n é l'insieme di tutte le coppie (a, b) in relazione con n, quindi tali per cui $a - b = n$. Ad esempio: le coppie $(0, 1)$, $(1, 2)$, $(5, 6)$ sono tutti elementi della classe di equivalenza di -1.

$$[n] = \{(a, b) \text{ tale che } (a, b) \sim n\} = \{(a, b) \text{ tale che } a - b = n\}$$

Per la prima volta la definizione di un insieme non avviene elencando tutti i suoi elementi ma definendo la caratteristica che accomuna gli elementi.

Un altro esempio potrebbe essere:

$$\text{Numeri pari} = \{n \text{ tale che } 2|n\}$$

Cioé i numeri pari sono tutti i numeri n divisibili per 2, cioé 2 divide n (in simboli: $2|n$). Esiste anche un simbolo per "*tale che*": ":". Quindi:

$$\text{Numeri pari} = \{n : 2|n\}$$

Tornando alla definizione di classe di equivalenza la possiamo compattare:

$$[n] = \{(a, b) : (a, b) \sim n\} = \{(a, b) : a - b = n\}$$

Cioé la classe di equivalenza di n, scritta come $[n]$, é l'insieme di tutte le coppie (a, b) in relazione con n, quindi tutte le coppie (a, b) tali che $a - b = n$. Sostanzialmente la classe di equivalenza raccoglie tutti gli elementi (in questo caso in forma di coppie, ma in altri casi possono essere insiemi, vettori e qualsivoglia oggetto matematico) che hanno un significato comune nella notazione che stiamo usando. In questo caso la classe di equivalenza raccoglie tutte le coppie che hanno lo stesso significato: rappresentano tutte allo stesso modo un numero intero. Si dice infatti che gli elementi della classe di equivalenza di un certo elemento n (che nel nostro caso é un numero) sono le *rappresentazioni* di questo elemento.

3.2.1 Operazioni sugli interi

Definiamo ora le operazioni tra numeri interi. Anche qui, lavorando su coppie di numeri naturali, le operazioni sono definite come manipolazioni di coppie. La somma é definita come:

$$n + m = (a, b) + (c, d) = (a + c, b + d)$$

La definizione prevede quindi una somma tra numeri naturali, cioé le componenti delle coppie. Un esempio:

$$-4 + 6 = (3, 7) + (6, 0) = (3 + 6, 7 + 0) = (9, 7) = 9 - 7 = 2$$

Piú interessante é il prodotto. Infatti se supponiamo che funzioni come la somma si avrebbe:

$$n \times m = (a, b) \times (c, d) = (a \times c, b \times d)$$

Ma é facile trovare un caso in cui questa definizione non é corretta:

$$-4 \times -3 = (1, 5) \times (2, 5) = (1 \times 2, 5 \times 5) = (2, 25) = -23$$

Per trovare la corretta definizione del prodotto basta ricordare la definizione di classe di equivalenza:

$$n \sim (a, b) \text{ con } a - b = n \qquad m \sim (c, d) \text{ con } c - d = m$$

Sfruttando ora $a - b = n$ e $c - d = m$ scriviamo:

$$n \times m = (a - b) \times (c - d) = ac - da - bc + bd$$

Si otteniene un prodotto tra sottrazioni, che si svolge al solito modo. Si hanno ora alcuni termini con segno negativo e alcuni termini con segno positivo la cui somma ha un certo valore intero, motivo per cui é possibile scriverla come coppia di numeri prendendo come prima componente i termini positivi e come seconda componente i termini negativi:

$$ac - da - bc + bd = (ac + bd, da + bc)$$

Quindi definiamo il prodotto:

$$n \times m = (a, b) \times (d, c) = ac + bd - da - bc = (ac + bd, ad + bc)$$

Diamo un esempio:

$$-2 \times -3 = (1, 3) \times (0, 3) = (1 \times 0 + 3 \times 3, 1 \times 3 + 3 \times 0) = (9, 3) = 6$$

3.3 Numeri razionali

Con numeri razionali si intende:

$$\mathbb{Q} = \left\{..., -5, -\frac{1}{2}, 0, \frac{1}{2}, \frac{2}{5}, ...\right\}$$

Per la costruzione, come é giá stato fatto, ci si appoggia ai numeri definiti in precedenza, in questo caso gli interi, costruendo appunto coppie di numeri interi (a, b) associate ad un numero razionale n quando $n = \frac{a}{b}$, quindi possiamo esprimere la relazione di equivalenza:

$$(a, b) \sim n \Leftrightarrow n = \frac{a}{b}$$

A parole "(a, b) *é in relazione con* n *é equivalente a chiedere che* $n = \frac{a}{b}$". La classe di equivalenza di un certo n si esprime come:

$$[n] = \{(a, b) : (a, b) \sim n\} = \left\{(a, b) : n = \frac{a}{b}\right\}$$

Alcuni esempi:

$$[2] = \left\{(2, 1), (4, 2), ...\right\}$$

$$\left[\frac{-1}{2}\right] = \left\{(-1, 2), (1, -2), (-2, 4), ...\right\}$$

3.3.1 Operazioni sui razionali

Come i numeri interi, anche i numeri razionali sono coppie di numeri, perció somma e moltiplicazione sono operazioni sulle coppie di numeri interi. Iniziamo con il prodotto, piú semplice tra i due:

$$n \times m = (a, b) \times (c, d) = (a \times c, b \times d) = \frac{ac}{bd}$$

É una definizione che non sorprende ricordando, ad esempio:

$$\frac{1}{2} \times \frac{3}{4} = \frac{1 \times 3}{2 \times 4} = \frac{3}{8}$$

Che corrisponde a:

$$\frac{1}{2} \times \frac{3}{4} = (1, 2) \times (3, 4) = (1 \times 3, 2 \times 4) = (3, 8) = \frac{3}{8}$$

Anche ora non é possibile estendere la logica della definizione del prodotto con la somma. Infatti se supponiamo:

$$n + m = (a, b) + (c, d) = (a + c, b + d) = \frac{a + c}{b + d}$$

diventa facile trovare esempi che dimostrano la non correttezza della definizione:

$$\frac{1}{2} + \frac{3}{4} = (1, 2) + (3, 4) = (1 + 3, 2 + 4) = (4, 6) = \frac{4}{6} = \frac{2}{3}$$

Oltre al risultato incorretto, possiamo riscrivere $\frac{1}{2}$ in altre forme equivalenti, cioé considerare altri elementi della classe di equivalenza di $\frac{1}{2}$:

$$\left[\frac{1}{2}\right] = \Big\{(1,2),(2,4),(-2,-4),...\Big\}$$

Scrivendo $\frac{2}{4}$ al posto di $\frac{1}{2}$, visto che fanno parte della stessa classe di equivalenza, non si dovrebbe ottenere un risultato diverso:

$$\frac{1}{2}+\frac{3}{4} = \frac{2}{4}+\frac{3}{4} = (2,4)+(3,4) = (2+3,4+4) = (5,8) = \frac{5}{8}$$

Cioé con questa definizione otteniamo come risultato $\frac{2}{3}$ quando usiamo la coppia $(1,2)$ della classe di equivalenza di $\frac{1}{2}$, mentre quando usiamo la coppia $(2,4)$ (che appartiene sempre alla classe di equivalenza di $\frac{1}{2}$) otteniamo come risultato $\frac{5}{8}$. Abbiamo quindi risultati diversi in funzione della coppia nella classe di equivalenza del numero razionale, ma per essere *ben definite* le operazioni **non devono** dipendere dall'elemento della classe di equivalenza. Cioé devono valere le uguaglianze:

$$\frac{1}{2}+\frac{3}{4} = (1,2)+(3,4) = \frac{2}{4}+\frac{6}{8} = (2,4)+(6,8) = ...$$

