Matematica per adulti

1 Prima settimana

intro

Giorno 1: quanti numeri?

Non so ci avete pensato, che possiamo contare per sempre. Dato un numero, posso sempre scrivere e dare un nome al successivo. Curiosamente non è sempre stato così.

Io ricordo distintamente quando da piccolo ho realizzato la cosa. Scherzando, ma poi non tanto, dico spesso agli studenti che quella è stata la prima e unica esperienza spirituale della mia vita. Per questo mi ha stupito realizzare che non tutti da piccoli sono passati per quell'esperienza. L'ho chiesto al forum e alcuni hanno stentato a arrivare al punto, qualcuno ha dovuto essere convinto che sa il nome delnumero 66 354 427 745 367. In fondo è sempre bello quando il mondo ti stupisce.

I romani avevano un numero finito di simboli con cui potevano scrivere un numero finito di numeri. Per esempio con I e V potete scrivere I II III IV V VI VII VIII.

Poi per scrivere 9 dovete inventare un nuovo simbolo X.

Loro avevano (a seconda del secolo) fino a un simbolo M per 1000 (poi aggiungevano barre sopra $\bar{M}$, $\bar{\bar{M}}$ per iterare la cosa ma senza cambiare il fatto che arrivavano a un certo numero) e poi si dovevano fermare.

Noi abbiamo lo zero, la notazione posizionale e la lingua (a parte i numeri 3, 11 e 20) è costruita in modo analogo. Conti fino a 10 poi 10-n arrivi fino a 20, 20-n arrivi fino a 30, 40, 50, ..., cento.

Poi si ricomincia con 1cento-nn, 2-cento–nn, ..., 9-cento–99.

Poi viene 1000 e si ricomincia 1-mille-nnn, 2-mille-nnn, ... nnn-mille-nnn. Poi viene 1 milione e si ricomincia, 1-milione-nnnnnn, fino a nnn-mille-nnn-milioni-nnnnnn, poi viene 1miliardo e si ricomincia fino a nnn-milioni-nnn-mila-nnn-miliardi-nnn-milioni-nnn-mila-nnn.

Voi potete dire che dieci cento mille milione miliardi funzionano come i romani. E forse è questo che trae in inganno i bambini, in fondo chi ha bisogno di contare fino a 1 miliardo?

Ma qui viene la novità, 1000-milioni-di-miliardi non hanno un nome vero (ce l'hanno perché la barbarie non ha limite ma non ne abbiamo bisogno).

Si chiamano 1 miliardo-di-miliardi

E si ricomincia. E poi 1-milione di miliardi di miliardi-nnnnnnnnn e così finché avete voglia.

Giorno 2: cardinali, ordinali, numerali

Abstract. Esistono infiniti numeri naturali.

Che differenza c'è tra numeri *cardinali*, *ordinali* e *numerali*?

I cardinali servono per contare gli oggetti (zero, uno, due, ...), gli ordinali servono per l'ordine (primo, secondo, terzo, ...) definiscono maggiore e minore, le operazioni di somma e prodotto in $\mathbb{N}$.

I numerali sono diversi modi di rappresentare un numero: 11 si può scrivere 11 in base 10, 1011 in binario, B in esadecimale, X in romano. Quando i carcerati contano i giorni sul muro della cella le 4 stanghette verticali tagliate da una stanghetta obliqua sono un numerale per 5.

Non ci occupiamo di numerali, sono solo rappresentazioni. Esistono cardinali (uno, due, tre, ...) e ordinali (primo, secondo, terzo, ...).

Il problema è che finché parliamo di numeri finiti, cardinali e ordinali sono in corrispondenza 1-a-1. Ok dovremo dare definizioni per bene. Lo faremo. Ma se è così, serve uno solo dei 2 l'altro non serve.

MA quando consideriamo insiemi infiniti i numeri ordinali sono molti di più. Quindi gli ordinali sono molto meglio. Ci torniamo in modo più preciso ma ci vuole pazienza che ci va un po'.

Per ora stiamo ancora a partire! Per essere sinceri questi primi giorni servono a far capire che ci sono un sacco di problemi, anzi che più si scava e peggio è. Ancora non abbiamo detto COSA è un numero naturale.

Qui i matematici si dividono in 2. Metà predilige le proprietà, le enuncia e se non si cura di cosa sia un numero. L'altra metà definisce cosa è un numero naturale (in genere come classe di equivalenza di insiemi finiti) e poi usando questa rappresentazione definire le operazioni (eg somma e prodotto) e per dimostrare le proprietà (eg commutativa, associativa, ...).

Siccome stiamo facendo turismo e nessuno ha fretta di arrivare, percorriamo entrambe le strade, ok?

Prima strada. Nell'800 Peano ha dato i seguenti assiomi per i numeri naturali.

1) 0 è un numero naturale.

2) esiste una funzione $s : \mathbb{N} \to \mathbb{N}$ e diciamo che $s(n)$ è il successore di n.

3) se x diverso da y allora $s(x)$ è diverso da $s(y)$

4) $s(x)$ non è mai 0 qualunque sia x

5) [Principio di induzione]

se U è un sottoinsieme di $\mathbb{N}$ e

a) $0 \in U$

b) se $n \in U$ allora $s(n) \in U$

allora $U = \mathbb{N}$

Questi assiomi, con un bel po' di lavoro permettono di dimostrare OGNI proprietà dei numeri naturali (che sappiamo dimostrare altrimenti).

Se conveniamo che non c'è un numero più grande di tutti (no "∞" non è un numero naturale se lo fosse, sapreste fare "$\infty+1$"), l'insieme dei numeri è infinito (in-finito) perché non posso finire di contare?

Per ora lasciate perdere cosa sia un numero, quello che conta è che sono infiniti, che hanno un nome, e che potremo fare operazioni coi numeri.

Giorno 3: somme e prodotto

Definiamo i numeri in $\mathbb{N}$

0

$1 = s(0)$

$2 = s(1) = s(s(0))$

$3 = s(2) = s(s(s(0)))$

$4 = s(3) = s(s(s(s(0))))$

$5 = s(4) = s(s(s(s(s(0)))))$

$6 = s(5) = s(s(s(s(s(s(0))))))$

$7 = s(6) = s(s(s(s(s(s(s(0)))))))$

$8 = s(7) = s(s(s(s(s(s(s(s(0))))))))$

e avanti così.

Definiamo la *somma* $a + b$ con le proprietà

$a + 0 = a$

$a + (s(b)) = s(a + b) = (a + b) + 1$

Se devo fare

$$5+3 = 5+s(s(s(0))) = s(5+s(s(0))) = s(s(5+s(0))) = s(s(s(5)))+0 = s(s(s(5)))$$

che è definito come 8.

Definiamo la *prodotto* ab:

$a \cdot 1 = a$

$a \cdot s(b) = a \cdot b + a$

Se devo fare

$$3 \cdot 2 = 3 \cdot s(1) = 3 \cdot 1 + 3 = 3 + 3 = 6$$

$$2 \cdot 3 = 2 \cdot s(s(1)) = 2 \cdot s(1) + 2 = (2 \cdot 1 + 2) + 2 = (2 + 2) + 2 = 4 + 2 = 6$$

Poi ci mettiamo con santa pazienza e dimostriamo le proprietà.

$a + 0 = 0 + a = a$	0 elemento neutro della somma
$(a + b) + c = a + (b + c)$	associativa della somma
$a + b = b + a$	commutativa della somma
$a1 = 1a = a$	1 elemento neutro del prodotto
$(ab)c = a(bc)$	associativa del prodotto
$ab = ba$	commutativa del prodotto
$(a + b)c = ac + bc$	distributiva della somma rispetto al prodotto

Non credo siano importanti i dettagli ma se vuoi ne dimostriamo qualcuna.

Giorno 4: insiemi

Abstract. Fin qui non abbiamo ancora fatto nulla. Abbiamo solo scoperto che:
1) i numeri naturali sono infiniti (quindi anche in prima elementare non si può parlare solo di roba finita anche se faccio 2+3). Cioè si può ma secondo me non si capisce cosa si lascia fuori e si lascia fuori il meglio.
2) esisteranno 2 tipi di numeri (cardinali e ordinali). Finché consideriamo numeri finiti non fa differenza, uno vale l'altro. Se consideriamo gli infiniti, invece, gli ordinali sono più fondamentali e "di più" dei cardinali.
3) i cardinali sono per contare le cose, gli ordinali per essere messi in fila (0, 1, 2, 3, ...). Coi numeri finiti fate entrambe le cose, con quelli infiniti molti ordinali diversi hanno la stessa cardinalità.
4) Abbiamo fatto gli assiomi di Peano per i numeri naturali. Questi permettono di definire le operazioni di somma e prodotto, di dimostrare un sacco di cose, ma non ci dicono cosa sono i numeri naturali. Negli approcci assiomatici uno non dice cosa sono le cose, dice le proprietà e usa solo quelle.
5) per un approccio non-assiomatico abbiamo bisogno di dire cosa è un insieme (e poi funzioni e relazioni). Questo è un vero casino (sempre a causa degli insiemi infiniti).

Insiemi: prima cosa da dire è che gli insiemi possono avere *elementi*. Per dire che 3 è un numero naturale, chiamiamo $\mathbb{N}$ l'insieme dei numeri naturali e diciamo $3 \in \mathbb{N}$, che si legge 3 appartiene a $\mathbb{N}$.

Seconda cosa esiste un insieme senza elementi. Si chiama l'insieme vuoto, lo chiamiamo $\varnothing$. Siccome 2 insiemi sono uguali a meno che non produca un elemento che sta in uno ma non nell'altro, esiste un solo insieme vuoto o se preferite ogni insieme vuoto e uguale all'altro.

Come ho detto un insieme finito è la lista senza ripetizione dei suoi elementi. I numeri primi minori di 10 sono l'insieme $P = \{2, 3, 5, 7\}$. Quanti elementi ha?

(ah! non potete rispondere perché ancora non abbiamo definito la cardinalità di un insieme e pure coi numeri andiamo ancora maluccio.)

Quando si passa agli insiemi infiniti, si è pensato (direi nell'800) di definirli dando una proprietà $P(x)$ che quando è vera per x allora x appartiene a A ($x \in A$), quando è falsa, allora x non appartiene all'insieme A ($x \notin A$).

Ad esempio i numeri pari corrispondono alla proprietà $P(n)$: esiste $k \in N$ tale che $n = 2k$.

per $n = 0$, esiste $k = 0$ tale che $2 \cdot 0 = 0$, quindi 0 è pari.

per $n = 1$, non esiste $k \in \mathbb{N}$ tale che $2k = 1$, quindi 1 non è pari.

(ovviamente bisognerebbe dimostrare che non esiste, mi credete?)

per $n = 2$, esiste $k = 1$ tale che $2 \cdot 1 = 2$, quindi 2 è pari.

per $n = 6$, esiste $k = 3$ tale che $2 \cdot 3 = 6$, quindi 6 è pari.