La corretta definizione della somma tra razionali é quella solita:

$$\frac{a}{b}+\frac{c}{d} = (a,b)+(c,d) = (ad+bc,bd) = \frac{ad+bc}{bd}$$

Un esempio:

$$\frac{1}{2}+\frac{3}{4} = (1,2)+(3,4) = (1\times 4+2\times 3,2\times 4) = (10,8) = \frac{10}{8} = \frac{5}{4}$$

Il risultato non cambia se considero un'altra coppia nella classe di equivalenza:

$$\frac{1}{2}+\frac{3}{4} = \frac{2}{4}+\frac{3}{4}$$
$$= (2,4)+(3,4) = (2\times 4+4\times 3,4\times 4) = (20,16) = \frac{20}{16} = \frac{5}{4}$$

L'ultima uguaglianza segue dal processo di semplificazione delle frazioni, che consiste nel prendere una specifica coppia di numeri della classe di equivalenza della frazione. Quando semplifichiamo cerchiamo infatti una frazione di piú piccoli numeri coprimi tra loro (numeri che non hanno primi in comune nella fattorizzazione), ugualmente cerchiamo la coppia di piú piccoli numeri coprimi nella classe di equivalenza. Dall'esempio sopra:

$$\left[\frac{20}{16}\right] = \{(5,4),(-5,-4),(10,8),(-10,-8),(20,16),(-20,-16),...\}$$

La coppia di piú piccoli (interi) coprimi é la coppia $(5,4)$, che quindi sará la rappresentazione della semplificazione di $\frac{20}{16}$.

3.4 Numeri irrazionali o reali

I numeri irrazionali, chiamati anche reali, da definizione, sono "*numeri non razionali*". Quello che si intende con numero irrazionale é quindi un numero non esprimibile come una frazione **tra numeri interi**. Sono numeri irrazionali, o reali:

$$\mathbb{R} = \{\sqrt{2}, \pi, ...\}$$

Data la definizione, colgo l'occasione per spiegare un *meme* molto popolare:

Un famoso meme matematico

"A rational number is any number that
can be represented by a fraction"
Math teacher: "π is irrational"
Me, an intellectual: "$\frac{\pi}{1}$"

La battuta fa leva sul fatto che un numero irrazionale, da definizione, non puó essere espresso come frazione. A questo punto peró il meme fa notare che, nonostante π sia irrazionale, é possibile esprimerlo come frazione nella forma $\frac{\pi}{1}$. L'errore sta nella definizione di numero razionale, che abbiamo definito essere un numero esprimibile come frazione tra **numeri interi**. Sappiamo che π é un numero non intero in quanto ha dei decimali ($\pi = 3,14...$) e quindi che $\frac{\pi}{1}$ non é un numero razionale, da cui ricaviamo che il meme é matematicamente insensato.

Tornando alla costruzione dei numeri reali, un primo modo che si potrebbe pensare per definire un numero irrazionale, quindi della forma $1.\overline{1}$, é attraverso infinite somme di numeri razionali:

$$1.\overline{1} = 1.111... = 1 + 0.1 + 0.01 + 0.001 + 0.0001 + ...$$

Il problema di questa costruzione é che abbiamo definito una somma tra razionali con addendi finiti (piú rigorosamente abbiamo definito una somma di due soli addendi), quindi non sappiamo come funzioni una somma di infiniti addendi e quindi non possiamo dare una costruzione dei numeri in questo modo.
Come alternativa possiamo definire un numero irrazionale come una frazione in cui si fanno infinite operazioni:

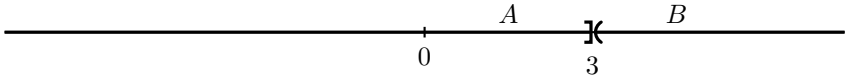
$1.\overline{1} = \frac{10}{9}$

```
 10 | 9
-9  | 1.1...
 10
 -9
  10
  ...
```

Anche qui peró si tratta di infinite operazioni da svolgere, situazione non ben definita del procedimento di divisione, definito appunto per una quantitá finita di operazioni.
Una costruzione priva del problema dell'infinitá dei passaggi é quella definita da Dedekind. Il matematico tedesco considera una coppia di sottoinsiemi di $\mathbb{Q}$, A e B, con le seguenti proprietá:

- $A \cap B = \emptyset$ ma con $A \neq \emptyset$ e $B \neq \emptyset$
- $A \cup B = \mathbb{Q}$
- Ogni elemento di A é minore di ogni elemento di B, in simboli:
$$\forall y \in B, \forall x \in A \Rightarrow x < y$$
- B **non** puó avere un minimo mentre A puó avere massimo

La prima proprietá impone che l'intersezione dei due insiemi sia vuota. Visto che i due insiemi sono sottoinsiemi dei numeri razionali é equivalente a chiedere che non abbiano numeri in comune e, dalla condizione dopo, che non siano vuoti.
La seconda proprietá $A \cup B = \mathbb{Q}$ chiede che l'unione dei due sia l'insieme dei numeri razionali, quindi che entrambi gli insiemi contengano infiniti elementi (se fosse infinito solo uno dei due si avrebbe una situazione simile: $A = \{0\}$ e $B = \mathbb{Q} \setminus \{0\}$, che non rispetta le altre condizioni)
La terza prevede che ogni elemento di A sia minore di ogni elemento di B, cioé che entrambi gli insiemi, se consideriamo la retta dei numeri (razionali), siano delle semirette. Cioé non é possibile avere:
$A = \{0, -1, 2, -3, ...\}$ e $B = \{1, -2, 3, -4, ...\}$, ci deve essere un numero tale per cui A contiene tutti i numeri minori e B tutti i numeri maggiori.
L'ultima condizione sui massimi e minimi serve per distinguere i numeri irrazionali dai numeri non irrazionali, come vedremo in un esempio.
Una coppia insiemi (A, B) si chiama *Sezione di Dedekind* ed é grazie a queste che costruiamo i numeri: ogni sezione, quindi coppia di insiemi, definisce un numero, ed é proprio il numero che divide l'insieme A dall'insieme B. Facciamo un esempio:



Dove con "] " si intende che il numero (in questo caso 3) appartiene all'insieme di numeri A, mentre " (" indica che il numero 3 non appartiene all'insieme B (dalla prima regola: i due insiemi non possono condividere elementi). Visto che i due insiemi rispettano le condizioni imposte da Dedekind, la coppia (A, B) forma una sezione. Il numero che divide i due insiemi é il numero 3, quindi la coppia di insiemi (A, B) definisce il numero 3. É chiaro quindi che quando si usano le sezioni

per definire un numero naturale, intero o razionale il numero sará il valore massimo contenuto nell'insieme A, in quanto un qualunque numero naturale, intero o razionale é anche un numero razionale, quindi, per le condizioni imposte da Dedekind, sará contenuto in A appunto. Diverso é per i numeri irrazionali visto che, dalle condizioni, A e B non possono contenere numeri irrazionali. In quel caso il numero non sará contenuto in A né in B, quindi dividerá i due insiemi.
Prima di mostrare la costruzione delle sezioni di Dedekind per il numero $\sqrt{2}$ riportiamo la dimostrazione della sua irrazionalitá.