[sto usando i numeri naturali di Peano per fare gli esempi]

L'insieme dei numeri pari $A = \{n \in \mathbb{N} : P(n)\}$ lo indichiamo pure in modo più impreciso come $A = \{0, 2, 4, ..., 2k, ...\}$ come se fosse un elenco. Lo indichiamo pure con $2\mathbb{N}$, ma sono solo syntax sugar.

L'unico piccola crepa nel nostro castello di buone intenzioni è che ci sono delle proprietà (antinomie) che non definiscono dei buoni insiemi.

> **Nota:** per gli informatici, quello che faccio è che definisco un linguaggio formale e una grammatica per scrivere enunciati e proposizioni. Dico proprio con una context free grammar. L'idea è che poi voglio definire un insieme come gli elementi che rendono vera una proposizione. Purtroppo non si riesce ad escludere le antinomie a livello sintattico. Cioè si può ma si è costretti a tipizzare fortemente il linguaggio e bisogna gerarchizzare i tipi molto più rigorosamente di come fate voi nei linguaggi di oggi. A quel punto dichiaro equivalenti 2 proposizioni che sono sempre vere o false sugli stessi oggetti e un insieme è una proposizione modulo equivalenti. Gli assiomi di Peano in buona sostanza sono una tale proposizione e definiscono l'insieme $\mathbb{N}$ (quando scrivo "per ogni $k \in \mathbb{N}$", sto dichiarando il tipo di k).

Giorno 5: operazioni tra insiemi

Ora che sappiamo cosa è un insieme (o almeno facciamo finta) possiamo definire un po' di operazioni.

Dati 2 insiemi A e B definiamo l'*unione*, scriviamo $A \cup B$ che è l'insieme che contiene tutti gli elementi x che sono in A o in B (o in entrambi ma sono elementi dell'unione una volta sola visto che $A \cup B$ è un insieme e nessun insieme può contenere 2 volte uno stesso elemento).

Dati 2 insiemi A e B definiamo l'*intersezione*, scriviamo $A \cap B$ che è l'insieme che contiene tutti gli elementi x che sono in A e in B (cioè gli elementi comuni a A e B).

Il *prodotto* $A \times B$ è l'insieme delle coppie (a, b) con il primo elemento $a \in A$ e il secondo $b \in B$. In pratica

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Nota: come puoi immaginare ora che sai come funziona la testa dei matematici prima o poi vorremo fare operazioni tra infiniti insiemi. Per ora ci accontentiamo.

Nota: un altro casino è che possiamo fare $(A \times B) \times C$ che in teoria avrebbe come elementi coppie $((a, b), c)$ ma facciamo finta che non ce ne accorgiamo e che $A \times B \times C$ contenga terne (a, b, c). sia $A \times B \times C$, che $(A \times B) \times C$ che $A \times (B \times C)$ contengono le terne (a, b, c).

Esercizio: Cosa contiene $\mathbb{N} \times \varnothing$?

Se ogni elemento di A è anche elemento di B allora A è un *sottoinsieme* di B e scriviamo $A \subset B$. Ovviamente $\varnothing$ è sottoinsieme di ogni insieme B ($\varnothing \subset B$ per qualunque B). Ovviamente per ogni insieme B, $B \subset B$, cioè B è sempre sottoinsieme di se stesso.

Dato A un sottoinsieme di B ($A \subset B$) possiamo definire il complemento di A in B, che è l'insieme $B - A$ che contiene tutti gli elementi $x \in B$ tale che non sono elementi di A, cioè:

$$B - A = \{x \in B : x \notin A \subset B\}$$

Nota: sui libri lo trovi anche definito quanto A non è sottoinsieme ma a me piace di più così al momento.

Nota: qui è uno dei posti dove i tipi importano. Se ho P, insieme dei primi minori di 10, cioè $P = \{2, 3, 5, 7\}$ e prendessi l'insieme delle cose che non stanno in P oltre a 6, in $-P$ ci troverei pure una mela, hookii, me e te. invece faccio $\mathbb{N} - P$ e ci trovo tutti **i numeri** che non sono in P. $\mathbb{N}$ funziona come un tipo.

Dato un insieme A, $P(A)$ è l'insieme di tutti i sui sottoinsiemi, si chiama l'*insieme delle parti*. Se $A = \{0, 1, 2\}$ allora

$$P(A) = \{\varnothing, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, A\}$$

ha 8 elementi, ops *avrà* 8 elementi.

Nota: $\{1\}$ e 1 sono due cose diverse. $1 \in A$ è un elemento di A. $\{1\}$ invece è un sottinsieme di A che contiene un solo elemento. Abbiamo $1 \in \{1\} \subset A$. Non si può scrivere né $1 \subset A$ né $\{1\} \in A$.

Nota: anche che $\varnothing$ è un oggetto, un elemento dell'insieme delle parti $P(A)$.

Esercizio: quanti elementi ha $P(\varnothing)$?

Nota: siccome gli insiemi sono definiti con delle proposizioni $P(x)$ non ti sfuggirà che l'unione intersezione e complemento di insiemi corrisponde agli operatori logici *.or.*, *.and.*, *.not.* tra le corrispondenti proposizioni. [In buona sostanza logica booleana e insiemistica sono la stessa cosa.]

2 Seconda settimana

intro

Giorno 6: relazioni e funzioni

Introduciamo 2 concetti molto importanti per dopo.

Dati 2 insiemi A e B, chiamiamo *relazione* da A a B un sottoinsieme $R \subset A \times B$. Diciamo che $a \in A$ è in relazione con $b \in B$ se e solo se $(a, b) \in R$

Esempio: definiamo una relazione su $\mathbb{N}$ (che significa da $\mathbb{N}$ a $\mathbb{N}$) che descrive la divisibilità. Diciamo che $(k, n) \in R \subset \mathbb{N} \times \mathbb{N}$ (che "k divide n" e scriviamo $k|n$) se il numero naturale k divide esattamente n. Ad esempio abbiamo $1|10$, $2|10$, $5|10$, $10|10$, ma non $3|10$. Possiamo quindi pensare alla relazione $|$ come il sottoinsieme

$$I = \{(k, n) \in \mathbb{N} \times \mathbb{N} : \text{ esiste } q \in \mathbb{N} : n = qk\}$$

Ci interessano 3 tipi di relazioni:

1) relazioni di equivalenza su un insieme A

2) relazioni di ordine su un insieme A

3) le funzioni da un insieme A a un insieme B (che può essere uguale a o diverso da A)

Una relazione di equivalenza $\sim$ è una relazione con le seguenti proprietà (liberamente ispirate da $=$)

1) $x \in A : x \sim x$ (ogni elemento di A è in relazione con se stesso)

2) $x, y \in A$: se $x \sim y$ allora anche $y \sim x$ (se x è un relazione con y allora anche y è in relazione con x)

3) $x, y \in A$: se $x \sim y$ e $y \sim z$ allora anche $x \sim z$.

> **Nota:** La relazione di divisibilità gode della proprietà 1 (per ogni $n \in \mathbb{N} : n|n$). Gode pure della proprietà 3) ($k|n|m$ allora $k|m$). Ma non gode della proprietà 2) ($3|6$ na non $6|3$). Quindi non è una relazione di equivalenza.

> **Esercizio:** definiamo la relazione di equivalenza su $\mathbb{N}$. Diciamo che $n =_{(3)} k$ se esistono $q, p \in \mathbb{N}$ e $r \in \{0, 1, 2\}$ tale che $n = 3q + r$ e $k = 3p + r$. Ad esempio $7/3$ ha resto 1, $10/3$ ha resto 1, quindi abbiamo che $7 =_{(3)} 10$. Siccome $12/3$ ha resto 0, non $12 \neq_{(3)} 10$. È facile convincersi che questa relazione d'equivalenza separa $\mathbb{N}$ in tre sottoinsiemi:
>
> $R_0 = \{n \in \mathbb{N} : \text{resto di } n/3 \text{ è } 0\}$, cioè dei numeri che si dividono esattamente per 3.
>
> $R_1 = \{n \in \mathbb{N} : \text{resto di } n/3 \text{ è } 1\}$, cioè dei numeri che hanno resto 1 quando li dividete per 3.
>
> $R_2 = \{n \in \mathbb{N} : \text{resto di } n/3 \text{ è } 2\}$, cioè dei numeri che hanno resto 2 quando li dividete per 3.
>
> Ogni numero naturale sta in uno e solo uno tra R_0, R_1, e R_2. In altre parole, l'unione $R_0 \cup R_1 \cup R_2 = \mathbb{N}$ e $R_0 \cap R_1 = \varnothing$, $R_0 \cap R_2 = \varnothing$, $R_1 \cap R_2 = \varnothing$.

Questi sottoinsiemi R_0, R_1, R_2, si chiamano le classi di equivalenza della relazione $k =_{(3)} n$. Potete rimpiazzare 3 con ogni numero naturale k che definisce k classi di equivalenza a seconda del resto $r = 0, 1, ..., k-1$.

Nota: Questa costruzione è piuttosto generica. Ogni volta che voglio dividere un insieme A in classi di equivalenza, lo fate definendo una relazione di equivalenza in modo da spezzare l'insieme A nelle classi di equivalenza desiderate. Le 3 classi di equivalenza R_0, R_1, R_2, tengono conto dei possibili resti e trascurano il rapporto. Abbiamo che $10 = 3 \cdot 3 + 1$ e $7 = 3 \cdot 2 + 1$, quindi $10 =_{(3)} 7$ perché hanno lo stesso resto anche se il rapporto con 3 è diverso (3 e 2, rispettivamente). Le relazioni di equivalenza sono di preciso un modo di considerare equivalenti elementi diversi che però hanno in comune alcune caratteristiche (il resto), e considerare ininfluenti le altre (il rapporto).

Delle relazioni di ordine ce ne occupiamo dopo, che ce ne sono tipi sottilmente diversi.

Invece definiamo una funzione $f : A \to B$ una relazione tra A e B tale che per ogni $a \in A$ esiste uno e in solo elemento $b \in B$ tale che (a, b) sono in relazione. Se (a, b) sono un relazione scriviamo $b = f(a)$ e diciamo che b è l'immagine di a attraverso la funzione f. Per riassumere tutto ciò, scriviamo una funzione $f : A \to B : a \mapsto f(a)$ per dire pure che la funzione f associa a a l'elemento $f(a) = b$.

Nota: A questo punto probabilmente vi chiedete perché uno deve fare le cose così complicate invece di dire che una funzione è $y = 3x + 1$, tu mi dai un valore x e io uso la funzione per calcolarmi il valore di y. Il problema è che poi uso funzioni in contesti diversi (coi numeri ma pure tra insiemi di spazi, di equazioni, ...). In questo modo, facciamo il lavoro una volta sola anche se serve un po' di sforzo iniziale ad abituarsi useremo molto di più questi concetti che i numeri!