$\sqrt{2}$ é irrazionale

La dimostrazione é per assurdo, cioé si suppone che $\sqrt{2}$ sia razionale e si trova una contraddizione. Se $\sqrt{2}$ fosse razionale si potrebbe scrivere:

$$\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2$$

Dimostriamo ora che questo non é possibile, cioé che é la contraddizione che cercavamo: considerando un generico numero n, nella fattorizzazione in numeri primi di n^2 l'esponente del 2 é un numero pari: se supponiamo che la fattorizzazione in numeri primi di n sia

$$n = 2^a \times 3^b \times ...$$

Allora la fattorizzazione di n^2 é:

$$n^2 = 2^{2a} \times 3^{2b} \times ...$$

L'esponente del 2 é $2a$, quindi un numero pari. Un esempio:

$$72 = 2^3 \times 3^2 \Rightarrow 72^2 = 2^6 \times 3^4$$

Dunque nella fattorizzazione sia di b^2 che di a^2 il 2 ha esponente pari. Dunque l'equivalenza:

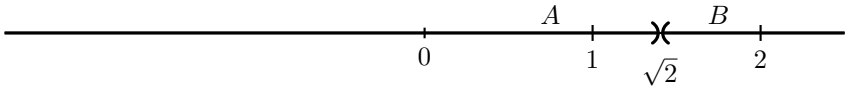
$$2b^2 = a^2$$

non puó valere, infatti:

$$b = 2^a \times 3^b \times ...$$
$$b^2 = 2^{2a} \times 3^{2b} \times ...$$
$$2b^2 = 2^{2a+1} \times 3^{2b} \times ...$$

Cioé nella fattorizzazione di $2b^2$ il 2 ha esponente dispari mentre abbiamo dimostrato pocanzi che il 2 nella fattorizzazione di a^2 ha esponente pari. Sapendo che due numeri uguali hanno fattorizzazione uguale, é una contraddizione dire $2b^2 = a^2$ per via degli esponenti del 2, pari in a^2 e dispari in $2b^2$; visto che hanno fattorizzazione diversa i due numeri devono essere diversi.
Abbiamo dimostrato che $\sqrt{2}$ non puó essere razionale, quindi deve essere irrazionale.

Passiamo ora alla costruzione della sezione di Dedekind per il numero $\sqrt{2}$



In questo caso $\sqrt{2}$ non appartiene né a A né a B, altrimenti non varrebbero le condizioni di Dedekind. Essendo il numero $\sqrt{2}$ l'unico numero che divide A e B, la sezione (A, B) definisce il numero $\sqrt{2}$.
Vediamo ora come trovare l'espressione di un numero irrazionale identificato dalle sezioni (A, B) prendendo in esempio $\sqrt{2}$. Concentriamoci su A: non contiene $\sqrt{2}$ ma contiene tutti i numeri precedenti a $\sqrt{2}$. Cioé é possibile avvicinarsi sempre piú a $\sqrt{2}$ senza arrivare mai al valore preciso (cosa impossibile in quanto ha infinite cifre decimali). É possibile quindi trovare un'approssimazione di $\sqrt{2}$ con un numero arbitrario di cifre decimali: per trovare un'approssimazione intera del numero (senza cifre decimali) é sufficiente trovare il numero naturale piú grande contenuto in A; per trovare un'approssimazione con una cifra decimale é sufficiente trovare il piú grande numero razionale con una cifra decimale; ugualmente, per trovare un'approssimazione con due cifre decimali é sufficiente trovare il piú grande numero razionale con due cifre decimali e cosí via. Nel caso di $\sqrt{2}$, A contiene tutti i numeri minori di $\sqrt{2}$, da cui é possibile estrapolare le approssimazioni:

Il piú grande intero: 1
Il piú grande razionale con un decimale: 1.4
Il piú grande razionale con due decimali: 1.41
Il piú grande razionale con tre decimali: 1.414
...

Ovviamente considerando le approssimazioni in A si arrotonda per difetto, mentre considerando quelle in B per eccesso.

Scostandosi per un momento dalle sezioni di Dedekind, c'é un'interessante dimostrazione nell'ambito dei numeri irrazionali: $0.\overline{9} = 1$. Attenzione: é un'uguaglianza e significa proprio che i due numeri sono uguali, non che "$0.\overline{9}$ *é un'approssimazione di* 1". É controintuitivo a prima vista, ma forniamo alcune dimostrazioni:

$0.\overline{9} = 1$

Dimostrazione 1:

$$1 = \frac{9}{9} = 9 \times \frac{1}{9} = 9 \times 0.1111... = 0.9999... = 0.\overline{9}$$

Dimostrazione 2:
Assegniamo il valore: $c = 0.999...$

$$10c = 9.999...$$
$$10c - c = 9.999... - 0.999...$$
$$9c = 9$$
$$c = 1$$

Ma inizialmente avevamo $c = 0.999...$, ora ci ritroviamo $c = 1$, segue quindi $0.999... = 1$

Dimostrazione 3 (per assurdo):
Dimostriamo per assurdo che $0.\overline{9} = 1$, partendo quindi dall'opposto:

$$0.\overline{9} \neq 1$$
$$0.\overline{9} \times 9 \neq 1 \times 9$$
$$0.\overline{9} \times 9 + 0.\overline{9} \neq 1 \times 9 + 0.\overline{9}$$
$$0.\overline{9} \times 9 + 0.\overline{9} \neq 9.\overline{9}$$
$$0.\overline{9} \times (9 + 1) \neq 9.\overline{9}$$
$$0.\overline{9} \times 10 \neq 9.\overline{9}$$
$$9.\overline{9} \neq 9.\overline{9}$$

Troviamo quindi un assurdo. Visto che $0.\overline{9} \neq 1$ porta ad una contraddizione, deve valere l'enunciato opposto, quindi $0.\overline{9} = 1$.

Ora che abbiamo visto le sezioni di Dedekind e come definire un numero irrazionale, vediamo la dimostrazione di $0.\overline{9} = 1$ con le sezioni: Il numero $0.\overline{9}$ é definito da una sezione di Dedekind, di cui il primo insieme contiene tutti i numeri minori di $0.\overline{9}$, quindi tutti i numeri nella forma $0.\overline{9} - n$ dove con n intendiamo un numero generico maggiore di 0.
Il numero 1, ugualmente, é definito da una sezione di Dedekind di cui il primo insieme contiene tutti gli elementi precedenti a 1, quindi nella forma $1 - n$.

Chiamando A il primo insieme della sezione di Dedekind di $0.\overline{9}$ e B il primo insieme della sezione di Dedekind di 1:

$$A = \{x \in \mathbb{Q} : x < 0.\overline{9}\} = \{x \in \mathbb{Q} : x = 0.\overline{9} - n \text{ con } n \in \mathbb{R}\}$$
$$B = \{x \in \mathbb{Q} : x < 1\} = \{x \in \mathbb{Q} : x = 1 - n \text{ con } n \in \mathbb{R}\}$$

Dimostrando che $A = B$, si dimostra che la sezione di Dedekind di 1 e di $0.\overline{9}$ é la stessa, quindi che 1 e $0.\overline{9}$ sono lo stesso numero. Dimostriamo $A = B$ al solito modo: $A \subset B$ e $B \subset A$.

Sicuramente vale $A \subset B$, in quanto gli elementi di A sono tutti i numeri $x < 0.\overline{9}$, ma tutti i numeri minori di $0.\overline{9}$ sono anche minori di 1, quindi appartengono anche all'insieme B.

Ogni elemento m di B invece é tale per cui $m < 1$, sapendo che m é un razionale lo posso scrivere come $m = \frac{a}{b}$ e quindi $\frac{a}{b} < 1$ (dove $b > a$ altrimenti $\frac{a}{b} > 1$. Consideriamo anche $b > 0$, supponendo, quando si tratta di un numero negativo, di avere $a < 0$ invece di $b < 0$). Serve dare alcune disuguaglianze prima di procedere:

$$1 - \frac{a}{b} = \frac{b-a}{b} \geq \frac{1}{b} > \frac{1}{10^b}$$

La prima uguaglianza é semplicemente da definizione di somme tra frazioni. Invece $\frac{b-a}{b} \geq \frac{1}{b}$ segue dal fatto giá citato che $b > a$ e da $a, b \in \mathbb{Z}$, cioé sono interi (stiamo lavorando con i razionali, frazioni di interi), chiaramente $b - a > 1$ e quindi segue anche la disuguaglianza tra le frazioni. Invece $\frac{1}{b} > \frac{1}{10^b}$ segue dal fatto che piú aumenta il denominatore e piú la frazione diventa piccola: $\frac{1}{10} = 0.1$ mentre $\frac{1}{100} = 0.01$. Sappiamo che $b > 0$, da cui segue che $10^b > b$ (non sarebbe vero se b fosse negativo), segue quindi che $\frac{1}{b}$ ha un denominatore piú piccolo di $\frac{1}{10^b}$ e quindi che vale la disuguaglianza di cui sopra. Trovate queste disuguaglianze ce ne serviamo per scrivere:

$$\text{Visto che } 1 - \frac{a}{b} > \frac{1}{10^b}$$
$$\text{Sposto i termini: } \quad \frac{a}{b} < 1 - \frac{1}{10^b}$$