Esempi di funzioni $f : \mathbb{N} \to \mathbb{N}$ considerate la funzione $s : \mathbb{N} \to \mathbb{N} : n \mapsto n + 1$ che ad ogni numero naturale associa il suo successivo. Questo è la funzione che compare negli assiomi di Peano. Solo bisogna sapere fare $n+1$ cioè aver definito la somma in $\mathbb{N}$. Gli assiomi di Peano sono emunciati prima di dire come si fa la somma. Abbiamo definito la somma su $\mathbb{N}$ usando la funzione $s : \mathbb{N} \to \mathbb{N}$ invece che usare la somma per definire s.

Sono anche funzioni $f : \mathbb{N} \to \mathbb{N} : n \mapsto 2n$, $f : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$, mentre non è una funzione $\sqrt{\ } : \mathbb{N} \to \mathbb{N} : n \mapsto \sqrt{n}$. Perché non è una buona funzione?

Nota: Guardate che a questo tipo di domande si risponde facilmente andando a prendere la definizione e capendo perché non funziona. Una funzione per un matematico è esattamente quello che c'è scritto nella definizione. Se un matematico definisce un cane come un quadrupede, allora per lui un gatto è un cane.

Una funzione $f : A \to B$ è detta biettiva se oltre al fatto che ad ogni elemento $a \in A$ corrisponde una e una sola immagine $f(a) \in B$ (se no f non è neanche una funzione) vale pure che per ogni $b \in B$ esiste un solo elemento $a \in A$ tale che $f(a) = b$ (cioè se esiste una e una sola *controimmagine* di b)

Esercizio: $f : \mathbb{N} \to \mathbb{N} : n \mapsto 2n$, $s : \mathbb{N} \to \mathbb{N} : n \mapsto n + 1$, $f : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ non sono biettive. Perché?

Per rispondere dovete trovare un numero naturale b che non è prodotto come immagine da nessun $a \in \mathbb{N}$ oppure che è prodotto come immagine da più di un numero.

Esercizio: definiamo i numeri pari $P = \{n \in \mathbb{N} : \text{ esiste } k \in \mathbb{N} : n = 2k\}$. La mappa $f : \mathbb{N} \to P : n \mapsto 2n$ è una funzione? È biettiva?

Ora abbiamo gli ingredienti per definire la cardinalità degli insiemi e dire cosa significa contare. La prossima volta.

Giorno 7: che stai a contare?

Se ti do una scatola di caramelle e ti chiedo quante caramelle contiene tu che fai?

Tiro a indivinare. Apri la scatola prendi una caramella e conti 1, prendi un'altra caramella e conti 2, ..., prendi la 13ma caramella e conti 13. Non ci sono più caramelle e dici che nella scatola c'erano 13 caramelle.

Ora lasciami fare una domandina. Che hai fatto in tutto ciò se non istituire una funzione biettiva tra le caramelle e il sottoinsieme $I_{13} = \{1, 2, 3, \ldots, 12, 13\} \subset \mathbb{N}$?

Contare *significa* stabilire una funziona bilineare tra un insieme da contare (la scatola di caramelle) e un sottoinsieme finito di $\mathbb{N}$.

Definizione: dati 2 insiemi A e B, diciamo che hanno la stessa *cardinalità* se esiste una funzione biettiva $f : A \to B$.

Avere la stessa cardinalità è una relazione di equivalenza sugli insiemi (e pure sugli insiemi infiniti). Le classi di equivalenza rispetto a questa relazione di equivalenza sono, ad esempio, tutti gli insiemi con 17 elementi. Esiste una classe di equivalenza ogni $n \in \mathbb{N}$, fatta di tutti gli insiemi finiti con n elementi.

Le classi di equivalenza *sono* una rappresentazione dei numeri naturali. Il numero $17 \in \mathbb{N}$ è identificato con tutti gli insiemi finiti con 17 elementi.

Dobbiamo notare 2 cose: primo, il numero è per definizione astratto, non importa se conti mele, pere, colori o unicorni. Secondo, la definizione di avere la stessa cardinalità si estende per costruzione anche agli insiemi infiniti.

Gli insiemi che hanno la stessa cadinalità di $\mathbb{N}$ sono detti *numerabili*. Il numero cardinale corrispondente si chiama $\aleph_0$ (letto *aleph-zero*). Ovviamente, un insieme numerabile è in corrispondenza biunivoca con $\mathbb{N}$, quindi $\aleph_0 \notin \mathbb{N}$ perché non può essere in corrispondenza con un sottoinsieme finito di $\mathbb{N}$. Sono i sottoinsiemi *finiti* di $\mathbb{N}$ che definiscono gli elementi di $\mathbb{N}$.

Esercizio: sono più i numeri naturali o i numeri pari?

[Siate certi di considerare la mappa $f : \mathbb{N} \to 2\mathbb{N} : n \mapsto 2n$. (È biettiva? Quindi?)]

Esercizio: Se consideriamo $A = \mathbb{N} \cup \{a\}$. È numerabile? Chi ha maggiore cardinalità, $\mathbb{N}$ o A?

Nota: notate che gli assiomi di Peano definiscono i numerali naturali, dicono che 0 è il primo, che esiste sempre il successivo e che il successivo e sempre un numero nuovo, che continuano per sempre a comparire numeri nuovi e che tutti i naturali sono ottenuti come il successivo di un numero naturale. Questo definisce già un (buon) ordine di $\mathbb{N}$.

Poi definiamo la cardinalità dei numeri naturali che si estende agli insiemi numerabili.

Ora prima di definire per bene il buon ordine andiamo in vacanza in montagna all'Hilbert hotel.

Giorno 8: l'hotel di Hilbert (numerabile)

L'hotel Hilbert è un albergo in un'amena località montana non meglio precisata che ha $\aleph_0$ stanze. Un giorno l'albergo risulta completo al momento della cena.

Nel mezzo della notte tempestosa un nuovo cliente bussa alla porta cercando una stanza per passare la notte al sicuro. In un primo momento il portiere risponde che sono al completo poi, mosso a compassione per il nuovo venuto, pensandoci un po' ha un'idea e trasmette in tutte le camere il seguente messaggio:

Stiamo affrontando un'emergenza, chiediamo ad ogni cliente a seguire le seguenti istruzioni: Se state occupando la nella stanza k, vi preghiamo di prendere la vostra roba e trasferirvi nella stanza $k+1$. In cambio, riceverete uno sconto del 10% sul conto.

Dopo di ciò, la stanza 0 è rimasta vuota visto che nessuno ci si è trasferito a fronte del suo occupante che ora dorme seneramente nella stanza 1. Il nuovo cliente quindi viene sistemato della stanza 0, non prima di essersi offerta a pagare di tasca sua il mancato incasso dovuto allo sconto. A questo proposito, il portiere ha gentilmente declinato l'offerta argomentando che malgrado le tariffe molto basse dell'albergo e lo sconto, l'incasso totale non sarebbe diminuto finché l'albergo fosse risultato completo o, per quel che conta, anche avesse avuto un numero finito di stanze vuote, o comunque con un numero numerabile di stanze occupate (ad esempio solo quelle pari).

Più tardi nella notte, un'altra infinita comitiva si presenta alla porta chiedendo una stanza per evitare la tempesta. A quel punto il portiere trasmette il seguente messaggio:

Mi spiace disturbarvi ancora ma stiamo affrontando una nuova emergenza. Vi chiediamo gentilmente di alzarvi, prendere le vostre cose, e se state nella stanza k trasferitevi nella stanza $2k+1$. In cambio, riceverete un ulteriore sconto del 10%.

Ciò ha reso disponibili tutte le stanze pari che così hanno potuto essere destinate alla comitiva giunta nella notte. Sembra che l'hotel di Hilbert non possa esaurire le stanze, [Ma può, come vedremo.]

Se ci pensate, tutta la storiella dice che la cosa particolare dell'albergo con $\aleph_0$ stanze è che le posso numerare coi numeri naturali $\mathbb{N}$. Tuttavia le sole stanze pari, quelle dispari da sole, e tutte le stanze hanno la stessa cardinalità. Non ci credete?

Allora controllate che la mappa $f : \mathbb{N} \to P : n \mapsto 2n$, dove

$$P = \{0, 2, 4, \dots, 2k, \dots\}$$

è biettiva, così come la mappa $g : \mathbb{N} \to D : n \mapsto 2n + 1$, dove

$$D = \{1, 3, 5, \dots, 2k + 1, \dots\}$$

Ok se ci pensate, magari dite: *e grazie dai sono entrambe infinite quindi sono tanti quanti.* Se è così ripetete con me: *la natura è malevola e non perde occasione di rendere le cose semplici meravigliosamente complicate.* Avete in parte ragione ma vedremo che ci sono infiniti e infiniti (se no perché la cardinalità di $\mathbb{N}$ l'avrei chiamata $\aleph_0$? Perché mi avanzava uno 0 o perché alla fine mi servirà una cosa più grande $\aleph_1$, poi una più grande $\aleph_2$, ...?).

Ma ora non possiamo occuparcene, prima dobbiamo definire i numeri interi, quelli razionali, quelli reali e vedremo che la cardinailtà dei numeri reali è più grande di quella di $\mathbb{N}$, cioè che i numeri reali sono una infinità non numerabile.

E vi sembra possibile quella sia la fine della storia? No, eh, vedete che la natura è malevola?

Prossime tappe: relazioni di ordine e buon ordine, così possiamo definire una rappresentazione (un modello) per i numeri ordinali. Poi ci dobbiamo occupare di definire i numeri interi, i razionali e i reali, estendendo le operazioni e definendone altre (ad esempio: la sottrazione, la divisione, le radici quadrate). A quel punto siamo arrivati ai tempi di Pitagora (che, non lui, diciamo la sua scuola, ha scoperto che $\sqrt{2}$ non è razionale).

Per questa strada estenderemo 2 volte l'hotel di Hilbert. A quel punto il finale di Interstellar vi sembrerà banalotto.

Giorno 9: relazioni d'ordine

Così come abbiamo visto che le relazioni di equivalenza catturano la nostra intuizione di uguaglianza sotto certi aspetti (2 persone diverse possono essere diverse ma uguali sotto la relazione d'equivalenza "sono alte uguali" oppure "pesano uguale" oppure "hanno lo stesso sesso"), le *relazioni d'ordine* catturano la

nostra intuizione di ordine in un insieme. A noi interessano principalmente gli ordini totali e i buoni ordini, ma ci sono diverse gradazioni di grigio e non conviene puntare dritto all'obiettivo, conviene fare lo sforzo di catalogare i diversi tipi di relazione d'ordine.