Ma visto che:

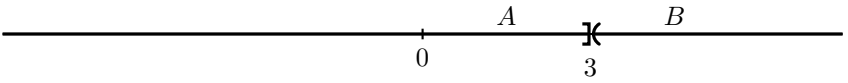
$$1 - \frac{1}{10^b} = 0.(9)_b < 0.\overline{9}$$

Infatti sappiamo che $\frac{1}{10^b} = 0.000...1$ con $b-1$ zeri, quindi $1 - \frac{1}{10^b}$ é uguale a 0.99999... dove 9 compare b volte, che é un valore minore di $0.\overline{9}$. Segue quindi che i numeri $\frac{a}{b}$ minori di 1 sono anche minori di $0.\overline{9}$, quindi che gli elementi dell'insieme B (minori di 1) appartengono anche all'insieme A (minori di $0.\overline{9}$), cioé $B \subset A$.

Abbiamo quindi dimostrato che $A = B$, cioé che $0.\overline{9}$ e 1 hanno uguale sezione di Dedekind, segue che i due numeri sono uguali.

3.4.1 Operazioni sui reali

Definiamo ora le operazioni con i numeri reali. In questo caso non dobbiamo preoccuparci della buona definizione, in quanto non stiamo piú lavorando con classi di equivalenza.
Per definire le operazioni é sufficiente lavorare con il primo dei due insiemi della sezione, quello contenente tutti gli elementi a sinistra del numero che definisce, in quanto il secondo insieme é ricavabile dal primo.
Nella sezione di Dedekind i due insiemi, per le proprietá che devono rispettare, sono di fatto delle semirette nella retta dei numeri:



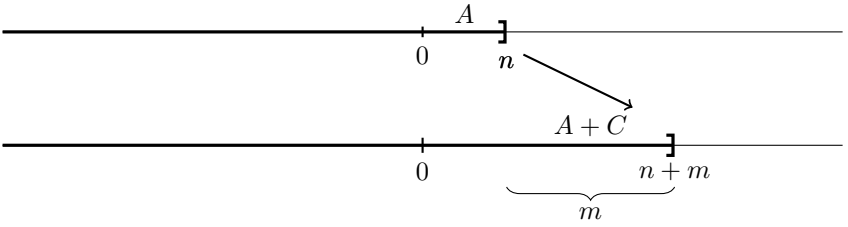
In questo esempio A é una semiretta che parte da 3 e va fino a $-\infty$, mentre B é una semiretta che parte da 3 (escluso) e va fino a ∞.
Dunque la somma tra due numeri reali consiste nel traslare il primo insieme della sezione di Dedekind del primo numero in funzione del primo insieme della sezione di Dedekind del secondo numero.

$$n = (A, B) \qquad m = (C, D)$$
$$n + m = A + C = \{a + c : a \in A \land c \in C\}$$

La somma di due numeri é definita dall'insieme $\{a + c : a \in A \land c \in C\}$ che é il primo insieme della sezione di Dedekind del numero $n+m$, quindi l'insieme di tutti i numeri precedenti a $n+m$. Questo insieme é costituito da tutti i numeri che sono la somma di un numero in A, quindi il primo insieme della sezione di Dedekind di n, e in C, primo insieme della sezione di Dedekind di m.
Per capire meglio perché sia il primo insieme della sezione di Dedekind di $n+m$, é possibile semplificare la definizione nel caso sia n che m siano numeri razionali:

$$n = (A, B) \qquad m = (C, D)$$
$$n + m = A + C = \{a + m : \forall a \in A\}$$

Cioé traslare l'insieme A di m a destra:



Non é possibile usare questa definizione con dei numeri irrazionali, perché staremmo chiedendo di spostare una semiretta di un numero con infinite cifre decimali, operazione non ben definita.

L'insieme $\{a + c : a \in A \wedge c \in C\}$ mi dice infatti di prendere tutti gli elementi di A e sommarli a tutti gli elementi di C, quindi ogni numero sempre piú vicino a n (appartenente a A) sará sommato, oltre a tutti gli altri infiniti numeri, ad ogni numero sempre piú vicino a m (appartenente a C), ottenendo un insieme che contiene tutti i numeri sempre piú vicini a $n + m$, cioé diventa l'insieme dei numeri precedenti a $n + m$, quindi il primo dei due insiemi della sua sezione di Dedekind.
Per la moltiplicazione la questione é molto simile. Vediamo la definizione di moltiplicazione solo per due numeri reali positivi.

$$n = (A, B) \quad m = (C, D)$$

$$\begin{aligned} n \times m &= A \times C \\ &= \{a \times c : a \geq 0 \wedge a \in A \wedge b \geq 0 \wedge b \in C\} \cup \{x \in \mathbb{Q} : x < 0\} \end{aligned}$$

Lavorando con numeri positivi, vengono considerati degli insiemi A e C solo i numeri positivi compensando la mancanza dei numeri negativi grazie all'unione con $\{x \in \mathbb{Q} : x < 0\}$, cioé tutti i numeri razionali negativi. Nel primo insieme dell'unione abbiamo tutti i numeri sempre piú vicini a n e tutti i numeri sempre piú vicini a m (oltre che agli altri numeri positivi precedenti a n e m) che moltiplicati tra loro sono tutti i numeri che si avvicinano sempre di piú a $n \times m$, definendo quindi il primo dei due insiemi della sezione di Dedekind di $n \times m$ e quindi definendo proprio il numero $n \times m$.

3.5 Numeri complessi

Concludiamo la costruzione dei numeri con l'insieme dei numeri complessi:

$$\mathbb{C} = \{i, 1+i, -1-i, ...\}$$
$$i = \sqrt{-1}$$

I numeri complessi sono nella forma $a + ib$, con i che viene chiamata l' "*unitá immaginaria*". Anche qui, similmente alle altre costruzioni, definiamo un numero complesso n come una coppia di numeri reali (a, b) tali che:

$$n = a + ib$$

Con questa notazione, a viene detto *parte reale*, mentre b, visto che é moltiplicata per l'*unitá immaginaria*, viene chiamata *parte immaginaria*.

3.5.1 Operazioni sui complessi

Quando si lavora con numeri complessi é possibile supporre di lavorare con polinomi di incognita i. Cosa significa? Significa che la somma e il prodotto tra numeri complessi segue le stesse regole della somma e del prodotto tra polinomi. Un esempio:

$$(1+x) + (3+2x) = (1+3) + (1+2)x = 4 + 3x$$

Che é la solita somma tra polinomi, ugualmente sommo i numeri complessi:

$$(1+i) + (3+2i) = (1+3) + (1+2)i = 4 + 3i$$

Come con i polinomi in cui si sommano i termini simili (termini senza x del primo polinomio con i termini senza x del secondo polinomio e i termini con la x del primo polinomio con i termini con la x del secondo) con i complessi si sommano le parti reali tra loro e le parti immaginarie tra loro. Dando la definizione rigorosa:

$$n + m = (a, b) + (c, d) = (a + c, b + d) = (a + c) + (b + d)i$$

Anche per il prodotto i numeri complessi seguono le regole dei polinomi:

$$(1+x) \times (3+2x) = 1 \times 3 + 1 \times 2x + x \times 3 + x \times 2x = 3 + 5x + 2x^2$$

Ugualmente per i numeri complessi:

$$\begin{aligned}(1+i) \times (3+2i) = 1 \times 3 + 1 \times 2i + i \times 3 + i \times 2i &= 3 + 5i + 2i^2 \\ &= 3 + 5i + (-2) \\ &= 1 + 5i\end{aligned}$$