Definizione: un *preordine* su un insieme A è una relazione $\leq$ che soddisfa la proprietà per ogni $x, y, z \in A$

$$x \leq x \qquad \text{(riflessiva)}$$
$$\text{se } x \leq y \text{ e } y \leq z \text{ allora } x \leq z \qquad \text{(transitiva)}$$

Nota: le relazioni di equivalenza soddisfano la proprietà riflessiva e la proprietà transitiva, quindi sono preordini. Non è vero il viceversa: non tutti i preordini sono relazioni di equivalenza perché non è richiesta la proprietà simmetrica.

Quindi la strada giusta dovrebbe essere definire i preordini e poi le relazioni di equivalenza come particolare preordini che hanno anche la proprietà simmetrica. Siccome dobbiamo tenere a mente un sacco di proprietà e abbiamo un numero finito di neuroni dovremmo abituarci a riorganizzare continuamente la nostra conoscenza in questo modo. Questa è una cosa che ci insegna la matematica anche se non ci interessa essere matematici: la conoscenza *deve* essere continuamente coccolata e riorganizzata mentre cresce, se no ci bastava Wikipedia.

Questa è, secondo me, *una* ragione per provare ad insegnare matematica per 13 anni a tutta la popolazione anche se evidentemente con scarsissimi risultati. Tra parentesi questo secondo me indica che lo scopo della scuola pubblica, quella dell'obbligo, non è insegnare cose ai bambini. I bambini sono costretti ad andare a scuola, come i carcerati sono costretti a stare in carcere. Non puoi chiedere a un carcerato di stare 13 anni in carcere e pure imparare a dare il bianco alla cella, al massimo puoi *consentirgli* di dare il bianco alla cella. La scuola dell'obbligo ha il compito di esporre tutta la popolazione al maggior numero di cose possibile e *consentire* loro di sviluppare i loro interessi in qualcuna di queste materie. Possibilmente di raggiungere un livello civile di navigazione in quelle discipline che non interessano.

Definizione: un *ordine parziale* è un preordine con la proprietà antisimmetrica

$$\text{se } x \leq y \text{ e } y \leq x \text{ allora } x = y$$

Esercizio: Dato un insieme A e l'insieme $P(A)$ delle sue parti, diciamo che un sottoinsieme $S_1 \in P(A)$ di A è *incluso* in un sottoinsieme $S_2 \in P(A)$, e scriviamo $S_1 \subset S_2$ se e solo se S_1 è anche un sottoinsieme di S_2.

L'inclusione è un ordine parziale di $P(A)$.

Ogni sottoinsieme è contenuto in se stesso (riflessiva). In più se $S_1 \subset S_2$ e $S_2 \subset S_3$ allora $S_1 \subset S_3$ (transitiva, quindi è un preordine).

Infine se $S_1 \subset S_2$ significa che tutti gli elementi di S_1 sono anche elementi di S_2, e anche se $S_2 \subset S_1$ significa che tutti gli elementi di S_2 sono anche elementi di S_1, allora S_1 e S_2 hanno gli stessi elementi, quindi sono lo stesso sottoinsieme (antisimmetrica).

Quindi l'inclusione è un ordine parziale.

Definizione: un *ordine totale* è un ordine parziale che in più ha la proprietà di comparazione, dati $x, y \in A$ si ha che $x \leq y$ oppure $y \leq x$.

Nota: L'inclusione è una ordine parziale che non è totale (due sottoinsiemi possono essere tali da non essere inclusi né $S_1 \subset S_2$ né $S_2 \subset S_1$).

I numeri naturali sono ordinati totalmente dalla relazione $n_1 \leq n_1$ che è un ordine totale in $\mathbb{N}$.

Per la cronaca dobbiamo definire tutto, quindi pure cosa significa $n_1 \leq n_2$. Se definiamo i numeri naturali con gli assiomi di Peano, diciamo che $n_1 \leq n_2$ dicendo che valgono le seguenti proprietà

$$n \leq n \qquad\qquad n \leq s(n)$$

Se vogliamo dimostrare che $3 \leq 5$ non dobbiamo fare altro che notare che $5 = s(s(3))$, quindi

$$3 \leq s(3) \leq s(s(3)) = 5$$

quindi $3 \leq 5$ per la proprietà transitiva.

Un *buon ordine* di A è un ordine totale tale che ogni sottoinsieme S, non-vuoto di A ha un elemento minimo, cioè più piccolo (rispetto all'ordine totale che stiamo considerando su A) di tutti gli altri elementi di S. L'insieme dei numeri naturali $\mathbb{N}$ con l'ordine $\leq$ è ben ordinato. Prendete un qualunque sottoinsieme non vuoto di $\mathbb{N}$ in esso esiste sempre un minimo.

Nota: Notate che non è vero che esiste sempre un massimo (abbiamo già detto che in $\mathbb{N}$, che è un sottoinsieme non-vuoto di $\mathbb{N}$, non esiste un numero più grande di tutti gli altri).

Se vi gira la testa, non vi preoccupate è come per chi vive al mare andare sulle Ande, è scarsità di ossigeno dopo un paio di giorni (o masticando foglie di coca) passa. Sì, stiamo dicendo che *ogni* sottoinsieme non-vuoto di $\mathbb{N}$ ha un minimo anche se i sottoinsiemi di $\mathbb{N}$ sono in numero infinito, anche se alcuni sottoinsieme di $\mathbb{N}$ sono infiniti. Ok, dovremmo dimostrarlo ma per quello hanno inventato le dimostrazioni, perché consentono di dimostrare infinite cose (nessun pari maggiore di 3 è primo, e grazie si divide per 2 oltre che per 1 e per n).

Ok non abbiamo ancora detto cosa è un primo, ma lo sapete. Ma questo vi conferma che la paranoia principale del matematici è non fare ragionamenti circolari. Non assumere cose senza dimostrazione e definizione che alla fine renda sbagliato il ragionamento. Per questo, per fare le cose per bene bisogna andare piano, dare gli assiomi dare le definizioni, dimostrare i teoremi e poi magari dare degli esempi. Non si può fare come stiamo facendo qui, dare gli esempi prima usando cose che non sono state definite. È pericoloso.

Poi quindi capite perché i matematici bestemmiano quando gli si dice *eh ma la matematica è astratta, non puoi parlare come mangi e fare un esempio di quello che mi stai dicendo così capisco?*

La risposta dovrebbe essere: *no ora non posso darti degli esempi, prima dimostriamo i teoremi poi tra 3 giorni ti faccio un esempio! Non me ne frega nulla della tua intuizione, se potevi intuire cosa era uno spazio di Hilbert, significa che stai pensando a un esempio con certe proprietà, è pericoloso avere in mente un esempio perché facilita aggiungere proprietà che magari il tuo esempio ha ma non tutti gli spazi di Hilbert e quando dimostri i teoremi è pericoloso avere delle proprietà in mente perché si finisce per sparare stronzate.*

A proposito, sui principia matematica di Russell il teorema $1 + 1 = 2$ è marcato col numero 10mila e qualcosa. Diecimila e rotti teoremi prima di sapere che 1+1=2. La matematica è lenta.

Giorno 10: odinali e albergo MultiHilbert

Dati due insiemi $(A, \leq)$ e $(B \leq)$ bene ordinati, diciamo che hanno la stessa *lunghezza* se esiste una mappa biettiva $f : A \to B$ che preserva l'ordine, cioè

che se $a_1 \leq a_2$ allora $f(a_1) \leq f(a_2)$. Questa è una relazione di equivalenza e possiamo considerare classi di equivalenza di insiemi bene ordinati che hanno la stessa liunghezza.

Ognuna di queste classi è un *ordinale*. L'ordinale degli insiemi di 3 elementi coincide con gli insiemi di cardinalità 3, quindi l'ordinale 3 e il cardinale 3 sono rappresentati dalla stessa classe di insiemi pur avendo definizione diversa.

L'insieme dei numeri naturali $\mathbb{N}$ è bene ordinato quindi determina un ordinale ω_0 infinito, che ha cadinalità $\aleph_0$. Se consideriamo l'insieme $\mathbb{N}_{+2} = \mathbb{N} \cup \{a, b\}$ con il buon ordine dato da $n \in \mathbb{N} : n \leq a \leq b$, allora $\mathbb{N}_{+2}$ definisce un altro ordinale $\omega_0 + 2$ (esistono mappe biettive tra $\mathbb{N}$ e $\mathbb{N}_{+2}$, ma non mappe biettive che preservino l'ordine). Tuttavia la cardinalità di $\mathbb{N}$ e $\mathbb{N}_{+2}$ è la stessa ed è sempre $\aleph_0$. Quindi ci sono più ordinali diversi di cardinali diversi.

Un ordinale è detto *ordinale limite* se non ha un *precedente* ad esempio ω_0 è un ordinale limite, mentre $\omega_0 + 1$ ha ω_0 come precedente perché $s(\omega_0) = \omega_0 + 1$.

Gli ordinali soddisfano gli assiomi di Peano. In particolare, se abbiamo un insieme che è ordinale $K = \{1, 2, \ldots, k\} \subset \mathbb{N}$ possiamo definire il successivo $K + 1 = \{1, 2, \ldots, k, k + 1\} \subset \mathbb{N}$

A questo punto: plot twist! Esiste una cosa che si chiama *assioma della scelta*:

> **Nota:** Dato un insieme X e ogni famiglia $A_\alpha \subset X$ di sottoinsiemi etichettati da $\alpha \in I$, esiste sempre una funzione $\sigma : I \to X : \alpha \mapsto \sigma(\alpha) \in A_\alpha$ che sceglie un elemento $\sigma(\alpha)$ in ogni sottoinsieme A_α della famiglia.
>
> Occhio che la famiglia può essere finita, infinita (numerabile o non numerabile). Ad esempio, se prendiamo $I = \mathbb{R}$ e $A_x = \{(x, y) : y \in \mathbb{R}, x \in I\} \subset \mathbb{R} \times \mathbb{R}$ allora esiste una funzione $\sigma : \mathbb{R} \to \mathbb{R} : x \mapsto \sigma(x)$. Vi sembra ovvio? Beh da un lato questo è il motivo per cui è un assioma, dall'altro è perché non avete idea di quanto può essere infinito un insieme infinito. E comunque per scegliere la funzione σ ci vorrebbe infinito tempo visto che devo scegliere infiniti elementi $\sigma(\alpha) \in A_\alpha$ e in generale ogni A_α può essere fatto a modo suo.

Con l'assioma della scelta si può dimostrare che su ogni insieme esiste un buon ordine. Questo significa che potete ordinare $\mathbb{Q}$ (o $\mathbb{R}$) in modo che ogni sottoinsieme abbia un minimo! E se ci pensate un attimo non avete la più pallida idea di come questo ordinamento sia fatto.

Ora se ogni insieme X ha (almeno) un buon ordinamento, significa che ogni coppia $(X, \leq)$ (ogni insieme ben ordinato) definisce un ordinale. Quindi ad esempio pure $\mathbb{R}$ definisce un ordinale.

Teorema: la cardinalità di $[0, 1)$ è più grande della cardinalità di $\mathbb{N}$.

> **Nota:** Se $I = [0, 1)$ avesse la cardinalità di $\mathbb{N}$, sarebbe numerabile, cioè esisterebbe una mappa biettiva $\lambda : \mathbb{N} \to I$, il che significa che potrei elencare gli elementi di I facendo una lista $(\lambda(0), \lambda(1), \lambda(2), \ldots)$. Questa lista sarebbe una

cosa tipo

$$0 \mapsto 0.277394776559\ldots$$
$$1 \mapsto 0.000473656649\ldots$$
$$2 \mapsto 0.9983664756349\ldots$$
$$3 \mapsto 0.1227365549000\ldots$$
$$\ldots$$

ma si può sempre costruire un numero $x \in I$ che non sta nella lista (quindi la funzione λ non può essere biettiva). Basta prendere $x = 0.d_1d_2d_3d_4\ldots$ dove d_1 è una cifra diversa dalla prima cifra di $\lambda(0)$, dove d_2 è una cifra diversa dalla seconda cifra di $\lambda(1)$, dove d_3 è una cifra diversa dalla terza cifra di $\lambda(2)$, e avanti così.

Il numero così costruito è diverso da tutti i numeri nella lista per almeno una cifra.

Ok, ci sono delle cosucce da sistemare ma in sostanza questo si chiama dimostrazione *diagonale di Cantor*. I punti di I sono infiniti, ma sono di più dei punti di $\mathbb{N}$. Tra l'altro non si può dimostrare né che ci siano, né che non ci siano infiniti più grandi di $\mathbb{N}$ ma più piccoli di $\mathbb{R}$. Pure questo è un assioma della matematica. Usualmente si assume che non ce ne siano e si definisce $\aleph_1$ la cadinalità di $\mathbb{R}$. Questo assioma si chiama *ipotesi del continuo*.

Tra l'altro poi le funzioni $f : \mathbb{R} \to \mathbb{R}$ sono infinite di una cadinalità più grande e si assume siano $\aleph_2$ e evanti così.

Quindi voi potete contare

$$0\,1\,2\,3\ldots\,\omega_0\,\omega_0+1\,\omega_0+2\,\omega_0+3\ldots\,2\omega_0\ldots\,3\omega_0\ldots\,4\omega_0\ldots\,(\omega_0)^2\ldots\,(\omega_0)^3\ldots\ldots$$

Ma siccome pure $\mathbb{R}$ definisce un ordinale prima o poi incontro un ordinale che non è più numerabile (che si chiama il *primo ordinale non numerabile*, che scriviamo ω_1, perché gli ordinali non numerabili sono un sottoinsieme dei numerabili e quindi devono avere un minimo). Poi si continua a contare fino ad arrivare a $\mathbb{R}$ (e tutti gli ordinali da ω_0 a $\mathbb{R}$ hanno necessariamnete cardinalità $\aleph_1$ per l'ipotesi del continuo.)

Mal di testa?

Ora possiamo rifare la storiella dell'albergo di MultiHilbert. Quello di prima è solo il piano terra che ha ω_0 camere, poi c'è il primo piano con le camere da $\omega_0 + 1$ a $2\omega_0$. E via così per tutti i piani numerabili.

Questo ha sempre $\aleph_0$ stanze tante quante le camere dell'albergo originale.

Poi abbiamo la dependance $\aleph_1$ che comincia con la stanza ω_1 e pure lei ha infiniti piani infiniti.

Poi la dependance ω_2 (il primo ordinale di cardinalità $\aleph_2$) e avanti così all'infinito.

Nota: quando Cantor ha scritto sta roba (intorno al 1850), il suo maestro Kronecher, ha detto che era pazzo. Questi si chiamano numeri transfiniti di Cantor. Oggi non c'è dubbio che Cantor avesse ragione. È tutto ben definito, tutto dimostrabile, tutto certificato.

Detto questo, Cantor aveva manie di persecuzione, forse era bipolare e passava 6 mesi fuori e sei mesi dentro il manicomio.

3 Terza settimana

Ora torniamo ai numeri naturali finiti $\mathbb{N}$. La situazione è abbastanza tipica della matematica. Abbiamo una formulazione assiomatica che fissa solo pochi fatti (esiste $0 \in \mathbb{N}$, ogni numero $n \in \mathbb{N}$ ha un successivo $s(n) \in \mathbb{N}$, procedendo di successivo in successivo si vedono sempre numeri nuovi, tutti i numeri naturali si raggiungono da 0 procedendo verso il successivo). Da questo solo possiamo dimostrare tutto quello che sappiamo sui numeri naturali e definire le operazioni (in questo caso somma e prodotto).

Poi abbiamo un modello basato su insiemi dei numeri naturali (i numeri naturali corrispondono a classi di insiemi con lo stesso numero di elementi, cioè la stessa cardinalità). Più o meno possiamo definire la somma come la cardinalità dell'unione (disgiunta) e la moltiplicazione come la cardinalità del prodotto cartesiano. Possiamo ordinare i numeri naturali.

Forse vale la pena di menzionare che in quasi tutte le teorie degli insiemi si assume che esista l'insieme vuoto $\varnothing$. E l'insieme vuoto è tutto quello che serve. Esso rappresenta il numero $0 = \varnothing \in \mathbb{N}$. Definiamo il successivo di $n \in \mathbb{N}$, l'insieme $s(n) = n \cup \{n\}$. Quindi $0 = \varnothing$, $1 = s(0) = \{\varnothing\} = \{0\}$, $2 = s(1) = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$, $3 = s(2) = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\}$, ...

Questo fa il servizio che deve fare, perché $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, ... sono tutti insiemi diversi, (tanto è vero che hanno cardinalità diversa)

I numeri naturali sono fatti per contare cose che non possono essere spezzate: le uova, i coniglietti, i compagni di scuola, le caramelle. Per questa ragione è demenziale proporre una immagine come la retta dei numeri che ha infiniti punti tra 2 e 3 che uno deve fare finta di non vedere. Tanto più che esiste una immagine mentale che è fatta esattamente di cose che non possono essere divise: una scala. Esiste un mezzo gradino? Non mi pare. Quindi i numeri naturali sono una scala infinita che parte da terra (0), e da ogni gradino (n) potete passare al prossimo gradino ($s(n) = n + 1$). Niente Escher, salendo non si passa sui gradini dove eravate già stati.

Dai tempi dei Sumeri, i numeri sono astratti: 2 galline e 2 caramelle sono lo stesso 2. Hanno inventato i numeri proprio per prescindere da quello che si conta. Non importa cosa c'è nell'insieme conta solo la cardinalità.

Ora concentriamoci sulle operazioni definite in $\mathbb{N}$.

Giorno 11: somma

Abbiamo definito la somma a seguito degli assiomi di Peano. Quando pensiamo ai numeri naturali come insiemi dati 2 insiemi finiti A_n e A_k di cardinalità n e

k definiamo l'unione disgiunta

$$A_n \coprod A_k = (\{1\} \times A_n) \cup (\{2\} \times A_k)$$

Un elemento dell'unione disgiunta è o nella forma $(1, a)$ con $a \in A_n$ oppure $(2, b)$ con $b \in A_k$. In questo modo se $a \in A_n \cap A_k$ esistono 2 elementi $(1, a)$ e $(2, a)$ nell'unione disgiunta.

> **Nota:** Ricordate che un insieme non può contenere 2 volte lo stesso elemento quindi se vogliamo 2 copie dobbiamo truccarle perché non siano lo stesso elemento.

La somma $n + k$ è il numero che rappresenta la cardinalità di $A_n \coprod A_k$.

Siccome tra $A_n \coprod A_k$ e $A_k \coprod A_n$ esiste una mappa biettiva ($i : (1, a) \mapsto (2, a)$ e $i : (2, b) \mapsto (1, b)$), cioè hanno la stessa cardnalità, segue che $n + k = k + n$, cioè la proprietà commutativa.

Lo stesso vale per $A \coprod (B \coprod C) \simeq (A \coprod B) \coprod C$ che corrisponde alla mappa biettiva $i : (a, (b, c)) \mapsto ((a, b), c)$ che mostra la proprietà associativa:

$$n + (k + h) = (n + k) + h$$

Siccome $\varnothing \coprod A \simeq \{2\} \times A \simeq A$, si ha che $0 + n = n + 0 = a$, cioè 0 è elemento neutro per la somma.

Quindi abbiamo una operazione *somma* che prende 2 numeri naturali $n, m \in \mathbb{N}$ e gli associa un nuovo numero $n + m \in \mathbb{N}$. La somma si può fare sempre qualunque siano i numeri da cui si parte e i matematici amano le funzioni che non possono tornare errore (come sanno gli informatici che hanno usato qualche linguaggio funzionale). La somma alla fine ha solo queste proprietà:

ammette elemento neutro 0

è associativa

è commutativa.

La sottrazione ha un ruolo ancillare perché non sempre si può fare ($5 - 8 \notin \mathbb{N}$). È importante cominciare a saper calcolare le sottrazioni ma in $\mathbb{N}$ hanno poco ruolo, sarebbe meglio introdurle dopo in $\mathbb{Z}$. Ma quando scriviamo $n - m = c \in \mathbb{N}$ stiamo cercando $c \in \mathbb{N}$ tale che $m + c = n$.

Sia la somma che la sottrazione possono facilmente essere calcolati in $\mathbb{N}$, se ci avvaliamo della not6azione posizionale. Ogni numero si scrive come sequenza di cifre e la posizione della cifra nella sequenza denota unità, decine, centinaia, migliaia, ... Ad esempio 5023 significa che abbiamo 3 unità, 2 decine 0 centinaia e 5 migliaia. L'algoritmo per la somma è basato nel prendere 2 cifre, commarle e romperle in decine e unità. Se prendo 2 e 3 ottengo 5 unità e 0 decine. Se prendo 9 e 3 ottengo 2 unità e 1 decina. Se prendo 9 e 9 ottengo 8 unità e 1 decina.

Se devo sommare 5263 + 2669, parto dalle cifre delle unità (3 e 9, le combino e ottengo 2 unità e 1 decina, annoto 2 per le unità nel risultato e riporto 1 decina).

Poi passo alle decine (6 e 6, le combino e attengo 2 unità e 1 decina, più ilriporto precedente fa 2 unità e 1 decina). Annoto 3 nelle decine e riporto 1centinaia.

Poi passo alle centinaia (2 e 6, 8 unità (+ 1 riporto 9) e 0 decine) segno 9 centinaia e non riporto migliaia.

Poi passo alle migliaia (5 e 2, 7 unità e 0 decine) segno 7 migliaia.

Risultato 7932.

Bisogna solo imparare le somme delle cifre (le tabelline per la somma) e non dimenticarsi dei riporti. Per il resto l'algoritmo è quello che fate per sommare i numeri sul pallottoliere che infatti è uno strumento per simulare la notazione posizionale.