Con l'unica differenza che sappiamo quanto vale $i^2 = \sqrt{-1}^2 = -1$

Fornendo di nuovo una definizione formale sulle coppie di numeri reali:

$$n + m = (a, b)(c, d) = (ac - bd, bc + ad) = (ac - bd) + (bc + ad)i$$

Dove il segno in $-bd$ deriva appunto da $i^2 = -1$

4 Criteri di divisibilitá

Quando parliamo di criteri di divisibilitá stiamo parlando di algoritmi che ci semplificano la vita quando dobbiamo valutare se un numero é divisibile o non é divisibile per un altro numero. Lo scopo di questi criteri é rendere piú veloce e piú semplice questa conclusione sulla divisibilitá e infatti, come ricorderete, consistono in semplici operazioni da eseguire sulle cifre.
Il capitolo ha come oggetto la dimostrazione di alcuni criteri e come obbiettivo quello di fornire gli strumenti necessari per trovare i criteri di divisibilitá per ogni numero. Questi argomenti non vengono trattati né alle superiori né alle medie per l'importante bagaglio di conoscenze che richiedono, conoscenze che in parte sono state spiegate negli altri capitoli. Nonostante ció é stato necessario semplificare gli argomenti e omettere proprietá e dettagli nella spiegazione per renderla il piú intuitiva possibile. Questi argomenti sono la parte conclusiva del libro, nonché la parte piú complicata. Sono argomenti trattati a metá del corso di Algebra del secondo semestre del primo anno quindi, nonostante siano adeguatamente semplificati, non cé da spaventarsi se non tutto é chiaro.

4.1 Anello dei resti

Abbiamo visto che quando sommiamo, moltiplichiamo o facciamo altre operazioni sui numeri, lavoriamo fondamentalmente con un insieme che definisce gli elementi su cui sto eseguendo determinate operazioni, quindi i numeri, e con l'operazione stessa, definita da regole e proprietá (a partire da quella di *buona definizione*).
Non vi sorprenderá sapere che esistono diverse tipologie di insiemi di numeri definiti da proprietá caratteristiche (tipologie che si basano fondamentalmente sul tipo di numeri su cui si lavora e sul tipo di operazioni e loro proprietá). Ad esempio, per dimostrare i criteri di divisibilitá dobbiamo lavorare con insiemi chiamati "*anelli*". Non entreró nel dettaglio, vi basti sapere che la principale caratteristica che ci interessa é quella di avere l'operazione di somma e di prodotto (non basta peró avere le due operazioni: i numeri naturali, ad esempio, hanno sia la somma che il prodotto ma non sono un anello).

Ci poniamo ora come obiettivo quello di trovare il criterio di divisibilitá del 3, motivo per cui bobbiamo lavorare con l'insieme:

$$A = \{0, 1, 2\}$$

Ci interessa questo insieme perché i suoi elementi sono tutti i possibili resti della divisione per 3, motivo per cui si chiama "*anello dei resti del 3*". Piú avanti sará chiaro il motivo della scelta di questo insieme, concentriamoci ora sui resti della divisione per 3.
Per capire perché i resti della divisione per 3 possono essere solo $0, 1, 2$ forniamo degli esempi: é facile trovare un esempio di un numero che diviso per 3 dia resto 0, basta considerare un numero divisibile per 3:

	6	3
	-6	2
Resto:	0	

Ora per trovare un numero con resto 1 é sufficiente, ad esempio, trovare un numero divisibile per 3 e aggiungere 1, ad esempio 7:

	7	3
	-6	2
Resto:	1	

Ugualmente, per trovare un numero con resto 2 é sufficiente sommare 2 ad un numero divisibile per 3 oppure sommare 1 ad un numero con resto 1. Ad esempio, 6 é divisibile per 3, quindi $6 + 2 = 8$ ha resto 2, ugualmente 7 ha resto 1, quindi $7 + 1 = 8$ ha resto 2:

	8	3
	-6	2
Resto:	2	

Ugualmente trovare un numero che diviso 3 dia resto 3 significa sommare 3 ad un numero divisibile per 3 ma cosí facendo si ottiene un altro numero divisibile per 3. Un esempio: $6 + 3 = 9$ divisibile per 3. Quindi dopo il resto 2 si ritorna al resto 0 e si ricomincia, quindi i resti possono essere 0, 1 e 2.

Tornando all'insieme A, ho omesso un dettaglio: i suoi elementi non sono semplici numeri ma sono classi di equivalenza, cioé:

$$A = \{[0], [1], [2]\}$$

Dove la relazione considera il resto della divisione per 3. Cioé:

$$n \sim 0_A \Leftrightarrow \frac{n}{3} \text{ ha resto } 0 \qquad n \sim 1_A \Leftrightarrow \frac{n}{3} \text{ ha resto } 1$$

$$n \sim 2_A \Leftrightarrow \frac{n}{3} \text{ ha resto } 2$$

Dove con 0_A si intende lo 0 dell'insieme A, diverso dallo 0 dei numeri interi in quanto quest'ultimo non é una classe di equivalenza. Ugualmente per 1_A e 2_A. Quindi un certo numero n é in relazione con 0_A é equivalente a dire che la divisione $\frac{n}{3}$ ha resto 0. Ugualmente con 1_A é equivalente ad avere resto 1 e con 2_A resto 2. Quindi possiamo scrivere le classi di equivalenza:

$$[0] = \{n : \frac{n}{3} \text{ ha resto } 0\} = \{0, 3, 6, 9, 12, ...\}$$

$$[1] = \{n : \frac{n}{3} \text{ ha resto } 1\} = \{1, 4, 7, 10, 13, ...\}$$

$$[2] = \{n : \frac{n}{3} \text{ ha resto } 2\} = \{2, 5, 8, 11, 14, ...\}$$

Un modo piú semplice di scrivere le classi di equivalenza:

$$[0] = \{n : \frac{n}{3} \text{ ha resto } 0\} = \{n : n = 3t, \text{ con } t \in \mathbb{Z}\}$$

Cioé ogni numero divisibile per 3 ha resto 0, quindi appartiene alla classe [0], e quindi é nella forma $3t$, basta pensare a $3 = 3 \cdot 1$, $6 = 3 \cdot 2$, ...
Abbiamo poi visto che se prendo un multiplo di 3 (nella forma $3t$) e aggiungo 1 ottengo resto 1, quindi é possibile semplificare la classe di equivalenza [1]:

$$[1] = \{n : \frac{n}{3} \text{ ha resto } 1\} = \{n : n = 3t + 1, \text{ con } t \in \mathbb{Z}\}$$

Similmente con la classe di equivalenza [2] é sufficiente sommare 2 ad un multiplo di 3:

$$[2] = \{n : \frac{n}{3} \text{ ha resto } 2\} = \{n : n = 3t + 2, \text{ con } t \in \mathbb{Z}\}$$

4.1.1 Somma

Definiti gli elementi dell'insieme A su cui stiamo lavorando, rimangono da definire le operazioni di somma e prodotto, in modo che A sia un anello (come ho giá detto non sono sufficienti le due operazioni, ma per altri dettagli che non riporto con la somma e il prodotto A diventa un anello). É chiaro che la somma funziona nel solito modo se consideriamo ad esempio:

$$0+0=0 \qquad 0+1=1 \qquad 1+1=2$$

Problema di notazione: visto che stiamo lavorando con elementi di A dovremmo scrivere $[0]+[0]=[0]$, cioé lavorare con le classi di equivalenza. Possiamo peró accordarci (cosa che succede spesso) e dire che togliamo le parentesi quadre ricordandoci peró di star lavorando sempre con classi di equivalenza in A! Da ora in poi quindi scriveremo gli elementi di A senza le parentesi ma intenderemo comunque le classi di equivalenza.
Ma cosa possiamo dire su $2+1$? Non puó essere $2+1=3$ poiché 3 non é un elemento di A (per meglio dire: [3] non é una classe di equivalenza che appartiene a A). Ricordiamo peró che 3, in quanto divisibile per 3, cioé la divisione $\frac{3}{3}$ ha resto 0, appartiene alla classe di equivalenza [0]; quando un numero appartiene ad una classe di equivalenza possiamo scrivere: $[3]=[0]$, o come ci siamo accordati: $3=0$. Cioé:

$$3 \in [0] \Leftrightarrow [3]=[0] \Leftrightarrow 3=0$$

Generalizzando:

$$x \in [n] \Leftrightarrow [x]=[n] \Leftrightarrow x=n$$

Seguendo questa notazione é possibile dire che tutti gli elementi di una classe di equivalenza sono uguali tra loro, cioé:

$$[0]=\{0,3,6,9,12,...\}$$
$$\Rightarrow [0]=[3]=[6]=[9]=[12]=... \Leftrightarrow 0=3=6=9=12=...$$

Cioé la classe di equivalenza [0] raccoglie tutti gli elementi in relazione con 0, cioé tutti i numeri che hanno valore 0 nell'insieme A. Quindi nonostante $0,3,6,9,...$ siano numeri diversi, visto che sono elementi della stessa classe di equivalenza in A hanno tutti lo stesso valore: valgono 0_A. Vengono chiamate anche rappresentazioni dello 0 nell'insieme A.
Dunque abbiamo la soluzione, visto che $[0]=[3]$ o equivalentemente $0=3$:

$$2+1=0$$

Visto che stiamo lavorando con l'insieme A, non posso scrivere numeri diversi dagli elementi di A! Fornendo altri esempi:

$$2+2=4=1 \text{ perché } 4 \in [1]$$
$$2+2+1=5=2 \text{ perché } 5 \in [2]$$
$$2+2+2=6=0 \text{ perché } 6 \in [0]$$

Il nome "*anello*" deriva appunto dal fatto che dopo il 2 (l'elemento massimo in A) si rinizia da 0, chiudendo un virtuale anello matematico. Un altro metodo per risolvere le somme é fare una tabella di corrispondenze tra i numeri e gli elementi di A:

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10	11
A	0	1	2	0	1	2	0	1	2	0	1	2

Tornando alla somma $2+1$ nei naturali vale $2+1=3$, cercando il corrispondente del 3 nel nostro anello A troviamo che $3=0$ e quindi $2+1=0$. Ugualmente, $2+2=4$ nei naturali, quindi in A vale $2+2=1$, visto che $4=1$ dalla tabella.
Quindi per quanto riguarda la somma tra classi di equivalenza si definisce:

$$[a]+[b]=[a+b]$$

Che é esattamente il modo con cui le abbiamo risolte noi senza parentesi (come da convenzione). Se le rivediamo con le parentesi:

$$2+1=[2]+[1]=[2+1]=[3]=[0]=0$$

Somme di questo genere non sono particolarmente complesse, piú ostiche sono somme con numeri piú grandi, in cui non é immediato capire in quale classe di equivalenza appartengono: $42+620$ ad esempio. Esiste comunque un modo per semplificare il calcolo: abbiamo visto che se un numero x appartiene a una certa classe di equivalenza $[n]$, allora anche $x+3$ appartiene alla classe di equivalenza $[n]$; allo stesso modo anche $x-3$ appartiene alla stessa classe di equivalenza ($6 \in [0] \Rightarrow 6-3=3 \in [0]$). Allo stesso modo se sottraggo o aggiungo un multiplo di 3 il risultato continua ad appartenere alla stessa classe di equivalenza:

$$9 \in [0]$$
$$\Rightarrow 9-3=6 \in [0]$$
$$\Rightarrow 6-3=3 \in [0]$$
$$\Rightarrow 9-6=9-(3\times 2)=3 \in [0]$$

Prendiamo ora in esempio il numero 42 e cerchiamo di capire in quale classe appartiene: per semplificare sensibilmente la somma é necessario sottrarre un multiplo di 3:

$$42 \in [n]$$
$$\Rightarrow 42-6=42-(3\times 2)=36 \in [n]$$

É giá chiaro che, visto che 36 appartiene alla stessa classe di equivalenza di 42 e visto che 36 é divisibile per 3, 42 apparterrá alla classe [0], in quanto 36 appartiene alla classe [0] (appunto perché é divisibile per 3) e quindi $[n] = [0]$. Se consideriamo ora 620:

$$620 \in [n]$$
$$\Rightarrow 620 - (3 \times 200) = 620 - 600 = 20 \in [n]$$
$$\Rightarrow 20 - (3 \times 6) = 20 - 18 = 2 \in [n]$$
$$\Rightarrow 2 \in [2] \Rightarrow 620 \in [2]$$

Sottraendo diversi multipli di 3 otteniamo che 620 é nella stessa classe di equivalenza di 2, il quale ovviamente appartiene alla classe di equivalenza [2], da cui segue appunto $620 \in [2]$.
Visto che $42 \in [0]$ e $620 \in [2]$ possiamo riscrivere:

$$42 + 620 = 0 + 2 = 2$$

Verifichiamo che il risultato della somma $42 + 620 = 662$ abbia resto 2:

	662	3
	-660	220
Resto:	2	

Buona definizione

Controlliamo ora se la somma é *ben definita*, cioé se il risultato non cambia in funzione dell'elemento della classe di equivalenza con cui si lavora. Ad esempio, visto che:

$$[1] = \{1, 4, 7, 10, 13, ...\}$$
$$[2] = \{2, 5, 8, 11, 14, ...\}$$

Allora deve valere:

$$2 + 1 = 5 + 1 = 5 + 4 = ...$$

Appunto perché 2 e 5 appartengono alla stessa classe di equivalenza, cosí come 1 e 4. Dimostrare peró che $2 + 1 = 5 + 4$ non assicura che la proprietá di buona definizione valga con tutti gli elementi. Per dimostrarlo globalmente é necessario usare la definizione di classi di equivalenza:

$$a \in [n] \Leftrightarrow a = 3t + n$$
$$b \in [m] \Leftrightarrow a = 3t + m$$

Consideriamo quindi due elementi a e b in due generiche classi di equivalenza $[n]$ e $[m]$ (di quelle contenute in A, quindi [0] o [1] o [2]), quindi $a \in [n]$ e $b \in [m]$, da cui segue che $[a] = [n]$ e $[b] = [m]$. Per valere la proprietá di buona definizione deve valere:

$$[a] + [b] = [a + b] = [m + n] = [m] + [n]$$

Appunto perché a e n sono nella stessa classe di equivalenza e anche b e m sono nella stessa classe di equivalenza.
Dunque se vale $[a + b] = [m + n]$ l'operazione di somma non dipende dall'elemento della classe di equivalenza, che é un rappresentante del valore della classe di equivalenza, e quindi la funzione é ben definita.

Visto che $a \in [n]$ allora vale $a = 3t + n$, e $b \in [m]$ allora $b = 3s + m$ (con a uso t e con b uso s perché potrebbero avere valori diversi), allora é possibile riscrivere:

$$a + b = (3t + n) + (3s + m) = 3(t + s) + n + m$$

É possibile riscrivere $t + s = v$ e ottenere:

$$a + b = 3v + (n + m)$$

Ma dalla definizione di classe di equivalenza:

$$a + b = 3v + (n + m) \Leftrightarrow (a + b) \in [n + m]$$

Inoltre $(a + b) \in [n + m]$ é equivalente a $[a + b] = [n + m]$ che era quello che volevamo dimostrare.