Altra storia per le proprietà associativa e commutative che invece bisogna *dimostrare*. Non basta dire che 2+3=3+2 come non basta dire che 2+2=2*2 per dimostrare che $n+n=n*n$ o che $16/64=1/4$ per dimostrare che $37/74=3/4$

Per la sottrazione, prima realizziamo che se vogliamo fare $n-m$ deve essere $n \geq m$ poi se questo è vero procediamo al contrario della somma, se serve prestando una decina.

5263 - 2669 = 2594

e si verifica che infatti 2669 + 2594 = 5263.

Bon così, assicuratevi solo di convincervi che potete sempre sommare 2 numeri naturali e togliere un naturale k più piccolo a qualunque naturale $n \geq k$. Lo potete fare in base 10, in base 3, in base 97. Più la base è grossa più sono grosse le tabelline da ricordare, più sono piccole e più sono i riporti (o i prestiti).

Tutto l'algoritmo è solo completa la decina. Se dovete sommare 5 numeri potete ordinarli in modo da semplificare il completamento delle decine (3+5+2+7+5+8= 3+7+2+8+5+5=30).

Un'ultima cosa, notate che possiamo scrivere $3+5+7$ solo perché sappiamo che $(3+5)+7=3+(5+7)$. Se la somma non fosse associativa siccome abbiamo definito solo la somma di 2 numeri, dovremmo specificare le parentesi per dire in quale ordine ci aspettiamo di fare le operazioni. Siccome la somme è associativa e commutativa possiamo sottintendere le paretesi e l'ordine degli addendi che tanto il risultato non cambia. Quindi $3+5+7=(3+7)+5=15$.

Come sempre le proprietà possono essere usate pure al contrario: $7+5=(5+2)+5=(5+5)+2=12$ con un po' di taglia e cuci e completa la decina.

Giorno 12: prodotto

Pure il prodotto è definito usando gli assiomi di Peano. Ma quando pensiamo ai numeri come insiemi possiamo definire il prodotto come la cardinalità del prodotto cartesiamo.

$$2*3 = \text{Card}(\{0,1\}\times\{0,1,2\}) = \text{Card}(\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}) = 6$$

Anche se $\{0,1\} \times \{0,1,2\}$ e $\{0,1,2\} \times \{0,1\}$ sono insiemi diversi, la loro cardinalità è la stessa (sotto la mappa biettiva $(a,b) \mapsto (b,a)$). Quindi il prodotto è commutativo

Stessa cosa per $A \times (B \times C)$ e $(A, \times B) \times C$, il primo contiene roba tipo $(a,(b,c))$ il secondo roba tipo $((a,b),c)$. Ma possiamo definire una mappa biettiva $(a,(b,c)) \mapsto ((a,b),c)$ che dimostra che $\text{Card}(A\times(B\times C)) = \text{Card}((A,\times B)\times C)$ e quindi la proprietà associativa del prodotto $(ab)c = a(bc)$.

Poi se prendiamo $1 = \{0\}$, quando facciamo

$$1 * 3 = \text{Card}(\{0\} \times \{0,1,2\}) = \text{Card}(\{(0,0),(0,1),(0,2)\})$$

Di nuovo, $\{0\}\times A$ e A sono insiemi diversi ma hanno la stessa cardinalità, quindi $1 * n = n * 1 = n$. Quindi 1 è elemento neutro per il prodotto.

> **Esercizio:** dimostrate che $0 * n = 0$, per qualunque $n \in \mathbb{N}$.
> Suggerimento: scrivete il prodotto cartesiano $\varnothing \times A$

In più avete la proprietà distributiva $(a+b)c = ac + bc$.

> **Nota:** che si dimostra trovando una mappa biettiva tra $(A \coprod B) \times C$ e $(A \times C) \coprod (B \times C)$...

Fine della storia sulle operazioni definite in $\mathbb{N}$. O quasi. Il punto è che da qui in avanti la rappresentazione di numeri e operazioni in termini di insiemi non ci serve più possiamo astrarre e procedere solo usando le proprietà delle operazioni.

Ad esempio, dalla proprietà distributiva, mettiamo $a = 1 = b$ e otteniamo $2n = n+n$ che è la definizione che si dà alle elementari. Mettiamo $a = 1$ e $b = 2$ e otteniamo $3n = n + n + n$ e avanti così.

Un altro giochino carino è il seguente teorema: l'elemento neutro 0 della somma è unico.

> **Nota:** Supponiamo che esista in altro elemento neutro a. Se scriviamo $a + 0$, siccome 0 'è elemento neutro abbiamo $a + 0 = a$. Ma siccome pure a è elemento neutro abbiamo anche $a + 0 = 0$. Quindi abbiamo $a = a + 0 = 0$, cioè $a = 0$, cioè ogni "altro" elemento neutro coincide con quello vecchio.

Potremmo pure dare una dimostrazione basata sugli insiemi dello stesso fatto, ma questa dimostrazione è più intelligente. Perché?

Perché, siccome usa solo la proprietà dell'elemento neutro $a + 0 = 0 + a = a$ e questa proprietà è condivisa da tutti gli elementi neutri (1 del prodotto, la funzione $f(x) = 0$ rispetto alla somma delle funzioni $f : A \to \mathbb{R}$) la stessa dimostrazione dimostra che 1 è l'unico elemento neutro del prodotto, e l'unicità dell'elemento neutro del gruppo delle rotazioni, dello 0 in ogni spazio vettoriale, di $0 + i0 \in \mathbb{C}$.

Algoritmo per il prodotto

Alle elementari abbiamo fatto pure l'algoritmo per eseguire il prodotto in $\mathbb{N}$. Se dobbiamo fare $1238 * 326$ in pratica usiamo questo trucco (di nuovo basato sulla notazione posizionale)

$$1238 * 326 = 1238(3 * 100 + 2 * 10 + 6) = 1238 * 3 * 100 + 1238 * 2 * 10 + 1238 * 6$$

Quindi se sappiamo moltiplicare un numero naturale per una cifra (e sappiamo che moltiplicare per 100 significa aggiungere 00 alla coda si un numero) sappiamo calcolarlo.

Per la moltiplicazione di un numero naturale per una cifra usiamo lo stesso trucco

$$\begin{aligned} 1238 * 3 =& 1 * 3 * 1000 + 2 * 3 * 100 + 3 * 3 * 10 + 8 * 3 = \\ =& 3 * 1000 + 6 * 100 + 9 * 10 + 24 = 3690 + 24 = 3714 \end{aligned}$$

In sostanza l'algoritmo che utilizziamo alle elementari è solo per minimizzare le cose che bisogna ricordare per tanto tempo durante l'esecuzione (vi dice dove scrivere i riporti mentre calcolate le somme parziali). A parte questo state facendo quello che fate qui sopra.

Di nuovo, può essere laborioso ma potete moltiplicare qualunque coppia di numeri naturali, basta che sappiate moltiplicare le cifre (tabelline) e fare le somme.

Divisione e resto

Come per la sottrazione la divisione in $\mathbb{N}$ ha un ruolo ancillare. Due numeri naturali $n, k \in \mathbb{N}$ si possono dividere solo se n è multiplo di k, cioè se esiste in $q \in \mathbb{N}$ tale che $n = qk$ e allora k divide n (abbiamo convenuto di scrivere $k|n$) e scriviamo $n : k = q$ (con resto $r = 0$).

In pratica se scriviamo che $n : k = q$ stiamo solo dicendo che $q \in \mathbb{N}$ è quel numero che moltiplicato per k dà n, cioè che $q * k = n$. In altre parole la divisione esatta è inversa al prodotto.

Possiamo essere più liberali e mostrare che per ogni coppia di numeri naturali $n, k \in \mathbb{N}$, esistono (e sono unicamente determinati) 2 numeri $q \in \mathbb{N}$ e $r \in \{0, 1, \ldots, k - 1\}$ tale che $n = qk + r$. Lo chiamiamo il *teorema dello Zecchino*

d'oro (*44 gatti in fila per 6 col resto di 2*) e q lo chiamiamo il quoziente di $n : k$, r lo chiamiamo il resto di $n : k$ che indichiamo anche con $r = n \mod k$ (che leggiamo n modulo k).

> **Nota:** L'operazione che associa a (n, k) i numeri (q, r) è ben definita. Se chiedete a me i microprocessori dovrebbero implementare questa, non i floating points.

Algoritmo di divisione

Se ho 2 numeri n e k e voglio dividere $n : k$ comincio a cercare il più grande q_1 tale che $q_1 * k \leq n$. Quindi definisco $n_1 = n - q_1 * k$. Se $n_1 \in \{0, 1, \ldots, k-1\}$ abbiamo finito se no cerchiamo il più grande q_2 tale che $q_2 * k \leq n_1$. Quindi definiamo $n_2 = n_1 - q_2 * k$ e avanti così finché $r = n_l = n_{l-1} - q_l * k \in \{0, 1, \ldots, k-1\}$ che è quindi il resto. Abbiamo che

$$\begin{aligned} n =& q_1 * k + n_1 = q_1 * k + q_2 * k + n_2 = \cdots = \\ =& q_1 * k + q_2 * k + \cdots + q_l * k + r = (q_1 + q_2 + \cdots + q_l) * k + r = q * k + r \end{aligned}$$

quindi il quoziente è $q = q_1 + q_2 + \cdots + q_l$ e il resto è r.

Come per la sottrazione l'algoritmo delle elementari è solo un modo per organizzare il calcolo senza dover ricordare (o capire) troppe cose.

Divisibilità e numeri primi

Ora che sappiamo cosa significa dividere esattamente $k|n$ (k divide n) possiamo notare che certi numeri $2, 3, 5, 7, \ldots$ hanno esattamente 2 divisori (1 e loro stessi). Li chiamiamo *numeri primi*. Un'altra definizione equivalente è che se un numero primo p divide un prodotto ab, siccome non potete spezzare p in un prodotto, allora p o divide a o divide b. Quindi possiamo dire che $p \neq 1$ è primo se e solo se

$$p|ab \Rightarrow p|a \text{ .or. } p|b$$

Notate che 1 non è un primo perché non ha esattamente 2 divisori ne ha 1 solo.

Fate una bella cosa, scrivere i numeri da 2 a 10 su un foglio e poi disegnare una freccia tra a e b se $a|b$. Ottenete dei grafi disconnessi, uno per ogni numero primo tra 2 a 10.

Ogni numero naturale n si può scrivere in maniera unica come prodotto di numeri primi (per avere l'unicità della decomposizione abbiamo escluso 1 dai primi).

I numeri primi sono infiniti.

> **Nota:** Supponiamo che i numeri primi siano in numero finito cioè $\{2, 3, 5, \ldots., p_n\}$. Quindi p_n dovrebbe essere il primo più grande di tutti. Sfortunatamente $p = 2 * 3 * 5 * \cdots * p_n + 1$ è primo ($p \mod p_k = 1$, quindi p_k non divide p) ed è più grande di p_k che quindi non è il primo più grande di tutti.

Nota: Supponiamo per assurdo che i numeri primi siano in numero finito cioè $\{2, 3, 5, ..., p_n\}$. Quindi p_n dovrebbe essere il primo più grande di tutti. Sfortunatamente se definiamo $a = 2 * 3 * 5 * \cdots * p_n + 1$, esso o è primo ($a \bmod p_k = 1$, quindi p_k non divide p) ed è più grande di p_k che quindi non è il primo più grande di tutti. Oppure a non è primo, quindi ammette un divisore. Scomponendo p in fattori primi si prova un divisore p di a, cioè $p|a$. Ma per quanto detto sopra p non può essere nessuno dei primi minori o uguali a p_n, quindi sarebbe necessariamente più grande di p_n.

In entrambi i casi è una contraddizione col fatto che p_n è il più grande dei primi. Dato un insieme finito di primi uno può sempre trovare un primo più grande di tutti gli elementi dell'insieme, quindi l'insieme dei primi deve necesssariamente essere infinito.

Quale dimostrazione vi convince di più?

Giorno 13: numeri interi

Ora che sappiamo vita, morte e miracoli (somma, prodotto e divisione con resto) di $\mathbb{N}$ dobbiamo scoprire i numeri interi. Il punto è il *riciclo*: non voglio tutte le volte ripartire da assiomi se posso evitarli. Se potessi evitarli gli assiomi sono sempre da evitare visto che arrivano senza dimostrazione.

Il punto è che possiamo definire i numeri interi (positivi e negativi) senza introdurre nuovi assiomi e le operazioni tra numeri interi (compresa la sottrazione) usando solo naturali e le loro operazioni.

Nota: Ma prima, perché ho bisogno dei numeri negativi? Perché senza 5-8 non lo posso fare. Coi numeri negativi la sottrazione diventa una buona operazione che posso sempre fare e che diventa l'inversa della somma. In altre parole imparo a risolvere le equazioni del tip $x + a = b$ qualunque siano a e b.

Questo pattern si ripeterà più volte. Inventiamo nuovi numeri per risolvere problemi in modo più generale. Varrà per le frazioni $\mathbb{Q}$ ($ax + b = c$) per i numeri reali ($x^2 = 2$) per i numeri complessi $x^2 = -1$.

Consideriamo le coppie di numeri naturali $(a, b) \in \mathbb{N} \times \mathbb{N}$. Diciamo che 2 coppie sono equivalenti $(a, b) \sim (c, d)$ se $a + d = b + c$. Questa è una relazione di equivalenza (dimostrare le proprietà che definiscono le relazioni di equivalenza). Definiamo un *numero intero* una classe di equivalenza $[(a, b)]$ che contiene tutte le coppie nella forma $(a + k, b + k)$ che infatti risultano equivalenti a (a, b). L'insieme di tutti i numeri interi si denota con $\mathbb{Z}$.

La *somma* di 2 numeri interi si definisce come $[(a, b)] + [(c, d)] = [(a + c, b + d)]$.

Nota: Il risultato non dipende dal rappresentante scelto per i numeri interi, infatti, siano $(a + k, b + k)$ e $(c + h, d + h)$ altri rappresentanti la somma sarebbe

$$[(a + k + d + h, b + k + c + h)] = [(a + d + (k + h), b + c + (k + h))] = [(a + d, b + c)]$$

Definiamo il *prodotto* in $\mathbb{Z}$ come

$$[(a, b)][(c, d)] = [(ac + bd, bc + ad)]$$

Nota: Tra tutti i numeri interi possiamo scegliere un sottoinsieme $[(a,0)]$. Se riscriviamo le operazioni per questi numeri interi abbiamo che essi rappresentano correttamente i numeri naturali.

$$[(a,0)]+[(b,0)]=[(a+b,0)] \qquad [(a,0)][(b,0)]=[(ab,0)]$$

Quindi identifichiamo $i:\mathbb{N}\to\mathbb{Z}:a\mapsto[(a,0)]$.

Possiamo sempre scegliere per un numero intero un rappresentante specifico: Se $a\geq b$ scegliamo $[(a,b)]=[(a-b,0)]$, se $a<b$ scegliamo $[(0,b-a)]$. E quindi inventiamo una notazione: denotiamo $[(a,0)]=a\in\mathbb{N}\subset\mathbb{Z}$ e $[(0,a)]=-a\in\mathbb{Z}$.

E come mai questo dovrebbe avere a che fare con i numeri interi?

Nota: Esempio: calcolare $[(a,0)]+[(0,a)]=[(a,a)]=[(0,0)]$. Quindi $[(0,a)]$ è un numero intero che sommato con $[(a,0)]$ dà 0.

Notate che la sottrazione è una somma di numeri interi: $a-b=[(a,0)]+[(0,b)]$ e per calcolare una *sottrazione* dobbiamo solo in generale fare 2 somme in $\mathbb{N}$.

I numeri interi contengono i numeri naturali $i:\mathbb{N}\to\mathbb{Z}:a\mapsto[(a,0)]$ e le operazioni definite sui naturali continuano a funzionare

$$i(a)+i(b)\mapsto[(a,0)]+[(b,0)]=[(a+b,0)]\mapsto i(a+b)$$

$$i(a)i(b)\mapsto[(a,0)][(b,0)]=[(ab,0)]\mapsto i(ab)$$

Esercizio: calcolare $1(-1)$ e $(-1)(-1)$.

$1(-1)=[(1,0)][(0,1)]=[(0,1)]=-1$ $\qquad$ $(-1)(-1)=[(0,1)][(0,1)]=[(1,0)]=1$

Salmodiate: *meno per più fa meno, meno per meno fa più.*

Se sapete moltiplicare i numeri naturali, sapete pure moltiplicare i numeri interi.

Abbiamo anche che

$$(-1)[(a,b)]=[(b,a)]=$$

quindi

$$[(a,b)]=[(a,0)]+[(0,b)]=[(a,0)]+(-1)[(b,0)]=a-b$$

quindi il numero intero $[(a,b)]$ coincide col numero intero $a-b$, a è la parte positiva, b la parte negativa.

In $\mathbb{Z}$ l'operazione di somma funziona molto meglio che in $\mathbb{N}$. Se in $\mathbb{N}$ non era sempre possibile, ora per qualunque $k\in\mathbb{Z}$ esiste un $-k\in\mathbb{Z}$ tale che $k-k=0$, $-k$ si chiama *l'opposto di* k oppure l'inverso rispetto alla somma.

Quando abbiamo che un insieme (in questo caso $\mathbb{Z}$) ha una operazione (in questo caso $+:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, che risulta associativa, commutativa, esiste l'elemento neutro 0, e ogni elemento k ha un opposto $-k$. Quando è così questo si chiama un gruppo commutativo. Gruppi commutativi ce ne sono tanti e siccome in ogni gruppo commutativo usiamo solo le proprietà che ne fanno un gruppo commutativo, se so risolvere l'equazione $x+a=b$ in un gruppo so risolverla in tutti

i gruppi. Da qui l'astrazione di risolvere l'equazione senza neanche sapere se a e b sono numeri interi, frazioni, vettori, funzioni continue, operatori su spazi di Hilbert o rotazioni del piano, tanto è uguale.

Quindi in $\mathbb{Z}$ c'è una sottrazione $a - b$ ben definita, che però è diventata la somma di a con $-b$. La divisione è sempre brutta perché $6 : 4$ continua a non avere un risultato in $\mathbb{Z}$.

Giorno 14: numeri razionali

Ora giochiamo lo stesso gioco per definire i numeri razionali $\mathbb{Q}$ su cui abbiamo che anche la divisione è ben definita.

> **Nota:** Da piccoli vi hanno detto che una frazione è una roba che si scrive con 2 numeri interi $n, d \in \mathbb{Z}$ (con $d \neq 0$) e si scrive $\frac{n}{d}$.
>
> Poi vi hanno insegnato a sommare e moltiplicare le frazioni. E lì è spesso per molti finito il mondo. Il fatto è che è antipatico definire le cose così perché $\frac{n}{d}$ è il numerale di un numero razionale. Invece noi che siamo uomini di mondo, prima definiamo i numeri razionali e poi introduciamo le frazioni come notazione per rappresentare i razionali. Come abbiamo introdotto la notazione $-a = [(0, a)]$ per rappresentare i numeri negativi.

Consideriamo le coppie di numeri interi $(a, b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$, con $b \neq 0$. Dichiariamo equivalenti 2 coppie $(a, b) \sim (c, d)$ se e solo se $ad = cb$.

Un numero razionale è una classe di equivalenza $[(a, b)]$ che è un sottoinsieme che contiene tutte le coppie $[(a, b)] = \{(ak, bk) : k \in \mathbb{Z} - \{0\}\}$. L'insieme dei numeri razionali si scrive come $\mathbb{Q}$.

Sui numeri razionali definite la somma e il prodotto come

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \qquad [(a, b)][(c, d)] = [(ac, bd)]$$

Quindi se sapete sommare e moltiplicare numeri interi, sapete farlo pure per le frazioni.

Potete definire la mappa $i : \mathbb{Z} \to \mathbb{Q} : a \mapsto [(a, 1)]$, che rappresenta i numeri interi come razionali preservando le operazioni

$$i(a) + i(b) = [(a, 1)] + [(b, 1)] = [(a + b, 1)] = i(a + b)$$
$$i(a)i(b) = [(a, 1)][(b, 1)] = [(ab, 1)] = i(ab)$$

come prima abbiamo mostrato che i numeri naturali erano particolari numeri interi.

Se prendete $[(a, 1)] \in \mathbb{Q}$ e lo moltiplicate per $[(1, a)]$ otteniamo $[(a, 1)][(1, a)] = [(a, a)] = [(1, 1)]$. Quindi $[(1, a)]$ è quel numero in $\mathbb{Q}$ che moltiplicato per il numero intero a (pensato come numero razionale) dà 1. Questo si chiama il *reciproco* di a, o l'inverso rispetto al prodotto.

Ora che sappiamo operare in $\mathbb{Q}$ con somma e prodotto, sono entrambe associative e commutative, entrambe ammettono elemento neutro $[0, 1]$ e $[(1, 1)]$ ed

entrambe ammettono inverso (tranne per il reciproco di 0), $-[(a,b)] = [(-a,b)]$ e $[(a,b)]^{-1} = [(b,a)]$ e in più vale in generale la proprietà distributiva della somma rispetto alla moltiplicazione, allora diciamo che $\mathbb{Q}$ è un *campo*.