4.1.2 Prodotto

Per la moltiplicazione la cosa é analoga:

$$1 \times 1 = 1 \qquad 2 \times 1 = 2 \qquad 0 \times 0 = 0$$

I problemi arrivano con prodotti nella forma:

$$2 \times 2 = 4$$

Anche qua ricorriamo alle classi di equivalenza e, ricordando che $4 \in [1]$:

$$2 \times 2 = 4 = 1$$

Analogamente alla somma, il prodotto si definisce:

$$[a] \times [b] = [a \times b]$$

Appunto perché implicitamente lo abbiamo risolto cosí:

$$2 \times 2 = [2] \times [2] = [2 \times 2] = [4] = [1] = 1$$

Buona definizione

Controlliamo se il prodotto é *ben definito*. Verifichiamo, ad esempio:

$$[1] = \{1, 4, 7, 10, 13, ...\}$$
$$[2] = \{2, 5, 8, 11, 14, ...\}$$

Per cui deve valere:

$$2 \times 1 = 5 \times 1 = 5 \times 4 = ...$$

Perché 2 e 5 appartengono a [2], e 1 e 4 appartengono a [1].
La dimostrazione della buona definizione ricalca quella data con la somma: consideriamo $a \in [n]$ e $b \in [m]$, quindi $[a] = [n]$ e $[b] = [m]$. Per valere la proprietá di buona definizione deve valere:

$$[a] \times [b] = [a \times b] = [m \times n] = [m] \times [n]$$

Da $a \in [n]$ segue $a = 3t + n$, e da $b \in [m]$ segue $b = 3s + m$, dunque:

$$\begin{aligned} a \times b = (3t + n) \times (3s + m) &= 3t \cdot 3s + 3t \cdot m + n \cdot 3s + n \cdot m \\ &= 3(3ts + tm + sn) + nm \end{aligned}$$

Riscrivo $v = 3ts + tm + sn$ e ottengo: $a \times b = 3v + (n \times m)$ e dalla definizione di classe di equivalenza:

$$a \times b = 3v + (n \times m) \Leftrightarrow (a \times b) \in [n \times m]$$

Inoltre $(a \times b) \in [n \times m]$ é equivalente a $[a \times b] = [n \times m]$ che era quello che volevamo dimostrare.

4.2 Dimostrazione dei criteri di divisibilitá

4.2.1 Criterio di divisibilitá per 3

Arriviamo ora al nocciolo della questione. Abbiamo visto che i numeri in relazione con 0_A sono i numeri che divisi per 3 hanno resto 0, equivalentemente sono divisibili per 3, quindi nella forma $3t$ con $t \in \mathbb{Z}$. Quindi se un numero é divisibile per 3 deve essere in relazione con 0_A. La cosa appare ovvia, ma come possiamo sapere, ad esempio, se il numero 167293 é in relazione con 0_A? Potremmo sottrarre multipli di 3 finché non si ottiene un numero sufficientemente piccolo da capire a occhio a che classe di equivalenza appartiene, ma la questione diventa troppo complicata ricordando che il senso dei criteri di divisibilitá é proprio trovare un modo semplice di determinare la divisibilitá di un numero. Una soluzione al problema consiste nello scrivere il numero come somma delle sue cifre

$$n = n_0 + n_1 \times 10 + n_2 \times 10^2 + n_3 \times 10^3 + ...$$

Un esempio:

$$\begin{aligned} 4132 =& 2 + 3 \times 10 + 1 \times 10^2 + 4 \times 10^3 \\ =& 2 + 30 + 100 + 4000 \end{aligned}$$

Ora la classe di equivalenza di n, che corrisponde al resto della divisione $\frac{n}{3}$, é riscrivibile come:

$$[n] = [n_0 + n_1 \times 10 + n_2 \times 10^2 + n_3 \times 10^3 + ...]$$

Infatti visto che vale l'uguaglianza tra n e la sua scomposizione, vale l'uguaglianza anche tra le rispettive classi di equivalenza, cioé i due numeri hanno lo stesso resto se divisi per 3. Per come sono definite le operazioni é possibile dividere le parentesi:

$$\begin{aligned} [n] &= [n_0 + n_1 \times 10 + n_2 \times 10^2 + n_3 \times 10^3 + ...] \\ &= [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ... \end{aligned}$$

Stiamo lavorando con le classi resto di 3, sappiamo che $[10] = [1]$, cioé $\frac{10}{3}$ ha resto 1, quindi possiamo riscrivere:

$$\begin{aligned} [n] &= [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ... \\ &= [n_0] + [n_1] \times [1] + [n_2] \times [1]^2 + [n_3] \times [1]^3 + ... \\ &= [n_0] + [n_1 \times 1] + [n_2 \times 1^2] + [n_3 \times 1^3] + ... \\ &= [n_0] + [n_1] + [n_2] + [n_3] + ... \\ &= [n_0 + n_1 + n_2 + n_3 + ...] \end{aligned}$$

Queste semplificazioni derivano dalla definizione delle operazioni. L'ultima riga sta dicendo che $[n]$ é la stessa classe di equivalenza della somma delle sue cifre. Cioé che $\frac{n}{3}$ ha lo stesso resto di $\frac{n_0+n_1+n_2+...}{3}$ e quindi che n é divisibile per 3 se lo é $n_0 + n_1 + n_2 + ...$, cioé se $[n_0 + n_1 + n_2 + ...] = [0]$ Questa é la formalizzazione del solito criterio che dice che un numero n é divisibile per 3 se la somma delle sue cifre é divisibile per 3. Abbiamo riproposto il criterio dicendo che la somma delle cifre di n deve appartenere a $[0]$, cioé divisa per 3 deve avere resto 0.

4.2.2 Criterio di divisibilitá per 5

La questione é esattamente uguale per gli altri criteri di divisibilitá, la differenza é l'insieme su cui stiamo lavorando, che per il criterio del 5 é l'insieme dei resti della divisione per 5, cioé:

$$A = \{[0], [1], [2], [3], [4]\}$$

In generale i resti della divisione per un numero n sono: $\{0, 1, 2, ..., n-1\}$. Il procedimento é analogo: consideriamo la scomposizione del numero come somma delle sue cifre

$$[n] = [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ...$$

Visto che 10 é divisibile per 5, allora vale $10 \in [0]$, cioé la divisione $\frac{10}{5}$ ha resto 0. Quindi sostituisco $[10] = [0]$:

$$\begin{aligned} [n] &= [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ... \\ &= [n_0] + [n_1] \times [0] + [n_2] \times [0]^2 + [n_3] \times [0]^3 + ... \\ &= [n_0] \end{aligned}$$

Cioé n appartiene alla stessa classe di equivalenza di n_0, la cifra delle unitá. Quindi n é divisibile per 5 se n_0 appartiene alla classe di equivalenza [0] e quindi se é divisibile per 5. Visto che n_0 é una sola cifra, quindi un numero compreso tra 0 e 9, gli unici due valori divisibili per 5 compresi in questo intervallo sono 0 e 5. Quindi si ottiene il solito criterio: n é divisibile per 5 se lo é la cifra delle unitá, quindi se finisce con 0 oppure 5.

4.2.3 Criterio di divisibilitá per 7

Probabilmente non ricorderete il criterio di divisibilitá del 7, ma sono sicuro ricorderete che é difficile da ricordare.
Ora é necessario lavorare con i resti della divisione per 7:

$$A = \{[0], [1], [2], [3], [4], [5], [6]\}$$

Si scompone un generico numero n:

$$[n] = [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ...$$

Questa volta é piú semplice sfruttare la tabella invece di calcolare il resto delle divisioni passo passo:

$\mathbb{N}$	0	1	2	3	4	5	6	7	8	9	10
A	0	1	2	3	4	5	6	0	1	2	3

Ricaviamo innanzitutto:

$$[10] = [3]$$

Vogliamo semplificare il piú possibile la scomposizione nella somma delle cifre, quindi ci interessa trovare i valori di $[10]$, $[10]^2$, $[10]^3$, ... per calcolare $[10]^2$ possiamo sfruttare l'uguaglianza $[10] = [3]$:

$$[10]^2 = [3]^2 = [9] = [2]$$

Nuovamente per calcolare $[10]^3$ sfruttiamo le uguaglianze ottenute:

$$[10]^3 = [10]^2 \times [10] = [2] \times [3] = [6]$$

Continuo:

$$[10]^4 = [10]^2 \times [10]^2 = [2] \times [2] = [4]$$
$$[10]^5 = [10]^4 \times [10] = [4] \times [3] = [12] = [5]$$
$$[10]^6 = [10]^5 \times [10] = [5] \times [3] = [15] = [1]$$

Da qui il pattern si ripete, infatti:

$$[10]^7 = [10]^6 \times [10] = [1] \times [3] = [3]$$
$$[10]^8 = [10]^7 \times [10] = [3] \times [3] = [9] = [2]$$
$$.....$$

Sostituiamo:

$$\begin{aligned}
[n] =& [n_0] + [n_1] \times [10] + [n_2] \times [10]^2 + [n_3] \times [10]^3 + ... \\
=& [n_0] + [n_1] \times [3] + [n_2] \times [2] + [n_3] \times [6] + ... \\
=& [n_0 + n_1 \times 3 + n_2 \times 2 + n_3 \times 6 + n_4 \times 4 + n_5 \times 5 + \\
& n_6 + n_7 \times 3 + n_8 \times 2 + n_9 \times 6 + n_{10} \times 4 + n_{11} \times 5 + ...] \\
=& [n_0 + 3n_1 + 2n_2 + 6n_3 + 4n_4 + 5n_5 + \\
& n_6 + 3n_7 + 2n_8 + 6n_9 + 4n_{10} + 5n_{11} + ...]
\end{aligned}$$

Visto che sono nella stessa classe di equivalenza, cioé condividono lo stesso resto se divisi per 7, n é divisibile per 7 se lo é il numero:

$$n_0 + 3n_1 + 2n_2 + 6n_3 + 4n_4 + 5n_5 + \\ n_6 + 3n_7 + 2n_8 + 6n_9 + 4n_{10} + 5n_{11} + ...$$

É possibile che vi ricordiate di un criterio vagamente diverso: n é divisibile per 7 se lo é il numero

$$n_0 + 3n_1 + 2n_2 - 1n_3 - 3n_4 - 2n_5 + \\ n_6 + 3n_7 + 2n_8 - 1n_9 - 3n_{10} - 2n_{11} + ...$$

In realtá é lo stesso criterio, poiché, come abbiamo giá visto, sono uguali:

$$[n] = [n + 7] = [n - 7]$$

Di cui abbiamo giá visto un esempio:

$$[0] = [0 + 7] = [7]$$

Infatti sia 0 che 7 sono divisibili per 7, quindi appartengono entrambi alla classe [0], dunque é possibile scrivere appunto $[0] = [7]$. Ma é possibile scrivere anche:

$$[0] = [0 - 7] = [-7]$$

Infatti anche -7 é divisibile per 7, quindi appartiene alla classe [0] e quindi $[-7] = [0]$. Dunque:

$$[6] = [6 - 7] = [-1]$$
$$[4] = [4 - 7] = [-3]$$
$$[5] = [5 - 7] = [-2]$$

Dunque il numero che avevamo trovato

$$n_0 + 3n_1 + 2n_2 + 6n_3 + 4n_4 + 5n_5 + \\ n_6 + 3n_7 + 2n_8 + 6n_9 + 4n_{10} + 5n_{11} + ...$$

é nella stessa classe di equivalenza di:

$$n_0 + 3n_1 + 2n_2 - 1n_3 - 3n_4 - 2n_5 + \\ n_6 + 3n_7 + 2n_8 - 1n_9 - 3n_{10} - 2n_{11} + ...$$

Quindi il numero n é divisibile per 7 se lo é quest'ultimo, esattamente come viene insegnato.

Non é molto semplice ricordare questo criterio, ma non é l'unico. Esistono altri criteri, ne riporto uno tra i piú semplici. Consideriamo:

$$n = n_0 + n_1 \times 10 + n_2 \times 10^2 + n_3 \times 10^3 + ...$$

É possibile raccogliere 10:

$$n = n_0 + n_1 \times 10 + n_2 \times 10^2 + n_3 \times 10^3 + ... \\ = n_0 + 10 \times (n_1 + n_2 \times 10 + n_3 \times 10^2 + ...)$$

Rinominando $b = (n_1 + n_2 \times 10 + n_3 \times 10^2 + ...)$ si ottiene:

$$n = n_0 + 10 \times b$$

Ragioniamo con le classi di equivalenza e moltiplichiamo la nuova espressione del numero n per 5:

$$[n_0 + 10 \times b] \times [5] = [5] \cdot [n_0] + [5] \cdot [10 \times b] = [5 \cdot n_0] + [5 \cdot 10] \times [b]$$

Ricordando che $[10] = [3]$, é possibile scrivere

$$[5] \times [10] = [5] \times [3] = [15] = [1]$$

Infatti 15, se diviso per 7, ha resto 1. Dunque:

$$[n_0 + 10 \times b] \times [5] = [5 \cdot n_0] + [b]$$

E riassumendo:

$$[n] \times [5] = [n_0 + 10 \times b] \times [5] = [5n_0] + [b]$$

Quindi:

$$[n] \times [5] = [5n_0] + [b]$$

Dunque se n é divisibile per 7, quindi $[n] = [0]$, allora $[n][5] = [0]$ e quindi anche $[5n_0] + [b] = 0$, visto che sono uguali. Cioé affinché $[n]$ sia divisibile per 7 é sufficiente che $[5n_0] + [b] = 0$, cioé che il numero $5n_0 + b$ sia divisibile per 7.

5 Fonti e bibliografia

Insiemi

* Paul R. Halmos, *Naive Set Theory*, Martino publishing, 2011, ISBN: 978-1-61427-131-4
* Wikipedia: Set (mathematics), https://en.wikipedia.org/wiki/Set_(mathematics)
* Wikipedia: Union (set theory), https://en.wikipedia.org/wiki/Union_(set_theory)
* Wikipedia: Intersection (set theory), https://en.wikipedia.org/wiki/Intersection_(set_theory)
* Wikipedia: Complement (set theory), https://en.wikipedia.org/wiki/Complement_(set_theory)
* Wikipedia: Euclid's theorem (Teorema dell'infinitá dei numeri primi), https://en.wikipedia.org/wiki/Euclid%27s_theorem
* ProofWiki: Union distributes over Intersection, https://proofwiki.org/wiki/Union_Distributes_over_Intersection
* ProofWiki: De Morgan's Laws (Set Theory)/Set Difference, https://proofwiki.org/wiki/De_Morgan%27s_Laws_(Set_Theory)

Costruzione dei numeri

* Paul R. Halmos, *Naive Set Theory*, Martino publishing, 2011, ISBN: 978-1-61427-131-4
* Wikipedia: Natural Number, https://en.wikipedia.org/wiki/Natural_number
* Wikipedia: Integer, https://en.wikipedia.org/wiki/Integer
* Wikipedia: Rational Number, https://en.wikipedia.org/wiki/Rational_number
* Wikipedia: Real Number, https://en.wikipedia.org/wiki/Real_number
* Wikipedia: Complex Number, https://en.wikipedia.org/wiki/Complex_number
* Wikipedia: Construction of the real numbers, https://en.wikipedia.org/wiki/Construction_of_the_real_numbers
* Wikipedia: Dedekind cut, https://en.wikipedia.org/wiki/Dedekind_cut

* Wikipedia: Square root of 2,
  https://en.wikipedia.org/wiki/Square_root_of_2
* Wikipedia: 0.999...,
  https://en.wikipedia.org/wiki/0.999...

Criteri di divisibilitá

* Andrea Caranti, *Note di Algebra - Capitolo 4: Congruenze*,
  http://www.science.unitn.it/∼caranti/Didattica/Algebra-A/static/Note/Algebra.pdf
* Wikipedia: Natural Number,
  https://en.wikipedia.org/wiki/Natural_number