In un campo se abbiamo l'equazione $AX + B = C$ possiamo risolverla come

$$AX + B = C \qquad AX = C - B \qquad X = A^{-1}(C - B)$$

Infine diciamo che il numero razionale $[(a,b)]$ si può scrivere come $\frac{a}{b}$. In $\mathbb{Q}$ abbiamo la divisione ben definita (a parte che non si può dividere per 0), nel senso che la divisione di $\frac{a}{b}$ e $\frac{c}{d}$ è quel numero $q \in Q$ tale che $q\frac{c}{d} = \frac{a}{b}$. Se scriviamo $q = n/m$ possiamo espandere quest'ultima condizione

$$\frac{n}{m}\frac{c}{d} = \frac{nc}{md} = \frac{a}{b}$$

che è vera se e e solo se $ncb = amd$ che è vera se $n = ad$ e $m = cb$ (infatti $adcb = acbd$). Quindi abbiamo la divisione

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b}\frac{d}{c} = \frac{ad}{bc}$$

Abbiamo anche il principio di semplificazione per le frazioni $\frac{ak}{bk} = \frac{a}{b}$ sempre quando $k \neq 0$.

Se ci pensate, avete ora quasi tutto quello che avete fatto alle elementari e qualcosa delle medie. Tutto quello che vi serve per risolvere qualunque equazione lineare in $\mathbb{Q}$. Abbiamo un bel contesto in cui sommare e dividere numeri in modo generale. Come si sa dai tempi di Pitagora, non sappiamo ancora risolvere le radici quadrate di tutti i numeri razionali. Ad esempio non sappiamo risolvere in $\mathbb{Q}$ l'equazione $x^2 = 2$.

E questo è fastidioso, nel senso che abbiamo un campo $\mathbb{Q}$ possiamo scrivere un'equazione in $\mathbb{Q}$ che però non possiamo risolvere in $\mathbb{Q}$ (come nei naturali possiamo scrivere $x + 3 = 0$ ma non possiamo risolverla, e come negli interi possiamo scrivere $3x = 2$ ma non possiamo risolverla). La situazione migliora a ogni giro (possiamo risolvere $x + 3 = 0$ in $\mathbb{Z}$ e $3x = 2$ in $\mathbb{Q}$) ma sempre troviamo nuove equazioni che non possono essere risolte dove sono definite.

E notate che non abbiamo ancora parlato di virgola, la frazione 3/2 per noi è una frazione e ancora neanche sappiamo cosa significa 1.5, tantomeno che $3/2 = 1.5$. Anche senza saperlo abbiamo risolto tutte le equazioni lineari.

Lasciatemi aggiungere una cosa: Il gruppo $(\mathbb{Z}, +)$ è abbastanza semplice, logicamente possiamo dimostrare che è un ambiente scevro da contraddizioni e in cui possiamo decidere di ogni proposizione se è vera o falsa. Già per $(\mathbb{Q}, +, *)$ vale il teorema di Gödel, cioè possiamo *dimostrare* che ci sono proposizioni indecidibili (una delle quali è che il sistema formale è coerente, un'altra è il problema dell'arresto). Non siamo neanche in 4 elementare e siamo già esposti al teorema di indecidibilità di Gödel!

Che volete farci: *la natura è malevola* pure quando parlavamo di numeri naturali eravamo comunque esposti agli infiniti visto che i numeri naturali sono infiniti.

Mi piace chiudere ricordando che in greco *máthema* è *ciò che si impara*, per dire che chi dice che la matematica è naturale banfa. La matematica si deve imparare perché non è lo stato naturale se no le scimmie sarebbero matematiche.

Giorno 15: numeri decimali

Tra i razionali ce ne sono di particolare per cui possiamo usare una notazione diversa. Ad esempio

$$\frac{12}{10} = 1.2 \qquad \frac{314}{100} = 3.14 \qquad \frac{66666}{10000} = 6.6666$$

sono numeri razionali che hanno un denominatore che è una potenza di 10. Il carattere . ci informa di quale potenza di 10 si tratta. Questi numerali si chiamano *notazione decimale*.

Se volete sommare 1.2 e 3.14 sappiamo già farlo

$$1.2 + 3.14 = \frac{12}{10} + \frac{314}{100} = \frac{120}{100} + \frac{314}{100} = \frac{434}{100} = 4.34$$

E questo è semplicemente il motivo per cui alle elementari ci tenevano tanto a farci allineare a destra i numeri da sommare, oltre alle cose tipo *sommate i numeri come se non ci fosse la virgola e poi rimettetela a posto*. Lo stesso vale per la moltiplicazione

$$1.2 * 3.14 = \frac{12}{10}\frac{314}{100} = \frac{12*314}{1000} = \frac{3768}{1000} = 3.768$$

> **Nota:** Ditemi se è così pure per voi, ma io ricordo che quando abbiamo fatto da piccoli i numeri decimali, i decimali all'inizio non erano approssimazioni di qualcosa (e.g. di numeri irrazionali). Quando si scriveva 1.2 era 1.2, era esattamente $\frac{12}{10}$, non l'arrotondamento di 1.2005. Gli arrotondamenti sono venuti dopo. Quindi, all'inizio, il punto era esattamente di estendere le operazioni e gli algoritmi per calcolarle ai numeri con la virgola. Quindi mi pare sia *esattamente* quello che abbiamo fatto qui.

Ovviamente, questa non è neppure matematica davvero. È una cosa che riguarda i numerali e il fatto che siamo affezionati alla base 10. Anche se lo rifate in una base qualsiasi, stiamo sempre parlando di un modo fantasioso di scrivere alcune frazioni particolare. Quando avete $\frac{1}{4}$ questo possiamo scriverlo esattamente in forma decimale $\frac{1}{4} = \frac{25}{100} = 0.25$ oppure $\frac{30}{4} = \frac{750}{100} = 7.5$.

Ma ci sono altri numeri razionali che non si possono scrivere in forma decimale. Ad esempio, $\frac{1}{3}$ non può essere scritto esattamente in forma decimale (con un numero finito di cifre decimali) perché posso moltiplicare 3 per qualunque cosa ma non potrà mai essere potenza di 10.

Nota: Se devo avere $3a = 10^k = 2^k 5^k$, siccome 3 è primo deve dividere $3|2^k$ oppure $3|5^k$ e nessuno dei 2 può essere. Quindi qualunque sia a, $3a$ non può essere una potenza di 10.

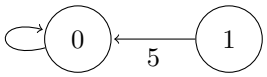
In altre parole, i razionali sono meglio dei decimali ($\frac{1}{3}$, $\frac{1}{7}$ non hanno una espressione esatta decimale). Oltretutto, quali frazioni non hanno espressione decimale esatta dipende dalla base che usiamo.

Nota: in base 3 i numeri *terziali* sono $\frac{(201)_3}{(100)_3} = (2.01)_3 = \frac{19}{9} = 2*3^0 + 0*\frac{1}{3} + \frac{1}{9}$ si scrive in forma terziale come $(2.01)_3$ e ovviamente conveniamo di sottintendere la base 10 (e di usare la notazione decimale per le basi).

In forma terziale abbiamo $\frac{1}{3} = (0.1)_3$ che è esatta e non periodica mentre lo stesso $\frac{1}{3}$ è periodico come numero decimale.

Anche se, in fondo è quindi una faccenda di notazione numerale, è interessante vedere perché e quali numeri sono periodici in base 10.

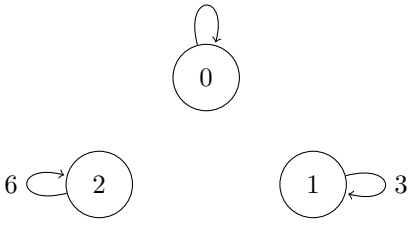
La risposta può essere cercata nel fatto che quando si dividono 2 numeri interi si ottiene un resto e da lì le cifre decimali in successione. Si ottengono dei cicli di cifre che possono intrappolarci per sempre. Per esempio, quando prendiamo un numero e lo dividiamo per 2 il resto può essere 0 o 1 e a seconda del resto che troviamo ad un certo punto poi proseguiamo seguendo le linee del grafico



(1)

Quindi da dovunque partiamo arriviamo ad una sequenza infinita di zeri, cioè le frazioni $\frac{n}{2}$ non sono periodiche.

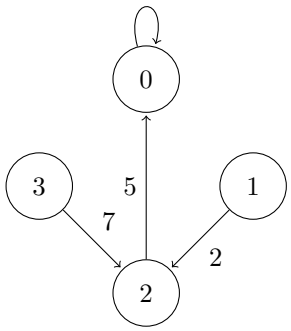
Quando dividiamo per 3 il resto può essere 0 o 1 o 2 e a seconda del resto che troviamo seguiamo



(2)

Quindi o un numero si divide per 3 oppure il risultato è periodico con periodo di una cifra sola, o 3 o 6.

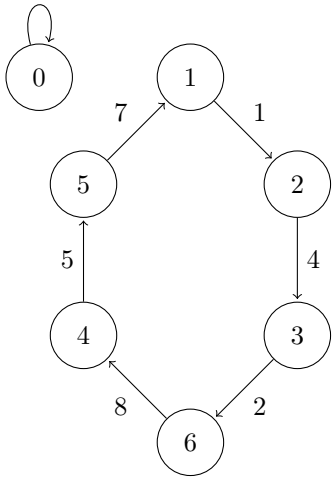
Se dividiamo per 4 abbiamo resto 0,1,2 o 3 e seguiamo le regole



(3)

quindi ancora nessun numero periodico.

Ci sono cose bellissime da scoprire, ad esempio dividendo per 7 abbiamo



(4)

Quindi dividendo un numero per 7 o si divide esattamente, oppure ha sempre un periodo di 6 cifre, che sono sempre prese nel ciclo (142857), cioè con lo stesso ordine solo iniziando da un punto qualunque.

Tutto ciò ha un certo fascino, può essere un buon esercizio sulle divisioni.

Quindi, riassumendo, come prima -3 e le frazioni, i decimali sono una notazione per denotare un po' di numeri. Ma i razionali $\mathbb{Q}$ sono comunque un insieme ben fatto di numeri su cui fermarsi. I numeri reali hanno bisogno di qualche nozione di limite infinito, quindi li rimandiamo. Per ora ci riteniamo soddisfatti da $\mathbb{Q}$ su cui sappiamo sommare e moltiplicare e quindi sottrarre e dividere in modo generico (a parte la non esistenza della divisione per 0).

A proposito, quanti sono i numeri razionali? Come mai Pitagora ha realizzato che qualcosa non era descritto da un numero razionale? Ci sono numeri peggiori dei numeri irrazionali?

4 Quarta settimana

Dobbiamo ancora finire qualche cosa sui numeri razionali (parlare di forma canonica (detto semplificare le frazioni), dimostrare che esistono numeri irrazionali e numeri trascendenti). Poi farei na pausa, visto che a spanne abbiamo finito il programma delle elementari, e parlerei un po' di sistemi formali, modelli e dimostrazioni. Poi abbiamo già accennato alle equazioni e quindi ripartiremo da lì.